Regulatory Studies Center
THE GEORGE WASHINGTON UNIVERSITY

Improving regulatory policy through research, education, & outreach

Biden's Ambitious Executive Order Does More for Data Security than Banning TikTok

In brief…

President Biden's Executive Order 14117 is an ambitious attempt to mitigate the exploitation of sensitive U.S. data. While the order's implementation faces uncertainty in an election year, its approach is more tailored to producing meaningful protections on data security than the recent legislation banning TikTok.

By: Mark Febrizio | April 26, 2024

On April 24, President Biden signed into law a foreign aid package (H.R. 815) containing provisions that would require ByteDance, a China-based company, to divest its ownership of the social media platform TikTok or be banned from distributing its application in Apple's App Store, Google Play, and similar software marketplaces.

Before signing the bill into law, President Biden had issued multiple executive actions with a related goal to the TikTok ban – protecting Americans' sensitive data from being exploited by adversarial "countries of concern." Most recently, the president signed Executive Order (EO) 14117 of February 28, which seeks to restrain data brokers from selling Americans' data to entities with ties to hostile nations.

Substantively, EO 14177 represents an ambitious attempt to mitigate the exploitation of sensitive U.S. data by applying a categorical approach to data transactions, in contrast to the case-by-case adjudications administered by the Committee on Foreign Investment in the United States. While the EO faces uncertainty as the Biden administration attempts to move forward its policy agenda before the 2024 presidential election, its approach is more tailored to producing meaningful protections on data security than the TikTok ban.

General Summary of Executive Order 14117

EO 14117 builds on President Trump's EO 13873 of May 15, 2019, which declared a national emergency related to the threat of "foreign adversaries" exploiting vulnerabilities in information and communications technologies and established initial criteria for identifying prohibited transactions. EO 14117 expands the scope of the national emergency in EO 13873 and seeks to restrict entities owned by, controlled by, or subject to the jurisdiction of certain countries from accessing sensitive U.S. data on national security grounds.

The EO is concerned with two categories of data, *Americans' bulk sensitive personal data* and *U.S. government-related data*. First, "sensitive personal data" includes combinations of certain personal identifiers, geolocation data, biometrics, human genomic data, and personal health or financial information that could be exploited to identify U.S. individuals or groups. It excludes publicly available data. Importantly, the order is concerned with sensitive personal data that is accessed in "bulk" – a term that may be further specified by subsequent Department of Justice (DOJ) regulations.

Second, U.S. government-related data refers to "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" and that either can be linked to active or former federal employees, contractors, or officials or contains information on sensitive government locations. Notice the emphasis on the sensitivity of the data regardless of the amount accessed. Also, DOJ will determine the specific scope of the data that fall under the implementing regulations.

In the remainder of this piece, I will generally refer to these two categories of data together as *sensitive U.S. data*.

The executive order's approach and scope differ from the legislation, as it does not mention TikTok or ByteDance by name, nor would it prohibit TikTok or similar platforms from operating in the U.S. The directive is also careful to say that it is not broadly (a) requiring sensitive U.S. data to be stored within the U.S., (b) mandating that computing facilities be located in the U.S, nor (c) prohibiting "[U.S.] persons from conducting commercial transactions … with entities and individuals located in or subject to the control, direction, or jurisdiction of countries of concern." This last provision underscores that the EO is not intending to protect public-facing data available from social media platforms, including TikTok. Finally, the EO's objectives are focused on national security threats to the U.S., rather than establishing a comprehensive data privacy regime to protect American consumers.

Specific Provisions of Executive Order 14117

The substantive provisions of EO 14117 are largely contained in five sections.

Section 2 directs DOJ to issue regulations that prohibit or restrict data brokers from engaging in transactions that may compromise national security by enabling countries of concern to access U.S. sensitive data. The order also directs the Department of Homeland Security (DHS) to request comments on and publish security requirements for restricted transactions that mitigate their associated national security risks.

Section 3 contains provisions for several federal bodies to safeguard access to sensitive U.S. data by taking actions related to (1) network infrastructure controlled by countries of concern (e.g., submarine cables that transmit data), (2) the U.S. healthcare market (e.g., entities accessing data "through partnerships and agreements with United States healthcare providers and research institutions"), or (3) the data brokerage industry (e.g., companies that sell consumers' personal information).

Section 4 requires DOJ, DHS, and the Director of National Intelligence to submit recommendations to the Assistant to the President for National Security Affairs (APNSA) that address the risk of prior transfers of sensitive U.S. data. The section contains two directives with deadlines based on the effective date of the DOJ regulations on prohibited and restricted transactions.

Sections 5 and 6 concern two reports to the president, the first dealing with the effectiveness and economic impact of the implementation of the order and the second evaluating whether "transactions involving types of human 'omic data other than human genomic data" should be regulated under the DOJ rules on prohibited or restricted transactions.

