wiley

ALERT

# Executive Order on Foreign Access to Sensitive Personal Data Will Increase U.S. Regulation of Cross-Border Data Transfers

March 4, 2024

On February 28, 2024, the White House released a highly anticipated and far-reaching Executive Order (EO) that directs several new regulatory steps to limit the transfer of sensitive personal data outside of the United States to "countries of concern." Impacted industries include, among others, those that generate and sell data gained from mobile apps, smartwatches, car sensors, and other digital devices.

The White House contends this is "the most significant executive action any President has ever taken to protect Americans' data security..." The EO announces that it is the policy of the United States to prohibit or restrict access by "countries of concern" to Americans' bulk sensitive personal data and U.S. Government-related data when such access would pose an unacceptable risk to the national security of the United States. The EO also reaffirms the United States' continued support for open, global, interoperable, reliable, and secure flows of data across borders to maintain the consumer, economic, scientific, and trade relationships the United States has with other countries.

The U.S. Department of Justice (DOJ) has already announced an Advance Notice of Proposed Rulemaking (ANPRM) to implement the EO and place limits on certain foreign transactions involving bulk sensitive personal data and U.S. Government-related data, with proposed regulations to follow in the coming months. Stakeholders will have the opportunity to weigh in as the government considers new restrictions on foreign transfers on sensitive data. Comments must be received within 45 days of the publication of the ANPRM in

## Authors


Megan L. Brown
Partner
202.719.7579
mbrown@wiley.law

Duane C. Pozza
Partner
202.719.4533
dpozza@wiley.law

Hon. Nazak Nikakhtar
Partner
202.719.3380
nnikakhtar@wiley.law

Jacqueline F. "Lyn" Brown
Partner
202.719.4114
jfbrown@wiley.law

Nova J. Daly
Senior Public Policy Advisor
202.719.3282
ndaly@wiley.law


## Practice Areas

Committee on Foreign Investment in the United States (CFIUS)
Cyber and Privacy Investigations, Incidents & Enforcement
Cybersecurity
Digital Trade
Government Contracts
International Trade
National Security
Privacy, Cyber & Data Governance
Team Telecom

the Federal Register.

**White House restricts transactions to covered countries due to national security concerns.**

The White House's move to prohibit or restrict certain transactions was triggered by the continuing efforts by countries of concern (identified in the ANPRM as contemplating China, Russia, North Korea, Iran, Cuba, and Venezuela) to access Americans' bulk sensitive personal data and U.S. Government-related data, because unrestricted transfers of this data may enable countries of concern to exploit such data for nefarious purposes, including engaging in malicious cyber-enabled activities. This sensitive data includes geolocation data, biometric data, personal health data, genomic data, financial data, and certain kinds of additional personal identifiers that will be defined in DOJ rulemaking.

The EO notes that the risk of access to Americans' bulk sensitive personal data and U.S. Government-related data is not limited to direct access by countries of concern. Instead, entities owned or controlled by a country of concern or subject to the jurisdiction or direction of a country of concern may enable the government of a country of concern to indirectly access the data. For example, a country of concern may have cyber, national security, or intelligence laws that obligate such entities or individuals to provide that country's intelligence services with access to Americans' bulk sensitive personal data and U.S. Government-related data. The EO finds that these risks may be exacerbated by developing artificial intelligence (AI) capabilities and algorithms that enable large datasets to be used or exploited to the detriment of U.S. national security.

**While the U.S. remains committed to promoting cross-border data flows, the EO restricts certain transactions where sensitive data could be accessed by a covered country's intelligence service.**

The new EO marks a shift in how the United States approaches the global movement of data, having long opposed data localization and transfer limits imposed by other countries. Nevertheless, the EO maintains that the United States remains committed to promoting cross-border data flows to enable international commerce, trade, and open investment. The EO emphasizes that it does not authorize the

imposition of generalized data localization requirements to store Americans' bulk sensitive personal data or U.S. Government-related data within the United States or to locate computing facilities used to process that data within the United States. The EO also does not broadly prohibit United States persons from conducting commercial transactions with countries of concern. Instead, the restrictions enabled by the EO are supposed to be tailored to address the national security threat to sensitive data.

