ALSTON & BIRD

WWW.ALSTON.COM

International Trade & Regulatory ADVISORY ■

SEPTEMBER 15, 2020

Uncertainty Surrounds Forthcoming Commerce Department Action on TikTok & WeChat "Bans"

by *Jason Waite*, *Jim Harvey*, *Helen Galloway*, and *John O'Hara*

Oracle Corp. has reportedly won the bid to buy TikTok, the globally popular video-sharing app that has been the subject of much debate since President Trump ordered the sale of the app back in mid-August. The announcement of TikTok's sale is a reminder that the clock is ticking on the forthcoming announcement by the U.S. Department of Commerce that will define the scope of President Trump's Executive Orders (EOs), reportedly intended to ban the Chinese-owned apps TikTok and WeChat from the U.S. Issued on August 6, the EOs provided Commerce with a September 20 deadline to identify which transactions involving TikTok and WeChat will be prohibited under the orders.

Smartphone users are familiar with the alerts that frequently appear on their screens requesting permission for a mobile application to access the user's camera, geolocation, ApplePay, information from social media profiles, and many more. This everyday sharing of personal data with apps (and consequently the apps' developers and owners) has become a concern of the U.S. government in certain circumstances, as it fears that allowing foreign access to U.S. citizens' personal data through apps may provide foreign governments with the means for sabotage and espionage. Over the last several weeks, the latest attempts by the U.S. to restrict such foreign access made headlines with the issuance of the two EOs pertaining to TikTok and WeChat. Both apps have achieved international popularity and reportedly have tens of millions of U.S. users.

Foreign access to personal data, also commonly referred to as personally identifiable information (PII), has increasingly become the subject of U.S. legislation and enforcement actions conducted by U.S. agencies, including the Federal Trade Commission (FTC) and the Committee on Foreign Investment in the United States (CFIUS). The EOs threatening to ban or restrict the operations of TikTok and WeChat are by no means the first attempts to regulate Chinese-owned apps with U.S. operations and are merely the latest examples in a long list of regulatory developments on the issue of protecting personal data from foreign regimes. The EOs raise a host of policy considerations and leave the global business community guessing about the scope of prohibitions, not to mention the future of foreign investments in the technology sector and cooperation between companies on the development and distribution of apps. Indeed, following his remarks at a press conference held on August 15, rumors are already circulating over whether the President will issue similar orders targeting other Chinese-owned apps. The legality of banning social media apps

This advisory is published by Alston & Bird LLP to provide a summary of significant developments to our clients and friends. It is intended to be informational and does not constitute legal advice regarding any specific situation. This material may also be considered attorney advertising under court rules of certain jurisdictions.

from the U.S. has also become the subject of debate. As of August 24, two lawsuits have already been filed (one by TikTok and the other by U.S. users of WeChat) challenging the legality of these EOs on the grounds that they violate the U.S. plaintiffs' rights to due process and free speech. Adding even further to this debate, on August 28, China announced an update to its export regulations, purportedly adding new categories of technology that would require government approval before export, which could have meaningful consequences in a future sale of TikTok.

The timing of these events is ironic as the Court of Justice of the European Union issued a landmark decision in July that invalidated the EU-U.S. Privacy Shield largely on the basis of concerns over surveillance law and practice in the United States. While that decision is postured quite differently than these events, the combination of the two illustrates the complexity of these issues from a global, legal, and political perspective.

There are a number of reasons for the uncertainty surrounding the TikTok and WeChat EOs, including:

- The EOs relegate the responsibility of implementation to the U.S. Department of Commerce, which lacks an existing sanctions enforcement regime.
- The intention of the EOs is unclear because they do not define what constitutes a "transaction" that will be subject to the prohibitions contained in the EOs.
- The parties most impacted by the EOs may be U.S. businesses.

The EOs Provide Little Guidance on What "Transactions" with TikTok and WeChat Will Be Prohibited

On August 6, President Trump issued two EOs relying on his authority to act to address national emergencies under the International Emergency Economic Powers Act (IEEPA). One purports to prohibit certain transactions with ByteDance Ltd. (the Chinese parent of TikTok) and the other purports to prohibit certain transactions with Tencent Holdings Ltd. (the Chinese parent of WeChat) that are related to WeChat. Specifically, the EOs set forth the following restrictions:

- The TikTok EO will prohibit "any transaction by any person, or with respect to any property, subject to the jurisdiction of the United States," with ByteDance "or its subsidiaries, in which any such company has any interest, as identified by the Secretary of Commerce."
- The WeChat EO will prohibit "any transaction that is related to WeChat by any person, or with respect to any property, subject to the jurisdiction of the United States," with Tencent "or any subsidiary of that entity, as identified by the Secretary of Commerce."

