King & Spalding

Client Alert

Special Matters and Government Investigations

MARCH 28, 2024

For more information, contact:

Zachary J. Harmon
+1 202 626 5594
zharmon@kslaw.com

Sumon Dantiki
+1 202 626 5591
sdantiki@kslaw.com

J. Philip Ludvigson
+1 202 626 9267
pludvigson@kslaw.com

Jacqueline Van De Velde
+1 404 572 2450
jvandevelde@kslaw.com

King & Spalding

Washington
1700 Pennsylvania Avenue, NW
Suite 900
Washington, DC 20006
Tel. +1 202 737 0500

Atlanta
1180 Peachtree Street, NE
Suite 1600
Atlanta, Georgia 30309
Tel. +1 404 572 4600

Executive Order Restricts Foreign Access to U.S. Data, Citing National Security Risks

On February 28, 2024, President Biden signed Executive Order (EO) 14117 titled "Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern." On March 5, 2024, the Department of Justice's (DOJ) National Security Division announced an Advanced Notice of Proposed Rulemaking outlining contemplated implementing regulations for the EO.

Together, the EO and proposed rule would either prohibit or restrict certain transactions involving bulk sensitive personal data or U.S. government-related data to countries of concern (including China and Russia) or covered persons who might be owned, controlled, or subject to the jurisdiction of countries of concern. This client alert summarizes the EO and the proposed requirements that would govern companies engaged in cross-border data transfers.

THE EXECUTIVE ORDER

The EO states continued efforts by countries of concern to access Americans' bulk sensitive data and U.S. government data poses an unusual and extraordinary threat to U.S. national security and foreign policy. The EO and Proposed Rule warn that countries of concern are accessing sensitive data through data brokerages, third-party vendors, employees and investments agreements, and that data can be used for malicious activities, including:

- Artificial Intelligence (AI): Bulk data could be used to train AI and advanced technologies.
- Personal Health Data: In large data sets, countries of concern may be able to re-identify or de-anonymize health data that reveals exploitable private health information and human genomic data of U.S. persons.

- Cybersecurity & Espionage: Countries of concern could exploit Americans' bulk sensitive personal data and government-related data to track and build profiles on U.S. persons, including those in national security roles, to support espionage operations and to identify and exploit vulnerabilities for malicious cyber activities.
- Consumer Protection: The data brokerage industry risks contributing to national emergencies by routinely collecting, assembling, evaluating, and disseminating bulk sensitive personal data and U.S. government-related data relating to U.S. consumers.
- Submarine Cables: Bulk sensitive personal data and U.S. government-related data is at risk of access when it passes through network infrastructure in countries of concern, particularly when it transits a submarine cable owned or controlled by, or subject to the jurisdiction of, a country of concern.

To address these national security threats, the EO directs DOJ to issue regulations to prohibit or restrict certain transactions involving “bulk sensitive personal data” or “U.S. government-related data” and “countries of concern” or “covered persons.”

The EO also directs the Departments of Defense, Health and Human Services, Veterans Affairs, and the National Science Foundation to consider prohibiting or restricting assistance that might enable access to bulk sensitive personal data, including personal health and genomic data, by countries of concern.

THE PROPOSED RULE

On March 5, 2024, DOJ issued an Advanced Notice of Public Rulemaking (the “Proposed Rule”) proposing regulations to implement the EO and requested public comments on the Proposed Rule. As outlined below, DOJ’S Proposed Rule contemplates prohibiting certain highly sensitive transactions while allowing other transactions, pursuant to compliance with predefined security requirements. Comments on the Proposed Rule are due by April 19, 2024.

COUNTRIES OF CONCERN AND COVERED PERSONS

The EO restricts data transfer to “countries of concern.” It defines a “country of concern” as any foreign government that has engaged in a long-term pattern or serious instances of conduct significantly adverse to U.S. national security or security and safety of U.S. persons, and that poses a significant risk of exploiting bulk sensitive personal data or United States government-related data to the detriment of national security or the security and safety of U.S. persons.

DOJ’s Proposed Rule suggests that it will identify six countries of concern in its final rule. Those are: China (including Hong Kong and Macau), Russia, Iran, North Korea, Cuba, and Venezuela.

