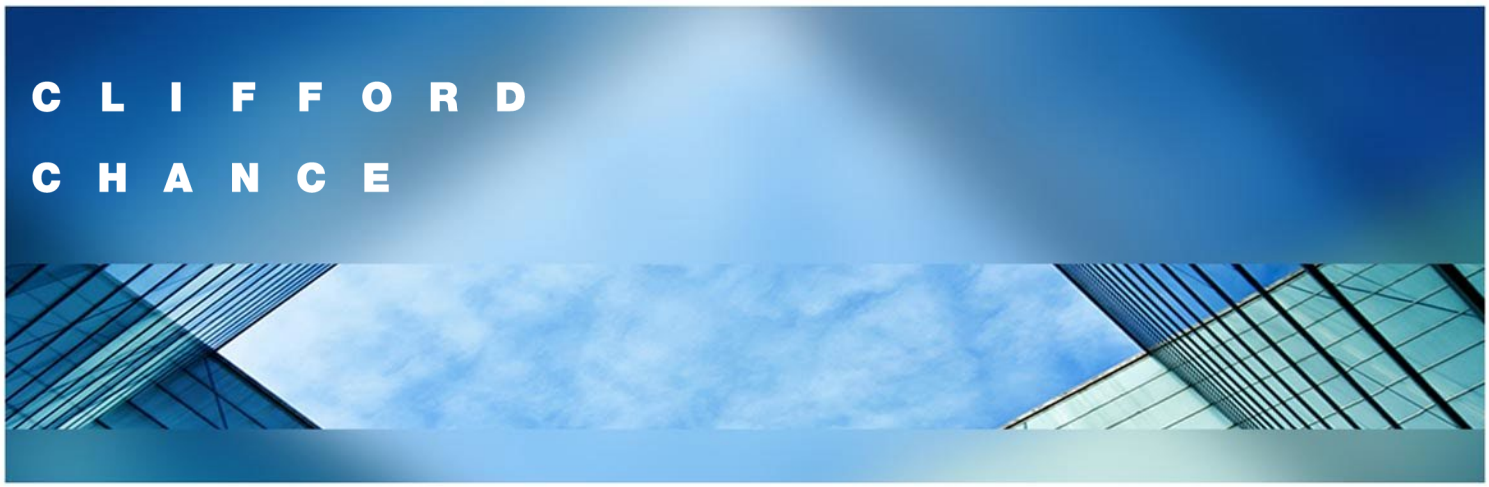

THE LATEST DOWNLOAD ON APPS: NEW RISKS FOR COMPANIES OPERATING IN BOTH THE US AND CHINA

President Biden continues to sharpen the focus and approach of the US government on tech, cyberthreats, human rights, and China. Most recently, the administration has suggested that the Department of Commerce is considering issuing subpoenas to collect information about certain software applications and ban or negotiate conditions for their use in the United States. At the same time, China has enacted new laws designed to counter further US restrictions with its own counter-measures. US companies doing business in China or with Chinese entities, Chinese clients doing business in the United States, and international companies doing business in both jurisdictions should assess their individual risks of being caught between competing legal frameworks and should anticipate their mitigation strategies.

On June 9, 2021, President Biden issued an Executive Order (EO 14034) on "Protecting Americans' Sensitive Data from Foreign Adversaries" to further address the national emergency with respect to the information and communications technology and services supply chain that was declared in the May 15, 2019 Executive Order (EO 13873) "Securing the Information and Communications Technology and Services Supply Chain." EO 13873 specifically targets connected software designed, developed, manufactured, or supplied by persons owned or controlled by, or subject to the jurisdiction or direction of, a foreign adversary. The list of “foreign adversaries” as defined under EO 13873 currently consists of the People's Republic of China (including Hong Kong), Cuba, Iran, North Korea, Russia, and the Venezuelan politician Nicolás Maduro. This list is subject to periodic review by the Commerce Department which may revise or amend the list based on consultation with appropriate US government agency heads.

Specifically, EO 14034 revokes and replaces several Trump-era Executive Orders, notably, those which should ban US persons from using certain foreign-

owned apps like WeChat and TikTok. In addition, EO 14034 calls for a new "risk-based analysis" of certain foreign- owned and controlled apps and calls specifically on certain US government agencies to recommend additional measures to address these risks, signalling that the Biden administration is committed to implementing additional restrictive measures, as deemed necessary, in this space.

EO 14034 fits within the administration's overall strategy to address the threat posed by China and certain foreign adversaries when it comes to emerging technologies, cyber security, and sensitive personal data. EO 14034 identifies the administration's concern regarding the potential that "*connected software applications can access and capture vast swaths of information from users, including United States persons' personal information and proprietary business information*."

Additionally, EO 14034 signals that the US government is scrutinizing apps associated with human rights abuses. The EO proclaims that "*the United States seeks to promote accountability for persons who engage in serious human rights abuse. If persons who own, control, or manage connected software applications engage in serious human rights abuse or otherwise facilitate such abuse, the United States may impose consequences on those persons in action separate from this order*."

Specific Measures of EO 14034

EO 14034 revokes three Trump-era EOs that sought to ban several foreign-owned apps including WeChat, TikTok, and certain other Chinese apps. US courts had previously blocked implementation of the WeChat and TikTok prohibitions, so the prohibitions never went into effect. However, compared to the Trump-era EOs, EO 14034 is better positioned to withstand judicial scrutiny and could be used to accomplish the same end result against the same entities. This approach appears to indicate that the Biden administration intends to adopt a standards-based approach with regard to foreign adversaries, which stands in contrast to the approach used by the Trump administration.

