Articles + Publications | April 1, 2024

Locke Lord QuickStudy: Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern

Locke Lord LLP

WRITTEN BY

Theodore P. Augustinos | Stephen P. Murphy | Alexander R. Cox | Ryan Last

RELATED OFFICES

Hartford

On February 28, 2024, by Executive Order ("EO") 14117,[1] President Biden issued "Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern." The EO directs the U.S. Attorney General (acting through the U.S. Department of Justice ("DoJ")), in coordination with the Secretary of the Department of Homeland Security and in consultation with the Secretary of State and Secretary of Commerce, to issue regulations that prohibit or otherwise restrict United States persons from engaging in any transaction if the transaction involves bulk U.S. sensitive personal data or U.S. Government-related data.

The EO empowers and orders the DoJ, as noted above, to issue regulations that identify:

- for prohibition specific classes of transactions that could enable countries of concern or covered persons access to Americans' bulk sensitive personal data or government-related data that are determined to pose unacceptable risk to U.S. national security and foreign policy; and
- identify specific classes of transactions that will be required to comply with certain security requirements to mitigate the risks of access to Americans' bulk sensitive personal data or government-related data by countries of concern.

On March 5, 2024, the DoJ issued an advance notice of proposed rulemaking ("ANPRM") seeking public comment related to its proposed regulatory program to implement the EO.

ANPRM Background

In the ANPRM, the DoJ notes that "[u]nrestricted transfers of bulk sensitive personal data and government-related data to countries of concern, through commercial transactions or otherwise, present a range of threats to U.S. national security and foreign policy. Countries of concern can use their access to Americans' bulk sensitive personal data to engage in malicious cyber-enabled activities and malign foreign influence, and to track and build profiles on U.S. individuals, including members of the military and Federal employees and contractors, for illicit

purposes such as blackmail and espionage. Countries of concern can also use access to U.S. persons' bulk sensitive personal data to collect information on activists, academics, journalists, dissidents, political figures, or members of non-governmental organizations or marginalized communities in order to intimidate such persons; curb political opposition; limit freedoms of expression, peaceful assembly, or association; or enable other forms of suppression of civil liberties."

In contrast, as the President stated in the EO and as the DoJ affirmed in the ANPRM, "the United States remains committed to promoting an open, global, interoperable, reliable, and secure internet; promoting open, responsible scientific collaboration to drive innovation; protecting human rights online and offline; supporting a vibrant, global economy by promoting cross-border data flows to enable international commerce and trade; and facilitating open investment."

Therefore, the EO requires that the regulations take specific, carefully calibrated actions to minimize the risks associated with access to Americans' bulk sensitive personal data and government-related data by countries of concern, while minimizing disruption to commercial activity.

DoJ Proposed Regulatory Program

In the ANPRM, the DoJ advises and seeks comment on its proposed program to regulate certain data transactions involving bulk U.S. sensitive personal data and government-related data that present an unacceptable risk to U.S. national security. The DoJ program would (1) identify certain classes of highly sensitive transactions that would be prohibited in their entirety ("prohibited transactions"), and (2) identify other classes of transactions that would be prohibited except to the extent they comply with predefined security requirements ("restricted transactions") to mitigate the risk of access to bulk sensitive personal data by countries of concern.

DoJ's Metered Approach to Regulation

The DoJ plans initially a metered approach by first designating discrete classes of prohibited transactions that raise the highest national-security risks and by focusing on data transactions between U.S. persons and countries of concern; the DoJ program would not regulate purely domestic transactions between U.S. persons (who are not otherwise designated as covered persons acting on behalf of a country of concern), such as the collection, maintenance, processing, or use of data by U.S. persons within the United States. Pursuant to Section 2(f) of the EO, the DoJ would engage in subsequent rulemakings to tailor the regulatory program to address national-security risks on a costs and benefits analysis. To the extent practical, the DoJ would leverage existing regulations based on IEEPA, which are similar to those administered by the United States Department of the Treasury's Office of Foreign Assets Control ("OFAC") and the United States Department of Commerce's Bureau of Industry and Security.

