Articles + Publications | November 12, 2024

Stronger Privacy Protections and Enforcement Still High on the Agenda in California

WRITTEN BY

LuAnne Morrow | Lindsey E. Kress

As we near the end of 2024, we consider a recent new round of California bills amending the California Consumer Protection Act ("CCPA")[1] and new laws concerning AI. This activity provides an opportunity to both reflect on the trends in California privacy law from a legislative and enforcement perspective and possibly draw some conclusions on the direction privacy law in California will take in the next year.

Legislation

Ten proposed pieces of legislation impacting privacy rights in California passed and were awaiting final approval at the end of the August legislative session. Seven were signed into law and three which were vetoed by Governor Newsom.

The bills revising the CCPA that were signed into law included laws on monetary thresholds, the format of personal data, an expanded definition of sensitive data to include neural data and recognition of prior opt-outs in commercial transactions. Three additional laws impacting privacy by way of the enactment of new laws on artificial intelligence (AI) and revision to the definition of AI in various California laws were also passed and signed into law. These include Title 15.2. Artificial Intelligence Training Data Transparency, the California AI Transparency Act and amendments to the Business and Professions Code, the Education Code, and the Government Code, relating to the definition of AI.

The new changes to the CCPA and AI laws show a trend towards fostering more clarity in the law, through updated and uniform definitions (SB-1223[2], AB-2885[3]) and continues the trend towards giving the California Privacy Protection Agency (the "Agency") more responsibility (AB-3286), by removing the responsibilities of the Attorney General in the CCPA to adjust the monetary thresholds of specified code sections in January of every odd-numbered year to reflect any increase in the Consumer Price Index, and instead requiring the Agency to determine and apply the percentage change in the Consumer Price Index for the monetary thresholds, as prescribed, and requiring the Agency to administer the grant program in place to promote and protect consumer privacy, educate children in online privacy and fund cooperative programs with international law enforcement.[4]

In the new AI laws, the predominant trend is transparency for consumers both with respect to data sets used in the development of a system or service as well as disclosure of when synthetic data has been used (AB-213). This trend is evident again in California AI Transparency Act, a new law, which requires providers of generative AI systems with one million monthly users on average to create and provide AI detection tools that a person can use to identify what image, video, or audio content (or combination thereof) was created or altered by the provider's

©2025 Troutman Pepper Locke

generative AI system and latent disclosure in such AI-generated content created by its system.

Perhaps most telling for the future of privacy and AI laws impacting privacy protection in California are the bills that were vetoed by Governor Newsom. The key requirement of AB-3048 was mandatory opt-out settings in web browsers and mobile operating systems offering consumers the ability to exercise their privacy preferences through an online tool called an "opt-out preference signal." The Governor's comments when vetoing the bill send a clear message that although the California AI Transparency Act requires technology companies to create new AI detection tools, there is a limit to where the government will go with respect to requiring significant changes that will require technological developments by large technology companies: "I am concerned, however, about placing a mandate on operating system (OS) developers at this time. No major mobile OS incorporates an option for an opt-out signal. By contrast, most internet browsers either include such an option or, if users choose, they can download a plug-in with the same functionality. To ensure the ongoing usability of mobile devices, it's best if design questions are first addressed by developers, rather than by regulators."

This trend toward encouraging technical solutions over regulatory ones is also evident in the Governor's comments on AB-1949, which would have amended the CCPA to prohibit the sale, sharing, disclosure, or use of minors' personal information, unless the minor's parent or guardian (for those under 13) or the minor themselves (for those aged 13-18) consents. The Governor reasons: "… this bill would fundamentally alter the structure of the CCPA to require businesses, at the point of collection, to distinguish between consumers who are adults and minors. I am concerned that making such a significant change to the CCPA would have unanticipated and potentially adverse effects on how businesses and consumers interact with each other, with unclear effects on children's privacy." Although not specifically mentioned, it would seem that the Governor is once again highlighting the need for a technical solution to allow business to effectively distinguish between adults and minors at the time of collection of personal information.

Finally, the Governor's rejection of AB-1047 – Safe and Secure Innovation for Frontier Artificial Intelligence Models Act was also based on the intersection of technology and regulation. AB-1047 would have required developers of large artificial intelligence (AI) models, and those providing the computing power to train such models, to put certain safeguards and policies in place to prevent catastrophic harm. The bill would have also established the Board of Frontier Models to oversee the development of these models. When he vetoed the Bill, the Governor indicated: "Adaptability is critical as we race to regulate a technology still in its infancy. This will require a delicate balance. While well-intentioned, SB 1047 does not take into account whether an AI system is deployed in high-risk environments, involves critical decision-making or the use of sensitive data. Instead, the bill applies stringent standards to even the most basic functions – so long as a large system deploys it. I do not believe this is the best approach to protecting the public from real threats posed by the technology … I do not agree, however, that to keep the public safe, we must settle for a solution that is not informed by an empirical trajectory analysis of AI systems and capabilities. Ultimately, any framework for effectively regulating AI needs to keep pace with the technology itself." The Governor's remarks do not necessarily signal a reluctance to create a California specific solution but rather a reluctance to curb innovation or adopt a solution that is not sufficiently targeted and based on empirical risk assessments.

Enforcement

After issuing the first public enforcement action under the CCPA in 2022, California Attorney General Rob Bonta

has continued to prioritize compliance with California privacy and consumer protection laws. The AG pursued several high-profile actions targeting a wide range of privacy violations, including the alleged failure to properly dispose of documents containing private health information, collection and sale of customer personal information without individuals' consent, failure to implement reasonable data security resulting in a data breach, and unlawful collection and sharing of children's data. These enforcement actions followed collaborative efforts between the AG and local district attorneys across the state and resulted in combined fines of over $150 million as of the time of this update.

