天同律师事务所 TIANTONG LAW FIRM

CLEARY GOTTLIEB

Introduction to the TianTong Law Firm – Cleary Gottlieb China Initiative

This is the first client briefing in a series to be prepared by leading Chinese law firm TianTong Law Firm and international law firm Cleary Gottlieb Steen & Hamilton LLP following developments relevant to Chinese companies doing business in the United States and U.S. companies working in China. The initiative aims to comprehensively follow developments with perspectives from leading lawyers in the U.S. and China, providing timely and integrated advice to our respective clients. Cleary Gottlieb litigators based in New York and Washington D.C. have partnered with TianTong lawyers based in Beijing in this joint initiative.

* * *

U.S. Regulatory Challenges for Chinese Companies: The TikTok Case Study

Data privacy concerns give U.S. regulators grounds to investigate and fine Chinese technology companies like ByteDance, which may be forced to reverse its $1 billion acquisition of Muscial.ly

Political tensions between the United States and China have brought Chinese companies increasingly into the focus of U.S. authorities. In the last year, Chinese companies have faced increasingly severe scrutiny across a variety of different regulatory regimes. TikTok's experience facing regulatory and legal scrutiny in the U.S. on both privacy and national security grounds is illustrative of the challenges Chinese firms may encounter from U.S. authorities – and how the long arm of U.S. regulation may affect even foreign transactions.

Background

In November 2017, the company which is now the world's most valuable startup bought what then became the world's No. 1 app on the iOS App store. The Beijing-based media and technology company ByteDance – which was valued at $75 billion at the end of 2018, overtaking Uber – acquired the teen karaoke app Musical.ly for $1 billion as part of a strategy to break into the U.S. market. Musical.ly was a popular Shanghai-based social media company founded by Chinese entrepreneurs Alex Zhu and Luyu Yang. At the time it was acquired, Musical.ly had 60 million users in the U.S. and Europe.

While ByteDance initially agreed that Musical.ly would operate a separate product, Musical.ly was later merged into ByteDance's own Chinese-based app – TikTok. In May 2019, the former Musical.ly, Inc., registered in California, officially changed its name to TikTok Inc., and is the entity currently responsible for operating TikTok. TikTok's growth quickly catalyzed ByteDance's record-breaking valuation. ByteDance is one of the few Chinese technology companies to grow an audience of hundreds of millions of users outside its home market. Since October 2019, ByteDance has gradually separated TikTok from its own Chinese version of the app, "Douyin."

How did a transaction involving two successful Chinese companies come under fire by U.S. regulators, raising the possibility that ByteDance will be forced to sell off TikTok? What are the general risks that

