HINSHAW

The February Compliance Love Edition of our Privacy, Cyber, and AI Compliance Alert

Privacy, Cyber & AI Decoded Alert | 5 min read
Feb 26, 2026

By: Cathy Mulrow-Peattie, Jason J. Oliveri, Claire Standish, Lily S. Elkwood

While Valentine's Day has come and gone, love for regulatory compliance remains in the air with the February edition of Hinshaw's *Privacy, Cyber, & AI Decoded* alert! Below are key trends that we are flagging for your consideration this month regarding children's privacy and AI.

Since We Love Our Children: *Youth Age Verification Developments*

Federal Trade Commission's Policy Statement on Age Verification

The Federal Trade Commission (FTC) issued a Policy Statement on February 25, 2026, to incentivize the use of age verification controls and to set out its enforcement approach. The policy statement, in essence, says that the FTC will not bring actions against general use and mixed use sites which collect information for age verification purposes that are in compliance with COPPA and certain other restrictive data requirements.

Our readers should be aware that several states have introduced legislation on age verification laws in 2026.

Key Takeaway: Proposed regulations on children's privacy remain critical as legislators and regulators are being lobbied by parents, communities, and educators to improve controls and age verification will continue to drive the discussion in Youth Privacy.

Since We Love to Talk: *AI Chatbots*

New York's AI Companion Systems

Effective November 5, 2025, New York's 2025 legislation (S.3008, Part U) establishes strict requirements for operators of AI companion systems. These are platforms that simulate sustained human-like relationships and engage in emotionally driven conversations.

The law mandates clear disclosure that users are interacting with AI at the start and at least every three hours during extended sessions. It also requires providers to implement protocols to detect suicidal ideation and refer users to crisis resources.

Enforcement lies with the Attorney General, who may seek injunctions and impose civil penalties of up to $15,000 per day for violations. All collected penalties fund a newly created Suicide Prevention Fund. The applies broadly to consumer-facing AI companions, excluding customer service or productivity bots.

Key Takeaway: For companies using chatbots with youth, this will be a highly regulated and litigious area. For companies using chatbots with consumers, there are learnings here about transparency and safety that should extend to other implementations. We also want to highlight that there are over 70 chatbot legislative initiatives being discussed in state legislatures.

For the Love of Creativity: *AI and Intellectual Property*

Arkansas Ownership Rights for Gen-AI Output, Trained Models, and US Copyright Office

Arkansas HB 1876 (Act 927 of 2025) establishes ownership rights for generative AI outputs and trained models. Under the law, a person who uses a generative AI tool to create content owns that output, provided it does not infringe existing intellectual property.

Likewise, anyone who supplies data to train an AI model owns the resulting trained model, assuming lawful data use and no contractual transfer of rights. However, if the AI output or trained model is created by an employee within the scope of employment, ownership belongs to the employer, mirroring "work made for hire" principles.

The statute also clarifies that no ownership can be claimed over infringing content (Arkansas HB 1876, 2025). Open questions remain about how Act 927's allocation of ownership will interact with federal copyright law and future federal AI legislation, including potential preemption risks, especially where the statute purports to assign rights in AI-generated works that may not qualify as copyrightable under current US law.

Key Takeaway: The US Copyright Office's Part Three of their study of copyright and artificial intelligence, to follow their May 2025 Copyright Ability Report, is still pending. As AI technology develops, it can blur how human contributions to AI-generated outputs occur, and we may see federal legislative changes to the current federal concept that authorship must be analyzed on a case-by-case basis.

For the Love of Complicated Employment Compliance: *AI in Employment*

Please see Hinshaw's *Employment Law Observer* blog posts on new requirements for employers regarding the use of AI in employment in Illinois and in California. We are tracking 14 current AI employment bills in several states.

Since we Love Our Health: *Embracing AI From our Healthcare Providers*

IL HB-1806 AI Therapy Services

Healthcare professionals' use of AI prohibits licensed therapy providers from using AI for anything beyond defined "supplementary support" (e.g., preparing client records, analyzing anonymized data, or identifying external resources) unless the client is informed in writing of the AI's use and purpose and provides consent.

It also bans entities from offering or advertising AI-delivered therapy "to the public of the State" unless the services are conducted by a licensed professional, with exemptions for religious counseling, peer support, and educational resources.