The EOs provide no further specifics about how a "transaction" is to be defined or the extent of the activities that will be prohibited. Instead, the EOs require the Secretary of Commerce to take action within 45 days to give substance to the President's facially broad pronouncements. Notably, however, the EOs themselves purport to go into effect 45 days after the date they were issued. Thus, substantial ambiguity remains over what activities will ultimately be prohibited.

The EOs Seek to Address Issues More Typically Handled by CFIUS

The use of IEEPA to broadly prohibit transactions with ByteDance and its subsidiaries (which presumably covers TikTok in the U.S.) was surprising given that CFIUS was already conducting a formal review of ByteDance's acquisition of TikTok. Under the Defense Production Act (DPA),[1] the President can and has required foreign companies to divest their interests in U.S. companies following a CFIUS determination that an acquisition poses a threat to national security. The more anticipated executive action was therefore an EO under the DPA ordering that ByteDance divest its interest in TikTok or in portions of the U.S. business of TikTok that it had previously acquired, which is precisely what occurred a mere eight days after the first TikTok EO was issued.

On August 14, the President issued another EO regarding TikTok, using his authority under the DPA to order ByteDance to divest all interests and rights in TikTok within 90 days. This is not an unprecedented move. In fact, the EO issued on August 14 marks the fourth time that President Trump has used his authority under the DPA to either block a foreign acquisition of a U.S. business or order a foreign buyer to divest its interests in a U.S. business. As recently as March 6, 2020, President Trump issued an EO requiring Beijing Shiji Information Technology Co. Ltd., organized in China, and its Hong Kong-based subsidiary to divest their interest in StayNTouch Inc., a U.S. hotel management software company. Shiji's potential access to U.S. hotels' guest data was reportedly the primary national security concern underlying the order to divest.

There are earlier examples of Chinese buyers divesting their interests in U.S. apps following a CFIUS investigation where the next step of a presidential determination was ultimately unnecessary since the Chinese buyers agreed to divest following CFIUS's determination that they should do so. For example, in May 2019, Beijing Kunlun Tech Co. Ltd., a Chinese gaming company, announced that CFIUS was requiring the divestment of its interests in Grindr, a U.S. dating app for members of the LGBTQ community, which it had acquired in 2018. Again in 2019, CFIUS determined that iCarbonX, a Chinese company backed by Tencent (also the parent of WeChat), should divest its interests in PatientsLikeMe, a U.S. app that helps patients connect with others with similar health conditions. Even earlier, in 2017, CFIUS prevented the acquisition of the U.S. payment app MoneyGram by Alipay. The common thread among all these transactions is that the U.S. business at issue maintains or collects "sensitive personal data" of U.S. persons.

While there are certainly financial hardships associated with these CFIUS actions, they are not the equivalent of sanctions or prohibitions on doing business with a particular company. CFIUS's purview is a tailored interagency review of a specific transaction conducted in accordance with CFIUS regulations. As summarized in our earlier advisory on the topic, the Foreign Investment Risk Review Modernization Act (FIRRMA) amended the DPA and expanded CFIUS's jurisdiction to cover not only its traditional review of foreign acquisitions of U.S. companies but also certain foreign investments in U.S. companies engaging in select business activities. The enactment of FIRRMA and the resulting 300 pages of regulations that were implemented earlier in 2020 put transactional parties on notice of what transactions require a CFIUS submission or may otherwise attract CFIUS's attention. One such category of transactions includes those involving U.S. companies that collect or maintain sensitive personal data of U.S. persons, and the regulations then specifically define the relevant categories of sensitive personal data. Although public opinions may differ on the foreign policy and national security considerations that underlie CFIUS reviews, the regulations that govern

---

[1] CFIUS derives its legal authority to conduct national security reviews of transactions involving foreign acquisitions and foreign investments from Title VII of the DPA. Originally enacted in 1950, the DPA is a federal law that provides the President with a number of substantial powers over matters of national security. In 1988, the DPA was amended with the Exon–Florio Amendment that granted the President the authority to block proposed or pending foreign mergers, acquisitions, or takeovers. The CFIUS-related provisions of the DPA have since been amended several times, the most recent being the Foreign Investment Risk Review Modernization Act of 2018 (FIRRMA).

the review process itself and that define the scope of transactions subject to CFIUS review are explicitly set forth in FIRRMA, a law enacted by elected representatives.

