Simpson Thacher

Report from Washington

U.S. Expanding Prohibitions on Transfer of Sensitive Data to China and Other Countries of Concern

June 12, 2024

On April 24, 2024, President Biden signed into law the *Protecting Americans' Data from Foreign Adversaries Act* ("PADFA"). Effective June 23, 2024, the PADFA prohibits any "data broker" from transferring "personally identifiable sensitive data"—including both traditional categories of personally identifiable information and also emails, texts and photos kept for personal use—of United States individuals (defined as a natural person residing in the United States) to any "foreign adversary" (China, Iran, Russia or North Korea) or entity "controlled by a foreign adversary."

PADFA is just the latest instance of the U.S. government's continuing and increasing focus on protecting U.S. data from transfer to or access by perceived foreign adversaries due to national security concerns. PADFA follows on President Biden's February 2024 Executive Order on *Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern* (the "Executive Order") and the U.S. Department of Justice ("DOJ") on February 28, 2024 in Advance Notice of Proposed Rulemaking ("ANPRM") implementing that Executive Order. There additionally is an ANPRM issued by the Bureau of Industry and Security of the Department of Commerce ("BIS") on March 1, 2024 that seeks public comment on potential restrictions relating to data gathered from vehicles (the "CV ANPRM").

Collectively, PADFA, the Executive Order, the ANPRM, and the CV ANPRM signal the U.S. government's clear intent to restrict and regulate sensitive individual data out of national security concerns. If and when fully enacted, these new regulations will impose significant restrictions and compliance obligations on any companies in the possession of U.S. personal data. PADFA and the ANPRM propose strict rules to prevent transfer to or even access by defined "countries of concern" (specifically defined to include China and Russia, among other countries) to U.S. sensitive personal data. Any company engaged in trade with relevant countries or in business dealings with counterparties, investors, vendors, consultants or employees in or associated with targeted countries, including China, should carefully evaluate whether they fall within the ambits of the PADFA and closely monitor the regulations issued pursuant to the Executive Order and ANPRM to ensure compliance with all applicable laws.

Protecting Americans' Data From Foreign Adversaries Act

WHO ARE DATA BROKERS UNDER THE PADFA?

Prohibitions of data transfers under the PADFA apply only to "data brokers"—the term is defined to include any entity that "for valuable considerations, sells, licenses, rents, trades, transfers, releases, discloses, provides access to, or otherwise makes available data of United States individuals that the entity did not directly collect from those individuals to another entity." In other words, PADFA targets only companies that sell or otherwise provide access to U.S. individual data for profit. The definition of "data broker" specifically *excludes* entities that are "providing, maintaining, or offering a product or service where personally identifiable sensitive data or access to that data is not itself the product or service." Other enumerated exceptions to this definition under PADFA include entities that transmit individual data at the request or direction of that individual, news reporters that publish information available to the general public, and "service providers" that collect, process or transfer data for, and receives data from, an entity not controlled by a foreign adversary or a federal, state or local governmental entity.

WHO ARE FOREIGN ADVERSARY COUNTRIES AND ENTITIES COVERED UNDER THE PADFA?

China, Russia, Iran and North Korea are named as foreign adversary countries under the PADFA. PADFA prohibits transfer of the protected data by data brokers to entities "controlled by a foreign adversary." That phrase is defined to include (A) a foreign entity domiciled, headquartered, with its principal place of business in, or organized under the laws of a foreign adversary country, (B) any entity with respect to which a foreign person described in (A) has a 20% or greater stake, or (C) a person subject to the direction or control of a foreign person or entity described in (A) or (B). Data brokers may encounter practical difficulties in evaluating whether a particular entity is "controlled by a foreign adversary" and will need to enhance due diligence processes to ensure compliance.

WHAT SENSITIVE DATA ARE COVERED UNDER THE PADFA?

PADFA covers 16 categories of protected personally identifiable sensitive data. These include government issued-identifiers, health, financial, biometric, genetic, racial, ethnicity, religious military status and precise geolocation information, login credentials and certain other personal information. PADFA is also unique in covering broad categories of data not previously addressed by similar regulations or bills. This includes private communications—emails, texts, direct messages, voicemails, phone and text logs—and also photos, videos, audio recordings, calendar information and address book information, where maintained by private use by an individual.

IS THE NEW LAW LIMITED TO BULK TRANSFERS?

No. PADFA applies to the transfer of data by data brokers about any U.S. individual without any bulk data or numerical threshold. Nor is there any minimum threshold for the size of the transaction.

HOW WILL THIS NEW LAW BE ENFORCED?

The Federal Trade Commission ("FTC") will enforce PADFA, with penalties up to approximately $50,000 per violation, which could potentially be large in number if each piece of personal data transferred is considered a separate violation. Violations will be treated as unfair or deceptive act or practice under the FTC Act.

The Executive Order and ANPRM

In addition to PADFA, the Executive Order and the ANPRM also propose significant data transfer restrictions that extend far beyond data brokers. While these proposed regulations are *not* yet effective and may be subject to change, the proposed regulations identify several categories of transactions that would be prohibited and additional categories that would be prohibited if companies fail to meet specified security requirements. While PADFA and the Executive Order/ANPRM share some overall objectives, there are significant differences between the two, as we discuss below.

