



Data Privacy and AI Regulatory *Quick Clicks* | Issue 35

October 2026

September brought a number of significant privacy and artificial intelligence (AI) developments in the United States and abroad, with several requirements taking effect in October or over the coming months. Connecticut's expanded privacy framework takes effect October 1, while California enacted new requirements governing AI auditors, companion chatbots and customer-service chatbots. European regulators finalized guidance addressing the interaction between the Digital Services Act (DSA) and the General Data Protection Regulation (GDPR), and regulators in Australia, South Korea and Hong Kong continued to develop privacy rules for automated and increasingly autonomous AI systems.

For businesses, the immediate work is increasingly use-specific. Companies should be looking not simply at whether they "use AI," but at where AI interacts with consumers or employees, makes or informs consequential decisions, processes personal information, interacts with children or acts autonomously across enterprise systems. Several of the developments within this newsletter also require attention well before their formal compliance dates.

Connecticut Privacy and AI Requirements Take Effect October 1

As of October 1, Connecticut Public Act 26-64, as subsequently amended by Public Act 26-100, significantly expands Connecticut's privacy requirements. Among other changes, the legislation prohibits the sale of precise geolocation data; regulates the use of personal data for individualized or "surveillance" pricing; imposes new requirements on facial recognition technology and direct-to-consumer genetic testing companies; narrows the treatment of certain information as "publicly available"; and expands deletion rights for profiles derived from publicly available information. Covered data brokers must begin registering with the Connecticut Department of Consumer Protection on January 1, 2027.

The amendments also broaden the Connecticut Data Privacy Act's (CTDPA) reach in important respects. Businesses that process sensitive data or sell personal data may now fall within the Act

even if they do not satisfy its otherwise applicable numerical processing thresholds, making it important to reassess coverage rather than rely on a prior Connecticut scoping analysis.

Connecticut's separate Public Act 26-15, An Act Concerning Online Safety, adds a separate set of AI requirements, with obligations staggered between 2026 and 2027. Effective as of October 1, the Act, as modified in part by Public Act 26-100, imposes disclosure requirements on certain subscription-based generative AI services, establishes protections for employees of large frontier-model developers and requires certain covered generative AI providers to incorporate provenance information into AI-generated or materially altered audio, images and video where commercially and technically reasonable. Public Act 26-100 replaced the original subscription provision with a narrower obligation generally requiring covered subscription-based generative AI providers to disclose key subscription terms and obtain the consumer's written acceptance before entering into or renewing a subscription, or collecting a subscription fee.

The Act also addresses AI in employment, but businesses should distinguish its two implementation dates. Effective as of October 1, use of automated employment-related decision technology is not itself a defense to specified employment-discrimination claims, although evidence of anti-bias testing and related measures may be considered. Certain Worker Adjustment and Retraining Notification (WARN) notices filed with the Connecticut Department of Labor also must identify whether layoffs relate to AI or another technological change. By contrast, the Act's principal developer and employer notice obligations (including disclosures when employees or applicants interact with covered technology and pre-decision notices concerning its use) apply to qualifying technology deployed on or after October 1, 2027, rather than October 1, 2026.

Businesses operating in Connecticut should therefore separate immediate October work from the longer implementation project: reassess CTDPA coverage and affected data practices now, review applicable AI subscription and provenance requirements, and begin inventorying employment AI well before the 2027 notice requirements become operative.

California Establishes AI Auditor and Independent Verification Frameworks

On September 9, Governor Gavin Newsom signed AB 1405 and SB 813, establishing complementary frameworks for independent assessments of AI systems.

AB 1405 requires the Government Operations Agency to establish an AI Auditor Registry by January 1, 2029. Beginning on that date, a person generally may not offer, sell or conduct a "covered AI audit"

without registering, and registered auditors will be subject to requirements addressing independence, disclosures, recordkeeping, reporting and professional integrity.

SB 813 separately requires the Government Operations Agency (Agency) to establish, by January 1, 2028, the application requirements, designation criteria and other standards for independent verification organizations with demonstrated expertise in assessing AI-system risks and the methodologies used to perform those assessments. The law requires the Agency to consider, among other things, technical expertise, conflicts of interest, independence, and relevant audit and assurance standards when developing the framework.

