ANALYSIS

TikTok Given Little Room to Maneuver as Broad Fears of Chinese Surveillance Prevail

The case against TikTok is the latest example of growing U.S. scrutiny of the overseas operations of Chinese companies amid worsening relations between the two countries. The U.S. is especially concerned about potential Chinese access to the personal data of U.S. citizens.

August 16, 2020 at 11:01 PM

By Vincent Chow | August 16, 2020 at 11:01 PM

TikTok is shaping up to be yet another casualty in the ongoing U.S.-China conflict.

The popular video-sharing app is fighting for its survival in the U.S. as the Trump administration inches closer to banning it from the market. But the lack of clarity in the legal bases for the sweeping actions is leaving the Chinese-owned company with limited options to respond.

“The real point of dispute for TikTok is that it’s a Chinese-owned company, therefore the U.S. government believes the Chinese government has access to the data under Chinese law,” said Jason Waite, an international trade and investment partner at Alston & Bird in Washington, D.C.

Earlier this month, President Donald Trump issued an executive order banning TikTok from the U.S. after Sept. 20 on national security grounds. Specifically, Trump alleged that the Chinese Communist Party could use TikTok to gain access to Americans’ personal and proprietary information, potentially allowing the country to “track the locations of Federal employees and contractors, build dossiers of personal information for blackmail, and conduct corporate espionage.”

The case against TikTok is the latest example of growing U.S. scrutiny of the overseas operations of Chinese companies amid worsening relations between the two countries. Last year, the U.S. banned Chinese telecom giant Huawei, stating that obligations of Chinese companies under China’s state security apparatus meant the company posed national security risks to the U.S.

In the case of TikTok, the allegations also demonstrate the U.S. government’s increasingly aggressive approach to tackling national security risks associated with Chinese access to the personal data of U.S. citizens.

“The recent actions must be seen in the context of an increasing focus by the U.S. government on concerns over foreign access to data of U.S. citizens,” said Scott Flicker, chair of Paul Hastings’ Washington D.C. office and head of the firm’s global trade controls practice.

The administration's interest in TikTok preceded the executive order. The app, a subsidiary of Chinese internet technology company ByteDance Ltd., has been under investigation since last year by the Committee on Foreign Investment in the United States, or CFIUS, for its 2017 acquisition of U.S. video app Musical.ly. The Treasury-led interagency body that probes foreign investment transactions with national security concerns has the authority to suspend or recommend termination of inbound investment. It may also impose mitigation measures as a condition for clearing transactions.

Waite said the collection of personal data is a known and ongoing concern of CFIUS, and other mobile applications have been subject to CFIUS review.

In its latest annual report covering its work in 2019, CFIUS specified several key examples of mitigation measures negotiated with parties under review during the year. Several of these were directly related to the collection and handling of personal data, including establishing guidelines for handling U.S. government customer information, allowing only authorized persons to have access to customer information, and restricting access of the foreign acquirer to sensitive information.

So far, CFIUS' conclusion regarding TikTok remains unclear. But the executive order and the fact that ByteDance has been in talks with Microsoft Corp. to sell TikTok's U.S. business indicate that a divestment is inevitable.

"I'm not sure why in TikTok's case mitigation does not appear to be an option. It could be the sheer size of the data platform, it could be the fact that it's been in operation for a couple of years," Waite said.

"When it comes to personal data, mitigation involves very technical analysis that I suspect TikTok has tried to do," he said. "There are other personal data cases where there has been mitigation where CFIUS has been satisfied with mitigation measures committed to by parties."

In TikTok's case, China's own data security regime could be of grave concern. Aimen Mir, a partner at Freshfields Bruckhaus Deringer based in Washington D.C. and former deputy assistant secretary for investment security at the Department of the Treasury from 2014 to 2018, believes that China's National Intelligence Law and Counterespionage Law are likely to be driving the U.S. government's concerns about TikTok.

First, Article 7 of the 2017 National Intelligence Law states that "any organization or citizen shall support, assist and cooperate with the state intelligence work in accordance with the law." And Article 22 of the 2014 Counterespionage Law states that "when the state security organ investigates and understands the situation of espionage and collects relevant evidence, the relevant organizations and individuals shall provide it truthfully and may not refuse."

These two Chinese laws were invoked last year by the Trump administration as the legal bases for blacklisting Huawei. And in the months prior to the Huawei ban, legal experts in China and the U.S. submitted legal opinions during Federal Communications Commission proceedings concerning the obligations of Huawei to participate in China's state security campaigns.

"[The] question is not what Chinese law says about the ability of the Chinese government to tell companies like Huawei what to do. The question is what the Chinese government can actually do, regardless of what the law might say."

Backing up Huawei's assertions that it is under no obligation to cooperate with the Chinese government, Jihong Chen and Jianwei Fang, partners at Zhong Lun Law Firm in Beijing, argued that the National Intelligence Law protects the "legitimate rights and interests" of organizations. Therefore, Huawei need not cooperate with the Chinese government, as that could lead to punishment under U.S. law, which would contravene those legitimate rights and interests. They also argued that Chinese laws including the National Intelligence Law and the Counterespionage Law regulate only Chinese entities and do not apply to overseas subsidiaries.

Their arguments were rebutted by Donald Clarke, a law professor at George Washington University Law School and a well-known expert in Chinese law. On the point of extraterritorial application of Chinese laws, he argued that overseas subsidiaries are subject to Chinese laws by dint of their parent companies being subject to Chinese laws. Moreover, he contended that language in Chinese laws about protecting "legitimate rights and interests" is "essentially meaningless boilerplate."

Whereas the Zhong Lun partners' analysis sought to directly refute claims that China's laws provide for obligations on Chinese companies and their overseas subsidiaries to cooperate with Chinese state security efforts, Clarke's rebuttals focused more on what companies are obligated to do in practice.

"[The] question is not what Chinese law says about the ability of the Chinese government to tell companies like Huawei what to do," he said. "The question is what the Chinese government can actually do, regardless of what the law might say."

President Trump's executive order suggests that CFIUS might have sided with Clarke's analysis of these Chinese state security laws, although the committee, known for its opaque operations, does not disclose its reviews or the reasoning behind its decisions.

"[The general public doesn't] get reports on what reviews are happening but the parties do receive indication of that. But even what the parties receive sometimes is not the entire set of concerns," Waite said.

In 2018, Congress passed the Foreign Investment Risk Review Modernization Act (FIRRMA), which made several significant changes to the CFIUS review process. One of these was an expansion of CFIUS's authority to put greater focus on companies that collect sensitive personal data of U.S. citizens.

According to TikTok's privacy policy, it automatically collects a range of "internet or other network activity information" from its users including IP addresses, geolocation-related data, unique device identifiers, browsing and search history, and cookies. The company claims to have 100 million users and approximately 1,500 employees in the U.S.

Read More:

CFIUS Is Slowing Chinese Investment in the US to a Crawl

China Outbound Investment Decline Continues, Inbound Rises Amid COVID and Regulatory Challenges

Wilson Sonsini Helps Secure CFIUS Clearance for Chinese Acquisition