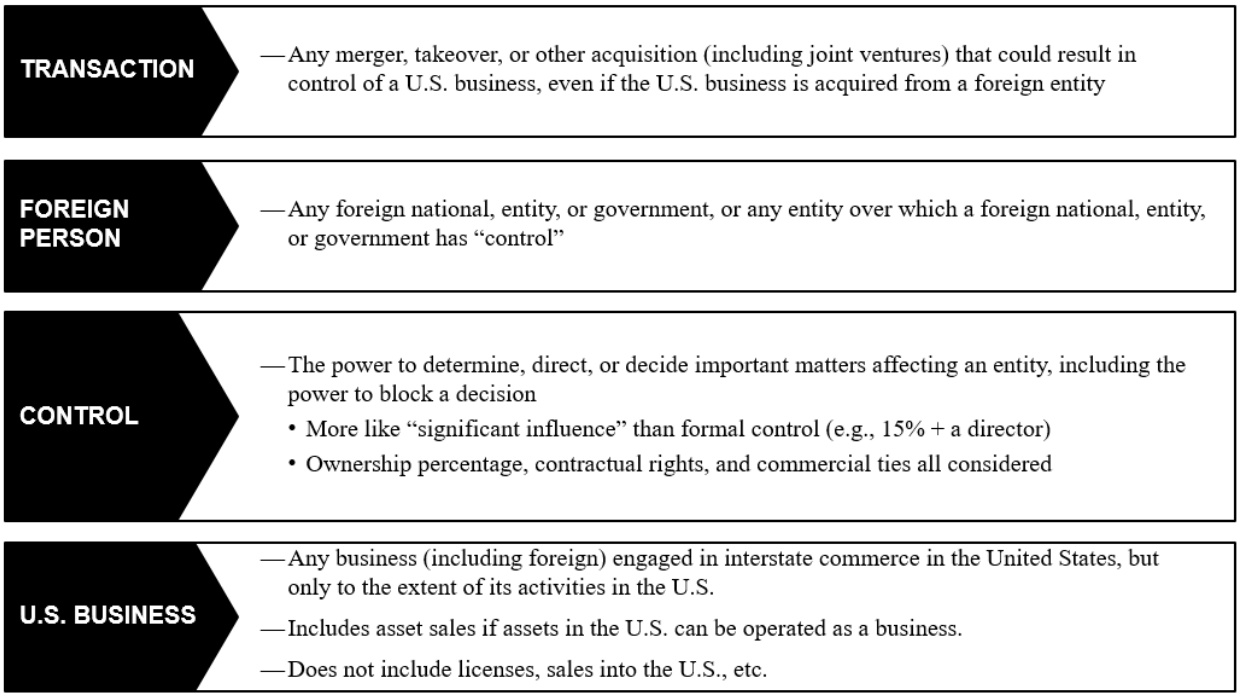
Chinese technology companies should be aware of when entering the U.S. market, and what compliance measures can be taken to mitigate these risks?

Relevant Legal Issues

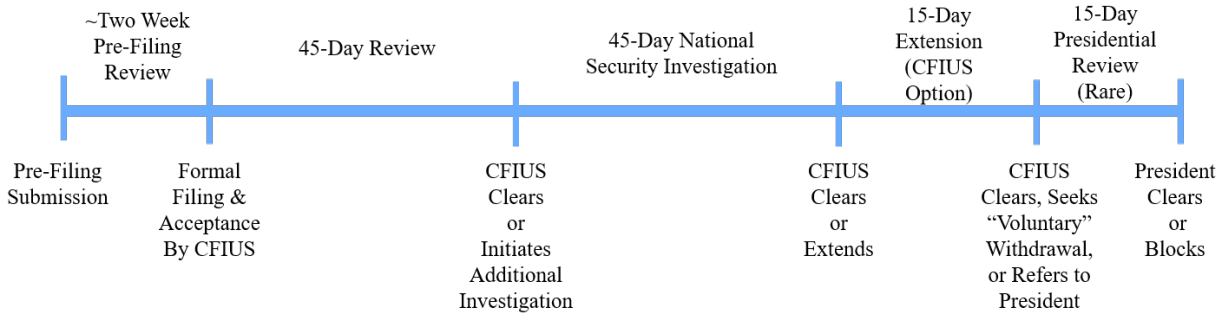
In the last year, TikTok has faced a slew of legal action in the U.S. across a wide variety of fronts. The most prominent of these is a national security review by the U.S. government's Committee on Foreign Investment in the United States (CFIUS).

Overview of CFIUS. CFIUS is an interagency committee charged with reviewing the national security implications of transactions that involve the acquisition of a U.S. business by a foreign person. Established by Executive Order 11858 in 1975, it is governed by the Exon-Florio Amendment (1988), the Foreign Investment and National Security Act (FINSA) (2007), and most recently, the Foreign Investment Risk Review Modernization Act (FIRRMA) (2018) and implementing regulations. CFIUS is chaired by the U.S. Secretary of the Treasury and consists of representatives from 16 government agencies and offices, including the Director of National Intelligence and Secretary of Labor.

CFIUS has the authority to review "Covered Transactions", which include any "transaction" by or with any "foreign person," which could result in "control" of a "U.S. business" by a foreign person.



