SQUIRE PATTON BOGGS

President Biden Announces Groundbreaking Restrictions on Access to Americans' Sensitive Personal Data by Countries of Concern

February 2024

On February 28, 2024, President Biden issued a groundbreaking executive order (EO) establishing the framework for new restrictions on transactions involving US persons' sensitive personal data and "countries of concern," including China, or related parties.

The EO and forthcoming regulations will impact the use of genomic data, biometric data, personal health care data, geolocation data, financial data and some other types of personally identifiable information. The administration is taking this extraordinary step in response to the national security risks posed by access to US persons' sensitive data by countries of concern – data that could then be used to surveil, scam, blackmail and support counterintelligence efforts, or could be exploited by artificial intelligence (AI) or be used to further develop AI. The EO, however, does not call for restrictive personal data localization and aims to balance national security concerns against the free flow of commercial data and the open internet, consistent with protection of security, privacy and human rights.

The EO tasks the US Department of Justice (DOJ) to develop rules that will address these risks and provide an opportunity for businesses and other stakeholders, including labor and human rights organizations, to provide critical input to agency officials as they draft these regulations. The EO and forthcoming regulations will not screen individual transactions. Instead, they will establish general rules regarding specific categories of data, transactions and covered persons, and will prohibit and regulate certain high-risk categories of restricted data transactions. It is contemplated to include a licensing and advisory opinion regime. DOJ expects companies to develop and implement compliance procedures in response to the EO and subsequent implementing of rules. The adequacy of such compliance programs will be considered as part of any enforcement action – action that could include civil and criminal penalties. Companies should consider action today to evaluate risk, engage in the rulemaking process and set up compliance programs around their processing of sensitive data.

Companies across industries collect and store more sensitive consumer and user data today than ever before; data that is often obtained by data brokers and other third parties. Concerns have grown around perceived foreign adversaries and other bad actors using this highly sensitive data to track and identify US persons as potential targets for espionage or blackmail, including through the training and use of AI. The increasing availability and use of sensitive personal information digitally, in concert with increased access to high-performance computing and big data analytics, has raised additional concerns around the ability of adversaries to threaten individual privacy, as well as economic and national security. These concerns have only increased as governments around the world face the privacy challenges posed by increasingly powerful AI platforms.

The EO takes significant new steps to address these concerns by expanding the role of DOJ, led by the National Security Division, in regulating the use of legal mechanisms, including data brokerage, vendor and employment contracts and investment agreements, to obtain and exploit American data. The EO does not immediately establish new rules or requirements for protection of this data. It instead directs DOJ, in consultation with other agencies, to develop regulations – but these restrictions will not enter into effect until DOJ issues a final rule.

Broadly, the EO, among other things:

- Directs DOJ to issue regulations to protect sensitive US data from exploitation due to large scale transfer to countries of concern, or certain related covered persons and to issue regulations to establish greater protection of sensitive government-related data
- Directs DOJ and the Department of Homeland Security (DHS) to develop security standards to prevent commercial access to US sensitive personal data by countries of concern
- Directs federal agencies to safeguard American health data from access by countries of concern through federal grants, contracts and awards

Also on February 28, DOJ issued an Advance Notice of Proposed Rulemaking (ANPRM), providing a critical first opportunity for stakeholders to understand how DOJ is initially contemplating this new national security regime and soliciting public comment on the draft framework.

According to a DOJ fact sheet, the ANPRM:

- Preliminarily defines "countries of concern" to include China and Russia, among others
- Focuses on six enumerated categories of sensitive personal 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
- Establishes a bulk volume threshold for the regulation of general data transactions in the enumerated categories but will also regulate transactions in US government-related data regardless of the volume of a given transaction
- Proposes a broad prohibition on two specific categories of data transactions between US persons and covered countries or persons – data brokerage transactions and genomic data transactions.

- Contemplates restrictions on certain vendor agreements for goods and services, including cloud service agreements; employment agreements; and investment agreements. These cybersecurity requirements would be developed by DHS's Cybersecurity and Infrastructure Agency and would focus on security requirements that would prevent access by countries of concern.

The ANPRM also proposes general and specific licensing processes that will give DOJ considerable flexibilities for certain categories of transactions and more narrow exceptions for specific transactions upon application by the parties involved. DOJ's licensing decisions would be made in collaboration with DHS, the Department of State and the Department of Commerce. Companies and individuals contemplating data transactions will also be able to request advisory opinions from DOJ on the applicability of these regulations to specific transactions.

A White House fact sheet announcing these actions emphasized that they will be undertaken in a manner that does not hinder the "trusted free flow of data" that underlies US consumer, trade, economic and scientific relations with other countries. A DOJ fact sheet echoed this commitment to minimizing economic impacts by seeking to develop a program that is "carefully calibrated" and in line with "longstanding commitments to cross-border data flows." As part of that effort, the ANPRM contemplates exemptions for four broad categories of data: (1) data incidental to financial services, payment processing and regulatory compliance; (2) ancillary business operations within multinational US companies, such as payroll or human resources; (3) activities of the US government and its contractors, employees and grantees; and (4) transactions otherwise required or authorized by federal law or international agreements.

Notably, Congress continues to debate a comprehensive Federal framework for data protection. In 2022, Congress stalled on the consideration of the American Data Privacy and Protection Act, a bipartisan bill introduced by House energy and commerce leadership. Subsequent efforts to move comprehensive data privacy legislation in Congress have seen little momentum but may gain new urgency in response to the EO.

The EO lays the foundation for what will become significant new restrictions on how companies gather, store and use sensitive personal data. Notably, the ANPRM also represents recognition by the White House and agency officials that they need input from business and other stakeholders to guide the draft regulations. Impacted companies must prepare to engage in the comment process and to develop clear compliance programs so they are ready when the final restrictions are implemented.

Our firm's multidisciplinary attorneys across industry sectors, data privacy, compliance, financial services, supply chain and public policy can assist with prudent due diligence and establishing compliance regimes based upon individual company risk profiles and other unique factors. We can also assist clients with seeking licenses and advisory opinions once the rule is finalized.

For more information, contact the authors or your relationship partner.

Contacts

David Stewart
Principal, Washington DC
T +1 202 457 6054
E david.stewart@squirepb.com

Bridget McGovern
Partner, Washington DC
T +1 202 457 6104
E bridget.mcgovern@squirepb.com

Ludmilla L. Kasulke
Partner, Washington DC
T +1 202 457 5125
E ludmilla.kasulke@squirepb.com

Caroline Spadaro
Associate, Washington DC
T +1 202 457 5545
E caroline.spadaro@squirepb.com

Alan L. Friel
Partner, Los Angeles
T +1 213 689 6518
E alan.friel@squirepb.com

Scott Warren
Partner, Tokyo
T +81 3 5774 1800
E scott.warren@squirepb.com

Kate Kim Tuma
Partner, Los Angeles/Tokyo
T +1 213 689 5147
T +81 5774 1800
E kate.tuma@squirepb.com