WILSON SONSINI

California Enacts Over Two Dozen Key Privacy and AI Bills into Law in 2026 Legislative Session

CONTRIBUTORS

Tracy Shapiro

Eddie Holman

Malcolm Yeary

Michelle Ullman

ALERTS

October 6, 2026

As the 2026 legislative session came to a close, California passed a wide-ranging assortment of privacy and artificial intelligence (AI)-related bills. In total, Governor Gavin Newsom signed over two dozen privacy and AI bills into law. The measures fall into six themes:

- **Protecting Minors Online**. California further cemented its position at the forefront of state minor safety regulation. New laws require high-privacy defaults for children, ban addictive features for users under 16, and require independent child safety audits of companion chatbots. Penalties are aggressive and often assessed per child.
- **AI Accountability**. California lays the groundwork for AI accountability. The state will register AI auditors and designate independent verification organizations, and employers may not rely solely on automated systems for discipline and termination decisions.
- **Consumer Data Rights**. The laws advance existing consumer privacy and data rights. They expand California Consumer Privacy Act (CCPA) deletion rights and shorten data broker deadlines.
- **Surveillance and Tracking**. The state addresses surveillance and tracking. New laws narrow private California Invasion of Privacy Act (CIPA) pen-register claims over website tracking and bar apps and operating systems from undoing users' privacy settings. Other laws ban AI-enabled emotion recognition and neural data collection in the workplace, and restrict workplace bathroom monitoring.
- **Clinical AI**. California sets guardrails for clinical AI. New laws preserve licensed providers' independent judgment when AI informs care and require developers and deployers to address bias in clinical decision support tools.
- **AI Transparency and Synthetic Media**. The state tackles AI transparency and synthetic media. New rules update the California AI Transparency Act, require customer service chatbot disclosures, and add synthetic performer and digital replica requirements.

Below, we highlight five of the most significant measures and then summarize other notable laws by category in the table that follows.

Spotlight: Noteworthy Measures

SB 690 (CIPA Pen-Register and Trap-and-Trace Reform). SB 690 was intended to curtail the wave of California Invasion of Privacy Act litigation targeting common website tracking. Plaintiffs have argued that pixels, cookies, and similar technologies function as "pen registers" or "trap-and-trace" devices under CIPA, capturing non-content information about visitors without consent. SB 690 removes the private right of action for those pen-register and trap-and-trace claims when the conduct occurs on a website, online application, or mobile application. Only the attorney general may bring those claims against a private actor. The bill leaves the rest of CIPA intact, so wiretapping and eavesdropping/recording claims under other CIPA provisions—which plaintiffs have frequently asserted in website-tracking lawsuits—remain available to private plaintiffs. In his signing statement, Governor Newsom applauded efforts to "protect[] small businesses from overzealous lawsuits based on a statute written without today's complex technological landscape in mind," but noted that "additional work in this area is needed, as CIPA contains other decades-old statutes that are also susceptible to abuse."

The reform reaches backward as well as forward. The limitation applies retroactively to any pending claim in an action commenced within two years before the bill's operative date of January 1, 2027. Companies facing or anticipating CIPA pen-register claims should assess how the bill affects active litigation and demand letters. It

Copyright © 2026 Wilson Sonsini Goodrich & Rosati. All Rights Reserved.

remains to be seen whether the law will achieve its intended aim or if CIPA plaintiffs will merely pivot to other theories.