The timeline for a CFIUS review begins from CFIUS "acceptance" of the discretionary filing. A realistic timeframe for a transaction with substantive issues is four to eight months, including drafting. Possible review outcomes include CFIUS clearing a transaction, clearing it with conditions, or recommending that the President block or unwind the transaction. CFIUS does not provide a reasoned decision to the parties, and by statute, there is no judicial review of its national security determination.



Historically, CFIUS notification has been voluntary for most transactions, with CFIUS reserving the right to compel a review either *a priori* or post-closing. However, new regulations which came into effect on February 13, 2020, implementing FIRRMA, imposed mandatory filing requirements for (1) foreign investments in businesses that develop "critical technologies" and also (2) for certain transactions in which an entity controlled by a foreign government acquires a "substantial interest" in an unaffiliated U.S. business involved in critical technologies, critical infrastructure, or sensitive personal information (TID U.S. Businesses).[1] These regulations are consistent with CFIUS's practice in recent years, which has also focused on transactions in the semiconductor space, "big data," telecommunications and cybersecurity, and the integrity of the defense industry/government supply chain.

CFIUS national security review of TikTok. Because the ByteDance acquisition of Musical.ly involved the acquisition of a U.S.-registered business by a Chinese company, it was a covered transaction subject to CFIUS review. Although ByteDance was not required to voluntarily seek CFIUS approval when it bought Musical.ly, CFIUS reserves the right to review any covered transaction even after the transaction has closed, and also retains the right to recommend unwinding the transaction.

It was the issue of sensitivity around personal information which triggered CFIUS to retroactively open a review of TikTok. Last September, *The Guardian* newspaper published an article suggesting that TikTok censors its content in line with Chinese foreign policy goals. U.S. Senators reacted by calling on CFIUS to retroactively assess the national security risks posed by TikTok. These Senators referenced new Congressional guidelines on the protection of personal information and cited a concern that the Chinese government would have access to the company's U.S. user data, due to a 2017 Chinese national intelligence law which requires Chinese companies to comply with the government's intelligence gathering operations. CFIUS subsequently opened an investigation.

There is a risk that ByteDance may be required by CFIUS to sell TikTok, similar to when CFIUS caused Chinese gaming company Kunlun to agree that it would sell the popular gay dating app Grindr by June 2020. That investigation was also based on personal information concerns. Kunlun had similarly not submitted its acquisition of Grindr for CFIUS review. Media reports suggest that a TikTok stake sale would likely push back any imminent plans by ByteDance to IPO. TikTok is accordingly engaged in mitigation talks with CFIUS about measures it can take to avoid divesting the Musical.ly assets.

Key Takeaways

Increasingly, U.S. policy priorities appear to be influencing enforcement of U.S. law with respect to foreign firms, particularly in sensitive fields such as data privacy and national security. For such firms, it

1. Note that there is a possibility CFIUS may consider the definition of "U.S. Businesses" under FIRRMA to reach non-U.S. operations, indicating a potential expansion of CFIUS jurisdiction to non-U.S. activities.

is therefore important to think strategically and proactively about how to anticipate and preemptively address issues that may invite regulatory scrutiny. In the case of TikTok, a number of lessons emerge:

- **Anticipate CFIUS review.** CFIUS filings are mandatory with respect to a broad array of transactions in which foreign persons either take control of U.S. businesses as well as when foreign persons take non-controlling interests in businesses in various strategic sectors, including technology, infrastructure, and businesses holding sensitive personal information. Companies seeking to invest in U.S. businesses should anticipate CFIUS review and plan, with the advice of relevant experts, as part of their deal strategy.