Covered Transactions

Initially, the DoJ plans to:

- prohibit two classes of data transactions between U.S. persons and countries of concern (or covered persons): (1) data-brokerage transactions; 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. To date, these classes of data transactions are not directly regulated under existing Federal laws; and

- identify three classes of data transactions for restriction, to the extent the transactions would involve countries of concern or covered persons and bulk U.S. sensitive personal data: (1) vendor agreements (including, among other types, agreements for technology services and cloud-service agreements), (2) employment agreements, and (3) investment agreements. The DoJ believes these classes of transactions represent significant risks that would allow countries of concern to access bulk U.S. sensitive personal data or government-related data; however, the DoJ believes the national-security risks can be mitigated through appropriate security-related conditions. The security requirements could include: (1) organizational requirements (e.g., basic organizational cybersecurity posture), (2) transaction requirements (e.g., data minimization and masking, use of privacy-preserving technologies, requirements for information-technology systems to prevent unauthorized disclosure, and logical and physical access controls), and (3) compliance requirements (e.g., audits)

Bulk Sensitive Personal Data

The DoJ program focuses on the following six categories of bulk sensitive personal data that could be exploited by a country of concern to harm United States national security if that data is linked or linkable to any identifiable United States individual or to a discrete and identifiable group of United States individuals: (i) U.S. persons' covered personal identifiers, (ii) personal financial data, (iii) personal health data, (iv) precise geolocation data, (v) biometric identifiers, and (vi) human genomic data, and any combinations of those categories. The DoJ will define these categories and, for covered personal identifiers, the DoJ expect that the definition will be significantly narrower than the broad categories of material typically implicated by privacy-focused regulatory regimes.

Bulk sensitive personal data will not include:

- data that is a matter of public record, such as court records or other government records, which is lawfully and generally available to the public;
- personal communications that are within the scope of section 203(b)(1) of IEEPA; or
- information or informational materials within the scope of section 203(b)(3) of IEEPA.

U.S. Government-Related Data

"U.S. Government-related data" means sensitive personal data that, regardless of volume, the Attorney General determines poses a heightened risk of being exploited by a country of concern to harm United States national security. The DoJ program will initially focus on two kinds of government-related data: (1) geolocation data in listed geofenced areas associated with certain military, other government, and other sensitive facilities (which could threaten national security by revealing information about those locations and U.S. persons associated with them), and (2) sensitive personal data that is marketed as linked or linkable to current or recent former employees or contractors, or former senior officials, of the U.S. government, including the military and Intelligence Community.

Countries of Concern

The Attorney General will, in coordination with the Secretary of Homeland Security, the Secretary of State, and the Secretary of Commerce, identify "Countries of Concern," and, as appropriate, classes of covered persons for the purposes of the EO. We expect that that Countries of Concern will include comprehensively sanctioned countries such as North Korea, Iran, Syria and Cuba, as well as Russia and China. For covered persons, we expect the list will include OFAC's SDN list.

Companion or Collision with CFIUS

What is curious about EO 14117 and the DoJ ANPRM is how closely it tracks the language of an existing regulation issued by the Committee on Foreign Investment in the United States ("CFIUS"), *see,e.g.,*31 CFR Part 800.241, without making any reference to the CFIUS regulation. This particular regulation is intended to require filings with CFIUS in the event that an acquisition or investment by a foreign entity is of a U.S. business that maintains or collects specified "sensitive personal data." This data includes but is not limited to: biometric enrollment data, geolocation data, financial data, U.S. government personnel security clearance status, genetic testing results (including genetic sequencing data), personal financial data, and personal health data, all of which is specifically identified in the DoJ ANPRM. Such close overlap begs the question of why the CFIUS regulations appear to be overwritten. Has the Administration determined that the CFIUS regulations do not cast a wide enough net (the CFIUS regulations do require a U.S. business target to collect or maintain such data for at least one million individuals) to stop the flow of sensitive personal data to countries of concern? Only future enactment and enforcement of the DoJ regulation will shed light on this question.

Conclusion

This paper is intended as a guide only and is not a substitute for specific legal or ?tax advice. ???Please ?reach out to the authors for any specific questions. We expect ?to continue to monitor the ???topics ?addressed in this paper and provide future ?client updates when useful.

—

[1] The EO was issued pursuant to the President's authority under the U.S. Constitution and laws of the United States, including the International Emergency Economic Powers Act (50 U.S.C. 1701 *et seq.*) (IEEPA), the National Emergencies Act (50 U.S.C. 1601 *et seq.*) (NEA), and section 301 of title 3, United States Code.

RELATED INDUSTRIES + PRACTICES

- Corporate
- International
- Privacy + Cyber
- Sanctions + Trade Controls