The President's Reliance on a Broadly Defined "National Emergency" Under IEEPA to Justify the EOs Highlights the Breadth of the President's View of His Authority Under IEEPA

The August 14 EO was issued under the authority that we would typically expect the President to use when seeking to prohibit activities by foreign investors in the U.S. In contrast, the EOs from August 6 were issued under IEEPA. IEEPA authorizes the President to regulate certain aspects of foreign commerce after declaring a national emergency "to deal with any unusual and extraordinary threat, which has its source in whole or substantial part outside the United States, to the national security, foreign policy, or economy of the United States." IEEPA is typically used as a statutory basis for economic sanctions regulations administered by the Office of Foreign Assets Control (OFAC) with the U.S. Department of the Treasury. The EOs issued on August 6, however, delegate the regulatory responsibility to the Department of Commerce rather than the Treasury, which creates uncertainty since Commerce does not have an existing regime designed to administer or enforce this proposed regulatory framework.

The basis for these two EOs is the national emergency declared in EO 13873 on May 15, 2019. EO 13873 sets forth a national emergency identified by the President regarding the exploitation of vulnerabilities in "information and communications technology and services" (ICTS) by "foreign adversaries." In our earlier advisory on this subject, we noted that the EO's broad definition of ICTS could cover virtually any electronic product, including mobile devices, apps, and tablets, since they can include data processing technology and communication capabilities. These EOs are an example of just how broadly the President views his authority to address this "national emergency."[2]

Without a definition of "transaction" in the EOs, it is unclear how Commerce will implement them and, without a history of an enforcement mechanism, it is unknown whether Commerce will follow OFAC's broad regime of administering sanctions. Significantly, however, IEEPA expressly prohibits the President from "directly or indirectly" restricting the import or export, "whether commercial or otherwise, regardless of format or medium of transmission," of "information or informational materials." Thus, the question of whether the ultimate implementation of the EOs will run afoul of these restrictions remains. This limitation on the President's authority under IEEPA is one of the claims upon which the early lawsuits challenging the EOs are based.

Practical Limitations and Unexpected Consequences

It has been widely reported across different media outlets that the ambiguity surrounding the proposed ban of WeChat and related transactions yet to be determined with its parent company Tencent may result in unintended and unexpected consequences that ripple across multiple industries. While the EO issued by President Trump ordering the divestment of TikTok is not an unprecedented action within the framework of CFIUS, the EO outlining a potential ban of WeChat is unique. The WeChat EO is a "coming attraction" of a potential future ban on using or supporting the app.

---

[2] EO 13873 also granted Commerce the authority to prohibit or restrict certain transactions involving the "acquisition, importation, transfer, installation, dealing in, or use of any information and communications technology or service" that pose undue risks to U.S. national security or the U.S. digital economy, among other things. The ensuing proposed regulations published by Commerce seemed to create a CFIUS-type review to be conducted by Commerce but were severely lacking in detail. Final regulations have yet to be issued.

While it is possible that nothing will happen at all, companies and individuals subject to U.S. jurisdiction should be prepared. U.S. companies should study and catalogue any nexus with WeChat and their relation to other Tencent operations. This includes supporting payments, back office support, common IT infrastructure, and software. Common infrastructure that U.S. companies share with overseas subsidiaries is fraught with risk, if that infrastructure is based in the U.S. or involves U.S. persons in its operations or management. For software developed in the U.S. that is exported to overseas locations to support WeChat operations, companies may need to halt future updates, patches, and related support.

Since the statutory basis for the WeChat EO is IEEPA, companies should be prepared to manage an OFAC-like sanctions regime akin to what is seen in Iran, North Korea, Cuba, and Syria, or perhaps something more akin to the "sectoral sanctions" that have been the hallmark of OFAC's Ukraine sanctions program. The threatened measures could restrict an array of transactions, including advertising or even offering and hosting the WeChat app in an app store, or they could be more targeted and seek to restrict specific types of transactions involving personal data. With September 20, 2020, approaching quickly – 45 days after the publication of the WeChat EO – impacted companies with some level of engagement with Tencent need to be on high alert.

You can subscribe to future ***International Trade & Regulatory*** advisories and other Alston & Bird publications by completing our **publications subscription form**.

If you have any questions or would like additional information, please contact your Alston & Bird attorney or any of the following:

Jason M. Waite
202.239.3455
jason.waite@alston.com

Kenneth G. Weigel
202.239.3431
ken.weigel@alston.com

Brian Frey
202.239.3067
brian.frey@alston.com

Helen Su
202.239.3300
86.10.85927588
helen.su@alston.com

Lucas Queiroz Pires
202.239.3235
lucas.queirozpires@alston.com

Bobbi Jo Shannon
202.239.3344
bj.shannon@alston.com

Chunlian Yang
202.239.3490
lian.yang@alston.com

Helen Galloway
202.239.3794
helen.galloway@alston.com

John O'Hara
202.239.3131
john.ohara@alston.com

Yuzhe PengLing
202.239.3132
yuzhe.pengling@alston.com

James A. Harvey
404.881.7328
jim.harvey@alston.com

ALSTON & BIRD

WWW.ALSTON.COM

© ALSTON & BIRD LLP 2020