Meanwhile, the proposed definition of “covered persons” would include countries of concern or entities and individuals who are owned by, controlled by, or subject to the jurisdiction of such countries. It would also extend to persons designated by the Attorney General as being owned or controlled by or subject to the jurisdiction or direction of a country of concern, or as acting (or purporting to act) on behalf of a country of concern or covered person, or knowingly causing or directing a violation of DOJ’s regulations.

DATA SUBJECT TO THE PROPOSED RULE

Bulk Sensitive Personal Data. The EO defines covered data, but DOJ is expected to elaborate on the definitions in final rule. The EO defines “sensitive personal data” as including six categories:

- Covered personal identifiers, meaning personally identifiable data reasonably linked to an individual, or that could be used with other data to identify an individual from a data set or link data across multiple data sets to an individual;
- Geolocation and sensor data that identifies individual locations with a certain amount of precision;
- Biometric identifiers, including facial images, fingerprints, and voice patterns;
- Human 'omic data, dealing with human genetic information;
- Personal health data, as defined by relevant portions of the Health Insurance Portability and Accountability Act (HIPAA) and Social Security Act; and
- Personal financial data, to include purchase and payment history.

The EO also notes that sensitive personal data does not include data that is a matter of public record, trade secrets, personal communications that do not transfer anything of value, and information and informational materials.

DOJ's Proposed Rule elaborates on what it proposes to include as "covered personal identifiers." These include government identification numbers, financial account numbers, demographic or contact data, and could include device identifiers such as IMEI, MAC addresses, Advertising IDs, Mobile Advertising IDs, and IP addresses.

DOJ proposes establishing establish volume-based thresholds for each category of sensitive personal data based on a risk assessment examining threat, vulnerabilities, and consequences as components of risk. For the six defined categories of sensitive data, DOJ proposes the following thresholds:

	Human Genomic Data	**Biometrics Identifiers**	**Precise Geolocation Data**	**Personal Health Data**	**Personal Financial Data**	**Covered Personal Identifiers**
Low	More than 100 U.S. persons	More than 100 U.S. persons (for biometric identifiers) or U.S. devices (for precise geolocation data)		More than 1,000 U.S. persons		More than 10,000 U.S. persons
High	More than 1,000 U.S. persons	More than 10,000 U.S. persons (for biometric identifiers) or U.S. devices (for precise geolocation data)		More than 1,000,000 U.S. persons		More than 1,000,000 U.S. persons

U.S. Government-Related Data. The EO also notes that U.S. government-related data is subject to data transfer restrictions. The Proposed Rule further clarifies that U.S. government-related data includes, without respect to volume, (1) geolocation data for any location from listed geofenced areas associated with military, government, or other sensitive facilities or locations, or (2) sensitive personal data marketed as linked or linkable to current or recent former employees, contractors, or former senior officials of the U.S. government, including those from the military or Intelligence Community.

COVERED DATA TRANSACTIONS

The EO directs DOJ to define the types of transactions involving bulk sensitive personal data or U.S. government-related data in which U.S. persons are either (a) prohibited or (b) restricted from engaging. Under the Proposed Rule, DOJ proposes defining prohibited or restricted transactions as "covered data transactions." The Proposed Rule defines a

"covered data transaction" as any "transaction" that involves any bulk U.S. sensitive personal data or government-related data and involves: (1) data brokerage; (2) human genomic data or human biospecimens from which human genomic data can be derived; (3) a vendor agreement; (4) an employment agreement; or (5) an investment agreement. Under the Proposed Rule, a "transaction" is defined as "any acquisition, holding, use, transfer, transportation, exportation of, or dealing in any property in which a foreign country or national thereof has an interest." Other proposed definitions for key terms, including "access," "U.S. devices," and "foreign person" are broad and require significant evaluation on the part of companies to determine whether their activities are considered covered data transactions under the Proposed Rule.

