HINSHAW

Keep Calm and Prepare to Gobble On a New Feast of Privacy, Cyber and AI Laws

Privacy, Cyber & AI Decoded Alert | 6 min read
Nov 24, 2025

In this November edition of Hinshaw's Privacy, Cyber and AI Decoded, in celebration of the U.S. Thanksgiving holiday, we are recommending that our readers **Keep Calm** as they are faced with a new surge of legal requirements, regulations and enforcement actions, and **Gobble On**. We are here, except when running in the turkey trot or cooking, to help you assess your Privacy, Cyber and AI risk in response to these changes!

Compliance Dates on the Platter!

As January 2026 privacy, cyber, and AI strategy planning ramps up, we wanted to remind you about some upcoming compliance dates.

- Indiana's **Consumer Data Protection Act** is effective on January 1, 2026.
- Kentucky's **Consumer Data Protection Act** is effective on January 1, 2026.
- Rhode Island's **Data Transparency and Privacy Protection Act** is effective on January 1, 2026.
- Delaware's and Oregon's **right to cure period** expire, as of January 1, 2026. Both states have active privacy enforcement teams.
- California's CCPA revised regulations are effective January 1, 2026, as are the Delete Act regulations. Please see our October edition of Privacy, Cyber and AI Decoded for more information and below.
- We will highlight more AI state legislation and their effective dates in our December edition.

California's CPPA Increases its Appetite for Enforcement Against Data Brokers with a Strike Force and the Delete Act.

On November 19, 2025, the CPPA announced it had established a dedicated strike force to enforce California's data brokers registration and privacy compliance requirements. A data broker is defined as a business that knowingly collects and sells to third parties the personal information of a consumer with whom the business does not have a direct relationship, with certain exceptions.

In October 2025, the CPPA approved regulations to implement the Delete Act (California Senate Bill No. 362). The new regulations, effective January 1, 2026, establish how California consumers can submit deletion requests through the CPPA's new Delete Request and Opt-out Platform ("DROP") and how data brokers must process them. DROP will be a state-run website enabling consumers to request the deletion of personal information held by multiple data brokers with a single click. It is already established that data brokers operating under the CCPA have an accurate, compliant privacy policy.

The Delete Act requires, among other things, the following:

- Data brokers must register with the CPPA, provide specific information regarding their privacy practices, and pay a registration fee.
- Beginning August 1, 2026, data brokers must check DROP at least every 45 days, retrieve submitted requests, and delete matching personal information as requested by consumers, process related opt-outs of the sale or sharing of personal information, and request that their service providers delete such personal information and also process the opt-outs, including inferences.
- Beginning January 1, 2028, and every three years thereafter, data brokers will be required to undergo an independent third-party audit to assess their compliance with the Delete Act.

Businesses should assess if they qualify as a data broker under these requirements before January 1, 2026, and—if they have not already—develop a road map for the appropriate compliance measures. Failure to comply may subject a data broker to administrative fines as well as the costs and expenses of enforcement actions.

More Privacy Regulators are invited to the Table!

Two more states, **Minnesota and New Hampshire,** have joined the Consortium of Privacy Regulators, a bipartisan effort aimed at implementing and enforcing state privacy laws nationwide. The Consortium holds regular meetings and coordinates enforcement. Members now include the California Privacy Protection Agency and state Attorneys General from California, Colorado, Connecticut, Delaware, Indiana, New Hampshire, New Jersey, Minnesota, and Oregon.

Organizations operating in these Consortium states and subject to their privacy laws should understand that there is an increased likelihood for multi-state privacy enforcement actions, potentially raising their privacy risk.

The Federal Government's AI Moratorium is angling for an invitation to the Feast!

President Trump is reportedly planning to issue an Executive Order that will block states from regulating artificial intelligence. The Congressional effort on a AI Moratorium failed over the Summer, and there are discussions of revitalizing a Congressional Moratorium in the current pending defense bill. It is expected that this Executive Order, if issued, will be challenged in the courts.