**The Attorney General will issue regulations restricting sensitive data transactions with covered countries.**

The EO will launch a rulemaking process led by the U.S. Attorney General, in coordination with the Secretary of Homeland Security, to promulgate regulations that prohibit or restrict United States persons from engaging in transactions involving bulk sensitive personal data or U.S. Government-related data that poses an unacceptable risk to national security. The Attorney General is directed to issue these proposed rules within 180 days of the EO being issued, or by August 26, 2024, and to identify the classes of transactions that would be covered. Indeed, the Department of Justice has already released an extensive draft Advance Notice of Proposed Rulemaking, which has not yet been published in the Federal Register.

The Director of the Cybersecurity and Infrastructure Security Agency (CISA) is directed to enact the security requirements that might mitigate the risk of access by countries of concern to data from restricted transactions that will be available for public comment. CISA's security requirements to address the unacceptable risk posed by restricted transactions will be based on the Cybersecurity and Privacy Frameworks developed by the National Institute of Standards and Technology (NIST).

In particular, the Attorney General is directed to issue regulations by August 26, 2024, that prohibit or otherwise restrict United States persons from engaging in "any acquisition, holding, use, transfer, transportation, or exportation of, or dealing in, any property in which a foreign country or national thereof has any interest (transaction)" where the transaction falls into one of the following enumerated categories:

- The transaction involves bulk sensitive personal data or U.S. Government-related data (as further defined by regulations that the Attorney General will issue);
- The transaction is part of a class of transactions that the Attorney General has determined pose an unacceptable risk to the national security of the United States because the transaction may enable countries of concern or covered persons to access bulk sensitive data or U.S. Government-related data in a manner that contributes to the national emergency addressed in EO 13873, *Securing the Information and Communications Technology and Services Supply Chain* (May 15, 2019) and EO 14034, *Protecting Americans' Sensitive Data from Foreign Adversaries* (June 9, 2021);
- The transaction was initiated, is pending, or will be completed after the effective date of the regulations to be issued by the Attorney General;
- The transaction does not qualify for an exemption or is not authorized by a license pursuant to the regulations to be issued by the Attorney General; and

- The transaction is not ordinarily incident to and part of the provision of financial services, including banking, capital markets, and financial insurance services, or required for compliance with any federal statutory or regulatory requirements.

In the regulations, the Attorney General will also need to identify the countries of concern, with the concurrence of the Secretary of State, and the classes of covered persons covered by the EO. The proposed regulations will have to establish a process to issue licenses authorizing transactions that would otherwise be prohibited or restricted. The regulations will also address appropriate coordination with other U.S. Governmental entities such as the Committee on Foreign Investment in the United States (CFIUS), the Office of Foreign Assets Control (OFAC) within the U.S. Department of the Treasury, the Bureau of Industry and Security (BIS) in the U.S. Department of Commerce, and the Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector (Team Telecom).

The proposed regulations will also establish thresholds and due diligence requirements for entities to use in assessing whether a transaction is a prohibited or restricted transaction. The proposed regulations are not supposed to establish generalized data localization requirements for storing bulk sensitive personal data or U.S. Government-related data within the United States or locating computing facilities used to process that data within the United States.

**Health care data must be protected from access by countries of concern.**

The EO notes that countries of concern with access to large data sets are increasingly able to re-identify or de-anonymize data which can lead to the exploitation of health care information of U.S. persons. To help protect U.S. persons' sensitive personal health data and human genomic data from these threats, the EO directs the Secretary of Defense, the Secretary of Health and Human Services, the Secretary of Veterans Affairs, and the Director of the National Science Foundation to consider taking steps, including issuing regulations or guidance, to prohibit the provision of assistance that enables access by countries of concern or covered persons to U.S. persons' bulk sensitive data, including personal health or genomic data or to impose mitigation measures with respect to such assistance. These officials are mandated to report back within one year on their progress.