Prohibited Transactions. Prohibited covered data transactions are covered data transactions categorically determined to pose an unacceptable risk to national security because they may enable countries of concern or covered persons to access bulk U.S. sensitive personal data or government-related data. Given the risk to U.S. national security, DOJ proposes barring U.S. persons from knowingly engaging in the following two categories of prohibited covered data transactions: (1) data-brokerage transactions between U.S. persons and countries of concern or covered persons; and (2) any transaction that provides a country of concern or covered person with access to bulk human genomic data (a subcategory of human 'omic data) or human biospecimens from which that human genomic data can be derived.

Restricted Transactions. Restricted covered data transactions are data transactions categorically determined to pose an unacceptable risk to national security—unless certain security requirements are implemented—because they may enable countries of concern or covered persons to access bulk U.S. sensitive personal data or government-related data. DOJ is continuing to develop the security requirements that would govern restricted transactions. The U.S. Department of Homeland Security (DHS), in coordination with DOJ, will issue and solicit public comments on the proposed security requirements as part of a separate process.

DOJ's current approach would permit covered data transactions only if the U.S. person:

1. implements Basic Organizational Cybersecurity Posture requirements;
2. conducts the covered data transaction in compliance with: (a) data minimization and masking; (b) use of privacy-preserving technologies; (c) development of information-technology systems to prevent unauthorized disclosure; and (d) implementation of logical and physical access controls; and
3. satisfies certain compliance-related conditions, such as retaining an independent auditor to perform annual testing and auditing of the requirements in (1) and (2) above, as the U.S. person relies on compliance with those conditions to conduct the restricted covered data transaction.

EXEMPT TRANSACTIONS AND LICENSING

The Proposed Rule contemplates exempting certain types of data transactions from security requirements. Exempt data transactions may include transactions involving personal communications and information and information materials; transactions for conducting official U.S. government business; transactions ordinarily incident to and part of the provision of certain financial services, payment-processing, and regulatory-compliance; intra-entity transactions incident to business operations; and transactions required or authorized by Federal law or international agreements.

In addition to these exemptions, DOJ is contemplating a licensing regime that would authorize covered data transactions that would otherwise be either prohibited or restricted. The regime would include both general and specific licenses. Although the obligations for each classification of licenses are yet to be resolved, general licenses will include requirements to file reports or statements as instructed, while specific licenses may require ongoing reports regarding authorized transactions and assurances to the U.S. government that transferred data may be recovered or permanently

deleted. Failure to comply with obligations may nullify authorization of the license and could result in a violation subject to an enforcement action.

COMPLIANCE AND ENFORCEMENT

With these new requirements comes new risk to companies with respect to potential non-compliance and resulting enforcement actions. The Proposed Rule suggests that companies should adopt risk-based and reasonable compliance programs to ensure compliance with the new regulations. DOJ notes that in the event of a violation, it will consider the adequacy of a company's compliance program in any resulting enforcement action.

Similarly, although DOJ does not contemplate imposing general due diligence, reporting, and recordkeeping requirements, specific requirements may apply as a condition of engaging in restricted covered data transactions or in order to receive a license for restricted or prohibited transactions alike. DOJ also suggests in that "certain narrow circumstances" it may impose additional reporting requirements so as to identify attempts to engage in prohibited covered data transactions. Those circumstances may include:

- U.S. persons that are (a) engaged in restricted transactions involving cloud computing services or licensed transactions involving data brokerage or cloud-computing services and (b) are 25 percent or more owned by a country of concern or a covered person through any contract, arrangement, understanding, or relationship; or
- U.S. persons who have received and affirmatively rejected an offer to engage in a prohibited transaction involving a data brokerage.

The Proposed Rule also contemplates auditing requirements for U.S. persons engaging in any restricted transaction or in prohibited transactions subject to a license. Requirements may include annual audits of applicable security requirements or license conditions, and audit results would be shared with DOJ. The Proposed Rule also discusses recordkeeping requirements, noting that U.S. persons that engage in any covered data transaction subject to prohibition or restriction will be required to maintain complete records related to that transaction.

DOJ is considering establishing a process for imposing civil monetary penalties similar to those imposed by the Office of Foreign Assets Control (OFAC) and the Committee on Foreign Investment in the United States (CFIUS). The contemplated penalty mechanisms would include a pre-penalty notice, opportunity to respond, and a final decision. Such penalties may be imposed based upon noncompliance with the rule, material misstatements or omissions, or false certifications or submissions. The amount of the penalty would hinge upon the facts surrounding the violation, including the company's effort to comply with the regulations.

