



Data Privacy Detective Podcast

Episode 35 – Hot Topics in Data Privacy – From the U.S. Front

May 13, 2019

Categories:

[Blogs](#)

[Podcast](#)

[Publications](#)

[Technology Blog](#)

Authors:

[Joseph J. Dehner](#)

[Michael E. Nitardy](#)

The May 2–3, 2019 International Association of Privacy Professionals (IAPP) Conference featured leading U.S. officials and participants in the data privacy field. The IAPP is the world's largest organization devoted to the issue. [Mike Nitardy](#), a certified Privacy Professional (U.S.) and data privacy attorney at Frost Brown Todd LLC shares highlights from the conference:

- **FTC** – The Chief of the Bureau of Consumer Protection of the U.S. Federal Trade Commission emphasized increasing enforcement activity of personal data protection rules. The FTC is pursuing businesses that fail to establish and maintain standards for protecting personal data from illicit access and unfair use. The Chief emphasized both sides of Article 5 of the statute under which the FTC regulates business. Activities to date have focused on businesses that say one thing in their privacy policies and marketing materials but act differently – as this falls within the ban on deceptive trade practices. But the Act also forbids “unfair” trade practices, and the FTC thus has authority to act against privacy abuse when it’s unfair, even if a business has not been deceptive in what it claims to do. The FTC official argued it is not necessary to establish a Data Protection Authority as is the rule in European and many other countries, as in his view the FTC already has that authority.
- **Health Data** – The head of the U.S. Department of Health and Human Services’ Office of Civil Rights (OCR) reported on three enforcement trends concerning health data:
 - Increasing attention to forcing holders of health data to provide prompt and effective access of persons to their own health data, based on widespread complaints about how difficult this has become for individuals to

access their own data.

- OCR's increased encouragement to businesses to use and observe HIPAA regulation exemptions as appropriate.
- The changing nature of data breaches, which has gone beyond stolen or lost hardware, and has increasingly focused on computer hacking and IT intrusion. The OCR expects health care organizations to have systems that identify and contain any intrusions.
- **California** – California's recent adoption of the CCPA, which is effective in 2020, is a departure from state privacy rules, with its emphasis on the value of personal data and how individuals should be able to decide whether to allow the use of their data by being informed about and paid something for such use beyond what they expect. This forces businesses with substantial California residents' personal data to review their data sharing agreements to ensure they will be informing data subjects of how data is being shared and whether the gatherer of their data may offer payment in exchange for the right to share the data (or for the gatherer to be paid for third-party use of such data).
- **Emerging hot topics** – New issues emerged from participants. The human body as personal data is one such subject. Technology including facial, eye scan and other identification techniques make our bodies as a transmitter of personal data. How will this be regulated? The internet of things and related developments race ahead of government and private sector efforts to prevent and address abuse of privacy expectations.

Listen to Podcast 35 to learn what leading privacy practitioners discuss among themselves at global gatherings. If you have ideas for more interviews or stories, please email info@thedataprivacydetective.com.

© 2026 FBT Gibbons LLP. May be considered attorney advertising in some jurisdictions.