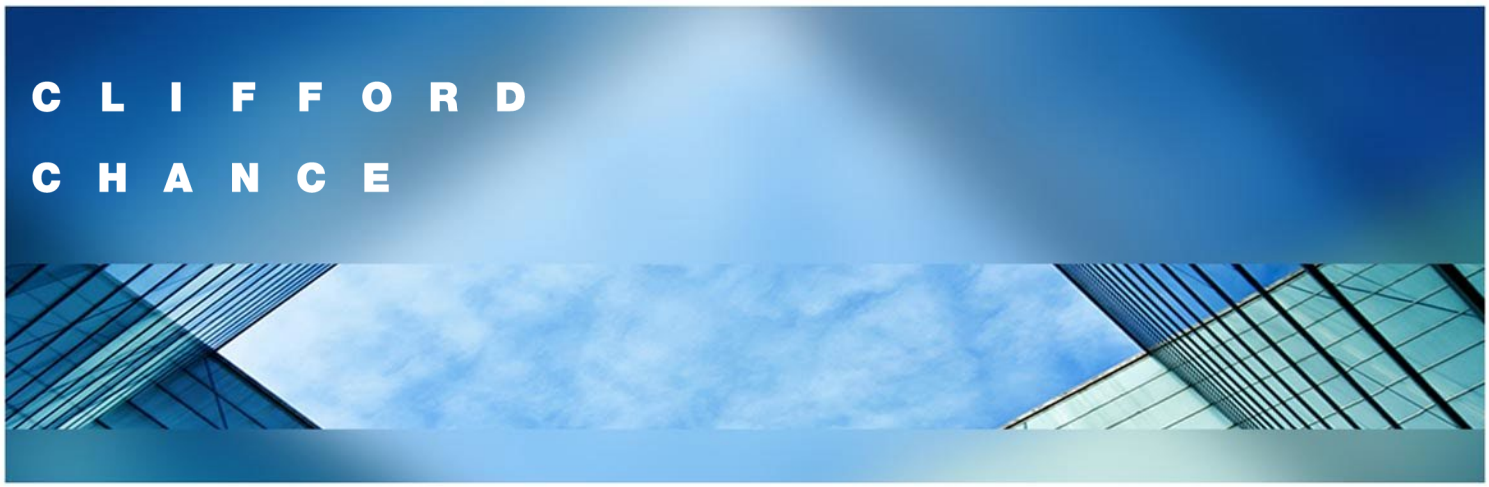

PRESIDENT BIDEN ISSUES EXECUTIVE ORDER TO PROTECT AMERICANS' SENSITIVE PERSONAL DATA: WHAT COMPANIES THAT DO BUSINESS IN COUNTRIES OF CONCERN NEED TO KNOW

On February 28, 2024, President Biden issued *Executive Order 14117: Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern* ("EO 14117"), directing the Department of Justice ("DOJ") and other US agencies to put measures in place to prevent and restrict access to US sensitive personal data by countries of concern. Heralded by the White House as the "most significant" executive action ever taken by a President to protect American data security, EO 14117 builds on steps the US government has taken in recent years to combat cyberattacks and related threats to national security by foreign adversaries, highlighting how these threats have been exacerbated by advances in artificial intelligence technology. Shortly following EO 14117, the DOJ published an Advance Notice of Proposed Rulemaking ("ANPRM") detailing the framework of the forthcoming regulations it will issue to implement the order's directives and filling in the details on what transactions will be impacted. Together, EO 14117 and the accompanying ANPRM from DOJ will likely have important implications for companies that do business in or otherwise operate in countries of concern, including notably China and Russia.

PROHIBITED AND RESTRICTED TRANSACTIONS

The headline for EO 14117 is the directive to prohibit or restrict transactions that may enable countries of concern (or related entities) to access data that could threaten US national security (discussed further below). The order provides

guidelines on how such prohibitions and restrictions would be implemented, but generally directs the DOJ to flesh out the details through rulemaking, in consultation and coordination with the Department of Homeland Security. Immediately following announcement of EO 14117, the DOJ issued an ANPRM that describes the DOJ's plan to implement the order.

Pursuant to the order, DOJ's ANPRM proposes to establish two categories of prohibited transactions:

- **Data brokerage** transactions (transactions that involve the direct sale, licensing, or similar of data); and
- Transactions (regardless of type) that provide access to **bulk human genomic data**.