AB 2246 (Age-Appropriate Design Code). AB 2246 repeals the previously existing California Age-Appropriate Design Code Act (parts of which courts enjoined as likely unconstitutional, including on vagueness grounds) and establishes a new framework that governs online services, products, and features that are "likely to be accessed by children" under the age of 18. The new law imposes similar obligations as the California Age-Appropriate Design Code Act but drops the "best interests of children" exceptions that previously qualified several restrictions such as default settings and data minimization—although the new law retains other carve-outs, including exceptions to the data minimization restriction for legal compliance and cooperation purposes described in CCPA Section 1798.145(a)(1)(A)–(D) and to the purpose limitation for safety, security, measurement, auditing, and system improvement. Under the new law, covered businesses must estimate child users' ages with a reasonable level of certainty appropriate to the risks of the business' data practices or extend children's protections to all users. They then must set all default privacy settings for users identified as children to a high level of privacy; implement specified transparency and privacy rights tools; limit the collection, sale, sharing, and retention of children's personal information to what is necessary to provide the service the child is actively and knowingly using; take reasonable steps to prevent four specified categories of harm to child users; and not use dark patterns to induce children to provide more personal information than is reasonably needed or to forgo privacy protections. They also may not profile a child by default except with appropriate safeguards in place and where the profiling is necessary either to provide the service with which the child is actively and knowingly engaged or to enhance the child's safety, privacy, or education, and may not collect, sell, or share a child's precise geolocation information by default unless strictly necessary to provide the requested service. Any contract provision that a child or parent entered into as a result of a covered business' design features is voidable at the child's election. The attorney general or public prosecutors may seek penalties of up to $5,000 per negligent violation and up to $15,000 per intentional violation—*per affected child*. The law takes effect January 1, 2027.

SB 923 (CCPA Deletion Expansion and Consumer Request Web Form). The CCPA currently allows a business, when it receives a consumer's deletion request, to delete only personal information that the business collected directly from the consumer but retain personal information it obtained from data brokers and other sources. SB 923 expands the CCPA right to delete beyond information a business collects *from the consumer* to information it collects *about the consumer*, subject to the existing deletion exceptions. The bill also amends Section 1798.130 to require businesses that operate exclusively online and have a direct relationship with the consumer to offer both an email address and an online method, such as a web form or portal, for submitting requests, whereas previously they could offer only an email address. The law takes effect January 1, 2027.

SB 813 and AB 1405 (AI Auditor Framework). SB 813 and AB 1405 create a state framework for third parties' independent auditing of AI systems. Neither bill mandates an AI audit; the practical effect of this framework depends on other laws that require an audit (more on this below). Together, SB 813 and AB 1405 establish a state designation for qualified AI auditors and require persons offering covered AI audits to register with the state. SB 813 directs the California Government Operations Agency (GovOps) to establish, by January 1, 2028, criteria for designating qualified auditors as independent verification organizations (IVOs). A prospective IVO must show, at a minimum, expertise in assessing AI risk and must satisfy GovOps requirements for technical competence, conflicts of interest, and independence from the parties it assesses. AB 1405 requires AI auditors conducting covered AI audits (i.e. assessments of the controls, processes, or systems built for an AI system or model that are necessary for compliance with state law) to register with the state by January 1, 2029.[1] SB 1119, signed the following day, is the first state law to require an outside AI audit. It requires certain companion chatbot operators to undergo independent third-party child safety audits beginning January 1, 2029. Also note that SB 813 provides that an audit performed under an identified standard "is relevant to, but not conclusive of," an action alleging that a defendant's development, modification, or use of an AI system or model caused harm.

Other Notable 2026 California AI and Privacy Laws

Protecting Minors Online	
AB 2 (Heightened Damages for Injuries to Children) Effective: January 1, 2027	This law raises the damages a social media platform with more than $100 million in annual gross revenue faces when it fails to exercise ordinary care and a child is injured as a result. The platform is liable for the greater of $5,000 per violation, up to $1 million per child, or three times the child's actual damages. The law applies only prospectively after its effective date and sunsets January 1, 2035.

Copyright © 2026 Wilson Sonsini Goodrich & Rosati. All Rights Reserved.

AB 1159 (Ban on Using Student Data to Train AI) Effective: January 1, 2027 (higher education provisions operative July 1, 2027)	Under this law, operators (and entities working on their behalf) of websites, online services, or applications designed or marketed for preschool/pre-K-12 school purposes (and known to be used for such purposes) may not knowingly use protected student personal data to train or develop AI systems. The law als enacts the Higher Education Student Information Protection Act (HESIPA), which generally protects the personal information of a higher education student in a similar manner as preschool/pre-K-12 students. It also adds a new ban on collecting, using, retaining, or disclosing covered information about reproductive or sexual health, immigration status, or sexual orientation or gender identity (plus precise geolocation under HESIPA). Harmed students or their parents can bring individual or class action lawsuits against these operators to recover the greater of actual damages or $500 per plaintiff per violation, injunctive relief, punitive damages, and reasonable attorneys' fees and costs—subject to a 60-day pre-suit notice and opportunity to cure.
AB 1709 (Addictive Features and Mandatory Age Verification) Effective: January 1, 2027	Under this law, covered websites, online services, and applications may not provide "addictive features" (e.g., autoplay and addictive feeds) to users under the age of 16. Covered platforms must verify users' ages in accordance with the Digital Age Assurance Act and either withhold addictive features from users under 16 or delete the accounts of such users. The attorney general may adopt implementing regulations to further the purpose of protecting minors online, including altering the scope of a "covered platform" under the law. The attorne general or a local public prosecutor may seek civil penalties of up to $25,000 per affected minor for negligent violations and up to $50,000 per affected minor for knowing violations.