Further, EO 14034 calls on the US Department of Commerce ("Commerce"), in consultation with the Departments of State, Defense, Health and Human Services, Homeland Security, the Attorney General, and the National Director of Intelligence, among other agencies, as deemed appropriate, to issue a report within 120 days (i.e., by October 7, 2021) on recommendations to protect US data acquired or accessible by companies owned or controlled by foreign adversaries. The EO also directs Commerce to provide recommendations concerning additional measures to be taken to address the national security risks posed by certain "connected software applications" within 180 days (i.e., by December 6, 2021). "Connected software application" is defined in EO 14034 to mean software, a software program, or a group of software programs that is designed to be used on an end-point computing device and includes as an integral functionality the ability to collect, process, or transmit data via the Internet. Commerce's review is limited to those connected software applications that are designed, developed, manufactured, or supplied by persons owned or controlled by or subject to the jurisdiction or direction of a foreign adversary (as previously

noted, which are currently defined to include China (including Hong Kong), Cuba, Iran, North Korea, Russia, and Venezuelan politician Nicolás Maduro).

In addition, EO 14034 calls for a "rigorous, evidence-based analysis" which identifies risk factors including: ownership, control or management by persons that support a foreign adversary's military, intelligence or proliferation activities; use of the connected software applications to conduct surveillance that enables espionage, including through a foreign adversary's access to sensitive or confidential government or business information, or sensitive personal data; ownership, control or management of connected software applications by persons subject to coercion or cooption by a foreign adversary; control or management of connected software applications by persons involved in malicious cyber activities; a lack of thorough and reliable third-party auditing of connected software applications; the scope and sensitivity of the data collected; the number and sensitivity of the users of the connected software application; and the extent to which identified risks have been or can be addressed by independently verifiable measures.

As part of the risk analysis, Commerce may, and ultimately is expected to, issue subpoenas to collect information about certain software applications. The likely results of this information collection will be restrictions, including potential bans or negotiated conditions for the use of these apps in the United States. The apps potentially covered by the review include several popular apps in addition to TikTok and WeChat that were targeted by the Trump executive order. This review could have significant ramifications both for these apps and for global business partners of the developers of these apps. Though the recent EO does not exclusively target China and addresses any app owned by a "foreign adversary," the immediate intended target is China. Escalating tensions between the United States and China, the US administration's concern over Chinese government's control over entities, and the widespread use of Chinese apps by Americans will result in heightened scrutiny by the US government of Chinese software and technology in the United States. Commerce will begin its review immediately in order to identify the apps to be designated under EO 14034. Until Commerce releases its reports, US companies should proactively evaluate their software applications with respect to the pending restrictions, paying special attention to those developed in China and other restricted "foreign adversaries".

Chinese Counter-Measures

Any future restrictions targeting China by the Biden administration could force global companies operating in China to face challenging conflicts-of-laws questions due to China's recent Anti-Foreign Sanctions Law passed on June 10, 2021. The Anti-Foreign Sanctions Law provides a legal basis for the State Council of China to introduce retaliatory sanctions in response to foreign sanctions targeting the internal affairs of China, such as those related to Xinjiang and Hong Kong. The law expands existing authorities to create a counter-sanction list and codifies a private right of action for parties to sue for losses resulting from foreign sanctions. The law enables Chinese citizens and organizations to file suit against individuals, their families, and organizations responsible for enforcing foreign sanctions. Additional measures include deportation, refusing visas or denying entry, freezing properties, and restricting relevant transactions and cooperation.

China has clearly signaled that it would take proportional responses to increased US actions.

Managing the Risk Going Forward

The Biden administration's EO 14034 keeps the pressure on Chinese technology companies and indicates that further restrictions that are more likely to withstand US judicial scrutiny are almost certainly forthcoming. Coupled with China's recent Anti-Foreign Sanctions Law, this creates additional uncertainty for all companies operating both in the US and China that may get caught between the competing national interests. Such companies will be well-advised to closely monitor these developments, assess their current and reasonably possible risk exposure, and update their risk mitigation strategies, including possible subpoena requests and risks if certain apps are banned/restricted or present unmanageable reputational risks.

Any advice above relating to the PRC is based on our experience as international counsel representing clients in business activities in the PRC and should not be construed as constituting a legal opinion on the application of PRC law. As is the case for all international law firms with offices in the PRC, whilst we are authorised to provide information concerning the effect of the Chinese legal environment, we are not permitted to engage in Chinese legal affairs. Our employees who have PRC legal professional qualification certificates are currently not PRC practising lawyers. This publication does not necessarily deal with every important topic or cover every aspect of the topics with which it deals. It is not designed to provide legal or other advice.

CLIFFORD
CHANCE

CONTACTS

David DiBari
Managing Partner

T +1 202 912 5098
E david.dibari
@cliffordchance.com

Joshua Berman
Partner

T +1 202 912 5174
E joshua.berman
@cliffordchance.com

Renée 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

Carol Lee
Associate

T +1 202 912 5194
E carol.p.lee
@cliffordchance.com

Laurence Hull
Associate

T +1 202 912 5560
E laurence.hull
@cliffordchance.com

Holly Bauer
Associate

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

Karina Bashir
Associate

T +1 202 912 5010
E karina.bashir
@cliffordchance.com

Christine Chen
Associate

T +1 202 912 5081
E christine.chen
@cliffordchance.com

www.cliffordchance.com

Clifford Chance, 31 West 52nd Street, New York, NY 10019-6131, USA

Clifford Chance US LLP

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

Clifford Chance has a co-operation agreement with Abuhimed Alsheikh Alhagbani Law Firm in Riyadh.

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