Neither law, standing alone, requires every AI developer or deployer in California to obtain an independent audit. SB 813 also provides that failure to comply with a standard identified under the statute does not, by itself, establish liability. At the same time, in litigation alleging that the development, modification or use of an AI system caused harm, an audit performed in accordance with an identified standard is relevant to, but not conclusive of, the action.

Companies already subject to AI assessment requirements or that use third-party audits voluntarily should therefore account for these emerging standards when structuring audit engagements, selecting outside assessors, documenting methodologies and evaluating auditor independence.

California Adds New Requirements for Companion and Customer-Service Chatbots

California also enacted two more immediately business-facing chatbot laws in September.

On September 10, Governor Newsom signed SB 1119, “Adam’s Law,” which establishes detailed requirements for operators of companion chatbots accessible to children. Beginning July 1, 2027, operators must use California’s age-assurance framework or extend specified child protections more broadly. Before making a new or substantially modified companion chatbot available in California, an operator must conduct and document a child-safety risk assessment and implement measures reasonably designed to mitigate identified risks. Operators that permit child users must also implement crisis-response protocols, parental controls, default settings, age-appropriate disclosures and other safeguards. Separate provisions restrict targeted and cross-context behavioral advertising, the sale and secondary use of children’s personal information and dark patterns associated with required safety controls.

SB 1119 also creates an independent audit regime. Initial child-safety audits generally are required by January 1, 2029, or before the chatbot is first made publicly available (whichever is later), followed by

audits every two years and in specified circumstances involving substantial modifications. Operators with less than \$500 million in prior-year gross revenue receive a temporary exemption from the audit requirements through January 1, 2032.

A separate law, AB 1609, signed on September 28, addresses customer-service chatbots. The law applies to private businesses with more than \$500 million in national annual revenue and prohibits representing a customer-service chatbot as human. Where a reasonable person is likely to be misled, the business must clearly and conspicuously disclose that the chatbot is artificially generated and not human. Covered businesses must also provide a simple mechanism to request a human customer-service agent during regular business hours and, subject to specified exceptions, make a good-faith effort to either connect the customer within 15 minutes or schedule an appointment within one business day. Public prosecutors may seek civil penalties of up to \$5,000 for an initial violation and \$10,000 for each subsequent violation; the statute does not create a private right of action.

AB 1609 contains several material exclusions. Among others, it does not apply to specified regulated utility services, exclusive employee and business-to-business communication channels, consumer reporting agencies or a covered hospital when the communication relates to the provision, coordination, management, administration, payment or operation of healthcare services. The hospital exclusion is therefore activity-specific rather than a general exemption for the healthcare sector.

Companies using conversational AI should distinguish these regimes from general chatbot disclosure laws. SB 1119 reaches product design, age assurance, data use, advertising, safety testing and auditing for companion chatbots used by children, while AB 1609 is principally a consumer-service law focused on transparency and access to human assistance.

California Expands the Right to Request Deletion under the California Consumer Privacy Act

On September 27, Governor Newsom signed SB 923, the Expanding Privacy Rights Act, which expands the California Consumer Privacy Act's (CCPA) deletion right to personal information a business has collected "from or about" a consumer. Existing law generally permits a consumer to require deletion of personal information collected directly from the consumer; beginning January 1, 2027, the right to delete will also extend to covered personal information obtained from third parties.

SB 923 also requires online-only businesses with a direct consumer relationship to offer an online method, such as a web form or portal, for submitting access, deletion and correction requests.

Organizations that buy, license, append or otherwise enrich their records with personal information from third parties should carefully measure their exposure and the expanded deletion requirements, particularly whether those workflows locate information based on its source rather than the consumer to whom it relates.

