IAPP Global Privacy Summit 2026: State AI Trends, FTC Signals, California's DROP Build-Out, and the Hard Work of Cookie Compliance

Joseph Cahill, Laura Riposo VanDruff

April 2, 2026

Conference season is upon us, and with the cherry blossoms at peak bloom, the IAPP held its annual Global Privacy Summit here in Washington. The Summit featured keynotes from Prince Harry and Salman Rushdie, both of whom discussed their challenging experiences with personal privacy. For privacy professionals, the Summit underscored that 2026 is shaping up to be a year of proving that compliance programs work in practice, not just on paper. Here are a few takeaways.

FTC Commissioner Meador's Fireside Chat

Commissioner Mark Meador's fireside chat with IAPP Vice President Caitlin Fennessy suggested a pragmatic enforcement posture. When asked whether the FTC may move beyond its usual set of consent order remedies, Meador said his primary question when evaluating potential remedies is "Does this [remedy] adequately solve the harm that was alleged in the complaint?" That perspective and focus on fit and effectiveness may shape what the FTC expects to see from companies demonstrating compliance. Commissioner Meador also noted that building out mechanisms to enforce the Take It Down Act is a top Agency priority.

Navigating the State AI Landscape

The state AI conversation is moving away from sweeping, definition-heavy proposals and toward narrower obligations tied to risk, youth harms, and specific deployment contexts. Travis Hall of the Center for Democracy & Technology and Connecticut State Senator James Maroney both offered perspective on the legislative landscape. Although over 1,000 AI-related bills have been introduced in state legislatures so far this year, Maroney noted that only about 200 of those bills directly impact private businesses. The trend, he said, is toward more targeted approaches focused on frontier models and high-risk use cases.

Transparency and human oversight remain central themes. Hall emphasized that both automated decision-making systems and the people accountable for them can easily become "black boxes," and that regulators are beginning to push back. Maroney similarly emphasized accountability and noted that state lawmakers generally would welcome a federal standard, so long as it operates as a floor rather than a ceiling.

Looking ahead, Maroney flagged agentic AI as a likely Connecticut priority and suggested that future

legislation will be more tailored to particular use cases. He also expects pricing and agentic AI to be especially active areas in the next legislative cycle.

A separate session featuring in-house counsel from the New York Times, Univision, and other organizations focused on the practical side of AI governance. Panelists pointed to recurring challenges, including accuracy and IP concerns, the difficulty of negotiating vendor terms that continue to evolve, and the value of review frameworks that define acceptable use cases at the outset. For legal teams, that means starting with a few basic questions: what data is going in, what processing is expected, what outputs are expected, and who is accountable for the deployment.

Contracting remains a key part of that work. Panelists suggested that companies look beyond standard data processing agreements and focus as well on restrictions on model training, core security terms such as encryption and audit rights, and responsibility for harms tied to hallucinations or bias.

California DROP Platform Update

Phil Laird and Liz Allen of CalPrivacy presented on the Delete Request and Opt-out Platform (DROP), which has now processed over 262,000 deletion requests from California consumers. We've written previously about the DROP, and the panel provided helpful insight on how the system is beginning to take shape in practice.

One definitional point from the session is worth emphasizing. Under the Delete Act, a company may qualify as a data broker if it knowingly collects and sells to third parties the personal information of a consumer with whom it does not have a direct relationship. But, as Phil and Liz emphasized, California evaluates "direct relationship" at the data level, not the entity level. In practice, that means a business can still be treated as a data broker even if it maintains a direct relationship with the consumer in one context, so long as it also buys or sells data about that consumer obtained from third parties.

For data brokers, the DROP will support two implementation paths: API integration or manual list downloads. The CalPrivacy panel reported that data brokers can expect published technical documentation and a sandbox environment by the end of April, leaving a relatively short runway before the August 1, 2026 deadline, when the 45-day processing and reporting cycle begins.

California continues to actively enforce opt-out rights, and has brought actions against data brokers that have failed to register. However, businesses should be aware that the statute authorizes significantly greater penalties of $200 per consumer per day for failure-to-delete violations. As these penalties apply on a per-consumer basis, potential exposure for failing to honor deletion requests can escalate quickly.

Cookie Compliance

Unlike many other corners of privacy law, website tracking technologies, collectively referred to here as "cookies," remain an area with no settled compliance playbook. Small misalignments between consent banners, privacy policies, and actual tracker behavior can quickly escalate into enforcement actions or litigation.

The most common compliance pitfalls stem from configuration and governance failures. Businesses that use third-party cookie management platforms should remember that these tools rarely work out of the box. They must be configured carefully and tested with regularity. Panelists highlighted

common issues, like cookies firing on subdomains or subpages outside of the intended scope, inconsistent behavior between authenticated and unauthenticated portions of a site, and tracker categorizations that do not match legal requirements (e.g., whether a cookie is truly “strictly necessary” or instead serves advertising purposes). Another common pitfall are trackers that remain active long after a marketing campaign or pilot program ends, creating unnecessary and easily avoidable risk.

On the enforcement side, regulators continue to press companies to minimize the information they require to process global privacy control (GPC) signals and opt-out requests. Recent state actions have penalized companies for requiring excessive verification, creating more friction to opt-out than to opt back in, treating GPC as device-specific rather than account-wide, and misconfiguring consent tools so that tracking continued after a user opted-out. The penalties have been significant, reaching seven figures in some cases, and often paired with substantial remedial obligations including quarterly scans, comprehensive cookie inventories, and senior-officer certifications.

The broader takeaway is that cookie compliance is not a one-time exercise. Banners and preference centers can quickly drift from actual practices as sites evolve, and the technical complexity of tracking means effective compliance programs must translate legal requirements into specific engineering controls, test those controls continuously, and budget for ongoing maintenance. With plaintiffs’ firms rapidly advancing wiretap and UDAP claims targeting session replay tools and cookie technologies, precise documentation and disciplined deletion practices are now essential.

Conclusion

Regulators increasingly want to see controls that work, documentation that reflects real practices, and technical systems that match legal commitments.

For AI, that means treating disclosures, testing, and internal review as operational work, not just policy drafting. For data brokers, it means getting the mechanics right: matching logic, deletion workflows, suppression processes, and reporting cadence. Finally, for cookies, it means maintaining a living compliance program that can keep pace with site changes, vendor changes, and evolving litigation risk.