Copyright © 2026 Wilson Sonsini Goodrich & Rosati. All Rights Reserved.

AB 1856 (Technical Amendments to the Digital Age Assurance Act) Effective: January 1, 2027	This law amends California's Digital Age Assurance Act age-signal regime before its obligations become operative on January 1, 2027 (the same date thes amendments take effect) by changing key definitions, specifying when operating system providers must collect age information, redefining "operatin system provider" to exclude open-license operating systems from the age-signal requirements, and restricting requests for such signals to circumstance required by law.
AB 1946 (Stricter CSAM Reporting Obligations) Effective: January 1, 2027	This law imposes stricter requirements for covered platforms to enable and respond to reports of child sexual abuse material (CSAM), including AI-generated intimate imagery of identifiable minors. Covered platforms must provide a clear and conspicuous user-reporting mechanism, ensure human review of reports (unless the reported content matches a known CSAM hash o has previously been blocked), contact reporting users in writing via the specified method of their choice, permanently block qualifying reported material within 48 hours and confirm actions taken within 72 hours, and produce a final written determination within seven days. The attorney general, district attorneys, city attorneys, and county counsel may enforce civil actions pursuant to this law, and penalties of up to $250,000 per day for violations and injunctive relief may be imposed. Furthermore, this law expands the private right of action to individuals depicted in the material who are not reporting users.
SB 867 (Temporary AI Chatbot Toy Moratorium) Effective: January 1, 2027	This law places a temporary moratorium on the manufacturing, sale, exchange offer for sale, or possession with intent to sell any toy that is designed, marketed, or manufactured for use in play by children under the age of 16 and includes an AI companion chatbot. This prohibition will remain in effect until January 1, 2031.

Copyright © 2026 Wilson Sonsini Goodrich & Rosati. All Rights Reserved.

SB 1119 (AI Chatbot Guardrails, or "Adam's Law") Key Dates: Effective January 1, 2027. Core obligations operative July 1, 2027. First audits are due January 1, 2029.	This law significantly expands California's existing companion chatbot protections for children. It requires operators of companion chatbots to either determine a user's age under the Digital Age Assurance Act or apply child-protective safeguards to *all* users. (Postsecondary education institutions that make a companion chatbot available exclusively for use in educational settings and entities making a companion chatbot available exclusively to employees, contractors, or other personnel for use in workplace settings are not included in the definition of "operator" under this law.) It also requires operators to conduct mandatory risk assessments before releasing a new or substantially modified companion chatbot. Operators are further required to provide timely referrals to mental health resources and streamlined access to crisis helplines or notices to parents of child users if the operator is aware that a child user engaged in self-harm (or if there is a credible threat of imminent self-harm). The law also mandates default settings that can only be changed by a parent (including disabling push notifications, time limits on usage, and limitations on persistent conversational memory) and prohibits targeted advertising at child users using personal information about the child in a conversational chat with the child. For operators with at least $500 million in gross revenue (and for all other operators as of January 1, 2032), operators must also complete their first independent child safety audit by January 1, 2029 or before the chatbot becomes publicly available—whichever is later—with an additional audit being conducted every two years thereafter. The law imposes liability on operators of AI chatbots for failure to take reasonable measures to prevent several categories of harmful outputs (including but not limited to self-harm, obscene matter or sexual abuse material, excessive praise or flattery, and emotionally manipulative outputs). It also creates a private right of action that allows a child harmed by certain violations—or a parent or guardian on the child's behalf—to bring suit against the operator. The core child-safety obligations under Adam's Law are set to take effect on July 1, 2027.

