HERZOG
HERZOG FOX & NEEMAN

October
2026

California's New Privacy & AI Legislation

Herzog's Guide



HERZOG
HERZOG FOX & NEEMAN

California's New Privacy & AI Legislation

Herzog's Guide



INTRODUCTION

California's 2026 legislative session has introduced significant new developments in privacy and artificial intelligence regulation.

These developments build on California's already extensive privacy and technology framework, including the California Consumer Privacy Act (CCPA), the California Invasion of Privacy Act (CIPA), the Delete Act and California's growing body of AI-specific legislation.

California has enacted a broad range of measures addressing children's online safety, AI transparency and provenance, synthetic content, automated decision-making, data broker obligations and workplace technology. These acts raise practical considerations for businesses, particularly in relation to product design, data practices, advertising and personalization, AI governance, age assurance, employment practices and consumer disclosures.

This update highlights the key 2026 legislative developments most relevant to businesses that operate online, process the personal information of California residents, develop or deploy AI systems or employ workers in California.



HERZOG
HERZOG FOX & NEEMAN

California's New Privacy & AI Legislation

Herzog's Guide



Privacy & Data Protection

Expansion of CCPA Deletion Rights (SB 923)

Entering into force: 1 January 2027

SB 923 **expands the CCPA's right to delete by requiring businesses to delete** personal information about a consumer that was **obtained from a source other than the consumer**, subject to specified exceptions.

The act also requires businesses that operate exclusively online and have a direct relationship with consumers to provide an **online method for submitting consumer privacy requests**, in addition to an email address.

Why it matters: Businesses that maintain or use third-party data for analytics, advertising, audience segmentation or other commercial activities should review their deletion processes to ensure that they address personal information obtained from third parties and that appropriate suppression mechanisms are in place to prevent deleted information from being reintroduced.

Prohibition on Silently Reverting Privacy Settings (AB 2561)

Entering into force: 1 January 2027

AB 2561 prohibits an operating system or application from **reversing a user's affirmative configuration of a privacy setting** without the user's consent, subject to specified exceptions.

The act applies to privacy settings governing the collection, use, sharing, disclosure, retention or processing of personal information.

Why it matters: Businesses operating consumer-facing applications should assess whether software updates, product changes, default-setting changes or policy changes could inadvertently reset or override users' privacy choices.





CIPA Pen-Register and Trap-and-Trace Reform (SB 690)

Entering into force: 1 January 2027

SB 690 significantly changes the litigation landscape surrounding website and application tracking technologies.

The act **limits private civil actions** based on specified violations of CIPA's pen-register and trap-and-trace provisions where the relevant conduct occurs on an internet website, online application or mobile application, while preserving public enforcement authority.

The reform **applies retroactively** to specified pending claims in actions commenced within two years before the act's operative date.

Importantly, SB 690 does not eliminate CIPA generally and does not affect other CIPA private claims, including claims under Section 631, which addresses unauthorized interception of communications (i.e., "wiretapping"), and Section 632, which addresses the intentional eavesdropping on or recording of a confidential communication without the consent of all parties.

Why it matters: Businesses facing CIPA litigation involving pixels, cookies and other tracking technologies should assess whether pending or threatened claims fall within the amended provisions. Companies should nevertheless continue to evaluate other applicable CIPA and federal wiretap legal risks.

Data Broker Obligations and DROP (AB 883)

Entering into force: 1 January 2027

AB 883 amends California's data broker framework and modifies specified timelines and operational requirements applicable to data brokers, including by shortening certain existing 45-day compliance periods to 30 days. The act also addresses data brokers' obligations in connection with California's Delete Request and Opt-Out Platform (DROP) and deletion requests submitted through the platform.

Why it matters: Businesses should assess whether their collection, enrichment, sale or disclosure of personal information may cause them to fall within California's definition of a "data broker." This is particularly relevant for businesses that collect personal information about consumers with whom they do not have a direct relationship and make that information available to third parties. Businesses that qualify as data brokers should review their registration status, DROP obligations, deletion procedures and ability to comply with the applicable shortened timelines.



Children's Privacy & Online Safety

California's New Age-Appropriate Design Framework (AB 2246)

Entering into force: 1 January 2027

AB 2246 **repeals and replaces** California's existing Age-Appropriate Design Code Act - which was subject earlier this year to mixed ruling in a federal appeals court - with a revised framework for businesses providing an online service, product or feature likely to be accessed by children.

