Title: California Leads Regulatory Frontier with New Privacy and Artificial Intelligence Laws for 2026

Brief Summary: California has again taken the national lead in regulating privacy and emerging technology with Governor Gavin Newsom recently signing a landmark package of privacy and artificial intelligence (AI) legislative proposals.

Collectively, these measures mark one of the most ambitious efforts by any U.S. jurisdiction to respond to the rapid evolution of AI systems and digital data practices.

Learn more about the several key privacy and AI proposals that companies should be aware of.

Full Article: California has again taken the national lead in regulating privacy and emerging technology with Governor Gavin Newsom recently signing a landmark package of privacy and artificial intelligence (AI) legislative proposals. Collectively, these measures mark one of the most ambitious efforts by any U.S. jurisdiction to respond to the rapid evolution of AI systems and digital data practices.

The legislative package underscores California's continued effort to balance innovation with accountability — ensuring that technological progress serves the public interest without eroding privacy or safety. The legislation tackles a wide spectrum of concerns, from requiring transparency in frontier AI development to mandating chatbot disclosures and giving consumers more control over their personal information. At the heart of this regulatory push is a recognition that the pace of technological advancement has outstripped existing legal frameworks, leaving consumers vulnerable to new forms of data exploitation and algorithmic harm. Many of these measures have far-reaching implications for companies doing business in California or with California residents operating across technology, media, retail, and consumer sectors.

Below, we summarize several key privacy and AI proposals that companies should be aware of.

Privacy Laws

- SB 446 (Data Breach Notification Timing): This law amends California's existing data breach notification law to require that notices to affected consumers be made within 30 calendar days of discovery or notification of the data breach. This law's effective date is **January 1, 2026**.

- SB 361 (Expanded Data Broker Transparency Requirements): This law amends California's existing data broker registration law (the 2023 DELETE Act) by requiring data brokers to provide more detailed information to the CPPA upon annual registration. It should also make it easier for Californians to request to have their data deleted. This law's effective date is **January 1, 2026**.

- AB 656 (Social Media Account "Delete" Button): This law mandates that specified social media platforms provide users with a transparent and accessible mechanism to terminate their accounts and permanently remove all associated personal data. The legislation prohibits platforms from employing deceptive interface designs or manipulative tactics, including dark patterns, that create barriers to account termination. This law's effective date is **January 1, 2026**.

- AB 566 (California Opt Me Out Act): This law requires web browser developers to include universal opt-out preference signal options like Global Privacy Control. Users have the ability to keep their personal data from being sold or shared from every site they visit. This law's effective date is **January 1, 2027**.

- AB 56 (Social Media Warning Law): This law requires certain online services that provide an "addictive feed" to users to display a "black box warning" to all minor users that states: "The Surgeon General has warned that while social media may have benefits for some young users, social media is associated with significant mental health harms and has not been proven safe for young

users." The warning must be clearly displayed each day the user initially accesses the platform, then again after three hours of cumulative active use, and thereafter at least once per hour of cumulative active use. The law's effective date is **January 1, 2027**.

- AB 1043 (Digital Age Assurance Act): This law establishes age verification requirements for device operators and application marketplaces, necessitating age collection during initial device setup and retroactively for current users. Users are segmented into four age categories: under 13, 13-15, 16-17, and 18 or older. Device operators share these age classifications with app developers at the point of download. The law does not require the submission of government-issued identification documents or impose parental consent obligations for minor users. This law's effective date is **January 1, 2027**.

AI Laws

- AB 325 (Algorithmic Price Fixing): This law amends California's antitrust law, the Cartwright Act, to prevent the use of algorithms to coordinate pricing among competitors, creates liability for efforts to coerce compliance with pricing tool recommendations, and clarifies the bar for plaintiffs pleading conspiracies under the Cartwright Act. This law's effective date is **January 1, 2026**.

- AB 316 (AI Defenses): This law precludes businesses involved in the development, modification, or implementation of AI from asserting AI autonomy as a liability defense. The legislation addresses scenarios where AI systems produce harmful outcomes by preventing defendants from deflecting responsibility based on the technology's independent decision-making capabilities. The law ensures that entities deploying AI technology remain accountable for resulting damages. This law's effective date is **January 1, 2026**.

- SB 53 (Transparency in Frontier AI Act): This law is a first-of-its-kind AI legislation in the U.S. that requires large AI developers to publicly disclose how they plan to mitigate potentially "catastrophic risks" posed by advanced frontier AI models (i.e., foundation models trained using a quantity of computing power greater than 1026 integer or floating-point operations). Critical safety incidents must be reported to the state's Office of Emergency Services. The law's effective date is **January 1, 2026**.

- AB 853 (Amendment to the California AI Transparency Act): AB 853 defers the California Transparency Act's operative date to August 2, 2026, providing an additional seven-month implementation period. The Act requires qualifying generative AI developers to offer detection tools for identifying AI-generated or AI-altered multimedia content. The Act enhances these obligations with dual provenance data requirements: California-sold recording devices must incorporate optional authentication markers for human-created content (effective January 1, 2028), while social media and online platforms must disclose content sourcing information via provenance metadata (effective **January 1, 2027**).

- SB 243 (Companion Chatbots): This law establishes specific requirements for companion chatbot platforms, mandating disclosure when users may reasonably believe they are communicating with a human, implementation of protocols to prevent content promoting suicidal ideation or self-harm, and warnings that the platform may be inappropriate for minors. Enhanced protections apply when platforms have actual knowledge of a minor user, including mandatory AI disclosure, reminders every three hours of the chatbot's non-human nature, and reasonable safeguards against sexually explicit content generation. This law's effective date is **January 1, 2026**.

Implications for Business

The new laws significantly heighten regulatory compliance obligations for companies processing consumer data or deploying AI systems. Organizations should prioritize a comprehensive review of current practices to identify gaps in compliance readiness with these new statutory requirements, particularly those with immediate or near-term effective dates.

As with California's Consumer Privacy Act and other privacy laws, these new laws are expected to influence other jurisdictions. States and federal agencies may look to California's model for guidance in crafting future AI and privacy rules. Early adoption and transparent implementation of these requirements may offer legal compliance benefits in an increasingly privacy-conscious marketplace. Companies should also remain vigilant for enforcement actions, private litigation, and administrative guidance that will shape the practical application of these statutes in the months ahead.

Authors:

Harry A. Valetk	*212 440 4416*	harry.valetk@bipc.com
Jennifer M. Oliver	*619 685 1990*	jennifer.oliver@bipc.com
Megan E. Smith-Beaty	*412 562 1368*	megan.smith-beaty@bipc.com