In September 2023, the AG announced a stipulated judgment with a major healthcare service provider resolving allegations that the provider unlawfully disposed of medical waste, hazardous waste, and protected health information at facilities throughout California. In addition to health and safety violations related to hazardous waste, the AG claimed the provider violated the California Confidential Medical Information Act[5] by failing to safeguard protected personal health information that was present on over 10,000 paper records that were allegedly sent to waste disposal facilities without adequate shredding, redaction, or deletion of protected health information. The provider entered into a stipulated judgment with the AG in which it agreed to a fine of $49 million, including $42.3 million in civil penalties, fees, and costs as well as $4.9 million for environmental projects.

That same month, the AG also published an enforcement action against a major technology company regarding the company's alleged collection, use and retention of consumers' geolocation data in violation of the California Unlawful Competition Law[6] and False Advertising Law.[7] The AG claimed the technology company deceived users into enabling location-based tracking and advertising and failed to adequately inform customers of the company's collection and use of their location data. The technology company agreed to pay $93 million to resolve the claims, in addition to injunctive relief requiring the company to provide users notice of location tracking and the ability to disable certain functions.

In February 2024, the AG announced its second public enforcement of the CCPA against a food delivery technology company concerning the company's exchange of customer personal information with unrelated businesses in a marketing co-operative, which the AG found to be a "sale" of personal information under the CCPA. The AG claimed the company violated the statute by not disclosing this exchange of personal information in its posted privacy policy and by failing to post a "Do Not Sell My Personal Information" link on its website and mobile application for customers to opt-out of this sale. The AG also alleged the company's failure to disclose the sale of personal information in its posted privacy policy violated the California Online Privacy Protection Act of 2003.[8] The company entered into a stipulated judgment with the AG in which it agreed to pay a $375,000 civil penalty and certain injunctive terms to ensure compliance with the CCPA.

In June 2024, a cloud software company agreed to pay $6.75 million to resolve alleged consumer protection and privacy violations related to a 2020 ransomware attack in which a threat actor accessed the company's database and stole personal information of California residents. The AG claimed the company violated the California Unlawful Competition Law and False Advertising Law by failing to use appropriate data security procedures to protect customer personal information, including by failing to maintain appropriate password controls and authentication protocols (i.e. multi-factor authentication), failing to implement appropriate network segmentation, and failing to prevent customers from storing personal information of customers in unencrypted fields. In addition to the monetary fine, the company agreed to improve its data security protocols to better safeguard personal and protected health information.

The AG also announced a stipulated judgment with a mobile video game developer to resolve allegations that the company collected and shared children's data without obtaining parental consent in violation of the CCPA and the Children's Online Privacy Protection Act.[9] The allegations related to a popular mobile app game that is targeted to children under the age of 13, older teens, and adults. The AG claimed the company's age screen was not neutral because it defaulted to a birth year of 1953 and therefore required minors to scroll over fifty years to find their actual birth year. The AG further alleged that the company collected and disclosed children's personal information without the required parental or opt-in consent, including disclosure to third parties for advertising purposes. The company agreed to pay a $500,000 fine and to take corrective action to prevent future collection and sale of children's data and advertising to children without parental consent in all of its games directed to children.

These comprehensive enforcement actions show that the AG's focus on privacy protection and compliance extends beyond the CCPA and that the AG's office (and local district attorneys across the state) are actively monitory and investigating companies for statutory violations that may involve a California resident's personal information.

Conclusion

The recent actions by the California Legislature and AG demonstrate that California will continue to lead the country in privacy legislation and enforcement in 2025. Companies doing business in California should stay up to date on the privacy landscape in California as the state continues its efforts to enhance and enforce privacy protections, including data privacy and online child safety issues. Governor Newsom's veto of the sweeping AI regulation scheme proposed in AB-1047 is not the last word on AI regulation in the state as the Governor emphasized California's commitment to formulating responsible guardrails for AI and confirmed that he "will continue to work with the Legislature on this critical matter in the next session."[10]

—

[1] Cal. Civ. Code § 1798.100 *et seq.*

[2] The bill adds to the definition of (ae), "sensitive personal information" to additionally include (G)(i) a consumer's neural data, and further defines (G)(ii)"neural data" to mean information that is generated by measuring the activity of a consumers central or peripheral nervous system, and that is not inferred from nonneural information.

[3] This bill amends Section 22675 of the Business and Professions Code Section 75002 of the Education Code, Sections 11546.45.5, 11547.5, and 53083.1 of the Government Code, to bring uniformity to the definition of the term "artificial intelligence" to mean an engineered or machine-based system that varies in its level of autonomy and that can, for explicit or implicit objectives, infer from the input it receives how to generate outputs that can influence physical or virtual environments.

[4] The bill also requires the Agency, when notifying in writing any person who makes a complaint under the CCPA, exclude from the notification any information that is subject to law enforcement exemptions and privileges, as specified.

[5] Cal. Civ. Code § 56 *et seq*.

[6] Cal. Bus. & Prof. Code § 17200 *et seq.*

[7] Cal. Bus. & Prof. Code § 17500 *et seq.*

[8] Cal. Bus. & Prof. Code § 22575 *et seq.*

[9] 15 U.S.C. § 6501 *et seq.*

[10] https://www.gov.ca.gov/2024/09/29/governor-newsom-announces-new-initiatives-to-advance-safe-and-responsible-ai-protect-californians/ (last accessed October 23, 2024).

RELATED INDUSTRIES + PRACTICES

- Privacy + Cyber