

New Privacy Perspectives Episode: Data Broker Laws Are Expanding. Is Your Business in Scope?

Alexander I. Schneider, Aaron J. Burstein, Céline Guillou

July 30, 2026

Data broker laws are expanding, and their reach may extend well beyond companies that traditionally think of themselves as data brokers.

In the latest [episode](#) of Privacy Perspectives, [Alex Schneider](#) is joined by [Aaron Burstein](#) and [Céline Guillou](#) to discuss the growing patchwork of state registration laws, California's DROP deletion mechanism, and the questions businesses should be asking regarding when they are subject to data broker registration obligations.

The conversation begins with New Jersey's recently enacted data broker law, which moved from introduction to enactment in only two days. The law includes annual registration fees that could reach \$1.5 million for some businesses, as well as a ban on the sale of sensitive data that took effect immediately. The law also bans all sales of New Jersey residents' sensitive data; this ban applies to all controllers, not just data brokers, and went into effect immediately on June 30.

Although data broker registration is not expected to begin until spring 2027, and the law could be amended before then, companies have already begun to assess whether their activities fall within the law's scope.

That analysis may not be straightforward. Data broker status often depends on specific data flows rather than a company's overall relationship with consumers. A retailer, for example, may collect information directly from its customers while also obtaining additional information from a third-party source. If the retailer later sells or licenses that enriched data, it may be engaging in activity covered by a data broker registration laws despite having a direct relationship with the consumer.

The group also discusses how these requirements may apply to advertising technology. Definitions of "sale," "sharing," and "direct relationship" vary across states, and regulators have not always provided clear guidance on how those terms apply to particular technologies.

California's Delete Request and Opt-out Platform, known as DROP, adds another operational challenge. The system allows California residents to submit one deletion request that is transmitted to registered data brokers. Compliance requires businesses to identify relevant records, process requests, communicate deletions, and address data held by service providers and other recipients. Companies that do not have a detailed understanding of their data flows may find those requirements difficult to implement.

The episode also examines New Jersey's new "data collector" category, which could require certain

businesses that obtain information directly from consumers and provide it to data brokers to register with the state. This approach could bring retailers and other first-party businesses into the fold even when data brokerage is not their primary business.

The discussion concludes with practical guidance for companies assessing these laws. Businesses should review their data sources and destinations, evaluate registration requirements consistently across jurisdictions, and avoid assuming that a first-party customer relationship places every data flow outside the definition of data brokerage.

One Feed, Multiple Formats

Privacy Perspectives episodes appear on the same Ad Law Access feed hosted by Simone Roach, so if you're already subscribed, you'll get these automatically. If not, subscribe now on your preferred podcast platform.

We've got more podcast conversations and formats planned for 2026. One subscription gets you everything. Find the episode and more [here](#).