The following table summarizes these provisions and any applicable deadlines.

Table 1. Substantive Provisions of EO 14117 by Section

Section	Description	Provisions
2	Prohibited and Restricted Transactions	• *Within 180 days*, DOJ to propose regulations on prohibited and restricted transactions • *Within 180 days*, DHS to publish security requirements for restricted transactions
3	Protecting Sensitive Personal Data	• Team Telecom to review licenses for submarine cable systems that transmit data and address related risks • Departments of Defense, Health and Human Services, and Veterans Affairs, and the National Science Foundation to consider steps to protect sensitive personal health data and human genomic data, and submit report to the APNSA *within one year* • Consumer Financial Protection Bureau to consider steps to address data broker activities that contribute to the national emergency
4	Prior Transfers of Bulk Sensitive Personal Data	• *Within 120 days of the effective date of regulations in Section 2*, DOJ, DHS, and DNI to submit recommendations to the APNSA • *Within another 30 days*, the APNSA to review recommendations and consult on implementation
5	Report on EO Implementation	• *Within one year of the effective date of regulations in Section 2*, DOJ to submit a report to the president on implementation of the EO
6	Report on Human 'omic Data	• *Within 120 days*, the APNSA and three other presidential advisors to submit a report to the president on what types of "human 'omic data" should be regulated under DOJ's regulations

Comparison with the TikTok Ban

The TikTok ban responds to a growing concern from lawmakers that the application facilitates China's access to Americans' sensitive data. Although banning TikTok might signal the impression of sweeping change, the EO and corresponding rulemaking actions would likely do more to constrain China (and other foreign nations) from accessing and exploiting sensitive U.S. data.

These differences stem from the policy mechanism each action has selected. The TikTok ban focuses on whether TikTok – and other applications that fall under the law's definitions – can be distributed, maintained, updated, and hosted. This approach, in part, relates to concerns about the political influence that China could leverage through the application. But as others have pointed out, banning TikTok would not prevent China from gaining access to sensitive U.S. data through data brokers.

By contrast, the EO seeks to tackle the data brokerage industry more directly by focusing on categories of transactions that may facilitate access to sensitive U.S. data by countries of concern. Several days after EO 14117 was signed, DOJ issued an advance notice of proposed rulemaking (ANPRM) related to establishing the regulations required by Section 2 of the order. DOJ's proposed framework would (1) prohibit data broker transactions and transactions involving bulk human genomic data between U.S. entities and entities subject to control by a country of concern, and (2) it would restrict vendor agreements, employment agreements, and investment agreements between such entities that involve certain categories of sensitive data.

Notably, DOJ indicates that it would exempt "information and information materials," under which social media activity likely falls, from the covered data transactions under the regulations. However, DOJ's regulations would plausibly regulate certain data transfers between TikTok and ByteDance, such as sharing bulk precise geolocation data on U.S. persons through a vendor agreement. The actual implementation details are in flux.

Other differences beyond the policy mechanism include how foreign adversaries or countries of concern are defined (the ANPRM applies to two additional countries, Venezuela and Cuba) and what constitutes control by a foreign country (the ANPRM specifies a 50 percent or more stake, while the congressional legislation included a lower threshold of 20 percent).

Prospects for Implementing Executive Order 14117 in 2024

With the 2024 election looming, what are the prospects for implementing the actions stemming from Biden's data security EO?

Practically, a future president could rescind EO 14117 on their first day or issue another directive that modifies how the EO's provisions are implemented. Given the degree of bipartisan agreement on the problem around data security and foreign adversaries, the latter option seems more likely. In fact, this is akin to the approach that the Biden administration has taken by retaining President Trump's original 2019

EO, revoking three Trump administration EOs that had taken additional steps addressing the national emergency (these directives had prescribed specific actions against TikTok, WeChat, and other applications or software "developed or controlled by Chinese companies"), and issuing its own EOs on the topic. A future administration will also control the implementation of the data security EO through political appointments in agencies and the regulatory review process managed by the Office of Information and Regulatory Affairs.

President Biden has an incentive to finalize rules implementing the EO before election day because any regulations that are left in a proposal stage could be withdrawn by a future president. If DOJ were able to finalize its regulations on prohibited and restriction transactions this year – admittedly, a very tall order – an incoming administration would need to undergo notice and comment to reverse or amend those provisions. However, finalizing a rule this close to a presidential election might make such regulations vulnerable to removal under the Congressional Review Act.

Of course, if President Biden wins re-election in November, then his administration has another term to implement his policy agenda on data security. While policymakers seem set on acting on data security regardless of the outcome of the election, the manner in which this takes place will be consequential. Banning TikTok, or other social media applications, is likely to produce marginal data privacy benefits and should not distract from other more promising efforts like implementing EO 14117.