The act requires covered businesses to take reasonable steps to **prevent specified harms to children** and imposes restrictions concerning the collection, sale, sharing and retention of personal information that is not necessary to provide the relevant service. It also addresses profiling and other practices involving children.

Why it matters: Online platforms, gaming companies, social media services, marketplaces and other consumer-facing businesses should assess whether their products are likely to be accessed by users under 18 and review age assurance, profiling, personalization, advertising and product-design practices.

Restrictions on Addictive Features (AB 1709)

Entering into force: 1 January 2027

AB 1709 restricts covered platforms from providing specified **"addictive features"** to users under 16 and requires covered platforms to take reasonable measures to prevent users under 16 from receiving such features.

The legislation addresses features including autoplay and algorithmic feeds based on a user's history or profile and establishes an e-Safety Advisory Commission.

Why it matters: Businesses offering social, content-sharing or other interactive online services should assess whether their products fall within the definition of a covered platform and whether engagement features need to be differentiated based on age.





Digital Age Assurance Act Amendments (AB 1856)

Entering into force: 1 July 2027

AB 1856 amends California's Digital Age Assurance Act and strengthens its **age-signaling framework for software applications**. Covered operating system providers must enable account holders to provide the primary user's age or birth date and make available a non-identifying signal placing the user into one of four age brackets: under 13, 13-15, 16-17 or 18 or older.

The act requires covered application stores to obtain and relay these signals, while **application developers must request** the signal when an application is downloaded and launched on a device. Developers generally must treat the signal as the primary indicator of the user's age and may be deemed to have actual knowledge of that age range across certain related app and website access points.

Why it matters: Application developers should assess how receipt of an age signal affects compliance with acts that impose age-specific privacy, advertising, product design, parental consent or safety requirements. The framework may effectively turn an age signal received at the operating-system or app-store level into legally relevant knowledge of the user's age for other parts of the service.

Enhanced Safety Requirements for Companion Chatbots (SB 1119)

Entering into force: Gradually, beginning on 1 January 2027

SB 1119 strengthens California's requirements for **companion chatbots used by children**. The act establishes additional safeguards concerning child safety, including crisis-response protocols for suicidal ideation and self-harm, parental controls and notifications when certain safety settings are disabled. It also introduces independent child-safety audits and annual risk assessments for covered operators.

Why it matters: Companies developing or deploying conversational AI products should assess whether their chatbot could qualify as a regulated companion chatbot and evaluate applicable age-assurance, safety, parental-control, crisis-response, risk-assessment and audit requirements.

AI Transparency, Synthetic Content & Digital Replicas

California AI Transparency Act Amendments (SB 1000)

Entering into force: Already in force from 30 September 2026

SB 1000 amends the California AI Transparency Act and expands the scope of the framework by removing the existing one-million monthly visitor/user threshold from the definition of a covered provider.

The act also modifies the disclosure framework, including requirements concerning machine-readable provenance disclosures for AI-generated content.

Why it matters: The amendments may bring additional AI providers within California's transparency framework. Businesses providing generative AI systems should reassess whether they are covered and review their technical provenance and disclosure mechanisms.



AI System Provenance Data (AB 2713)

Entering into force: 1 January 2027

AB 2713 amends the California AI Transparency Act to impose additional requirements on large online platforms concerning provenance information associated with content made available on their services.

The act addresses the detection and display of provenance information and provides users with mechanisms to inspect certain provenance data associated with online content.

Why it matters: Platforms hosting or distributing user-generated content should evaluate whether they fall within the definition of a large online platform and, if so, how they detect, preserve and surface provenance information indicating that content was AI-generated, substantially altered by a GenAI system or captured by a device, including through appropriate user-facing disclosures.

Synthetic Performer Advertising Disclosure (SB 1050)

Entering into force: 1 January 2027

SB 1050 requires a clear and conspicuous **disclosure** in video or audio advertisements that prominently feature a **synthetic performer.**

The act generally covers AI-generated digital figures, voices or representations used in advertising and prohibits the continued use of advertisements that violate the disclosure requirements. It includes an exception for certain expressive works, including video games, where the use of the synthetic performer is consistent with its use in the underlying work.

Why it matters: Advertisers, agencies, gaming companies and creative teams using AI-generated human-like performers should review their advertising approval and disclosure processes.