Copyright © 2026 Wilson Sonsini Goodrich & Rosati. All Rights Reserved.

AI Accountability: Human Oversight and Independent Assurance	
SB 947 (Automated Decision Systems in Employment) Effective: July 1, 2027	This law prohibits employers from relying solely on an automated decision system (ADS) to make disciplinary or termination decisions. An employer that primarily relies on ADS output must direct a human reviewer to corroborate the decision and must provide the affected employee a post-use written notice The law carries a civil penalty of $500 per violation.
Consumer Data Rights and Deletion	
AB 883 (DROP Deadlines and Deletion for Elected Officials and Judges) Key Dates: Effective January 1, 2027. Notice and enforcement provisions operative July 1, 2027.	This law shortens data brokers' Delete Request and Opt-Out Platform (DROP) deadlines from 45 to 30 days. Beginning January 1, 2027, data brokers must access DROP, process deletion requests, and repeat deletions at least every 30 days. The law also requires state and local officials to notify elected officials an judges that they may use DROP, and it authorizes the attorney general, county counsel, and city attorneys to sue noncompliant data brokers on their behalf, with punitive damages available for willful violations. These notice and enforcement provisions become operative July 1, 2027.
Surveillance, Tracking, and Workplace Monitoring	
AB 1331 (Workplace Surveillance in Restrooms) Effective: January 1, 2027	This law prohibits employers from using a workplace surveillance tool to monitor or surveil employees in a workplace bathroom, unless a court order directs otherwise. The Labor Commissioner and public prosecutors enforce th law, and violations carry a penalty of up to $500 each.

Copyright © 2026 Wilson Sonsini Goodrich & Rosati. All Rights Reserved.

AB 1883 (AI Workplace Surveillance, Emotion Recognition and Neural Data) Effective: January 1, 2027	This law prohibits employers from using a workplace surveillance tool that uses artificial intelligence on employees to recognize, or make inferences or predictions about, an individual's emotional state, or to collect neural data. The Labor Commissioner and public prosecutors enforce the law, and violations carry a penalty of up to $500 each.
AB 2561 (Operating System and Application Privacy Settings) Effective: January 1, 2027	This law prohibits operating systems and applications from undoing a user's affirmative configuration of a privacy setting without the user's consent, excep as required by law, court order, or subpoena. The law defines a privacy setting as any user-configurable option in an application's privacy or similarly labeled menu that governs the application's handling of personal information. Businesses may still discontinue services or privacy options if the change preserves existing protections for data already collected or increases privacy protection.
Health and Clinical AI	
AB 1979 (AI Clinical Decision Support and Health Care Chatbots) Effective: January 1, 2027	This law requires health facilities, clinics, and physician and group-practice offices to take reasonable steps to preserve a licensed provider's independent professional judgment when care is informed by a clinical decision support system. It bars those entities from using AI to independently perform clinical functions reserved to licensed professionals. It also brings businesses that offe healthcare chatbots to consumers within the Confidentiality of Medical Information Act as providers of healthcare.
SB 503 (AI Clinical Decision Support Systems) Effective: January 1, 2027	This law requires developers and deployers of clinical decision support systems, meaning AI that aids clinical decisions on timing of care, diagnosis, o treatment, to make reasonable efforts to identify systems that pose a known or reasonably foreseeable risk of biased impacts. Developers must give deployers documentation on intended uses, training data, performance evaluation, and bias mitigation. Deployers must regularly monitor the systems and mitigate that risk.

Copyright © 2026 Wilson Sonsini Goodrich & Rosati. All Rights Reserved.