A transaction that falls into these categories would be prohibited unless it qualified for an exemption. The ANPRM creates a licensing process through which entities seeking to pursue a transaction that would otherwise be prohibited under these categories could seek an exemption from the DOJ.

The ANPRM states that the DOJ does not intend the rules to create a strict liability regime (unlike, for example, sanctions violations and many export controls violations). The proposal explains that the prohibition would only apply to transactions whose circumstances the parties knew (or should have known) would have fallen into the prohibited categories. However, the prohibition would apply to transactions that do not restrict onward transfers of relevant data to countries of concern (regardless of whether such onward transfers are known or contemplated at the time of the transaction).

The ANPRM also describes three proposed categories of restricted transactions:

- **Vendor agreements** (e.g., technology or cloud computing services that involve data processing, but not tangential services like facility cleaning that do not involve data processing);
- **Employment agreements** for individuals that would provide access to relevant data; and
- **Investment agreements** that create a risk of access to relevant data and that involve either (i) real estate located in the United States; or (ii) a US legal entity.

These categories of transactions would be prohibited unless they meet certain security requirements that would reduce the risk of access to relevant data by countries of concern. The ANPRM notes that the exact details of these security requirements are still under development and will be issued separately, but that they will be based on the NIST Cybersecurity Framework and related security guidelines.

Importantly, the ANPRM makes clear that these restrictions would only apply to transactions that occur after the effective date of the regulations. However, EO 14117 leaves open the possibility for some retroactive application, directing that after finalizing the rules, the DOJ should, in coordination with other agencies, investigate and consider actions to mitigate prior transfers to countries of concern.

RELEVANT DATA CATEGORIES AND APPLICABLE THRESHOLDS

EO 14117 and the DOJ's ANPRM identify six categories of personal data that would be regulated:

- Precise geolocation data;
- Biometric identifiers;
- Human genomic data;
- Personal health data;
- Personal financial data; and
- Covered personal identifiers whose access by countries of concern could create a risk to national security.

With regards to the catch-all category of covered personal identifiers, the ANPRM explains that the term is meant to be limited to sensitive data and would be much narrower than what is typically covered by general privacy laws.

The Order directs that certain data be explicitly excluded from any of the identified categories, including data that is lawfully public, personal communications that do not transfer anything of value, and information or informational materials. The ANPRM further clarifies that information or informational materials includes videos and artwork, in line with free speech requirements. Guidance issued by the DOJ to accompany the ANPRM explains that the rules are not meant to address the broader domestic privacy challenges posed by social media and will not ban apps or social-media platforms. The ANPRM also adds to the list of explicit exclusions trade secrets and proprietary information that do not relate to an individual (see below for discussion of exemptions).

Interestingly, EO 14117 and the ANPRM also discuss eventual plans to regulate a catch-all category of "human 'omic data." The Executive Order directs the Assistant to the President for National Security Affairs ("APNSA") to coordinate a report within 120 days assessing the risks and benefits associated with regulating transactions involving non-genomic data, such as proteomic data, epigenomic data, and metabolomic data. Inclusion of this data within the categories of data covered by the rules will follow this report and recommendations.

Covered data is subject to the regulations where either (i) it meets certain "bulk" volume-based thresholds; or (ii) it relates to the US government in a manner that threatens US national security (regardless of volume). DOJ's ANPRM explains that the specific thresholds for what would be considered "bulk" would be based on a risk assessment of the different categories of data and vary according to the sensitivity (and accompanying risk to national security) of the type of data. Current thresholds being considered by the Department range from as few as 100 US persons for human genetic data to as high as 1,000,000 US persons for covered personal identifiers. As for data related to the US government, the ANPRM proposes to include data related to current (or recent) employees, contractors, senior officials, and military personnel, as well as data (including precise geolocation data) relating to geographical areas associated with the military, government, or other sensitive facilities or locations.

COUNTRIES OF CONCERN AND COVERED PERSONS

EO 14117 directs the DOJ to define what countries will be considered "countries of concern" under the transaction restrictions. Under this authority the DOJ has preliminarily identified six countries of concern:

- China (including Hong Kong and Macau);
- Russia;
- Iran;
- North Korea;
- Cuba; and
- Venezuela.

The restrictions apply to not only direct access to covered data by countries of concern, but also access by covered persons, defined to include entities subject to the jurisdiction or direction of one of these countries, foreign employees or contractors of a country of concern or other covered entity, and foreigners primarily resident in a country of concern. The DOJ would also have the ability to designate covered entities, to be maintained on a public list (separate from and independent of other designated lists, including that maintained by the Office of Foreign Assets Control, or "OFAC").