**Data broker risks also to be addressed by the Consumer Financial Protection Bureau**.

The EO identifies the data broker industry as enabling access by countries of concern to bulk sensitive personal data and U.S. Government-related data because these entities routinely engage in the collection, assembly, evaluation, and dissemination of this data. The EO encourages the Director of the Consumer Financial Protection Bureau (CFPB) to consider taking steps to address this threat as well as ways to enhance compliance with federal consumer protection law through its rulemaking process.

As referenced in the EO, the CFPB is in the early stages of starting a rulemaking that would address certain data broker practices under the Fair Credit Reporting Act (FCRA). However, as we have explained, because the FCRA applies far beyond third-party data brokers, that rulemaking is likely to have a much broader impact

on consumer data sharing practices.

**Risks associated with human 'omic data will be reviewed.**

By June 27, 2024, the Assistant to the President for National Security Affairs (APNSA) will submit a report to the President assessing the risks and benefits of regulating transactions involving types of human 'omic data other than human genomic data such as human proteomic data, human epigenomic data, and human metabolomic data.

**Team Telecom will review network infrastructure and submarine cables involving countries of concern.**

In trying to protect sensitive data from being accessed by countries of concern, the EO focuses on the transmission of data via network infrastructure that is subject to the jurisdiction or control of countries of concern. The EO finds that the risk of access by countries of concern is exacerbated where the data transits a submarine cable that is owned or operated by persons owned or controlled by, or subject to the jurisdiction of, a country of concern or that connects to the United States and terminates in the jurisdiction of a country of concerns. These same risks also exist when a submarine cable is designed, built, or operated to transfer data to a specific data center located in a foreign jurisdiction.

To address this threat, the EO directs Team Telecom to prioritize reviews of existing licenses for submarine cable systems that are owned or operated by persons owned or controlled by or subject to the jurisdiction or direction of a country of concern or that terminate in the jurisdiction of a country of concern. Team Telecom is also directed to issue policy guidance regarding its reviews of license applications and existing licenses, including the assessment of third-party risks regarding access to data by countries of concern. Finally, Team Telecom will be expected to address the national security and law enforcement risks related to access by countries of concern to the bulk sensitive data covered by the EO that may be presented by any new application or existing license to land or operate a submarine cable system.

**Prior transfers will be reviewed for national security risks.**

By June 27, 2024, the Attorney General, the Secretary of Homeland Security, and the Director of National Intelligence must submit a report to the President recommending appropriate actions to detect, assess, and mitigate the national security risks arising from prior transfers of U.S. persons' bulk sensitive personal data to countries of concern. The White House will review the recommendations and will consult with the Attorney General, the Secretary of Homeland Security, and the heads of relevant agencies on implementing the recommendations within 150 days of the Attorney General issuing the regulations on prohibited or restricted transactions.

**Who will be affected?**

The EO affects a broad range of commercial transactions involving Americans' bulk sensitive personal data or U.S. Government-related data that could be accessed by countries of concern. The EO specifically mentions telecommunications or data transmission via network infrastructure and focuses in particular on the risks of

data transits using a submarine cable that is owned, operated, or controlled by a country of concern.

Health care data will also be subject to the EO due to the concerns that even if it is anonymized, it may still be accessed by countries of concern.

The data broker industry is also highlighted in the EO as posing a particular risk of collecting and disseminating bulk sensitive personal data or U.S. Government-related data to countries of concern.

In addition to strictly commercial businesses, government contractors are affected by this EO because of the sensitive data they routinely encounter as a result of their federal contracts and grants.

**What is the President's claimed authority for doing this?**

The EO indicates that it was issued pursuant to the authority vested in the President by the Constitution and the laws of the United States including the International Emergency Economic Powers Act (IEEPA), 50 U.S.C. § 1701, *et seq.*, the National Emergencies Act (NEA), 50 U.S.C. § 1601, *et seq.*, and Section 301 of Title 3 of the United States Code.