California Attempts to Curb Demand Letters Asserting Claims Under California Invasion of Privacy Act

On September 30, Governor Newsom signed SB 690 into law. SB 690 amended the California Penal Code to eliminate private rights of action for claims under §638.51. This amendment is notable because §638.51 was used by plaintiffs to target organizations for tracking technologies such as pixels, cookies and other analytic tools. Moving forward, enforcement under §638.51 exclusively rests with the California Attorney General, which should narrow the scope of enforcement. SB 690 will go into effect January 1, 2027, and will retroactively apply to claims filed within two years prior to that date.

Notably, SB 690 does not eliminate all California Invasion of Privacy Act (CIPA) claims or the risk of website tracking litigation. Plaintiffs are expected to bring similar claims under §631 and §632. Governor Newsom alluded to this risk when he urged the legislature to pursue broader CIPA reforms in his signing message. Accordingly, organizations may still face continued exposure.

European Data Protection Board Finalizes Guidance on the Interaction Between the DSA and GDPR

On September 17, the European Data Protection Board (EDPB) adopted the final version of its Guidelines 3/2025 on the interplay between the Digital Services Act (DSA) and the General Data Protection Regulation (GDPR), following the consultation on the version originally issued in September 2025. The EDPB identifies the September 17 publication as Version 2 and the final post-consultation text.

The Guidelines address how GDPR requirements apply when online platforms process personal data to satisfy or operate within the DSA framework, including in connection with advertising, recommender systems, notice-and-action mechanisms, platform design, protections for minors and systemic-risk assessments.

A recurring theme is that the DSA does not displace the GDPR. DSA transparency obligations and GDPR transparency duties remain distinct, and a platform cannot rely on a GDPR lawful basis to

circumvent the DSA's separate prohibition on profiling-based advertising using special-category data. The EDPB also addresses the potential application of GDPR automated-decision rules to recommender systems, and emphasizes data minimization and privacy-by-design when platforms implement age-assurance and other measures required by the DSA.

Platforms subject to both regimes should therefore map the personal-data processing embedded in their DSA compliance processes, rather than treating the DSA as an independent authorization to collect or use personal information.

Australia Issues Final Guidance Ahead of Automated-Decision Transparency Requirements

On September 30, the Office of the Australian Information Commissioner published final implementation resources addressing new automated-decision transparency requirements that take effect on December 10.

Under amended Australian Privacy Principle (APP) 1, an APP entity must include specified information in its privacy policy where it has arranged for a computer program to make or take an action substantially and directly related to making a decision that could reasonably be expected to significantly affect an individual's rights or interests, and the program uses that individual's personal information. The disclosures must address the kinds of personal information used and the kinds of qualifying decisions made or informed by the program.

The amendments do not establish a general prohibition on automated decisions or a general right to human review. They do, however, require covered organizations to identify qualifying use cases before December 10 and update their privacy policies accordingly. Employment, credit, insurance, eligibility, fraud, account-access and comparable decision processes warrant particular attention.

South Korea Expands AI Data Use While Tightening Privacy Governance

South Korea made two separate sets of amendments to its Personal Information Protection Act (PIPA) that move in different but complementary directions.

First, amendments promulgated as Act No. 21445 took effect on September 11 and materially strengthened corporate privacy governance and enforcement. The amendments expressly place ultimate responsibility for personal-information protection on the business owner or representative; expand the statutory responsibilities of chief privacy officers; and, for controllers meeting prescribed thresholds, require board approval of a Chief Privacy Officer's appointment, replacement or removal

and reporting of those actions to the Personal Information Protection Commission (PIPC). The amendments also allow penalties of up to 10 percent of total annual turnover for specified repeated or serious violations involving intentional conduct or gross negligence.

Separately, Act No. 21910, promulgated on September 8 and effective March 9, 2027, creates a new statutory pathway for certain uses of lawfully collected personal information in AI development. The amendment addresses circumstances in which development would be difficult or materially constrained when relying solely on anonymized or pseudonymized data and permits qualifying uses subject to statutory conditions, additional safeguards and PIPC deliberation and approval. It is not a general authorization to repurpose personal information for AI training.

Organizations operating in Korea should treat the two amendments separately: the September changes now affect governance and enforcement, while the 2027 AI provisions may create a new route for qualifying development activities that will require documented necessity, risk analysis and regulatory engagement.