- **Consider pro-active mitigation.** Foreign investors should consider pro-active mitigation that may be negotiated with U.S. companies. Most often, this may include changes to the foreign management structure, including the introduction of U.S. persons to the board of directors. Such steps may not be realistic options for foreign state-owned or state-controlled enterprises, but such entities may consider alternatives such as structuring their investments through intermediary entities that are controlled by U.S. persons. Alternative potential mitigation steps include separating U.S. and foreign operations. Anticipating the CFIUS review, ByteDance separated TikTok's product, business development, marketing, and legal teams in late 2019. ByteDance has additionally sought to build up its U.S. operations, establishing additional U.S. data centers to segregate local information.

- **Invest in foreign expertise.** Relying on outside expertise, particularly (in the case of U.S. exposure) from U.S. consultants or outside experts who have strong domestic reputations, may support arguments against regulatory scrutiny. Foreign firms looking to bolster their credentials before U.S. authorities may successfully do so with the addition of foreign expertise – which may provide comfort to U.S. authorities, who are often circumspect that Chinese firms may be subject to significant government influence. Likewise it is critical to involve experienced U.S. CFIUS counsel from the early stages of deal planning. More information on Cleary Gottlieb's experience is available here: https://www.clearygottlieb.com/practice-landing/international-trade-and-investment.

- **Implement transparent data privacy and content moderation policies.** In response to the CFIUS investigation, TikTok issued a statement on its data security and content moderation policies. TikTok purports to store all TikTok U.S. user data in the U.S., with a backup of data in Singapore. Additionally, none of TikTok's data centers are located in China, and none of its data is subject to Chinese law. It also has a team specifically dedicated to issues of cybersecurity, data privacy, and general data security. Likewise, TikTok's content moderation team is based in California. The team is mandated to review content for compliance with U.S. policies. TikTok has retired the content moderation guidelines that were published by *The Guardian* and gave rise to U.S. regulators' concern.

- **Anticipate and plan for delay.** While CFIUS review is constrained to specified review periods – an initial 45-day review period, followed by a 45-day investigation period in case the initial review identifies a potential concern – in practice the review period can be much longer because CFIUS can "stop the clock" for a variety of reasons, in particular by requiring refiling of the application which may have the effect of resetting the review period.

* * *

TianTong Commentaries: Chinese Enforcement Agencies' Power of Obtaining Personal Information

Overview of the PRC Personal Information Protection Law Regime

Presently, China has not promulgated a unified law on personal information protection. Rules of personal information protection are splintered across various laws, administrative regulations and industry standards centering around the PRC Cybersecurity Law.[2] Article 76 of the Cybersecurity Law, which came into effect on June 1, 2017, defines "personal information" as "information which is recorded in electronic or other formats and used alone or in combination with other information to recognize citizens' identities, including but not limited to citizens' names, dates of birth, ID numbers, biological identities, addresses and telephone numbers." According to this definition, the user data collected by online platforms, including but not limited to registration information, account information, payment information, correspondence information and telecommunication, all belong to the category of "personal information" under the Cybersecurity Law.

Article 42 of the Cybersecurity Law stipulates the duty of network operators to maintain strict confidentiality of the personal information they collect, but the Law also specifies exceptions to such duty. For instance, Article 28 of the Law provides that "network operators shall provide technical support and assistance to the public security and state security authorities in their attempts to safeguard national security and investigate criminal offenses." This implicates that businesses subject to the regulation of the Cybersecurity Law are obliged to provide law enforcement agencies with users' personal information they have collected without the prior consent of those users. [3]

Limitations on Chinese Law Enforcement Agencies' Power

However, certain restrictions on law enforcement agencies' obtainment of personal information do exist: (1) law enforcement agencies must be authorized by laws and regulations; (2) the scope and procedures of the information obtainment shall comply with relevant statutes and regulations. The below table lists, under Chinese law, the agencies which have the power to collect personal information from network operators, their respective authorization basis, the circumstances and the scope of the information collection process, and the relevant procedures or restrictions.[4]

2. The main Chinese laws concerning personal information protection include: Cybersecurity Law, Administrative Measures for Internet Information Services, Provisions on Protecting the Personal Information of Telecommunications and Internet Users, and Personal Information Security Specification.

