HINSHAW

Alerts

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

April 5, 2024
Privacy, Cyber & AI Decoded

We recently attended the International Association of Privacy Professionals (IAPP) 2024 Global Summit. The event provided great insights into privacy, artificial intelligence (AI), and regulatory issues, and we wanted to share those with our readers. Here are our top four takeaways from the conference:

1. Privacy Professionals' Scope of Work is Rapidly Growing

IAPP CEO Trevor Hughes' statement that the breadth of the work privacy professionals do is constantly growing is without question. Data protection, cybersecurity, AI, consumer protection, and legal and compliance issues are converging as new technologies and capabilities are used throughout the globe, and regulators' concerns grow. Of course, our use of AI is growing, but so are other emerging technology uses, such as AR/VR, biometrics, connected cars, and wearable technologies.

2. Understanding Your Data is Crucial in Product Development

What is clear from regulators, including Federal Trade Commission (FTC) Commissioner Slaughter, is that your ideation processes for developing products and solutions must take regulatory compliance and a clear understanding of your data into account. "We will fix it up later" will not be an accepted approach.

3. Data 'Brokers' Practices are Being Increasingly Reviewed by Regulators and Legislators

Consumer Financial Protection Bureau (CFPB) Director Rohit Chopra relayed that the CFPB is currently working on its plan to extend the Fair Credit Reporting Act (FCRA) to cover data brokers. According to Chopra, many businesses that build large consumer data sets and license or share them often do not comply with the FCRA's obligations.

Attorneys

Cathy Mulrow-Peattie

Jason J. Oliveri

Service Areas

Consumer Financial Services

Fair Credit Reporting Act

Privacy, Security & Artificial Intelligence

The CFPB is considering proposals that would include a data broker that sells certain types of consumer data into the definition of a "consumer reporting agency." Under such a proposal, a company's sale of data regarding, for example, a consumer's payment history, income, or criminal records would generally be a consumer report, triggering requirements for ensuring accuracy and handling disputes of inaccurate information, as well as prohibiting other misuse.

This move is aligned with the recent Executive Order restricting the sharing of certain sensitive information by data brokers with foreign adversaries. It follows state legislation in California, increasing the regulation of data brokers through registration metrics, deletion requirements, and audits.

4. Consumer Protection is a Top Priority for Regulators

It was also clear that consumer trust and protection are at the top of all regulators' minds. It is expected that we all dive deep and ensure that we raise any blind spots or unexpected results from the use of personal data as data-centric solutions are put into the market. Slaughter also stated that companies need to know what personal data they are collecting, how they are using it, and how minimization principles can and should apply. Do not just wait for harm to occur.

There was much debate during and after sessions about sensitive data and the need for better and consistent definitions to guide organizational compliance.

Regulators from the European Union (EU) also noted that the failure to understand personal data could have serious consequences for businesses—and not just for large companies. On that front, Commissioner Bertrand du Marais of CNIL indicated the possibility of changing the roles of Data Protection Authorities (DPA) and new challenges in light of the EU's Digital Services Act (DSA) package, which builds off of the General Data Protection Regulation (GDPR). We heard agreement among EU regulators that the difficulty with enforcement of GDPR and increasing new EU laws is a lack of technical expertise and the rising complexity of cases.

Beyond these topics, AI panels were abundant. Interesting discussions took place about data scraping, AI governance, the potential growing role of the Data Protection Officer (DPO) for AI, and EU regulatory sandboxes. Company speakers discussed that they were using technological solutions to manage AI risk and bias compliance.