crowell moring

CLIENT ALERT

Executive Order Prohibits Transactions with Eight Chinese Software Applications

Jan.08.2021

On January 5, 2021, President Trump issued an Executive Order prohibiting transactions "with persons that develop or control" eight "Chinese connected software applications", including Alipay, CamScanner, QQ Wallet, SHAREit, Tencent QQ, VMate, WeChat Pay, and WPS Office (the "order" or the "EO"). The prohibitions, which also apply to subsidiaries of the software developers, would go into effect 45 days from the date of the order, February 19, at the earliest. The order directs the Secretary of Commerce to identify the transactions and targets of the prohibitions *not earlier than* 45 days after the date of the order. Notably, these dates will fall in the Biden Administration, and it's unclear whether the new Administration will elect to implement the order, extend the date of implementation, or revoke the order entirely. There are no current restrictions on dealing with the listed applications or their developers or owners.

A provision in the order suggests that additional software applications may become subject to the prohibitions as the order directs the Commerce Secretary "to continue to evaluate Chinese connected software applications that may pose an unacceptable risk to the national security, foreign policy, or economy of the United States, and to take appropriate action . . . ". The order defines "connected software application" to mean "software, a software program, or group of software programs, designed to be used by an end user on an end-point computing device and designed to collect, process, or transmit data via the Internet as an integral part of its functionality."

Further, the order directs the Commerce Secretary, in consultation with the Attorney General and the Director of National Intelligence, to provide a report to the Assistant to the President for National Security Affairs with recommendations to prevent the sale or transfer of United States user data to, or access of such data by, foreign adversaries, including through the establishment of regulations and policies to identify, control, and license the export of such data. This report is to be provided *no later than 45 days* from the date of the order, so could be completed prior to conclusion of the Trump Administration.

The order, which is strikingly similar to the executive orders issued last August prohibiting transactions with the Chinese-owned parent companies of the mobile applications WeChat and TikTok, cites the same national emergency first set forth in Executive Order 13873 (Securing the Information and Communications Technology and Services Supply Chain). Specifically, the order describes the threat posed by the use of these apps: the collection of sensitive personally identifiable information (PII) made accessible to the government of the People's Republic of China (PRC) and the Chinese Communist Party (CCP). According to the order, the concern – similar to that set forth in the WeChat and TikTok executive orders – extends beyond the ability of the apps to track Federal employees and contractors to the millions of users in the United States, whose use of the apps "would allow the PRC and CCP access to Americans' personal and proprietary information."

The order also cites the PRC's and CCP's "intent to use bulk data collection to advance China's economic and national security agenda", as demonstrated through the 2014 cyber intrusions of the Office of Personnel Management, the 2015 breach of the health insurance company Anthem, and the Department of Justice's indictment of members of the Chinese military for the 2017 Equifax cyber intrusion.

The Commerce Secretary, in consultation with the Secretary of the Treasury and the Attorney General, shall adopt rules and regulations necessary to implement the order under the International Emergency Economic Powers Act (IEEPA).

Commentary

Depending on how the EO is interpreted and implemented, it could, based on the language of the order itself, apply domestically and extraterritorially to prohibit any person from using these software applications while in the United States and prohibit the use of the applications by U.S. persons outside the United States. Similar to the WeChat and TikTok orders, this order leaves ambiguity as to its scope, and its remains for the Commerce Secretary to define the "transactions" subject to the prohibitions and the persons to which it applies. For example, as was an initial question upon the issuance of the WeChat order, Tencent has ownership stakes in several U.S. companies other than Tencent QQ, especially in the video gaming industry. Accordingly, using the EO as grounds for prohibiting transactions with other companies or apps backed by Tencent could have far-reaching effects.

Also of note is the provision requiring a report with recommendations to prevent the sale or transfer of United States user data to, or access of such data by, foreign adversaries. This provision could be used as the basis for an entirely different set of policies and regulations designed to halt the transfer of U.S. person user data, whether done intentionally through a sale, business transfer, or as a result of inadequate safeguards (while "personally identifiable information" is defined in the order, "user data" is not). The term "foreign adversaries" is not defined in the EO, and the report could therefore touch broader group of nations than the China-specific elements of the current order. Given that almost every consumer facing business today collects personal data and accumulates that data rather readily, such regulations could disrupt existing business models that include the sale or transfer of user data or require more stringent security protocols.

Despite the litigation that has resulted in court orders preliminarily enjoining the WeChat and TikTok bans from taking effect, this order largely mirrors those August 2020 executive orders, and perhaps answers the lingering question of whether those orders would serve as a template for future ones targeting additional Chinese software applications. Concerns over the collection of sensitive information and subsequent access by the PRC government has also been part of the rhetoric surrounding the Clean Network program, which includes in its five lines of effort the goal of removing trusted apps from untrusted PRC smartphones and their app stores.

This order is the latest in a series of actions that have targeted Chinese-owned companies over the past several months. This includes, but is not limited to: (1) an Executive Order issued in November 2020 that prohibits certain investments in designated Chinese companies with military ties; (2) expanded export controls (*e.g.*, Entity List designations) of several of the entities on the list; (3) the Clean Network initiative's targeting of Huawei; (4) recent restrictions by the Federal Communications Commission (FCC) that prohibit the use of universal service funds to purchase Huawei and ZTE equipment; (5) additional action by the FCC regarding several Chinese-owned telecoms, including China Mobile and China Telecom, both of which were named as Communist Chinese military companies by the Department of Defense and subject to Executive Order 13959; (6) a set of executive orders in August that targeted the mobile applications TikTok and WeChat (the Department of Commerce's implementing rules have been temporarily enjoined by court order); and (7) the Committee on Foreign Investment in the United States' (CFIUS) rejection of several transactions involving Chinese-owned companies as part of a stricter approach towards Chinese investment in the United States.

U.S. businesses, persons and institutions potentially affected by the new EO should, at a minimum, assess the degree to which their current or planned operations may be affected by the order, monitor developments and where appropriate provide input to the Executive Branch about further definition, implementation and impact of the order.

For more information, please contact the professional(s) listed below, or your regular Crowell & Moring contact.

Caroline E. Brown
Partner – Washington, D.C.
Phone: +1 202.624.2509
Email: cbrown@crowell.com

Evan Y. Chuck
Partner – Shanghai, Los Angeles
Phone: +1 213.310.7999
Email: echuck@crowell.com

Robert Holleyman
Partner and C&M International President & CEO – Washington, D.C.
Phone: +1 202.624.2505
Email: rholleyman@crowell.com