3. Pursuant to Articles 2, 10, and 76 of the Cybersecurity Law, "network operator" is the owner, manager, and network service provider. Among them, "network service provider" refers to subjects that provide services through the Internet. Therefore, the Cybersecurity Law applies not only to traditional Internet companies, but also to all commercial subjects providing products and services through the Internet.

4. Owing to space limitations, the table is not exhaustive.

Agencies	Authorized by	Circumstances	Scope	Procedures or Restrictions
The People's Procuratorates Public Security Organs	Criminal Procedure Law Cybersecurity Law Provisions on Several Issues concerning the Collection, Obtainment, Examination, and Judgment of Electronic Data in the Handling of Criminal Cases Rules of Obtainment of Electronic Data as Evidence by Public Security Authorities in Handling Criminal Cases	When handling criminal cases, the People's Procuratorates and the public security organs can collect and obtain electronic data from internet service providers	Information published by internet platforms Correspondence information including text messages and electronic mails User information including registration information, identity authentication information, and electronic transaction records Electronic documents including texts pictures, audios and videos	Investigation organs obtaining electronic data shall produce a Notice of Evidence Obtainment, specifying the relevant information on the electronic data needed and notifying the internet service provider to comply with Electronic data obtained by public security organs must be pertinent to the case investigated, materials irrelevant to the case shall be returned or destructed
State Security Organs	National Security Law Cybersecurity Law National Intelligence Law	To obtain information on acts impairing national security, the state security organs have the right to gather evidence from Chinese citizens and organizations	Information concerning acts impairing national security	Employees of the state security organs shall produce their credentials when performing official duties Any person or organization has the right to report or make an accusation to the state security organ at a higher level about a state security organ or its employees, exceeding or abusing their authority or their other unlawful conduct
The Cyberspace Administration	Cybersecurity Law Critical Information Infrastructure Security Protection Regulations (Opinion-seeking Draft) Measures for Security Assessment of	When a significant amount of personal information collected in China is made available overseas, the Cyberspace Administration has the power to conduct safety assessments of the cross-border data The Cyberspace Administration has the power to make random safety examinations on critical information	Personal information collected within the territory of China that is provided overseas Personal information and important data that are generated as a result of critical infrastructure operators' activities within the territory of China	The Cyberspace Administration shall limit its use of information obtained from safety examinations on critical information infrastructures to the maintenance of internet security only

	Cross-border Transfer of Personal Information and Important Data (Opinion-seeking Draft)	infrastructures		
Administrative Departments for Industry and Commerce	Law on Administrative Penalty Interim Provisions on the Procedures for Administrative Punishments for Market Supervision and Administration Guiding Opinions of State Administration for Industry and Commerce on Administrative Departments for Industry and Commerce Obtaining Electronic Data as Evidence Administrative Measures for Online Trading	When the administrative departments for industry and commerce investigate unlawful online transactions and related services, they may obtain electronic evidence from relevant service operators, including third-party trading platforms providing network access, payment and settlement, logistics, and delivery services for online commodity transactions	Electronic data that can be the proof of or are relevant to unlawful acts Personal information, including registration information, contact information, transaction data and address of online commodity traders suspected of unlawful business operation	The obtainment of electronic data shall be carried out by at least two investigators, who shall produce their credentials to the relevant parties. If the collection and obtainment of evidence is carried out for the first time, investigators shall inform the relevant parties about their rights to statement, to defend oneself, and to apply for challenge With the exception of electronic evidence pertinent to the cases being investigated, the investigators shall not make copies of or leak at will the private information and business secrets stored in the computer system of the relevant parties

TikTok Case Analysis

Could the Chinese government obtain electronic data, including personal information, collected by Chinese technology companies that conduct business overseas like ByteDance? We believe that the power of law enforcement agencies to obtain data from relevant organizations is regulated by Chinese law and therefore is not unfettered.