Hong Kong Issues Guidance on Agentic AI

On August 25, Hong Kong's Privacy Commissioner for Personal Data (PCPD) published *Protecting Personal Data Privacy in the Use of Agentic AI*, applying Hong Kong's existing privacy framework to AI systems capable of autonomously performing multistep tasks.

The PCPD's recommendations address data minimization and access ring-fencing, transparency, data accuracy, retention of histories and memory, purpose limitation, least-privilege access, access and correction rights, continuing risk assessment, human involvement in decisions likely to significantly affect individuals, and governance of employees and third-party providers. The guidance does not create a new statutory regime, but it is a useful compliance benchmark for organizations allowing AI agents to access email, customer records, payment functionality, enterprise applications or other sources of personal information.

Additional Developments

- In the Philippines, the National Privacy Commission (NPC) issued an August 11 notice confirming that an identifiable person's face or likeness constitutes personal information, and that generating and sharing AI-created media depicting an identifiable person constitutes processing under the Data Privacy Act. The NPC emphasized that the processing must have a legitimate purpose and satisfy an applicable, lawful-processing criterion; the notice does not impose a

categorical consent requirement for every use of an identifiable likeness.

The NPC also cautioned that unlawful use of a person's likeness may constitute unauthorized processing or another offense under the Data Privacy Act, carrying potential criminal, civil and administrative liability. For example, unauthorized processing of ordinary personal information under Section 25 carries a prison term of one to three years, and a fine of PHP 500,000 to PHP 2,000,000. Unauthorized processing of sensitive personal information and other offenses are subject to different, and in some cases higher, penalties.

- In California, Governor Newsom signed SB 1050 on September 16. The law makes it unlawful to create and cause to be published any advertisement that prominently includes a statutorily defined “synthetic performer” without a clear and conspicuous disclosure. The required disclosure must use wording substantially similar to “this performance features a synthetic performer” or “no human performer is depicted.” The law does not apply to every use of AI-generated imagery, and includes exclusions for certain advertisements for expressive works and uses involving only language translation or accessibility features.

A violation of SB 1050 constitutes a violation of California Business and Professions Code Section 17500, and may be enforced through the state's Unfair Competition Law framework. The statute also expressly preserves rights and remedies otherwise available under Sections 17200 and 17500, as well as other laws governing deceptive, unfair or misleading practices. Companies should therefore treat the new disclosure as an advertising law requirement rather than simply another voluntary AI transparency practice.

Upcoming Deadlines and Developments To Watch

Date	Jurisdiction	Development
Oct. 19, 2026	United Kingdom	Information Commissioner's Office (ICO) consultation on draft guidance concerning anonymisation and pseudonymisation for research, archiving and statistical purposes closes.
Oct. 26, 2026	Colorado	Scheduled deadline for comments on proposed Automated Decision-Making Technology and Chatbot Safety Rules; the underlying statutes become effective January 1, 2027.

Date	Jurisdiction	Development
Oct. 30, 2026	European Union	Comments close on draft EDPB Guidelines 02/2026 on Anonymisation and draft Guidelines 03/2026 on web scraping in the context of generative AI. Both remain open consultation texts, rather than final guidance.
Nov. 13, 2026	European Union	Comments close on draft EDPB Guidelines 04/2026 concerning the application of GDPR administrative fines in relation to other corrective powers.
Dec. 2, 2026	European Union	Limited transition period ends for the AI Act Article 50(2) machine-readable marking and detection requirements for qualifying AI systems placed on the market before August 2, 2026.
Dec. 10, 2026	Australia	New APP 1 privacy-policy requirements for qualifying automated decision-making take effect; the OAIC must also finalize and register the Children's Online Privacy Code by this date.
Jan. 1, 2027	Colorado / Connecticut	Colorado's revised Automated Decision-Making Technology (ADMT) Act and Chatbot Safety Act take effect; Connecticut data brokers become subject to the new registration requirement.
Jan. 1, 2027	California	California's SB 923 extends CCPA deletion right to personal information collected "from or about" a consumer.
Jan. 1, 2027	California	California's AB 883 takes effect; registered data brokers must access the state's deletion mechanism and process consumer deletion requests every 30 days (previously 45 days).
Mar. 9, 2027	South Korea	Act No. 21910's new PIPA provisions addressing use of personal information for qualifying AI development take effect.
July 1, 2027	California	Principal child-safety, risk-assessment, data-use, advertising and design requirements under SB 1119 become operative.
July 1, 2027	California	Annual Delete Act reporting obligations for registered data brokers begin.