EXEMPTIONS, LICENSES, AND ADVISORY OPINIONS

While emphasizing the need to combat threats from foreign adversaries, EO 14117 stresses that the regulations are meant to be targeted and not designed to impede global trade and commerce or open investment. In this regard, the order directs the DOJ to issue regulations that would exempt such transactions. The DOJ's ANPRM accordingly proposes to mirror OFAC's approach to sanctions by identifying classes of data transactions that are exempt from the prohibitions and restrictions, including:

- Transactions involving personal communications or information or informational materials that are statutorily exempt from the International Emergency Economic Powers Act ("IEEPA"), the authorizing statute for EO 14117;
- Official business of the US Government;
- Financial-services, payment-processing, and regulatory-compliance-related transactions;
- Internal transactions incident to business operations (e.g., transfers with subsidiaries and affiliates located in a country of concern for payroll or human resources); and
- Transactions required or authorized by federal law or international agreements.

EO 14117 also specifically clarifies that the order does not and is not meant to create any data localization requirements.

The DOJ's ANPRM also identifies certain categorical exclusions for investments. Specifically, the ANPRM identifies categories of passive investments that do not convey ownership interests or rights or otherwise allow investors to wield influence that could be used to obtain access to relevant data. To this end, the DOJ has proposed identifying three categories of passive investments that would be exempt from restrictions:

- Investments in a publicly traded security, in a fund offered by an investment company or private investment fund, or as a limited partner in a pooled investment fund (where the contribution is solely capital and does not convey any formal or informal ability to influence or participate in the fund's decision-making or operations);
- Investments below a to-be-defined inconsequential threshold in total voting and equity interests; and
- Investments that otherwise do not give any rights beyond those reasonably considered to be standard minority shareholder protections.

EO 14117 also requires the DOJ to establish a process for entities to seek licenses for and advisory opinions regarding the legality of a transaction that may otherwise be prohibited or restricted. The DOJ's ANPRM notes that this licensure regime would be modeled upon OFAC's established process and provide both general and specific licenses that approve (or approve with conditions) covered transactions. Similarly, the DOJ proposes to create a program akin to the processes used by OFAC to issue written advisory opinions and other guidance.

CFIUS AND COORDINATION WITH OTHER REGULATORY REGIMES

Recognizing that its directives overlay onto a complex existing regulatory framework of international data flows and trade, EO 14117 directs the DOJ to consider coordination with other government entities, including notably CFIUS. To this end, the ANPRM explains that the DOJ does not anticipate that there would be significant overlap with existing authorities. Regarding coordination with CFIUS, the DOJ explains that EO 14117 focuses on prospective outbound flows of sensitive data, in contrast to CFIUS's case-by-case review of specifically negotiated inbound acquisitions. In this regard, EO 14117 would primarily regulate the activities of a foreign acquirer following its acquisition of a US company holding sensitive personal data and the receipt of CFIUS approval. The ANPRM further clarifies that the DOJ would independently regulate and restrict covered investment agreements that are also covered transactions subject to CFIUS review unless and until CFIUS determines that mitigation measures are required to resolve national security risks—but that once such mitigation measures are imposed and agreed upon, the transaction would be exempt from DOJ's review under EO 14117. The DOJ thus appears to be sensitive to the possibility of imposing overlapping and potentially conflicting regulatory obligations on parties to an investment transaction that would otherwise be subject to both the DOJ's review under EO 14117 (including post-acquisition) as well as CFIUS review (limited to pre-acquisition).

OTHER DIRECTIVES

While the prohibited and restricted transaction rules headline EO 14117, the order also includes other important directives, including:

- Directing the Committee for the Assessment of Foreign Participation in the US Telecommunications Service Sector to consider threats to Americans' sensitive personal data in reviewing and issuing **submarine cable licenses**;
- Directing the Departments of Health and Human Services, Defense, and Veterans Affairs to consider and address risks that grants and federal assistance programs lead to access by countries of concern to **personal health and biometric data**; and
- Encouraging the Consumer Financial Protection Bureau to follow through on its previously-announced work on proposing new rules to enhance compliance with consumer protection law by the **data brokerage industry**.

In the announcement accompanying the Executive Order, President Biden also calls on Congress to pass bipartisan privacy legislation, especially to protect the safety of children.

