Top Trends in Data Privacy

6 Takeaways from IAPP Global Summit

By:Kevin S. Olson and Ryan J. Perry
June 12, 2023



Following our attendance of the International Association of Privacy Professionals Global Privacy Summit 2023, we're sharing our Top 6 Takeaways from this year's conference. These are the big ticket items that we heard repeated as key issues and trends in data privacy and protection for the year and beyond – beginning with the two letters on everyone's lips: AI.

1. Artificial Intelligence Regulation Will Change the Game, but it is not the Wild West here in the U.S.

With all new technologies, there is an impulse to view the space as entirely unregulated. This view has certainly gained some traction with the endless wave of news regarding improvements to generative artificial intelligence (AI) chatbots, such as ChatGPT. But as FTC Commissioner Alejandro Bedoya helpfully reminded attendees, AI products are still subject to the FTC's authority under §5 of the FTC Act to regulate unfair and deceptive trade practices. Moreover, there is still the possibility for general tort and product liability claims. As such, companies developing generative AI solutions should be wary about the lack of AI ***specific*** regulations. Creating a product that is a black box, without the ability to predict risks or explain its functioning is a risky path forward, in part because the laws that regulate AI are so general in nature. Instead, to reduce the risk of future regulator or consumer inquiries, companies should be building products with privacy and safety in mind as part of the design process. The risks AI poses to individual autonomy will be of paramount concern going forward – the power to make anyone appear to say or do anything is potent indeed. AI has great potential for good when practiced ethically, but great potential for evil if not. As Commissioner Bedoya noted, many of those ethical obligations are not amorphous – they are necessary to avoid unfair and deceptive business practices and the liabilities that go with those practices.

2. Italy's Ban of ChatGPT may only be the Beginning

AI is far from unregulated across the pond either. The vast amounts of data processing necessary to train AI models remains regulated by the EU's General Data Protection Regulation (GDPR) and the United Kingdom's equivalent. Earlier this year, the Italian Supervisory Authority banned ChatGPT because of concerns about that data processing. Following a number of privacy focused changes in response to the Supervisory Authority's list of demands, ChatGPT services have resumed in Italy for the time being. However, data processing in connection with training the AI models may only be the beginning. Indeed, even if data about an individual is not accurate, it is still *data about that individual* – in other words, it is ***personal data***. In the past, accuracy of data, while featured in laws like the GDPR, has often felt like an afterthought. This clearly is not good enough anymore and the right to data correction under the GDPR will require renewed attention. As noted above, AI poses real risks because those at the helm of generative AI programs can make anyone appear to say or do quite literally anything. The resulting images or video are clearly still personal data relating to the individual who is the subject of the work product. And under the GDPR, where it applies, they have rights to their data – including to have

it corrected.

3. Are you Sure your Data is Pseudonymous?

The GDPR's high standard for anonymous data – data that cannot be reidentified by any means available to anyone (and it means *anyone*) – is very difficult to achieve while producing useful data sets. For some use cases, it may approach impossibility. That is why many businesses choose to pseudonymize data instead. Although pseudonymous data is still regulated, it has many benefits over raw data, including lowering the risk that the data will be compromised in a personal data breach and lightening the burden in addressing data subject requests. However, businesses should take care to make sure a data set is truly pseudonymous to ensure that the business can reap these benefits. The GDPR defines pseudonymization as "the processing of personal data in such a manner that the personal data *can no longer be attributed to a specific data subject without the use of additional information*, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person" (*emphasis added*). Simply removing a handful of identifiers is likely insufficient. Businesses depending on pseudonymization should methodically assess whether their process meets this standard.

4. Move to a Cookie-Less Future Comes With New Privacy Considerations

Google's decision to phase out third-party cookies is already underway and will continue to have an enormous impact on the digital advertising world. One increasingly popular decision among digital advertisers will be to utilize first-party data, meaning that more companies will move toward using data they directly collect from customers for analytics and targeted advertising. While moving away from using third-party data might mitigate certain concerns, businesses should be wary of thinking that first-party data is a privacy compliance cure all. Notice and consent from individuals are still required under many circumstances, and companies will also need to be mindful of the increased amounts of data that they will be handling directly. Another key point to consider is the use of other identifiers such as device fingerprints. Many companies may think this a win-win for privacy in that they can identify users, but the users' direct identifiers are not being processed. However, device fingerprints would still be personal information under laws that broadly define personal information (e.g., the EU's General Data Protection Regulation (GDPR) or the California Consumer Privacy Act (CCPA)) as *any* information related to an identified or identifiable natural person. If the entire purpose of processing a piece of data is to uniquely identify a user so that you can market to them, it is a safe bet you would be handling personal information.

5. U.S. State Law Compliance Will Continue to Get Complicated

With the proliferation of state privacy laws, including California, Colorado, Connecticut, Utah, Virginia, and just this year, Iowa, Indiana, Montana, and Tennessee, the compliance picture continues to get murkier. With more such laws on the way a common solution is to find the highest standard across these states and apply it to all users. But as the types of new state laws continue to diverge between a more business friendly approach following the Virginia model and a more robust GDPR-style law in California, the simplest solution may not always be best. For companies that need to process certain types of data or simply cannot operationalize the need to provide data subject rights to all users across all states, a more piecemeal approach is still a workable option. And for those holding out hope for a revival of the American Data Privacy and Protection Act (ADPPA), there was little optimism among conference attendees that a federal law would be passed anytime soon. The biggest takeaway here is that companies should focus on privacy measures that are both practical and defensible. The patchwork, unfortunately, is getting patchier.

6. California Regulators Are Gearing Up for Enforcement (and More Regulations)

With the recent enactment of the California Privacy Rights Act (CPRA) regulations, many companies might think that they can finally catch their breath with California privacy compliance. But according to California regulators this is just the beginning. Actual enforcement of the CCPA, which was amended by the CPRA, will begin in July 2023 with the California Attorney General's office focusing on traditional civil enforcement and the newly created California Privacy Protection Agency (CPPA) bringing administrative actions. Furthermore, CPPA Executive Director Ashkan Soltani noted that the CPPA will be engaged in "perpetual rulemaking." There are a number of areas the CPPA did not address in its initial round of rulemaking with rules regarding areas such as artificial intelligence and data protection impact assessments (DPIAs) still to come. That said, the issues underlying recent regulatory action against Sephora, such as the rights of individuals where their data is being used for cross-context behavioral advertising were the main focus of the regulators. Companies who engage in cross-context behavioral advertising should hurry to get their data protection house in order ahead of the July 2023 deadline.

For more information on the CCPA, GDPR, or any of the other top trends in data explored above, and how your business can become compliant with data protection regulatory regimes, please contact Ryan Perry, Kevin Olson, or another member of the Privacy and Data Security Team.