

# US launches counterattack in battle over data

n 28 February 2024, President Biden issued Executive Order ("EO") 14117 to prevent "countries of concern" from gaining access to sensitive US personal data as well as US government-related data under the authority of the International Emergency Economic Powers Act ("IEEPA"). This EO is far-reaching and seeks to stop foreign adversaries, including China, Russia, Iran, North Korea, Cuba, and Venezuela, from obtaining highly sensitive US personal data, including health, financial, and precise location information, through legal means such as the commercial sale of such information from data brokers or through intermediaries, third-party vendor agreements, or employment or investment agreements. Motivated by China's efforts to achieve global data dominance and US adversaries' efforts to exploit vast amount of US personal data for a strategic and detrimental advantage, the President unveiled national security prohibitions to regulate data transfers determined to pose an unacceptable risk. These new restrictions will bar bulk transfers of US sensitive data, such as genomic data, and transfers of any US government data to "countries of concern." Nation state adversaries are already using advanced technologies and AI tools to exploit US personal data to commit cyberwarfare, espionage, and other malicious activities. Simultaneously, the US Congress is considering a bill, the BIOSECURE Act, to ban federal agencies from contracting with Chinese biotechnology companies of concern, including BGI (formerly known as Beijing Genomics Institute) and WuXi Apptec.

The Department of Justice ("DOJ") has already announced an advanced notice of proposed rulemaking ("ANPRM") to

implement the EO establishing an entirely new regulatory regime.¹ DOJ – the agency that the President designated to lead this effort – intends to design and implement this new national security program using the same model as IEEPA-based economic sanctions programs. This means companies will face significant criminal penalties for knowing violations of these new prohibitions and restrictions. Although we do not yet know the precise date of when the final rules implementing the EO will go into effect, organizations need to begin

These new restrictions will bar bulk transfers of US sensitive data, such as genomic data, and transfers of any US government data to "countries of concern."

preparing for these broad and complex compliance requirements. These rules will not only impact data brokers. They will affect a large number of companies engaged in cross-border data transfers or share US data with foreign entities or persons - especially those in the life sciences and health industries that maintain healthcare and human genomic information of US persons. There will be bulk threshold exemptions, but these new rules will apply to any data set regardless of whether the data is anonymized, pseudonymized, de-identified, encrypted.

#### Overview of EO

The EO describes the effort of countries of concern to gain access and exploit "Americans' sensitive personal data and United States Government-related data" as "an usual and extraordinary threat" to US national security and foreign policy. The EO and the ANPRM reflect growing concerns that China, Russia, and other foreign adversaries will weaponize bulk data and use AI tools to target Americans for espionage and blackmail. As the Office of the Director of National Intelligence made clear in its 2023 Annual Threat Assessment, "[o]ur adversaries increasingly view data as a strategic resource" and the acquisition and exploitation of data makes their espionage operations and cyberattacks more effective, thereby giving them a "strategic advantage over the United States." Accordingly, the EO states that countries of concern can manipulate and analyze "bulk sensitive data to engage in espionage, influence, kinetic, or cyber operations or to identify other potential strategic advantages over the United States." Further, the risks are not limited to countries of concern, but rather extend to entities or persons owned or controlled by, subject to the direction or jurisdiction of, acting as an employee or contractor of, or primarily living in, a country of concern (covered persons).2 Thus, the EO directs DOJ to issue regulations establishing the parameters of this new national security program and delineate the transactions that will be outright banned or severely restricted between US persons and countries of concern or covered persons.

# Critical elements of new regulatory regime

The EO adopts a two-tiered approach requiring DOJ to identify two categories of transactions – those that will be flatly prohibited and those that will be restricted. First, DOJ is contemplating prohibiting two classes of transactions

between US persons and countries of concerns or covered persons: (1) data-brokerage transactions involving the transfer of bulk US sensitive personal data or any US government-related data; and (2) any transaction involving the transfer of bulk human genomic data or human biospecimens from which such data could be derived.

Second, DOJ is considering restricting three types of data transactions involving bulk US sensitive personal data and countries of concern or covered persons unless certain cybersecurity requirements (these will be established by the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency) are met: (1) vendor agreements (including cloud service agreements); (2) employment agreements; and (3) investment agreements.

DOJ is contemplating adopting some bulk volume exemptions applicable to each category of sensitive data, but those exemptions will not apply to data transactions involving sensitive data concerning US government personnel and geolocation data associated with certain military, governmental, or sensitive facilities. The EO also exempts data transactions that are ordinarily incident to and part of financial services, payment processing, or required for compliance with any federal statutory or regulatory requirements.