Digital Replica Protections (SB 1111)

Entering into force: 1 January 2027

SB 1111 amends California's existing name, image and likeness protections to expressly address **digital replicas.**

The act clarifies and expands the concept of a person's "voice or likeness" to encompass certain computer-generated representations of an individual's voice or visual likeness, including highly realistic digital replicas.

Why it matters: Businesses using AI-generated replicas of actors, creators, influencers, employees or other individuals should reassess consent, licensing and contractual protections.



Automated Decision-Making & Employment and Workplace

Automated Employment Decisions (SB 947)

Entering into force: 1 January 2027

SB 947 regulates employers' use of **automated decision systems in employment decisions** that materially affect employees, including disciplinary and termination decisions.

The act prohibits employers from relying solely on an automated decision system for specified disciplinary or termination decisions and requires appropriate human corroboration and notice where an employer primarily relies on an automated system.

Why it matters: Employers using AI or automated decision-making tools in HR should inventory those systems and establish appropriate human-review, documentation and employee-notification processes before the act takes effect.

Technological Displacement Notice (SB 951)

Entering into force: 1 January 2027

SB 951 amends California's Worker Adjustment and Retraining Notification Act (Cal-WARN).

Where an employer is otherwise required to provide notice of a mass layoff, relocation or termination, and the action is caused **in whole or in substantial part** by an AI system or other automated technology replacing or automating employment positions, the employer must include additional information in the notice.

This includes the number, classification or occupation, and work location of affected positions; the job functions that will be automated; the specific category or type of AI system or other technology that substantially resulted in the technological displacement; and a statement at the top of the notice stating: **"This notice is for a technology displacement."**

Why it matters: Employers implementing AI-driven automation should assess whether planned workforce reductions or operational changes trigger existing Cal-WARN notice obligations and, if so, whether the additional technology-displacement disclosures apply.

Workplace Surveillance (AB 1331)

Entering into force: 1 January 2027

AB 1331 regulates employers' use of workplace surveillance tools.

A "workplace surveillance tool" broadly covers systems, applications, instruments or devices that collect or facilitate the collection of employee data, activities, communications, actions, biometrics or behaviors by means other than direct human observation, including video or audio surveillance, continuous time-tracking tools, geolocation, electromagnetic tracking and other tracking technologies.

Why it matters: Employers using employee badges, wearables, location tracking, time-tracking systems, biometric technologies or other workplace surveillance tools should assess whether those technologies and related workplace policies comply with the new restrictions.



AI Workplace Surveillance and Neural Data (AB 1883)

Entering into force: 1 January 2027

AB 1883 restricts employers from using specified AI-enabled workplace surveillance tools to collect neural data, recognize an individual's emotional state, or engage in other specified forms of workplace monitoring.

Why it matters: Employers using AI-powered employee monitoring, wearable technologies or other workplace surveillance tools should assess whether their systems collect, infer or process information covered by the new restrictions.

AI Oversight & Independent Auditing

Independent Verification Organizations (SB 813)

Entering into force: 1 January 2027

SB 813 establishes a framework for **Independent Verification** Organizations (IVOs) within California's AI regulatory framework.

The act directs the Government Operations Agency, by **1 January 2028**, to establish application requirements, procedures and criteria for designating AI auditors as IVOs. An IVO must demonstrate expertise in assessing risks posed by AI systems or models and in identifying the metrics and methodologies underlying those assessments. The framework also addresses independence, conflicts of interest, technical expertise, documentation and cybersecurity.

Designated IVOs will be required to submit annual reports concerning their standards, methodologies, governance and funding relevant to independence.

Importantly, SB 813 does not require AI developers, deployers or operators to engage an IVO or undergo a covered AI audit as a condition of developing, deploying or operating an AI system or model in California. It also does not itself create liability solely for failure to comply with an IVO standard.

Why it matters: The act creates an emerging third-party assurance infrastructure for AI in California. Businesses subject to existing or future AI audit requirements should monitor the standards and designation criteria developed by the Government Operations Agency and consider how IVO assessments may interact with other regulatory audit or assurance obligations.



HERZOG'S TECHNOLOGY REGULATION DEPARTMENT

Herzog's Technology Regulation Department is a recognized market leader in its field.

The team is led by domain experts who possess a unique combination of **legal, technological and operational** expertise, and is uniquely positioned to advise a wide range of clients, including leading multinational technology companies as well as start-ups and vendors of disruptive technologies, on regulatory and compliance considerations across the digital ecosystem.