KEY TAKEAWAYS AND WHAT'S NEXT

Given the expectation of a strong DOJ enforcement mechanism, it is imperative that companies prepare now for the coming rules that will define the details of prohibited and restricted covered data transactions. This key takeaway was further reinforced in a speech given shortly after the Proposed Rule was released, in which the head of DOJ's National Security Division (NSD) predicted that enforcement of the EO would have "real teeth" and would be "backed by the full suite of civil and criminal authorities under the International Emergency Economic Powers Act." To prepare for the requirements to be imposed by the EO and Proposed Rule, the NSD head suggested that companies:

- *Know your data*, including understanding fully what categories of data you transact in and what safeguards are in place for that data;

- *Know where* that data is going, including whether agreements with third parties provide all relevant parties confidence in where the data is going;
- *Know who has access to the data,* including parties like non-U.S. consultants and investors based in countries of concern; and
- *Know your data sales,* including direct and indirect transactions that involve data.

Additionally, the EO and the Proposed Rule reflects continued focus by the Biden Administration on disrupting evolving cyber threats posed by state actors. Thus, companies must recognize that strong data privacy protocols, a strong cybersecurity posture, and a secure technology supply chain are all critical to protecting the underlying data that is collected, stored, and transferred using digital means.

Special Matters & Government Investigations Partners

Gary Adamson
New York
+1 212 556 2113
gadamson@kslaw.com

Adam Baker
New York
+1 212 556 2376
abaker@kslaw.com

Matthew H. Baughman
Atlanta
+1 404 572 4751
mbaughman@kslaw.com

J.C. Boggs
Washington, DC
+1 202 626 2383
jboggs@kslaw.com

Amy B. Boring
Atlanta
+1 404 572 2829
aboring@kslaw.com

Christopher C. Burris
Atlanta
+1 404 572 4708
cburris@kslaw.com

Craig Carpenito
New York
+1 212 556 2142
ccarpenito@kslaw.com

Steve Cave
Northern Virginia
+1 703 245 1017
scave@kslaw.com

Michael J. Ciatti
Washington, DC
+1 202 661 7828
mciatti@kslaw.com

Daniel R. Coats
Washington, DC
+1 202 626 2642
dcoats@kslaw.com

Patrick M. Collins
Chicago
+1 312 764 6901
pcollins@kslaw.com

Alexander M. Crenshaw
Washington, DC
+1 202 626 8996
acrenshaw@kslaw.com

Sumon Dantiki
Washington, DC
+1 202 626 5591
sdantiki@kslaw.com

Ethan P. Davis
San Francisco
+1 415 318 1228
edavis@kslaw.com

Alan R. Dial
Washington, DC
+1 202 661 7977
adial@kslaw.com

Dan Donovan
Washington, DC
+1 202 626 7815
ddonovan@kslaw.com

Robert L. Ehrlich, Jr.
Washington, DC
+1 202 626 9710
rehrlich@kslaw.com

David Farber
Washington, DC
+1 202 626 2941
dfarber@kslaw.com

Zachary Fardon
Chicago
+1 312 764 6960
zfardon@kslaw.com

Ehren Halse
San Francisco
+1 415 318 1216
ehalse@kslaw.com

Zachary J. Harmon
Washington, DC
+1 202 626 5594
zharmon@kslaw.com

Ted Hester
Washington, DC
+1 202 626 2901
thester@kslaw.com

Max Hill, K.C.
London
+44 20 7551 2130
mhill@kslaw.com