Date	Jurisdiction	Development
Oct. 1, 2027	Connecticut	Principal developer and deployer disclosure requirements for automated employment-related decision technologies begin applying to qualifying deployments.

Moving Forward

Businesses should prioritize the deadlines closest at hand. Organizations operating in Connecticut should reassess CTDPA coverage and affected data practices, and distinguish the AI requirements that take effect now from the employment-technology disclosures that begin applying in 2027. Companies subject to Australia's Privacy Act should identify qualifying automated decisions and update privacy policies before December 10. Registered data brokers should confirm they can access California's deletion platform and are prepared for the 30-day processing cycle beginning January 1, 2027. Businesses offering conversational AI should also determine whether California's new companion-chatbot or customer-service requirements apply, including whether an AB 1609 exclusion is available, and begin building age assurance, risk assessment, escalation and human-support processes where necessary.

More broadly, AI inventories should identify the purpose of each system, the individuals affected, the personal information involved, the system's role in decision-making, whether minors may interact with it and the extent of access or autonomy provided to the system. That information increasingly determines which privacy, transparency, assessment and governance requirements apply.

More News to Know

- **Planning Ahead: Preparing for New Privacy and AI Laws in 2027**

Please join us for our webinar, co-hosted with [Women in Security and Privacy \(WISP\)](#), which will look ahead at key privacy and artificial intelligence laws taking effect in 2027. As new compliance obligations take effect in the United States and abroad, companies must prepare for implementation and possible enforcement. This presentation will explain which companies may be affected, what compliance requires and what practical steps businesses can take now to prepare. The webinar is open to all in-house legal, privacy, compliance, risk management and AI governance professionals.

- **Katten Strengthens Privacy, Technology and AI Capabilities with Addition of Ex-Meta Counsel Brandy Worden**

Brandy's arrival at Katten's Los Angeles office as a partner in its Intellectual Property practice "reflects the rapidly growing client demand for sophisticated counsel on privacy, data governance, AI and emerging technologies," said Deepto Mukerjee, chair of Katten's global Intellectual Property department. [Read more about Brandy's experience and practice focus here.](#)

- **California Partially Eliminates California Invasion of Privacy Act Claims Faced By Many Companies**

By Brandy Worden, Camille Brooks, Gregory Korman, Jessica Kraver and Stuart Richter

On September 30, 2026, California Governor Gavin Newsom signed Senate Bill 690 (SB 690), eliminating the private right of action for claims for violation of California Penal Code Section 638.51, the pen register and trap-and-trace section, based on conduct occurring on an internet website, online application, or mobile application. SB 690 will take effect on January 1, 2027, and will apply retroactively to claims filed within two years of that date. [Read the full article.](#)

CONTACTS

Katten attorneys regularly advise clients on AI, privacy and data governance matters, including global privacy requirements, AI governance and transparency, automated decision-making, data use and retention, and emerging regulatory and litigation risks. For additional information concerning any of the developments discussed in this alert, please contact the authors or your Katten attorney.



Brandy L. Worden

+1.310.788.4434

brandy.worden@katten.com

Fred Bingham

+1.310.788.4433

fred.bingham@katten.com

Cyrus Borhani

+1.310.788.4634

cyrus.borhani@katten.com

Attorney advertising. Published as a source of information only. The material contained herein is not to be construed as legal advice or opinion.

©2026 Katten Muchin Rosenman LLP.

All rights reserved. Katten refers to Katten Muchin Rosenman LLP and the affiliated partnership as explained at katten.com/disclaimer.