Ad tracking tools subject to further scrutiny under US bulk data rule

27 Oct 2025 | 19:10 GMT | **Comment**
By Xu Yuan

As digital advertising faces the increasing scrutiny that comes with mounting litigation and tightened regulation, the US bulk data rule that originated from national security concerns over hostile foreign countries' access to American data has imposed fresh obligations on companies and restrictions on the flow of data.

As digital advertising faces increasing scrutiny on the back of mounting litigation and tightened regulation, the US bulk data rule that originated from national security concerns over hostile foreign countries' access to American data has imposed fresh obligations on companies and restrictions on the flow of data.

The bulk data rule, also known as the Data Security Program, imposes prohibitions and restrictions on the sale or sharing of Americans' personal data with certain countries. The rule, implemented by the National Security Division of the US Department of Justice, became effective April 8 and went through a grace period that ended July 8.

The broad coverage of the rule, which has both civil and criminal consequences, brings under its scrutiny the practice of using website tracking tools for the purpose of delivering ads by a company with a public-facing website or mobile app, which has become almost ubiquitous across sectors.

This means not only suppliers of ad trackers, which are usually considered data brokers, but companies that use these trackers will be targets of the rule. They will be required to examine their data flow and set up guardrails such as contractual obligations on vendors to prevent running afoul of the regulations.

The DOJ's program establishes what are effectively export controls preventing foreign adversaries, and those subject to their control, jurisdiction, ownership and direction, from accessing US government-related data and bulk genomic, geolocation, biometric, health, financial and other sensitive personal data. The six foreign adversaries are China, including Hong Kong and Macau; Russia; Iran; North Korea; Cuba; and Venezuela.

The rule defines data brokerage as the sale of data, licensing of access to data, or similar commercial transactions that involve the transfer of data from one person to another, where the recipient did not collect or process the data directly from the individuals linked to the data. "This definition covers both first-party data brokerage (by the person that directly collected the U.S. person's data) and third-party data brokerage (by a person that did not directly collect the U.S. person's data, such as a subsequent reseller)," the DOJ's FAQ says.

"Although we tend to think of data brokerage as the selling of data by companies that don't have direct relationships with consumers, the DOJ rule defines it more broadly and specifically. It includes a consumer-facing company's use of tracking pixels or [software development kits] or cookies or other mechanisms that make certain types of personal data available to third parties," said Aaron Burstein, a partner at Kelley Drye & Warren.

In an example given in the rule, if the tracking pixels or SDKs used by a US company on its website or app transfer data covered by the rule to a country of concern for targeting advertising, the US company is considered to engage in prohibited data brokerage.

The DOJ rules will apply regardless of whether a company considers itself a data broker, according to David Aaron, a partner at Perkins Coie. "It's not who you are. It's what you do," he said.

Some companies are not aware their use of ad trackers is subject to the rule.

"A lot of people don't realize that these ad trackers, many of them, are considered data brokerage," Tracy Bordignon, a senior director at FTI Consulting who works on privacy and security, said during a recent webinar*. "Companies are not necessarily thinking that their ad trackers will fall into the scope, and because they do, that's something to focus on."

The use of ad trackers has become such a widespread practice that sometimes a company could be in the dark about what exactly is happening on their website. In certain instances, the number of trackers on a website is said to reach about 100.

The promulgation of the rule will further push companies to take stock of what data they are collecting, sharing or selling. “As part of knowing your data, I am suggesting that you need to really know your ad trackers,” Bordignon said.

“The DOJ has made it very clear that it expects companies to know their data, and so any ignorance or lack of awareness by one part of the company is unlikely to limit that company's responsibility,” Aaron said.

The bulk data rule is consistent with the tightening of regulation of the data broker industry following years of rampant growth that has led to surveillance scandals, like the one that exposed Cambridge Analytica.

"It definitely raises the risk of engaging in data brokerage,” Aaron said.

While the rule covers four categories of data transactions — data brokerage, vendor agreements, employment agreements and investment agreements — only data brokerage is outright prohibited. The other three, considered restricted transactions, can be carried out if certain security guardrails are in place.

This shows that “data brokerage is probably a high priority for the Department of Justice,” Aaron said.

The use of ad trackers, such as Meta Platforms’ Pixel, has triggered a deluge of lawsuits raising claims under California’s wiretapping law. Despite the defense argument that the law was not enacted to be applied to new technologies such as the trackers, federal judges have allowed many to proceed.

The bulk data rule has already been used as a ground for litigation. Lawsuits have been filed in San Francisco and Chicago federal courts targeting digital ad companies Index Exchange and Xandr, which are accused of illegally sharing data with Chinese company Temu (see here).

Compliance requirements with the new regime are not entirely new, but can be built on what is required under state privacy laws that have also tightened the scrutiny of third-party collection and processing of data.

“It builds on a foundation that has been established over the past several years for state privacy law compliance. But it adds further steps of analysis to see whether the rule is triggered,” Burstein said.

The proliferation of state privacy laws and regulations has had an impact on companies’ use of ad trackers. Conducting sufficient due diligence on third parties that receive and process data has become “more and more commonplace for state privacy law compliance, and it also supports compliance with the bulk data rule,” Burstein said.

Thanks to state privacy laws, private litigation and now the DOJ rule, there has been “a tremendous shift in terms of how advertising and analytics trackers are managed and a lot more attention to creating the inventory of what's currently present on the site, as well as establishing and formalizing a process to add new trackers, because there is exposure from multiple fronts,” he said.

In the past, a company’s marketing department has usually been in charge of adding ad trackers, “without a lot of oversight from legal,” FTI’s Bordignon said.

As the screw keeps tightening, “the old way of letting marketing or IT teams add trackers whenever they felt the need is disappearing,” Burstein said.

**Demystifying the Bulk Data Rule, Foley Hoag, Oct. 9, 2025.*

Please email editors@mlex.com to contact the editorial staff regarding this story, or to submit the names of lawyers and advisers.

Related Portfolio(s):
Data Privacy & Security - Regulation - Executive order Preventing Access to Americans’ Bulk Sensitive Personal Data

Areas of Interest: Data Privacy & Security, Financial Services, Technology, Trade

Industries: Banking & Finance, Banking, Lending & Credit Services, Computing & Information Technology, Financial Technology, Pharmaceuticals & Biotechnology

Geographies: North America, United States