wiley

ALERT

New Federal Data Broker Law Will Restrict Certain Foreign Data Sales Effective June 23

May 7, 2024

On April 24, 2024, President Biden signed into law H.R. 815, which includes the Protecting Americans' Data from Foreign Adversaries Act of 2024 (PADFA or the Act), a significant restriction on foreign data sales by U.S. companies that will be effective June 23, 2024. The Act generally prohibits "data brokers" from selling, licensing, or transferring for consideration an American's "personally identifiable sensitive data" to certain "foreign adversary" countries – China, North Korea, Russia, and Iran – *or* to any entity "controlled" by those foreign adversary countries.

Notably, PADFA applies to sensitive data sales to entities with 20% or more ownership by an individual or business domiciled or with a principal place of business in any of the foreign adversary countries. Further, the Act applies to a broad set of "sensitive data," including device geolocation data to certain information on "an individual's online activities." PADFA will be enforced by the Federal Trade Commission (FTC), which will be able to seek civil penalties for violations.

The passage of PADFA adds to the already complex landscape for data brokers and cross-border data sales. For example, PADFA follows a recent Executive Order directing restrictions on certain personal data transfers to "countries of concern," and adds a federal component to existing state laws that regulate data brokers. Companies engaged in data sales and cross-border data transfers will have to navigate all of these legal and regulatory frameworks, which do not always use the same definitions or thresholds. For example, PADFA applies an ownership threshold for foreign control of 20%, which is different than a similar ownership threshold being proposed by the U.S. Department of Justice (DOJ) under the Executive

Authors

Duane C. Pozza
Partner
202.719.4533
dpozza@wiley.law

Hon. Nazak Nikakhtar
Partner
202.719.3380
nnikakhtar@wiley.law

Kathleen E. Scott
Partner
202.719.7577
kscott@wiley.law

Stephanie Rigizadeh
Associate
202.719.4736
srigizadeh@wiley.law

Practice Areas

FTC Regulation
National Security
Privacy, Cyber & Data Governance

Order.

Companies engaged in personal data sales or other personal data transfers should pay close attention to PADFA. In particular, if companies are engaged in personal data sales or transfers that might involve foreign entities, they should closely review PADFA to determine if their activities are covered and what steps may be necessary to comply, and they should do so quickly, as the law becomes effective in less than two months.

The Protecting Americans' Data from Foreign Adversaries Act of 2024

Under the Act, "data brokers" cannot "sell, license, rent, trade, transfer, release, disclose, provide access to, or otherwise make available the personally identifiable sensitive data of any United States individual to any foreign adversary country or entity controlled by a foreign adversary."

Companies should look closely at the following definitions to see whether any of their activities are covered:

- **Data Broker:** The Act defines "data broker" as "an entity that, for valuable consideration, sells, licenses, rents, trades, transfers, releases, discloses, provides access to, or otherwise makes available" an American's data – if the entity did not collect the information directly from the consumer – to another entity that is not acting as a service provider.
    - PADFA includes several exemptions to this definition, including to the extent that entities transmit data at the direction of an individual, as part of a news report, or incidental to a product or service that is not the data itself.
- **Sensitive Data:** The Act provides a detailed definition of "sensitive data" that covers a wide range of information, including "information identifying an individual's online activities over time and across websites or online services." The definition also includes government-issued identifiers, information indicative of an individual's health conditions or treatment, financial information, biometric and genetic information, private communications, account or device log-in credentials, calendar information, photos, and videos.
    - In particular, "sensitive data" includes "precise geolocation data," defined as geolocation data linkable to a device and reveals an individual's past or present physical location.
- **Foreign Adversary Country:** PADFA aligns "foreign adversary country" with 10 U.S.C. Section 4872(d)(2), which includes North Korea, China, Russia, and Iran.
- **Controlled by a Foreign Adversary:** The Act considers an entity "controlled by a foreign adversary" as one that is "domiciled in, is headquartered in, has its principal place of business in, or is organized under the laws of a foreign adversary country" – and includes businesses that are at least 20% owned by such entities. The definition also includes businesses "subject to the direction or control of" such entities.
- **Service Provider:** The Act defines "service provider" as an entity that "collects, processes, or transfers data on behalf of, and at the direction of" government entities or individuals or entities that are not foreign adversary countries or controlled by such countries.

What the Act Could Mean for Businesses Across All Sectors

PADFA is not sector-specific, so it could apply to any company that meets its thresholds, as detailed above. Even companies not currently registered as data brokers, but who are engaged in consumer data sales, including for advertising-related purposes, should review current policies and procedures around customer diligence.

As noted above, there is already a complex legal and regulatory framework for data brokers and cross-border data transfers that companies subject to PADFA will need to navigate. For example:

- PADFA follows a recent Executive Order directing restrictions on certain personal data transfers to "countries of concern," which will be implemented following the conclusion of the ongoing DOJ rulemaking. While PADFA is narrower than the Executive Order in some ways – including by focusing on data sales – it also applies to a potentially broader set of data and has a different threshold requirement for foreign ownership than has been proposed by the DOJ. For companies subject to these frameworks, it will be important to understand the requirements and restrictions that are common between the two frameworks, as well as the requirements and restrictions that are unique.
- The Act may also add new compliance obligations for businesses currently subject to state data broker laws, which have been enacted in Vermont, California, Oregon, and Texas. The state laws have their own definitions, which vary from PADFA's definitions, and establish different restrictions and requirements from those established in PADFA. As such, companies subject to these state laws should pay close attention to the new federal law and update their compliance programs as needed.

***

Wiley's Privacy, Cyber & Data Governance and FTC Regulation practice groups assist companies in navigating complex data regulations and FTC enforcement. Along with our International Trade and National Security practices, we advise companies on privacy, security, digital trade, data localization, trade controls, and related issues. If you have any questions, please contact one of the attorneys listed on this alert.