Additionally, the EO seeks to expand the scope of the national emergency declared in EO 13873, *Securing the Information and Communications Technology and Services Supply Chain* (May 15, 2019) and the additional measures addressed in EO 14034, *Protecting Americans' Sensitive Data from Foreign Adversaries*, (June 9, 2021). The President indicates that this EO is needed due to the continuing effort of certain countries of concern to access Americans' sensitive personal data and U.S. Government-related data, which presents an unusual and extraordinary threat to the national security and foreign policy of the United States.

**What comes next?**

- The Attorney General will issue draft regulations subject to public notice and comment on prohibited or restricted transactions.
- The Attorney General will publish a proposed rule for public notice and comment by August 26, 2024, that identifies the class of transactions that meet the criteria for prohibited transactions; identifies classes of transactions that can have the risk of access mitigated pursuant to security requirements established by CISA for restricted transactions; identifies countries of concern; establishes a process to issue licenses authorizing transactions that would otherwise be prohibited or restricted transactions; coordinates with other U.S. Governmental entities like CFIUS, OFAC, BIS, and Team Telecom; and addresses the need for appropriate recordkeeping and reporting of transactions to inform the investigative, enforcement, and regulatory efforts.
- CISA will publish security requirements for public comment that address the unacceptable risk posed by restricted transactions based on the NIST Cybersecurity and Privacy Frameworks.
- CISA will issue interpretive guidance regarding security requirements.

- The Attorney General will issue enforcement guidance regarding CISA's security requirements.
- Team Telecom will address the threat posed by the transmission of sensitive data via network infrastructure and submarine cables in covered countries.
- The Secretary of Defense, the Secretary of Health and Human Services, the Secretary of Veterans Affairs, and the Director of the National Science Foundation will consider taking steps, including issuing regulations or guidance to prohibit assistance that enables countries of concern or covered persons from accessing U.S. persons' bulk sensitive personal data.
- The Secretary of Defense, the Secretary of Health and Human Services, the Secretary of Veterans Affairs, and the Director of the National Science Foundation will submit a report to the President detailing their progress.
- The Director of the Consumer Financial Protection Bureau will consider taking steps to address the threat to consumers and how to enhance compliance with federal consumer protection law.
- Within 120 days of the effective date of the Attorney General's regulations, the Attorney General, the Secretary of Homeland Security, and the Director of National Intelligence will recommend to the White House appropriate actions to detect, assess, and mitigate national security risks arising from prior transfers of U.S. persons' bulk sensitive personal data to countries of concern.
- Within one year of the effective date of the Attorney General's regulations, the Attorney General will submit a report to the President assessing the effectiveness of the measures imposed and the economic impact of the implementation of this EO.
- By June 27, 2024, the APNSA and other executives within the White House will submit a report to the President assessing the risks and benefits of regulating transactions involving types of human 'omic data other than human genomic data.

In the past, agency activity directed by the President under IEEPA or by Congress in the National Defense Authorization Act (NDAA) has sometimes resulted in the release of Interim Final Rules that come before opportunities for public comment or before resolution of the issues raised by comments. Given the numerous agencies being directed to act in the EO, and the planned roles for DOJ, CFIUS, and other activities that are not marked by substantial transparency, we expect several aspects of implementation to occur without substantial public input.

We suggest that clients closely track the issuance of draft rules and regulations and avail themselves of the opportunity to comment either individually or through a trade association. Comments on DOJ's ANPRM will be due in mid-April.

***

Wiley's Telecom, Media & Technology and Privacy, Cyber & Data Governance teams, along with the International Trade and National Security practices, have focused on privacy, security, digital trade, data localization, and related issues for decades. This includes advising companies in CIFUS reviews, negotiating

data transfer agreements, and supporting compliance with various U.S. and international legal obligations related to the movement and use of data. Whether from a compliance or a policy perspective, our team can address any questions about this EO or the work it has directed.