HINSHAW

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

Privacy, Cyber & AI Decoded Alert | 4 min read

Apr 30, 2025

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

The International Association of Privacy Professionals (IAPP) once again delivered an outstanding 2025 Global Summit.

Hinshaw partners and associates were proud to participate in the event and are pleased to provide our readers with valuable insights from this year's conference, as we did last year. This year's conference focused on the evolving landscape of privacy, artificial intelligence (AI), and cybersecurity regulations. We outline these significant takeaways for privacy compliance professionals in this alert below.

1. Federal Trade Commission's Enforcement Priorities

In her keynote, U.S. Federal Trade Commissioner (FTC) Melissa Holyoak outlined the FTC's top enforcement priorities under new agency leadership. These include:

- Protecting sensitive U.S. data as a matter of cybersecurity;
- Safeguarding children's privacy; and
- Addressing consumer protection issues, such as deceptive AI claims, while supporting innovation and competition.

Commissioner Holyoak also highlighted advances in age verification and digital parental controls and the FTC's amendments to the Children's Online Privacy Protection Act (COPPA) (effective June 2025).

She also emphasized the threat of foreign adversaries and reinforced the FTC's commitment to utilizing existing tools, including enforcement of the Protecting Americans' Data from Foreign Adversaries Act of 2025 and collaboration with the Department of Justice (DOJ) on the Bulk Sensitive Data Rule.

2. Harmonizing Innovation and Privacy Regulation

Keynote speaker, Sam Altman, CEO of OpenAI and chair of Tools for Humanity, addressed growing privacy and compliance concerns about emerging technologies, including biometric ventures. He emphasized that society's understanding of this technology is still developing and also spoke about the natural tension between technology and law.

Altman cautioned against overly broad AI regulations that could hinder innovation, while acknowledging the need to respond with regulations as issues arise. He discussed that we may need to develop a new regulatory framework for AI, as new issues arise, such as privileged data in AI.

3. State Privacy Enforcement

Regulators from the FTC, California's Privacy Protection Agency (CPPA), and Connecticut's Attorney General's Office explained their different approaches to privacy enforcement, signaling to the audience the continued patchwork quilt of privacy compliance.

While Connecticut's Office of the Attorney General spoke about working with businesses towards a compliance plan once an inquiry has been initiated, the CPPA indicated that its advisories are signals to the privacy community about their enforcement priorities down the road.

All speakers reminded the audience that stalling or not providing documents does not put your business in a strong position when responding to a regulator. It was clear that regulators expect organizations to have requested documentation of compliance readily available, including data protection assessments and service provider and third-party data protection agreements.

4. Cookie and Digital Tracker Compliance

Cookie and digital tracker compliance remains a key topic as Google announced that it would not deprecate third-party cookies in Chrome. Compliance efforts require an understanding of what cookies are used on a website, what personal data these cookies collect, as this data differs across websites, and what cookies are not used. It was recommended that organizations designate a team or individual for cookie and digital tracker compliance.

In addition, we would like to remind our readers that any digital tracker compliance needs to take into consideration wiretapping class action lawsuits.

5. DOJ's Bulk Sensitive Data Cybersecurity Rule

The DOJ's April 8, 2025, effective date for the Bulk Sensitive Data Rule made this session standing room only. The panel discussed the new administration's guidance issued on April 11, 2025, regarding the implementation of

Executive Order 14117, 28 CFR Part 202, for National Security purposes.

Under this Rule, the U.S. federal government is restricting access to certain Bulk Sensitive Data of U.S. citizens from foreign adversaries in China, Russia, Cuba, Venezuela, Iran, and North Korea.

The term "foreign adversaries" includes vendors, employment contracts, and investments owned by persons from these countries. Numerous contractual and other compliance requirements are required under this regulation, which are causing concerns for many businesses.

6. Artificial Intelligence

AI compliance discussions were prevalent again this year. Specific discussion points included AI integration and how best to handle that process. For example, answering the following questions could help your organization avoid redundancies down the road:

- Have you vetted your AI vendor and its product?
- Have you confirmed that the product will work with the systems you already have in place, or is it possible that you already have a product doing the same thing?
- In other words, have you identified any shadow tech/AI?

Other topics included children and AI, which are deemed high risk because of the harms they can and have caused, including AI telling children to self-harm. In light of these risks, age verification and its challenges were an important topic of this conversation. Identified challenges include technical immaturity, First Amendment implications, and restricting access to eligible users. No specific tool was recommended, but again, it comes down to vetting your vendor and the product.

Of course, assessing liability structures was also an AI issue discussed. Specifically, who is liable if the AI product your organization purchases ends up causing harm? Is it the developer or the deployer? Given that this issue will likely be addressed via contracts, we recommend that lawyers and business professionals alike scrutinize these contracts carefully.

Conclusion

The 2025 IAPP Global Summit highlighted the rapidly evolving regulatory landscape for privacy, AI, and cybersecurity. Organizations must remain vigilant, proactive, and adaptable in their compliance efforts. Our Privacy, Security, and Artificial Intelligence practice regularly advises companies on critical issues like those outlined above.

For further guidance or to discuss recent data privacy and cybersecurity developments, please contact our team.

Related People

Cathy Mulrow-Peattie

Partner

212-655-3875

Jason J. Oliveri

Partner

212-471-6237

Claire Standish

Associate

212-655-3842

Related Capabilities

Data Breach

Data Privacy, AI & Cybersecurity

Regulatory & Compliance

Website Data Privacy

Related Insights

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

Subscribe to receive timely legal insights directly in your inbox.