Unsurprisingly, DOJ is considering identifying China (including Hong Kong and Macau), Russia, Cuba, Iran, Venezuela, and North Korea as "countries of concern." In addition to categorically defining "covered persons" (as described above), the EO authorizes DOJ to supplement these categories by designating specific entities or individuals.<sup>3</sup>

The EO broadly defines "sensitive personal data" to cover transactions involving six categories of bulk US

- See DOJ, National Security Division, Provisions Regarding Access to Americans' Bulk Sensitive Personal Data and Government-Related Data by Countries of Concern, 89 Fed. Reg. 15,780 (5 March 2024) (to be codified at 28 CFR Part 202). DOJ is soliciting public comments from industry. These comments are due by 19 April 2024, 45 days after the ANPRM was published in the Federal Register.
- <sup>2</sup> The specific parameters of each of these categories of covered persons will be further defined by DOJ.
- <sup>3</sup> This could include, for example, the entities identified as Chinese Military Companies Operating in the United States in accordance with Section 1260H of the National Defense Authorization Act for Fiscal Year 2021.
- <sup>4</sup> The EO actually uses the term "human 'omic data." Pursuant to its role in defining the contours of the definitions and rules, DOJ has chosen to omit that term from the definition of "Sensitive Personal Data" and replace it with "human genomic data," which is a subcategory of human 'omic data.

sensitive data: (1) covered personal identifiers; (2) geolocation and related sensor data; (3) biometric identifiers; (4) human genomic data; (5) personal health data; and (6) personal financial data. DOJ is contemplating further refining these categories to specifically exclude any data that is a matter of public record, or

This EO and ANPRM highlight the importance of understanding what data your organization collects, how that data is used, with whom it is shared, and the potential downstream use by your vendors and third parties.

involve personal communications or expressive information. In addition, it would not apply to all geolocation data, only precise location data.

### Who will be affected?

This new national security regulatory regime will be sweeping in scope and will apply to transactions across various industries ranging from life sciences and health care to technology and financial services where transactions have any nexus to China, Russia, or other countries of concern or any foreign person or entity designated as a "covered person." Organizations will need to fully vet any foreign persons or entities that will have access to US sensitive data or government data for any purpose (e.g., IT service providers, software developers, data storage providers, cloud computing services, etc.) to ensure compliance with these new rules.

#### **Timing**

The EO and the ANPRM will not impose any immediate new legal obligations. Because this EO is designed to combat a current and ongoing national security threat - the exploitation of US personal data by China and other countries of concern for malicious cyber-enabled activities and espionage - the Biden administration will want to move quickly to get the new regulations finalized by the end of 2024. The ANPRM was published on 5 March 2024 and the public has until 19 April 2024 to submit comments, including responses to a myriad of questions. The EO requires the US Attorney General to publish the proposed

rule by 26 August 2024. The public will then have a second opportunity to comment. Once the final rule is issued, companies and individuals will be required to comply.

## **Compliance and enforcement**

These rules will include specific transaction restrictions similar to IEEPAbased economic sanctions programs administered by the Department of Treasury's Office of Assets Control. DOJ is also considering implementing a license regime that would authorize certain data transactions, which would otherwise be prohibited or restricted. Any violations of the EO or its implementing regulations will likely be prosecuted under IEEPA, 50 U.S.C. §1705, which is a 20-year felony. In addition to criminalizing knowing and willful violations of any license, order, regulation or prohibition issued under IEEPA, Section 1705 also makes conspiracies and attempts to violate them illegal. DOJ is also contemplating establishing civil monetary penalties.

To avoid potential criminal and civil liability, US organizations will be expected to develop and implement risk-based compliance programs that ensure violations of these new rules do not occur. Recordkeeping requirements may also be imposed as a condition of engaging in a restricted covered data transaction or as a condition of general or specific license.

#### **Closing thoughts**

This EO and ANPRM highlight the importance of understanding what data your organization collects, how that data is used, with whom it is shared, and the potential downstream use by your vendors and third parties. Once these new rules are enacted, it will be critical for organizations to implement comprehensive due diligence measures for any data transactions in which it intends to share or provide access to US sensitive data or US government-related data and to document that. Any violations of these new rules could bring significant penalties, especially if the government determines that your company was responsible for jeopardizing US national security.

About the author:

B. Stephanie Siegmann is Chair of International Trade and National Security and Co-Chair of the Cybersecurity, Privacy, and Data Protection Practice at law firm Hinckley, Allen & Snyder LLP.

www.hinckleyallen.com