KEY TAKEAWAYS

A lot still remains to be seen with regards to how EO 14117 will be implemented. While the DOJ issued its ANPRM shortly after the order was signed, there are still a number of administrative processes that need to be completed before any rules become effective. The ANPRM calls for a 45-day period of public comment and includes 114 specific questions relating to all aspects of the proposed rules. The DOJ will study and consider implementing this feedback before issuing a formal Notice of Proposed Rule Making ("NPRM"), which EO 14117 contemplates can take as long as 180 days from the date of the order. This NPRM will then be followed by another round of public comments before the DOJ issues a final rule, meaning it may still be some time before any restrictions or prohibitions become effective.

Despite the extended timeline, however, companies would be wise to begin taking steps now to prepare. While the exact contours of the rules are yet to be finalized, the White House and the DOJ have made clear what kinds of transactions and data are of focus. And while enforcement under the rules themselves cannot occur until after they are finalized, nothing prevents the White House, the DOJ, and other Government bodies like CFIUS from using any existing authority to investigate and restrict foreign transactions and data flows. And as mentioned above, while the rules will not be retroactive, the Executive Order specifically contemplates that the DOJ would consider and take actions to address risks arising from past transactions that involve countries of concern.

Companies looking to take action should consider:

- **Heightening scrutiny of proposed transactions that involved countries of concern.** Especially given the possibility of some retroactive application—not to mention the uncertain timelines associated with any transaction—companies would be wise to consider augmenting diligence and compliance regimes now. Indeed, the DOJ's ANPRM specifically mentions that its

contemplated enforcement regime would take into account existing diligence and compliance programs—including considering the failure to develop an adequate diligence program an aggravating factor in any enforcement. This is especially important because IEEPA provides for the possibility of criminal penalties.

- **Revisiting and ensuring they understand their data flows (data mapping).** While the executive order and ANPRM both state that the regulations will not restrict data transfers incidental to legitimate business activities and internal business operations, the potential for scrutiny highlights the importance for companies to understand their data processing and transfer activities. As companies have already experienced in wrestling with compliance with the GDPR and the increasingly complex web of international data protection laws, changing business operations and redirecting data flows takes time. Having a clear picture of existing and contemplated data flows will also help when seeking licenses, advisory opinions, or even in defending against an inquiry or enforcement action.
- **Placing controls on downstream use of data transfers by third parties.** The good news for companies is that the DOJ does not contemplate the rules to create strict liability, a welcome respite for companies already faced with the prospect of strict liability in other enforcement regimes. However, the DOJ has also stated that the prohibitions would apply to transactions that do not restrict onward transfers of relevant data to countries of concern—even if such onward transfers are not known or contemplated at the time of the transaction. Accordingly, companies should consider reviewing and modifying the contracts now to include restrictions on such onward transfers. This may also align with contractual requirements that are popping up in state privacy law regimes.

CONTACTS

Megan Gordon
Partner

T +1 202 912 5021
E megan.gordon
@cliffordchance.com

Renee Latour
Partner

T +1 202 912 5509
E renee.latour
@cliffordchance.com

Michelle Williams
Partner

T +1 202 912 5011
E michelle.williams
@cliffordchance.com

Jamal El-Hindi
Counsel

T +1 202 912 5167
E jamal.elhindi
@cliffordchance.com

Brian Yin
Associate

T +1 202 912 5902
E brian.yin
@cliffordchance.com

Andrew Astuno
Associate

T +1 202 912 5083
E andrew.astuno
@cliffordchance.com

Holly Bauer
Associate

T +1 202 912 5132
E holly.bauer
@cliffordchance.com

Martina Kneifel
Law Clerk

T +1 202 912 5066
E martina.kneifel
@cliffordchance.com

www.cliffordchance.com

Clifford Chance, 2001 K Street NW, Washington, DC 20006-1001, USA

Clifford Chance US LLP

Abu Dhabi • Amsterdam • Barcelona • Beijing • Brussels • Bucharest • Casablanca • Delhi • Dubai • Düsseldorf • Frankfurt • Hong Kong • Houston • Istanbul • London • Luxembourg • Madrid • Milan • Munich • Newcastle • New York • Paris • Perth • Prague • Riyadh • Rome • São Paulo • Shanghai • Singapore • Sydney • Tokyo • Warsaw • Washington, D.C.

AS&H Clifford Chance, a joint venture entered into by Clifford Chance LLP.

Clifford Chance has a best friends relationship with Redcliffe Partners in Ukraine.