First, although the Cybersecurity Law may have jurisdiction over corporations outside of China, the chance of it applying to TikTok is relatively slim. Article 2 of the Cybersecurity Law provides that the law shall apply to "the construction, operation, maintenance and use of the network within the territory of the People's Republic of China." According to the "Information Security Technology- Guidelines for Data Cross-Border Transfer Security Assessment," issued by the National Information Security Standardization Technical Committee, "operating within the territory" means: (1) conducting business within the territory of China, or (2) providing products or services within the territory of China. More specifically, this includes using the Chinese language, using CNY as the clearing currency, and

distributing goods and commodities in China. Accordingly, even if a company is registered overseas, it may be considered as "operating within the territory of China" if it conducts business or provides goods and services to Chinese customers. Such a company would be subject to the Cybersecurity Law and shall comply with the duty to disclose information as required by the statutes. However, as long as TikTok does not take part in business in China and does not provide any product or service to individuals or organizations in China, the risk of it being caught by the Cybersecurity Law would remain relatively low.

Second, for a subsidiary company registered in a foreign country and conducting business overseas, certain precautionary measures could be made to reduce its risk of being regulated by Chinese law enforcement agencies. The company could make a policy that prevents sharing data with the Chinese parent company and store its overseas users' information in separate servers and data centers outside China. However, if cross-border data sharing is permissible within the corporate group, like TikTok have stated in its privacy policy,[5] the risk of overseas users' information being disclosed to Chinese government may increase accordingly.

* * *

This client briefing is the result of a collaboration between TianTong Law Firm (http://www.tiantonglaw.com) and Cleary Gottlieb Steen & Hamilton LLP (www.clearygottlieb.com) to monitor and address legal developments that may be of interest to our clients in China, the United States and around the world.

TianTong Law Firm is a leading Chinese law firm solely dedicated in complex civil and commercial dispute resolution. The firm has consistently been recognized by Chambers and Partners and Asian Legal Business as a leading firm in dispute resolution. Headquartered in Beijing, TianTong has established six branches across the country. In the past decade, TianTong has been keeping one of the highest winning rates among all Chinese firms before the Supreme People's Court. TianTong advises on all types of commercial disputes, e.g., litigation, arbitration, contentious bankruptcy and enforcement proceedings with its most impressive achievements in banking and finance, construction and engineering, corporate and M&A disputes. In addition, TianTong has extensive experience in representing clients in domestic and international arbitration cases, and is specialized in advising clients on recognition and enforcement of foreign arbitral awards in China.

Cleary Gottlieb is a leading international law firm with 16 offices in the U.S., Latin America, Europe and Asia. The firm is consistently ranked as one of the leading international firms for government investigations, white collar criminal defense, litigation, and a variety of related fields. The team includes nine former federal prosecutors, including two recent Acting U.S. Attorneys for the Southern District of New York; several former senior officials of the U.S. Securities and Exchange Commission, including its most recent Chief Litigation Counsel of the Enforcement Division; and several former senior officials from the Federal Trade Commission and the Department of Justice's Antitrust Division, including its most recent Deputy Assistant Attorney General for Litigation and Assistant Chief of the International Section. Cleary Gottlieb is routinely instructed with respect to many of the highest-profile cross-border matters in the financial services, technology, anti-corruption, antitrust and competition, and related fields.

5 https://www.tiktok.com/legal/privacy-policy?lang=en#privacy-eea

For more information, please contact:

TianTong Law Firm
Yard 3 Nanwanzi, Nanheyan Avenue
Dongcheng District, Beijing
100006, PRC
+86 10 51669666
ttchinainitiative.list@tiantonglaw.com

CLEARY GOTTLIEB STEEN & HAMILTON LLP
One Liberty Plaza
New York, New York 10006
+1.212.225.2000
2112 Pennsylvania Avenue NW
Washington, D.C. 20037
+1.202.974.1752
cgshchinainitiative@cgsh.com