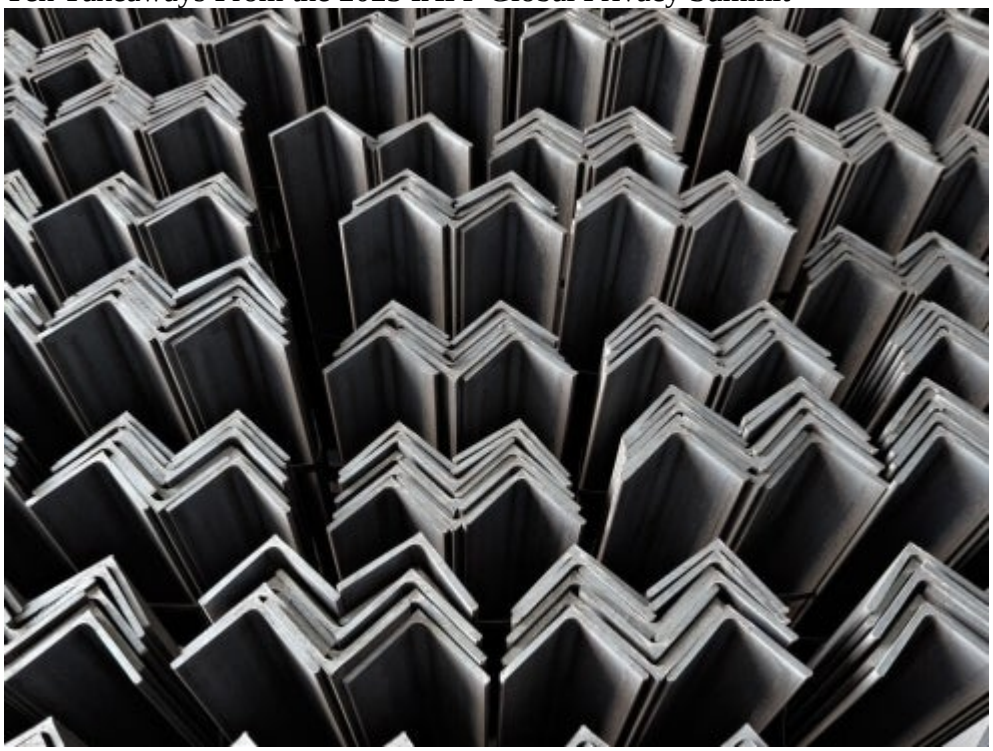
Blogs
April 25, 2023
Ten Takeaways From the 2023 IAPP Global Privacy Summit



International, federal, and state privacy regulators highlighted their ambitious agendas at the 2023 IAPP Global Privacy Summit in Washington, D.C. They, along with speakers from an array of private organizations, underscored the following takeaways that should be top of mind for businesses:

1. Generative AI is a high priority for regulators. A wide variety of content focused on artificial intelligence (AI), including the keynote remarks by Federal Trade Commission (FTC) Commissioner Alvaro Bedoya, who explained that he does not see "existential threats" to our society from generative AI. Commissioner Bedoya also pushed back on assertions that generative AI is unregulated. According to Commissioner Bedoya, AI technology is subject to prohibitions on unfair and deceptive trade practices in Section 5 of the FTC Act; civil rights laws like Title VII of the Civil Rights Act, the Fair Housing Act (FHA), and the Equal Credit Opportunity Act (ECOA); and tort statutes and common law claims. Commissioner Bedoya cautioned developers to "think twice" before they deploy a product that misleadingly leads people to think it is a human or injures individuals' mental health, especially that of teens or children.

2. California authorities plan active CCPA enforcement. Stacy Schesser, the Supervising Deputy Attorney General at the California Department of Justice, and Ashkan Soltani, the Executive Director of the California Privacy Protection Agency (CPPA), distinguished between legacy obligations under the California Consumer Privacy Act (CCPA) as it first came into effect in 2020 and new requirements that become enforceable later this year. Schesser and Soltani reminded the audience that the mandatory cure period under the statute has expired but explained that good-faith efforts to comply with new requirements may be viewed differently from obligations in effect since 2020. Schesser and Soltaini explained that while the CPPA will lead administrative enforcement and the Attorney General's office will continue to manage civil enforcement, the two will plan to cooperate on enforcement matters.