AI Transparency and Synthetic Media	
AB 1609 (Customer Service Chatbot Disclosure and Human Access) Effective: January 1, 2027	This law prohibits businesses with more than $500 million in national gross annual revenue from representing that a customer service chatbot is human and requires a clear and conspicuous disclosure where a reasonable person would likely be misled. Covered businesses must also offer a simple way to request a human agent on every customer service platform during regular business hours. They must make a good faith effort to connect with the customer within 15 minutes or schedule an appointment within one business day.
AB 2713 (AI Transparency Act Amendments for Large Online Platforms) Effective: January 1, 2027	This law revises duties and prohibitions applicable to large online platforms relating to AI. Covered platforms must let users see whether provenance data or a digital signature is available and inspect it via a display in the platform's user interface, by letting the user download the provenance data, or by providing a link to the provenance data hosted by the platform or a third party. Platforms are also barred from knowingly stripping compliant provenance dat or digital signatures from content uploaded to, distributed on, or downloaded from the platform to the extent it is technically feasible. Additionally, new express carve-outs in this law confirm that such platforms owe no obligations regarding provenance data that is not interoperable with a widely adopted standard, and the law does not require them to maintain, display, or let users download personal information as part of provenance data.
SB 1000 (AI Transparency Act Amendments for Generative AI Providers)	This law is an urgency measure that rewrites the California AI Transparency Act (CAITA) (enacted through SB 942 and subsequently amended by AB 853). This law deletes the 1 million-monthly user threshold from the definition of

Copyright © 2026 Wilson Sonsini Goodrich & Rosati. All Rights Reserved.

Effective: September 30, 2026	"covered provider," which extends the law's disclosure obligations to any publicly accessible generative AI system in the state. It also replaces the existing requirement to make an "AI detection tool" available to users at no cos with a requirement to provide a "disclosure verification tool." Furthermore, thi law eliminates the previous requirement that covered providers offer users the option to include a manifest disclosure in qualifying content created or altered by their generative AI systems. Before January 1, 2029, this law does not apply to a generative AI system that is primarily designed to function as assistive technology.
SB 1050 (Synthetic Performer Disclosures in Advertising) Effective: January 1, 2027	This law makes it unlawful to create and publish an advertisement that prominently includes a synthetic performer in California without a "clear and conspicuous disclosure" that the advertisement includes a synthetic performe Such disclosures must be difficult to miss, be easily understandable, be presented in a manner sufficient for a reasonable consumer to notice, read, an comprehend them, and use language substantially similar to: "this performance features a synthetic performer" or "no human performer is depicted." The law does not apply to advertisements for expressive works (e.g., films, television shows, video games, etc.) if the use of a synthetic performer ir the advertisement is consistent with its use in the expressive work.
SB 1111 (Digital Replicas and Right of Publicity) Effective: January 1, 2027	This law clarifies that a person's protected "voice" or "likeness" includes a digital replica—defined as a computer-generated, highly realistic electronic representation readily identifiable as an individual's voice or visual likeness. The law also removes the rebuttable presumption that an employee's incidental, non-essential appearance in an advertisement or publication was not a "knowing use" that required consent.

Copyright © 2026 Wilson Sonsini Goodrich & Rosati. All Rights Reserved.

Notable Vetoed Legislation

Governor Newsom also vetoed several bills—most notable of which are AB 1542 and SB 1130. AB 1542 would have amended the CCPA to ban the selling and sharing of consumers' sensitive personal information. SB 1130 would have prohibited a person or entity from manufacturing, selling, delivering, holding, or offering for sale in commerce a wearable recording device without a light, sound, or other indicator that is sufficiently prominent so that a reasonable person in the vicinity would be alerted to the capturing activity.

In his veto message, Governor Newsom noted that he decided to veto AB 1542 to defend consumer choice. He noted that state law requires companies to provide California consumers with the option to limit the sharing of their sensitive personal information, and that removing consumers entirely from the decision process would go a step too far. Additionally, the governor noted that the implementation of this bill would result in significant costs not included in the 2026 Budget Act. As for SB 1130, the governor acknowledged that reports of invasive conduct involving wearable recording technology warrant a legislative response but concluded that the bill defined several key terms too broadly or imprecisely. In particular, he noted that the bill's definition of a wearable recording device could sweep in smartwatches and other commonly worn devices. He further observed that existing California law already criminalizes recording individuals where they have a reasonable expectation of privacy.

Wilson Sonsini Goodrich & Rosati routinely helps companies navigate complex privacy and AI regulatory issues. For more information or advice concerning your privacy and/or AI practices, please contact Tracy Shapiro, Eddie Holman, Malcolm Yeary, Michelle Ullman or any member of the firm's Data, Privacy, and Cybersecurity and AI and Machine Learning practices at Wilson Sonsini.

---

[1] A business's self-conducted CCPA risk assessment is not covered by these laws.

Copyright © 2026 Wilson Sonsini Goodrich & Rosati. All Rights Reserved.