While Illinois' direct regulation of "AI therapy" is something of an outlier, other states are moving in a similar direction. For example, Nevada's AB 406 adopts a closely related approach for mental and behavioral health by prohibiting AI systems from being offered or represented as providing professional mental or behavioral healthcare, while still permitting administrative or supportive uses overseen by licensed providers.

Texas's SB 1188, while not banning AI therapy, requires physicians who use AI in electronic health records and diagnostic support to review AI-generated information, disclose that AI is being used in patient care, and remain responsible for the use of those tools, reinforcing that licensed professionals–not AI systems–must control clinical decision making. Utah's SB 169 requires AI therapy chatbots to clearly disclose to consumers that they are interacting with a machine, not a human therapist.

Key Takeaway: Together, these laws signal a clear trend that states are starting to draw bright lines around "AI as assistant, human as decision-maker," demanding transparency, consent, and professional oversight wherever AI touches mental health or other sensitive aspects of care.

Spreading the Love of Cyber and AI Compliance: *AI on the Attack–Cyber Threats*

The report, "Disrupting the First Reported AI-Orchestrated Cyber Espionage Campaign," (Anthropic, November 2025) describes how a Chinese state-sponsored group, GTG-1002, leveraged advanced AI to conduct large-scale cyber espionage with minimal human oversight.

Using Anthropic's Claude code as an autonomous orchestration engine, the attackers executed up to 90 percent of the attack lifecycle, including reconnaissance, vulnerability exploitation, credential harvesting, lateral movement, and data exfiltration, across roughly 30 high-value targets, including technology firms and government agencies.

Critically, human operators had to convince Claude to engage in the attack because the model is extensively trained to avoid harmful behaviors. They achieved this by posing as employees of legitimate cybersecurity firms and framing their requests as authorized penetration testing, effectively social-engineering the AI into believing its actions were ethical. This manipulation enabled the campaign to proceed largely autonomously, marking the first documented instance of AI-driven cyberattacks achieving operational scale.

There was also a recent *Bloomberg Law* news report that an unknown hacker used Claude and other Gen-AI to attack Mexican taxpayer accounts. Anthropic quickly shut down the accounts and increased its security.

Key Takeaway: The report underscores how Generative AI can dramatically lower barriers to sophisticated attacks, prompting us to recommend stronger compliance safeguards and policies, proactive cyber detection systems that are AI resilient, and defensive AI adoption in cybersecurity operations.

Love Notes: *Current Litigation on AI Notetaking Technologies*

As new technologies proliferate for recording our meetings, recent class action litigation under Illinois' BIPA and California's CIPA laws provides some key learnings for compliance professionals.

In Cruz v. Fireflies.AI Corp. (December 2025) and Valencia v. Invoca, Inc. (November 2025), class action plaintiffs raised claims surrounding adequate biometric and wiretapping notice and consent for the use of AI notetaking technology. Key additional issues in these cases include secondary use of vendor data, data deletion, and data anonymization.

Key Takeaway: Organizations should review the technologies, consents, notices, and deletion policies regarding these tools and related vendor contracts in light of these increased risks.

Hinshaw & Culbertson LLP is a U.S.-based law firm with offices nationwide. The firm's national reputation spans the insurance industry, the financial services sector, professional services, and other highly regulated industries. Hinshaw provides holistic legal solutions—from litigation and dispute resolution, and business advisory and transactional services, to regulatory compliance—for clients of all sizes. Visit www.hinshawlaw.com for more information and follow @Hinshaw on LinkedIn and X.

Related People

Lily S. Elkwood

Associate

☎ 212-655-3898

Cathy Mulrow-Peattie

Partner

☎ 212-655-3875

Jason J. Oliveri

Partner

☎ 212-471-6237

Claire Standish

Associate

☎ 212-655-3842

Related Capabilities

Data Privacy, AI & Cybersecurity

Employment Advice & Counseling

Healthcare

Intellectual Property

Labor & Employment

Regulatory & Compliance

Website Data Privacy

Related Insights

Illinois Adopts AI-in-Employment Regulations: What Employers Must Know for 2026

Employers: Ensure You Are in Compliance with California’s New AI Anti-Discrimination Rules