3. Don't overlook the CCPA "guidance" already available. Soltani responded to feedback that the CPPA has not provided sufficient guidance through its rulemaking proceeding, underscoring that he believes companies *do*

have sufficient guidance. First, he explained that examples offered within the text of the regulations themselves *are* guidance that were not required as part of the rulemaking process, but the CPPA elected to include them to help companies. Second, he directed attendees to view any published enforcement summaries or decisions as guidance to help inform their compliance strategies. Finally, Soltani reminded the audience that the "statement of reasons" and comment responses published by the CPPA are another source of information for understanding the intent of the regulations.

4. The FTC and state attorneys general are focused on online safety for kids and teens, not just privacy. FTC speakers emphasized that in addition to the FTC's long-standing emphasis on children's privacy through enforcement of the Children's Online Privacy Protection Act (COPPA), the FTC is focused on how product design decisions affect the online safety of children and teens. Specifically, using its authority to enforce against unfair trade practices, the FTC is now seeking to police whether the design of online products and services subjects children and teens to harassment, bullying, addiction, self-harm, depression, anxiety, and similar harms. Similarly, representatives of the California Attorney General's Office discussed the protections of the forthcoming California Age-Appropriate Design Code (CA AADC), highlighting the need to think beyond privacy and consider the safety and well-being of kids and teens.

5. Individual liability may be on the rise in FTC data security enforcement. For years, the FTC has nearly always named individuals as defendants in its so-called "fraud" cases rather than in its cases against legitimate businesses, but that may be changing. An FTC speaker opined that individual liability is now "always on the table" in FTC data security enforcement matters.

6. Don't overlook the CFPB as a privacy enforcer. When the Consumer Financial Protection Bureau (CFPB) was first launched, consumer privacy was seemingly not among its top priorities. But CFPB Director Rohit Chopra made clear that those days are long gone and that the CFPB should not be forgotten as a privacy enforcer along with the FTC, where Director Chopra used to serve as a commissioner. Director Chopra highlighted the proposed data rights rule that the CFPB expects to finalize later this year as an example of the CFPB's commitment to consumer privacy. Director Chopra also claimed that the CFPB is the leading federal agency addressing dark patterns, including as outlined in the CFPB's recent guidance on dark patterns in autorenewal subscription practices.

7. The CFPB is seeking to crack down on repeat offenders. CFPB Director Chopra reiterated his interest (which he also emphasized when he was at the FTC) in targeting repeat violators. Director Chopra said that companies have viewed fines as merely a cost of doing business. He suggested that the CFPB would seek to end that by limiting recidivists' right to engage in certain data processing activities and in holding individuals personally liable. Director Chopra explained that he sees curbing violations by repeat offenders as both protective of consumers as well as small businesses, which are (unlike their larger competitors) unable to absorb civil penalties as a cost of doing business.

8. Privacy regulations by another name. The array of regulatory sessions also highlighted that an effective privacy program cannot look solely to privacy laws. Regulations in other areas may introduce substantive privacy obligations for particular businesses or classes of technology. For instance, while Europe set the stage for privacy regulation globally with the General Data Protection Regulation (GDPR), it continues to introduce new privacy-related requirements, such as the privacy obligations applicable to "gatekeepers" under the Digital Markets Act (DMA), including with respect to data access and ad targeting as well as under the Digital Services Act (DSA), which requires increased ad transparency and restricts certain uses of minors' data by online intermediaries and platforms.

9. The future of cookies is top of mind. With major changes to advertising technology underway in both the Google and Apple ecosystems, the future of advertising technology and related privacy implications were a

major focus of the conference. Two sessions centered on the evolution and future of online advertising and envisioned the ad tech ecosystem entering a new phase, refocused around first-party cookies, as well as "cookieless" identifiers that can better leverage the trust relationship between the user and the provider. Another session discussed the role of universal opt-out preference signals such as the Global Privacy Control (GPC) as mechanisms to opt out of widespread advertising practices, reminding companies that they must honor GPC signals in California, and that more such requirements are to come in other states.

10. Increased need for regulatory convergence and reciprocity. The proliferation of privacy laws, both in the United States and abroad, underscore the need for more global solutions and reciprocity across regulatory regimes. In the closing keynote panel, Andrea Jelinek, Chair of the European Data Protection Board (EDPB), emphasized the need for convergence and the establishment of a reciprocal system for international data systems that maintain fundamental rights and establish bona fide standards rather than a system based largely upon exceptions. Similarly, in a session on the DMA and DSA, panelists acknowledged the increasing interplay between multiple privacy laws and concepts, and the need for collaborative approaches to ensure consistency and reconciliation across laws.

Authors

Explore more in

Privacy & Security