NYS Department of Financial Services Sets the Compliance Table with New Cybersecurity Guidance for Suppliers and Insights on Voice Cloning

The New York State Department of Financial Services (NYDFS), the nation's leader in financial cybersecurity compliance, issued "Guidance on Managing Third Party Risks Related to Third Parties Services Providers" on October 21, 2025. These best practices state that New York State licensed financial institutions remain fully accountable for cybersecurity risks posed by vendors, specifically raising cyber concerns raised by AI, fintech, and cloud cybersecurity vendors, and that this cyber risk compliance will be reviewed during DFS examinations and investigations. Outsourcing these obligations must come with controls--due diligence, strong contracting cyber requirements, monitoring, and ongoing critical oversight.

The guidance highlights the need for strong cybersecurity policies, including a risk-based procurement approach and the availability of alternative providers with more adequate cyber controls, and how cyber controls are cascaded to downstream providers, often the target of a security incident.

We also wanted to note that NYDFS issued an "Insight" regarding the use of increasingly sophisticated voice cloning technologies in cyber attacks. Voice recognition software is used by financial institutions, often in authentication.

NYSDFS licensed entities using voice recognition technology are urged to integrate AI-related risks into their cybersecurity processes, policies, and training, conduct enhanced risk assessments regarding new AI use, including board-level oversight of AI deployments.

Florida's Enforcement Action is the Unexpected Guest at the Feast

Florida Attorney General James Uthmeier filed a civil enforcement action against Roku, Inc. and Florida Roku, Inc. (collectively "Roku"), a digital streaming content vendor, on October 1, 2025, for alleged violations of the Florida Digital Bill of Rights and the Florida Deceptive and Unfair Trade Practices Act.

- The complaint asserts that Roku collected and shared sensitive personal information from consumers, including children, without providing clear notice or obtaining valid parental consent. This personal information allegedly includes viewing activity, voice recordings, precise location information, and device identifiers, and the ability for third parties to combine this information in ways that could identify individual users.
- Similar to California's enforcement actions in other cases, the complaint further states that Roku misrepresented the effectiveness of its privacy settings, did not provide a functioning method for users to opt out of targeted advertising.

- Florida is seeking civil penalties that may reach one hundred fifty thousand dollars for each violation involving a known child.

Businesses operating in Florida should be aware that the state is committed to enforcing its privacy law and consumer protection laws, and organizations should swiftly move to ensure compliance.

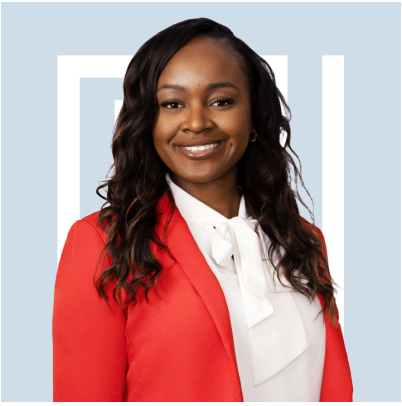
California's Attorney General's Office Reminds Us They Are Not a Side Dish with Sling TV CCPA Enforcement

On October 30, 2025, California Attorney General Rob Bonta settled with Sling TV $530,000 in fines for CCPA compliance violations, as well as additional ongoing compliance obligations involving children's personal information and consumer opt-outs. The investigation indicated, among other items, that Sling TV combined cookie preferences with a CCPA opt-out, and their technology did not opt consumers out. SlingTV also did not implement adequate safeguards for children's personal information.

Businesses subject to the CCPA should be aware that California has two active privacy regulators and one of the largest privacy regulatory enforcement teams globally. Businesses should review privacy notices, test their data subject action request processes and technology, audit their third-party data sharing activities and contracts, and validate their safeguards for the use of data of minor children.

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



Kelechi Ajoku

Associate

212-655-3837

Cathy Mulrow-Peattie

Partner

212-655-3875

Sharonda D. Roberson

Associate

945-229-6369

Related Capabilities

Consumer Financial Services

Data Breach

Data Privacy, AI & Cybersecurity

Financial Services

Healthcare

Insurance

Website Data Privacy

Related Insights

Don’t Be Spooked by 2026 Privacy Compliance Regulations