The Bulk Data Access Rule: What Advertisers Need to Know

Aaron J. Burstein, Alysa Z. Hutnik

April 22, 2025

On April 11, the Department of Justice issued an extensive set of FAQs on its Bulk Data Access Rule and advised that it "will not prioritize civil enforcement actions against any person for violations" of the Rule through July 8, 2025, "so long as the person is engaging in good faith efforts" to comply with the Rule. (DOJ refers to the "Data Security Program" or "DSP." We refer to "the Rule" to emphasize that it is a legally binding regulation with obligations that extend beyond data protection.)

This post takes a closer look at how the Rule applies to publishers, adtech vendors, and data vendors. The FAQs underscore that the Rule covers many of the identifiers and data transactions that are common in digital advertising. With a limited enforcement reprieve in place, the next few months provide companies that engage in digital advertising with an opportunity to better understand their obligations under the Rule.

Most importantly, the Rule prohibits certain types of "data brokerage" to "countries of concern" and certain "covered persons." The concept of "data brokerage" as well as the categories of personal data covered by the Rule are broad enough to apply to a significant amount of digital advertising activity. The Rule also imposes contractual restrictions on data brokerage to "foreign persons" who are not covered persons. Knowing violations of the Rule are subject to criminal prosecution and potential monetary penalties of up to $1 million and 20 years in prison.

Note: The Rule restricts a wide range of data transactions other than data brokerage, and this post does not provide a comprehensive overview of all of them. Agreements with employees, vendors, or investors in countries of concern warrant a close look for compliance with the Rule.

Is Digital Advertising Really a National Security Issue?

In the view of the Biden and Trump administrations, yes – primarily because hostile countries may be able to use data and modeling techniques from digital advertising for adversarial purposes.

Executive Order 14117, which directed DOJ to develop the Rule, asserts that access by countries of concern to "bulk data sets" fuels "the creation and refinement of AI and other advanced technologies, thereby improving their ability to exploit the underlying data and exacerbating the national security and foreign policy threats." The Federal Register notice announcing the final Rule (the "Final Notice") states that modeling techniques commonly used in digital advertising allow countries of concern to "glean valuable information about the health and financial well-being of a large number of Americans through smaller datasets."

Congress also weighed in on national security risks in the commercial data marketplace, though not

with a specific focus on digital advertising. The Protecting Americans' Data from Foreign Adversaries Act of 2024 ("PADFA") prohibits "data brokers" from selling "personally identifiable sensitive data" about U.S. individuals to any "foreign adversary country" (China, Iran, North Korea, and Russia) or an entity that is controlled by a foreign adversary. A "data broker" is an entity that makes available personal data that it "did not collect directly" from individuals.

It is important to note that the Rule and PADFA are separate. The Rule is based on the President's authority under the International Emergency Economic Powers Act and other national security authorities, is enforced by DOJ, and violations are subject to criminal penalties. PADFA went into effect on June 23, 2024, does not have any implementing regulations, and is enforced by the FTC.

How Does the Rule Apply to Digital Advertising?

The Rule **prohibits** U.S. persons from knowingly engaging in "data brokerage" of "bulk U.S. sensitive data" with "countries of concern" or "covered persons." The Rule permits data brokerage to "**foreign persons**" who are not covered persons but requires data providers to prohibit onward transfers of bulk U.S. sensitive data to countries of concern and covered persons. The Rule defines "foreign persons" in the negative as "any person that is not a U.S. person." A U.S. person, in turn, includes any "entity organized solely under the laws of the United States" or a U.S. jurisdiction.

The countries of concern are China, Cuba, Iran, North Korea, Russia, and Venezuela. "Covered persons" include entities that are 50 percent or more owned by countries of concern or certain other covered persons. However, as noted in FAQ 58, if a covered person is known to direct a transaction (e.g., by signing an agreement on behalf of a foreign person that is not a covered person), the transaction may be prohibited. This FAQ, however, makes an effort to draw some lines around due diligence obligations, stating that "absent evasion, U.S. persons engaging in vendor agreements and other classes of data transactions with foreign persons are generally not expected to conduct 'second-level' due diligence on the employment practices of those foreign persons to determine whether their employees qualify as covered persons."

The other key terms break down as follows (and we summarize them in this diagram):

- **Bulk U.S. sensitive data**" consists of two main parts: "sensitive" data and thresholds that define "bulk" transfers of sensitive data. These definitions are broad enough to cover many digital advertising data flows.
    - "**Sensitive personal data**" ("SPD") about U.S. individuals. SPD includes usual suspects such as precise geolocation data and personal health data. But it also includes "listed identifiers," such as mobile advertising identifiers ("MAIDs"), device identifiers, and contact information. The Rule does not exempt pseudonymized, deidentified, or anonymized identifiers.
    - The combination of any two listed identifiers, or a listed identifier combined with other data sensitive personal data elements, is SPD.
    - **"Bulk" thresholds.** A U.S. company that engages in SPD data brokerage provides access to "bulk U.S. sensitive data" – and is subject to additional Rule provisions – when the company meets certain volume thresholds. For combinations of listed identifiers, the threshold is 100,000: a company that brokers the identifiers of more than 100,000 U.S. persons during a 12-month period – a limit that many publishers and data providers would easily exceed – is engaged brokering bulk U.S. sensitive data. This threshold considers all

covered data transactions during the 12-month period. For instance, 12 separate transactions involving 10,000 identifiers per transaction exceeds the threshold. The bulk thresholds for other types of SPD are lower, ranging from 10,000 for personal health or financial data to 100 for human genomic data.