Amy Schuller Hitchcock
Sacramento/San Francisco
+1 916 321 4819

ahitchcock@kslaw.com

John A. Horn
Atlanta
+1 404 572 2816
jhorn@kslaw.com

Andrew C. Hruska
New York
+1 212 556 2278
ahruska@kslaw.com

Mark A. Jensen
Washington, DC
+1 202 626 5526
mjensen@kslaw.com

Dixie L. Johnson
Washington, DC
+1 202 626 8984
djohnson@kslaw.com

William Johnson
New York
+1 212 556 2125
wjohnson@kslaw.com

Allison F. Kassir
Washington, DC
+1 202 626 5600
akassir@kslaw.com

M. Alexander (Alec) Koch
Washington, DC
+1 202 626 8982
akoch@kslaw.com

Yelena Kotlarsky
New York
+1 212 556 2207
ykotlarsky@kslaw.com

Steve Kupka
Washington, DC
+1 202 626 5518
skupka@kslaw.com

Jade R. Lambert
Chicago
+1 312 764 6902
jlambert@kslaw.com

Jamie Allyson Lang
Los Angeles
+1 213 443 4325
jlang@kslaw.com

Raphael Larson
Washington, DC
+1 202 626 5440
rlarson@kslaw.com

Carmen Lawrence
New York
+1 212 556 2193
clawrence@kslaw.com

Brandt Leibe
Houston
+1 713 751 3235
bleibe@kslaw.com

Aaron W. Lipson
Atlanta
+1 404 572 2447
alipson@kslaw.com

Daniel E. Lungren
Washington, DC
+1 202 626 9120
dlungren@kslaw.com

William S. McClintock
Washington, DC
+1 202 626 2922
wmcclintock@kslaw.com

Amelia Medina
Washington, DC
+1 202 626 5587
amedina@kslaw.com

Kendrick B. Meek
Washington, DC
+212 626 5613
kmeek@kslaw.com

Andrew Michaelson
New York
+212 790 5358
amichaelson@kslaw.com

Jim C. Miller III
Washington, DC
+1 202 626 5580
jmiller@kslaw.com

Patrick Montgomery
Washington, DC
+1 202 626 5444
pmontgomery@kslaw.com

Paul B. Murphy
Atlanta/Washington, DC
+1 404 572 4730
pbmurphy@kslaw.com

Grant W. Nichols
Austin/Washington, DC
+1 512 457 2006
gnichols@kslaw.com

Alicia O'Brien
Washington, DC
+1 202 626 5548
aobrien@kslaw.com

Patrick Otlewski
Chicago
+1 312 764 6908
potlewski@kslaw.com

Michael R. Pauzé
Washington, DC
+1 202 626 3732
mpauze@kslaw.com

Michael A. Plotnick
Washington, DC
+1 202 626 3736
mplotnick@kslaw.com

Olivia Radin
New York
+1 212 556 2138
oradin@kslaw.com

John C. Richter
Washington, DC
+1 202 626 5617
jrichter@kslaw.com

Rod J. Rosenstein
Washington, DC
+1 202 626 9220
rrosenstein@kslaw.com

Daniel C. Sale
Washington, DC
+1 202 626 2900
dsale@kslaw.com

Greg Scott
Sacramento/San Francisco
+1 916 321 4818
mscott@kslaw.com

Richard Sharpe
Singapore
+65 6303 6079
rsharpe@kslaw.com

Kyle Sheahen
New York
+1 212 556 2234
ksheahen@kslaw.com

Michael Shepard
San Francisco
+1 415 318 1221
mshepard@kslaw.com

Thomas Spulak
Miami
+1 305 462 6023
tspulak@kslaw.com

Aaron Stephens
London
+44 20 7551 2179
astephens@kslaw.com

Cliff Stricklin
Denver
+1 720 535 2327
cstricklin@kslaw.com

Jean Tamalet
Paris
+33 1 7300 3987
jtamalet@kslaw.com

Courtney D. Trombly
Washington, DC
+1 202 626 2935
ctrombly@kslaw.com

Rick Vacura
Northern Virginia
+1 703 245 1018
rvacura@kslaw.com

Richard Walker
Washington, DC
+1 202 626 2620
rwalker@kslaw.com

Anthony A. Williams
Washington, DC
+1 202 626 3730
awilliams@kslaw.com

David K. Willingham
Los Angeles
+1 213 218 4005
dwillingham@kslaw.com

David Wulfert
Washington, DC
+1 202 626 5570
dwulfert@kslaw.com

Sally Q. Yates
Atlanta/Washington, DC
+1 404 572 2723
syates@kslaw.com