

Trump Administration Seeks to Ban Transactions Using Popular Chinese Mobile Apps

by Lawrence Ward, Dave Townsend, and T. Augustine Lo

With only two weeks left in its term in office, the Trump Administration issued yet another 11th hour Executive Order (“EO”) on January 5 that purports to create a new legal framework to ban transactions with certain Chinese companies or their subsidiaries that offer specified mobile phone software applications. The ban would impact several popular Chinese payment platforms and other applications that are widely used around the world.

As issued, the new EO targets the following frequently-used software applications: Alipay, CamScanner, QQ Wallet, SHAREit, Tencent QQ, VMate, WeChat Pay, and WPS Office (collectively, the “Restricted Apps”). However, the new EO states that its prohibitions will only come into effect in 45 days (on February 19). By that time, the Biden Administration will have replaced the Trump Administration. On its face, the new EO is thus not yet legally binding on any U.S. persons or companies reliant on the Restricted Apps, and it remains to be seen if the Biden Administration will leave this EO in effect or if it may choose to revoke it, either in whole or in part.

Potentially Broad Impact Subject to Further Specification

As written, the EO’s prohibition against dealing with persons and property related to the Restricted Apps is set to take effect 45 days after the EO’s date, which will be February 19. However, the EO also states that the U.S. Secretary of Commerce must consult with the Attorney General and the Director of National Intelligence to identify the particular U.S. persons and transactions that would be subject to the EO’s prohibition and that such identification is to occur “[n]ot earlier than 45 days after the date of this order.” That means such crucial identification defining the actual scope and effect of the EO will not become publicly available until the same day as or even after the prohibition actually takes effect. Because of this decidedly awkward situation, interested parties should look to further clarification from the U.S. Department of Commerce, which the EO makes responsible for issuing the Commerce Secretary’s identification.

Related People

- Lawrence Ward
- Dave Townsend
- T. Augustine Lo

Related Capabilities

- International Trade
- China
- Emerging Companies
- National Security Law

Once the Commerce Department specifies the prohibited persons and transactions, the EO would then prohibit U.S. persons from engaging in such specified transactions with the identified persons who develop or control the Restricted Apps, unless otherwise authorized by the Commerce Department through a license. In addition, the EO would prohibit any other dealings with the property of the specified persons that are subject to U.S. jurisdiction. Accordingly, if the EO's prohibitions were ever to come into effect, they could affect the ability of U.S. companies, persons located in the United States, and U.S. citizens and permanent residents located anywhere else in the world from engaging in certain transactions involving the Restricted Apps. Depending on Commerce's identification of the prohibition's scope, this prohibition could potentially also affect electronic payments, technology licensing, software downloads and updates, and many other similar activities. Moreover, because the EO allows the Commerce Secretary to target persons who "develop or control" the Restricted Apps, the EO could potentially reach third party software developers or internet service companies that host the Restricted Apps.

In many ways, this ambitious and yet inherently ambiguous regulatory arrangement resembles the EOs against WeChat and TikTok issued in August 2020. Those EOs similarly deferred the task of identifying persons and transactions subject to those orders to further notice from the Commerce Secretary and the Commerce Department. Those EOs remain suspended from implementation because of pending lawsuits in federal district courts. It remains to be seen whether the latest EO will now face similar legal challenges in the courts, which could further undercut the EO's actual impact.

The EO in Context

This new EO builds upon EO 13873 of May 15, 2019, which we summarized [here](#). In EO 13873, the Trump Administration provided the Commerce Department with authority to block or require mitigating measures related to certain transactions involving information and communications technology. Although EO 13873 was neutral as to the source of threats to the United States, given the simultaneous announcement of sanctions on Huawei Technologies Co. Ltd. at the same time by the Commerce Department, the action certainly appeared to target China. The Trump Administration confirmed that focus when it subsequently issued EO 13942 and EO 13943 on August 6, 2020 that targeted transactions involving, respectively, the popular TikTok and WeChat social media platforms. Again, however, both of those earlier EOs remain effectively suspended because of pending litigation and thus have had essentially no practical effect upon their users.

The latest EO similarly targets the popular Chinese mobile phone software that were named as the Restricted Apps. The EO does not actually tie the Restricted Apps to any specific allegations of national security threats or misuse of sensitive information. Instead, the EO only alleges that "the pace and pervasiveness of the spread in the United States of certain connected mobile and desktop applications and other software developed or controlled by persons in the People's Republic of China, to include Hong Kong and Macau (China), continue to threaten the national security, foreign policy, and

economy of the United States.” The EO also claims that, by using the Restricted Apps, U.S. persons might lose control of sensitive personally identifiable information, private information, proprietary information, and other sensitive data that could potentially be accessed and collected by Chinese Government or the Chinese Communist Party. However, rather than provide any specific evidence against the Restricted Apps themselves, the EO merely refers to three other cyber incidents that are generally attributed to China: the 2014 hacking of the personnel records at the Office of Personnel Management, the 2015 hacking of U.S. insurer Anthem, and the 2017 hacking of U.S. personal data maintained by Equifax.

Biden Administration Would Have to Implement EO

Because the EO’s effective date will be several weeks after President-elect Biden’s inauguration, it will actually be up to the incoming Biden Administration to decide how, if at all, and to what extent to implement this new EO. The Biden Administration could opt to delay or decline to take further action under the EO or even to revoke it entirely. Given the EO’s potential sweeping impact on U.S. commerce, particularly because so many personal electronic payments now rely on the Restricted Apps and given the many other pressing issues that will confront the new Biden Administration in the U.S.-China relationship, it is far from certain whether this EO will actually go into effect as its authors intended.

However, the Biden Administration will also face considerable bipartisan, bicameral Congressional pressure to confront and challenge China. If the Biden posture toward China were to seem too “soft,” Congress could conceivably take matters into its own hands and enact new legislation that might mandate specific Executive action against the Restricted Apps or the responsible Chinese companies, as Congress has done recently in imposing other sanctions against certain Chinese and Russian entities.

If you have any questions about this eUpdate, please contact any of the attorneys profiled below. Dorsey’s international trade attorneys routinely assist clients with U.S. national security requirements including economic and trade sanctions. With offices located across the United States, Canada, the United Kingdom, and Asia, Dorsey has extensive experience counseling clients on such cross-border matters.