HINSHAW

6 Key Takeaways From the IAPP 2026 Global Summit for Privacy Compliance Professionals

Privacy, Cyber & AI Decoded Alert | 4 min read

Apr 9, 2026

By: Jason J. Oliveri, Sabrina Janeiro

The International Association of Privacy Professionals' (IAPP) 2026 Global Summit brought together regulators, in-house counsel, privacy officers, and technologists to discuss a complete spectrum of modern privacy issues.

Hinshaw attorneys were proud to attend the event and are pleased to share some insights from this year's conference, as we have for the last two years. The 2026 Summit covered a wide range of topics affecting the evolving privacy landscape–from cookies, wiretapping theories, and health data, to children's privacy, dark patterns, and AI governance.

Rather than treating AI as a standalone topic, the program showed how it now sits alongside, and depends on, traditional privacy and cybersecurity fundamentals. We outline these key takeaways for privacy compliance professionals in the alert below.

The Big Picture: Privacy Programs Under Pressure

Speakers repeatedly emphasized that privacy programs are being tested on multiple fronts at once: online tracking and wiretapping claims, expanding definitions of health data, children's privacy and design requirements, and the layering on of AI use cases into already complex data ecosystems.

Enforcement bodies are building institutional knowledge and new audit capabilities, particularly in California and other active jurisdictions, and are increasingly focused on whether companies can demonstrate operationalized privacy, not just policies on paper.

Online Tracking, Cookies, and Wiretapping Theories

One major track revisited cookies and online tracking through both EU and US lenses:

- EU-style consent requirements under the privacy directive for cookies and similar technologies.
- US plaintiffs' and regulators' use of state wiretapping and interception statutes to challenge pixels and third-party scripts on websites and apps.
- Practical questions around cookie banners, consent flows, and honoring browser/global signals in a way that avoids dark patterns.

California-based and health-related services were cited as particular flashpoints, illustrating how classic tracking tools can be recast as unlawful interception or unauthorized disclosure to third parties depending on configuration and context.

Health Data and Sector-specific Risks

The conference devoted time to exploring health-related data beyond traditional HIPAA-covered entities, including:

- How broadly "health" or "health-related" data should be defined, including symptom searches, wellness content, and inferences about conditions.
- Recent state developments (including new health privacy laws and state Attorney General actions) which treat consumer health data as a distinct category deserving heightened protection.
- The role of self-regulatory bodies and guidance (for example, in advertising standards) as practical benchmarks for health-related targeting and analytics.

Participants were encouraged to reconcile how their organizations define "health data" across privacy notices, internal data classifications, ad-tech, and analytics practices.

Children's Privacy, COPPA, and Design

Children's and teens' privacy stood out as a distinct concern, not just an AI issue:

- Updates and proposals on the Children's Online Privacy Protection Act (COPPA), along with newer state minors' privacy and design laws.
- Focus on dark patterns, nudging, and engagement-driven designs that may be inappropriate in services likely to be accessed by young users.
- Expectations that companies adopt age-appropriate defaults and clearer controls, even where services are not explicitly branded as child-directed.

The takeaway for in-house teams: children's and teen-oriented risks now cut across product design, marketing, data sharing, and governance, demanding cross-functional coordination.

Core Program Themes: Data Minimization, Dark Patterns, and Governance

Across many non-AI-specific sessions, familiar privacy principles were recast in more operational terms:

- Data minimization as a live compliance standard, affecting both legacy systems and new initiatives (including but not limited to AI training and analytics).
- Dark patterns as a hook for enforcement across consent flows, privacy controls, and commercial practices, regardless of whether AI is involved.
- The growth of audit-style oversight, especially in California, with dedicated functions looking for systemic compliance gaps separate from traditional investigation teams.

These themes stressed that enforcement is increasingly about how programs operate day to day, not just whether policies cite the right legal terms.

Where AI Fits in: One Part of the Story

AI was a prominent strand, but importantly, tied back to existing privacy doctrines:

- AI tools were framed as new ways of using personal data already subject to privacy, health, and children's laws, rather than an entirely new regulatory universe.
- Sessions on AI governance emphasized inventorying AI use cases, integrating AI into existing privacy and security governance, and applying data minimization, transparency, and fairness principles that privacy teams already know.
- Speakers stressed that law is about use cases, not technology labels: the same statute can apply to cookies, mobile SDKs, or AI models, depending on what they are used for.

Framing AI this way helps in-house counsel avoid reinventing the wheel, while still recognizing that AI can amplify existing risks and expectations.

Practical Next Steps for In-House Counsel

Reflecting the conference as a whole, organizations should consider:

1. **Refreshing tracking and cookie governance** with both EU consent and US wiretapping theories in mind.
2. **Clarifying internal boundaries for health and health-related data**, including how those categories affect advertising, analytics, and disclosures.
3. **Reassessing children's and teen-facing use cases** across design, marketing, and data sharing, not only where AI is explicitly used.

4. **Embedding data minimization and dark pattern review** into product and screen design workflows for all major user flows.
5. **Preparing for audit-style oversight**, especially from California, by building documentation around privacy controls, assessments, and governance.
6. **Integrating AI into existing privacy governance**, treating it as one of many data-intensive use cases that must be mapped, assessed, and monitored.

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

Sabrina Janeiro

Associate

305-428-5092

Jason J. Oliveri

Partner

212-471-6237

Related Capabilities

Data Privacy, AI & Cybersecurity

Healthcare

Healthcare Regulation, Compliance & Licensing

Regulatory & Compliance

Website Data Privacy

Related Insights

Top 6 Takeaways for Privacy Compliance Professionals From the IAPP 2025 Global Summit

4 Key Takeaways for Privacy Professionals Taken From the IAPP 2024 Global Summit