1. **ANPRM regulates broader categories of companies.** The ANPRM not only prohibits protected sensitive data transactions that involve data brokerage but it also restricts non-data brokerage transactions that implicate vendor agreements, employment agreements, and investment agreements. For instance, the ANPRM would cover a U.S. company that collects bulk sensitive data from U.S. users through an app and enters into a vendor agreement with a Chinese company to process and store this data. Under such circumstance, the U.S. company may not be considered a data broker, but it must comply with the security requirements to be established by the Cybersecurity and Infrastructure Security Agency under the ANPRM. Similarly, the ANPRM also restricts data transfers in employment and investment contexts, such as when employing individuals that are citizens of and primarily reside in a country of concern to provide back-end services in connection with protected data, or when accepting capital from a foreign private-equity fund located in a country of concern for a majority ownership stake in data center storing protected data.

2. **Differing definitions of individual sensitive information**. As noted, PADFA applies to the transfer of the personally identifiable sensitive data of ***any*** U.S. individual, without any bulk or quantity threshold as under the ANPRM. Generally speaking, PADFA defines a greater number of and broader categories of protected sensitive information. For example, PADFA's definition of sensitive data even includes emails, text messages and other personal communications maintained for private used by an U.S. individual. On the flip side, however, PADFA does not contemplate the inclusion of the more expansive definition of "human'omic data," which is included in the EO and corresponding ANPRM.

   In addition, the ANPRM captures sensitive personal data only above defined bulk-volume thresholds, with exceptions for government-related data regardless of volume. The exceptions are for geolocation data in listed geofenced areas associated with military and other sensitive facilities, and sensitive

personal data linked to current or recent former employees or contractors, or former senior officials, of the U.S. government, including the military and intelligence community.

3. **Differing definitions of controlled entities.** PADFA implements a broader scope of "controlled by a foreign adversary" by reducing the ownership threshold in its definition. Under ANPRM, "controlled by a foreign adversary" entities included entities 50% or greater owned by foreign adversary entities while PADFA reduces the threshold to entities owned 20% or greater.

4. **Slightly different countries of concern.** The countries of concerned identified in the ANPRM largely mirror PADFA, but the ANPRM expressly includes Hong Kong and Macau and also Venezuela.

5. **The ANPRM sets forth prohibited transactions and also restricted transactions.** The ANPRM proposed that some categories of transactions will be absolutely prohibited, including all data-brokerage transactions involving protected data and any transaction that provides access to bulk human genomic data. It proposes that other categories of transactions, including vendor agreements, employment agreements and investment agreements, will be allowed if and only if they meet defined security measures (to be defined and announced by the U.S. government); such restricted transactions will be prohibited absent compliance with the requisite security measures.

6. **PADFA is enforced by FTC while the DOJ would be enforcing the ANPRM.** The DOJ indicated in the ANPRM that it is considering establishing a process for imposing civil monetary penalties for violations, and does not explicitly mention potential criminal penalties. However, given the nature of DOJ investigations and that the Executive Order was issued under the International Emergency Economic Powers Act, violations of rules contemplated under the ANPRM could carry criminal liability. We expect the DOJ to amend the proposed regulations in light of the PADFA and set forth further guidance that implicates companies beyond data brokers. The DOJ implementation of the ANPRM may include general licenses and specific licenses in a framework similar to that has long been employed by the U.S. Department of Treasury's Office of Foreign Asset Control ("OFAC").

Implications Going Forward

While there remains uncertainty about what will be contained in the final regulations issued in accordance with the ANPRM and CV ANPRM, and it also remains to be seen how the statutory scope of the PADFA on protected data will inform any changes to the definition of "sensitive personal data" in the context of reviews by the Committee on Foreign Investment in the United States ("CFIUS"), we expect that the final regulations will impose significant restrictions on companies in possession of or with access to U.S. sensitive personal data. Any company engaged in cross-border trade with (or who have other connections to) countries of concern should review the potential applicability of the PADFA and proposed regulations, and begin to consider the design and implementation of appropriate measures to ensure compliance going forward with evolving and tightening U.S. national security regulations aimed at protecting the personal data of U.S. individuals that is considered sensitive.

For further information regarding this Report, please contact one of the following authors:

WASHINGTON, D.C.

Abram J. Ellis
+1-202-636-5579
aellis@stblaw.com

Malcolm J. (Mick) Tuesley
+1-202-636-5561
mick.tuesley@stblaw.com

Mark B. Skerry
+1-202-636-5523
mark.skerry@stblaw.com

NEW YORK CITY

George S. Wang
+1-212-455-2228
gwang@stblaw.com

David H. Caldwell
+212-455-2612
dcaldwell@stblaw.com

Daniel S. Levien
+1-212-455-7092
daniel.levien@stblaw.com

Anais Bourbon
+1-212-455-3427
anais.bourbon@stblaw.com

BEIJING

Shuhao Fan
+86-10-5965-2987
shuhao.fan@stblaw.com

The contents of this publication are for informational purposes only. Neither this publication nor the lawyers who authored it are rendering legal or other professional advice or opinions on specific facts or matters, nor does the distribution of this publication to any person constitute the establishment of an attorney-client relationship. Simpson Thacher & Bartlett LLP assumes no liability in connection with the use of this publication. Please contact your relationship partner if we can be of assistance regarding these important developments. The names and office locations of all of our partners, as well as our recent memoranda, can be obtained from our website, www.simpsonthacher.com.