- "**Data brokerage**" means selling or providing access to data that the *recipient* did not collect or process. The data *provider*'s relationship to individuals in a dataset is irrelevant, and a wide range of common digital advertising data flows are likely to be considered data brokerage. For instance, a first party likely engages in "data brokerage" when the first party provides its own customer data to a third party. A website publisher that allows adtech vendors to collect user-level information also is likely engaged in data brokerage.

- **Examples.** The Rule provides a couple of examples to illustrate how these terms fit together in the digital advertising context. For instance, according to the Rule, "tracking pixels or software development kits" that are knowingly incorporated into mobile apps and which provide access to bulk U.S. sensitive personal data constitute data brokerage. (And, if the recipients of the data are countries of concern or covered persons, it is *prohibited* data brokerage.) As noted above, the combination of two "listed identifiers," such as a MAID or other advertising identifier and an IP address, is SPD.

- In a twist on this example, the Rule states that if a U.S. company engages a non-U.S. contractor to develop the app described above, then *both* companies are potentially in violation of the Rule.

- The scope of data brokerage has some limits that are relevant to digital advertising. For instance, a digital audience reflecting a non-sensitive interest – "Knitting Enthusiasts," for example – and that identifies its members only through a MAID or similar identifier likely is not SPD and would not be prohibited in data brokerage transactions.

What Is Required to Engage in Data Brokerage with Foreign Persons?

The Rule permits data brokerage transactions with foreign persons other than covered persons but imposes three significant conditions on these transactions.

- First, although data brokerage transactions with foreign persons (other than covered persons) are allowed, agreements for these transactions must include onward transfer restrictions. Specifically, the agreement must prohibit the data recipient from transferring the brokered data to a country of concern or covered entity. DOJ will consider data transactions that occur under agreements that pre-date the Rule to be covered by the Rule. As stated in the Final Notice (90 Fed. Reg. 1645):

"The [R]ule applies to covered data transactions engaged on or after the effective date. Covered data transactions completed prior to the effective date are not regulated by the [R]ule. However, unless exempt or otherwise authorized, U.S. persons knowingly engaging in a prohibited or restricted covered data transaction on or after the effective date are expected to comply with the [R]ule, notwithstanding any contract entered into or any license or permit granted before the effective date. . . . Restricted and prohibited transactions will not be grandfathered in as compliant simply because any resulting covered data transactions are subject to a preexisting contract or agreement."

- In response to FAQ 4 ("What is the effective date for the DSP?"), DOJ further recommends

amending agreements as necessary during the current period of enforcement forbearance, as a sign of "good faith efforts to comply with or come into compliance with the [Rule] during that time."

- Second, the Rule's knowledge standard implies some due diligence obligations. "Knowledge" under the Rule includes actual as well as constructive knowledge. If a person or entity "reasonably should have known" from the circumstances that they are transacting with a covered person, for example, they act "knowingly" under the Rule. For instance, determining whether a foreign is a covered person may be a complex, fact-intensive exercise. Conducting diligence to understand how a foreign recipient will use and disclose (if at all) any bulk U.S. sensitive personal data is an important complement to the required contractual restrictions.
- Neither the Rule nor the FAQs are prescriptive about the due diligence required for data brokerage transactions with foreign persons. Questions that could be helpful in conducting due diligence on foreign persons include:
    - Is the foreign person's signatory on a data brokerage agreement a covered person?
    - Is the data brokerage use case consistent with prohibiting data access by covered persons/countries of concern?
    - Does the foreign person have internal controls that are reasonably designed to prevent data access by covered persons or countries of concern?
    - Does the foreign person have policies and procedures to detect and report of access by covered persons or countries of concern?
- Third, companies that are subject to the Rule must report known or suspected violations of any of their contractual onward transfer prohibitions to DOJ within 14 days. The same knowledge standard applies here. Developing internal processes to identify, investigate, and respond to potential violations will help companies to reduce their risks.

The Rule is complex, and the potential for criminal penalties raises the stakes of compliance beyond other laws that regulate digital advertising. For many companies, the immediate priorities will likely revolve around identifying "data brokerage" transactions, data recipients that qualify as "foreign persons," and determining whether relevant contracts need to be amended. These steps have become part of the muscle memory of many companies in the digital advertising ecosystem, and we expect that they will provide a strong foundation for compliance with the Rule.

We will watch closely for any further guidance about the Rule.