We understand that companies operating in digital environments face regulatory scrutiny that extends far **beyond one jurisdiction or discipline**. As our clients are often at the forefront of rapidly evolving markets, we recognize the impact that **global enforcement trends, platform rules and design related compliance requirements** have on their products and operations. Our team maintains in depth knowledge of the growing body of regulation, enforcement actions and industry standards that govern online interfaces, user journeys and commercial communications. This enables us to offer practical and holistic solutions for complex situations arising from innovative technologies and fast moving regulatory expectations.

Digital products, online platforms, eCommerce, advertising and userfacing interfaces now form a core component of almost every business. Advising on these issues requires deep understanding of the intersection between legal requirements, UX and UI design practices, behavioral economics, product architecture and commercial strategy. We help clients navigate interdisciplinary and sometimes conflicting obligations that arise under privacy, consumer protection, online safety and advertising laws together with platform guidelines and industry codes.

Our advisory support for online platforms, including social platforms and platforms involving heightened regulatory sensitivity, spans the full lifecycle of product development and ongoing operations. This includes:

- Analyzing product flows, content journeys and monetization mechanics to identify potential dark patterns, safety risks, age-related compliance gaps and areas of regulatory exposure;
- Advising on global regulatory frameworks applicable to online platforms, including content moderation obligations, online safety regimes, age assurance and verification requirements, and restrictions on manipulative or exploitative design practices;
- Supporting the structuring of platform policies, community guidelines, notices and disclosures, including those tailored to sensitive content environments;
- Developing governance frameworks and internal processes for content moderation, escalation, trust and safety, and cross-functional compliance integration across product, legal and operations teams;
- Assisting with regulatory engagement and enforcement matters, including investigations relating to user protection, harmful content, deceptive practices and platform accountability.

HERZOG
HERZOG FOX & NEEMAN

California's New Privacy & AI Legislation

Herzog's Guide





Ariel Yosefi | Partner
Head of Technology Regulation
yosefia@herzoglaw.co.il



Ido Manor | Partner
Technology Regulation
manori@herzoglaw.co.il



Ruly Ber | Partner
Technology Regulation
berr@herzoglaw.co.il



Dan Shalev | Partner
Technology Regulation
shalevd@herzoglaw.co.il



Eden Lang | Partner
Technology Regulation
lange@herzoglaw.co.il



Dima Zalyalyeyev | Partner
Technology Regulation
zalyalyeyevd@herzoglaw.co.il



Or Noy | Partner
Technology Regulation
noyo@herzoglaw.co.il



Kevin David Gampel | Associate
Technology Regulation
gampelk@herzoglaw.co.il



On Dvori | Associate
Technology Regulation
dvorio@herzoglaw.co.il



Tal Habas | Associate
Technology Regulation
habast@herzoglaw.co.il



Zohar Malul | Associate
Technology Regulation
malulz@herzoglaw.co.il



Adaya Ziv-Kisos | Associate
Technology Regulation
Zivkisosa@herzoglaw.co.il



Liron Adar | Associate
Technology Regulation
adarl@herzoglaw.co.il



Omri Bar On | Associate
Technology Regulation
barono@herzoglaw.co.il



Eden Lapid | Associate
Technology Regulation
lapide@herzoglaw.co.il



Yuval Glazer | Associate
Technology Regulation
glazery@herzoglaw.co.il



Gal Mechtinger | Associate
Technology Regulation
mechtingerg@herzoglaw.co.il



Tal Schapiro | Associate
Technology Regulation
schapirot@herzoglaw.co.il



Clara Qubti | Associate
Technology Regulation
qubtyc@herzoglaw.co.il



Korin Arbel | Intern
Technology Regulation
arbelk@herzoglaw.co.il



Roni Sharir | Intern
Technology Regulation
sharirR@herzoglaw.co.il



Itay Siani | Intern
Technology Regulation
sianii@herzoglaw.co.il



Tamar Oppenheim | Intern
Technology Regulation
oppenheimt@herzoglaw.co.il



Max Shternberg | Pre-Intern
Technology Regulation
shterenbergm@herzoglaw.co.il



Noya Schwartz | Pre-Intern
Technology Regulation
schwartzn@herzoglaw.co.il



Musa Assi | Law Student
Technology Regulation
AssiM@herzoglaw.co.il