BRIDGING DIGITAL DIVIDES: NAVIGATING DATA GOVERNANCE AND SECURITY IN THE U.S.-CHINA TECHNOLOGICAL ARENA

Harvard-Fudan U.S.-China Student Dialogue
Spring 2024

Authors:
Zhe Tian (Fudan Lead)
Aqib Zakaria (Harvard Lead)
Adam Latif
Shefali Prakesh
Liliana Price
Oscar Zijie Wei
Cerena Wu
Zhenyang Wu
Luke Yuan
Yuchen Zhang

Advisors:
David Yang, Professor at the Department of Economics, Harvard University
Wu Xin Bo, Director of the Center for American Studies, Fudan University

Outline

I. Introduction

On the morning of March 23, 2023, TikTok's CEO, Shou Zi Chew, found himself in the hot seat as he testified before the U.S. House Energy and Commerce Committee. The hearing unfolded as a high-stakes “political trial,” marked by intense scrutiny from Republican Representatives who honed in on three key areas: TikTok's handling of user privacy, national security implications, and content-related concerns. As a representative of China's expanding digital technology industry on the global stage, TikTok faced formidable challenges in the backdrop of prevailing geopolitical tensions.

Over the course of the five-hour hearing, Shouzi Chew endured questioning and accusations from approximately fifty bipartisan and assertive members of Congress. The focal points of concern were TikTok's safeguarding of American user data privacy, with some representatives drawing parallels to a "spy" that allegedly monitors and pilfers user information. Despite the absence of concrete evidence substantiating TikTok's threat to U.S. national security, the accusations persist, contributing to the contentious atmosphere surrounding the platform.

In the broader context of globalization, the transmission of business data has become an integral facet of the daily operations of multinational corporations. However, in the age of widespread internet usage and technological advancements, data and the internet have evolved into critical elements entwined with national security and strategic interests.

The influx of data facilitated by the global expansion of Chinese enterprises has triggered security concerns in the United States, impacting the operations and viability of these enterprises. Conversely, U.S. companies operating in China face constraints imposed by newly enacted laws. Examining the TikTok hearing as a case in point, the efforts of U.S. congress members, pre-existing public opinion, and policy groundwork aimed to forcefully connect TikTok with national security concerns and its alleged ties to the Chinese government.

Moreover, instances like Didi Chuxing's public debut in the United States necessitated the submission of corporate data to U.S. authorities, potentially crossing China's national security boundaries. While this data may not overtly contain classified information, the context of big data analysis means seemingly innocuous data can be dissected to unveil critical strategic insights. The Chinese government’s sudden crackdown on Didi Chuxing after its IPO raises questions regarding the seemingly arbitrary nature of Chinese private intervention. Such obscurity regarding private-public relations creates an obstacle to more transparent and deeper U.S.-China business relations.

Similar tensions regarding classified or private data exist in China, where U.S. companies such as Apple and Tesla encounter demands for localizing data storage. The delicate balance

between the globalization of corporate operations and meeting national data security requirements presents an urgent issue. Striking a harmony that prevents data misuse without impeding the normal operations of multinational enterprises is crucial and has far-reaching implications for economic and trade relations between countries like China and the United States.

The issues surrounding data, including data flow, privacy protection, and generative artificial intelligence, are increasingly becoming pivotal factors in shaping the relationship between the United States and China. At the APEC Summit in San Francisco in November, both sides engaged in discussions on these aspects. As the data security team of the Fudan-Harvard China-U.S. Young Leaders Dialogue (2023-2024), we aim to review the paths, challenges, and progress in data governance that the U.S. and China have traversed in recent years.

The focus of this dialogue is to illustrate the cooperation and differences between the two countries on emerging data issues and business policies. Through in-depth analysis, we will propose pertinent solutions and look ahead to the future of mutual collaboration in addressing challenges. This includes strengthening international cooperation mechanisms and establishing common standards for data governance and public offerings to ensure ease of business and the reasonable flow of data while protecting individual privacy rights. We also believe that the U.S. and China can collaborate on research and development in generative artificial intelligence, fostering innovation in this field through joint projects for mutually beneficial outcomes.

Through the Dialogue, we aspire to build bridges for cooperation between the U.S. and China in data governance, promoting deeper understanding and trust. In this challenging moment, we are confident that through collaboration, the two countries can collectively address the various challenges posed by data issues and achieve mutual benefits.

II. U.S. Policies on Mobile Apps Data Collection

A. Laws and Regulations

Concerns over data privacy and national security have led almost all developed nations to scrutinize foreign mobile apps and attempt to strike a balance between regulation of data collection, protection of user privacy, and maintenance of national security. This section aims to review the legal approaches of the United States, China, and the European Union to understand the differences among nations and reach an understanding of what a successful legal policy should look like.

United States

Unlike China and the European Union, the United States lacks a comprehensive federal framework for data protection. In lieu of one, the United States relies on a patchwork of federal laws and Executive Orders and otherwise hands the responsibility of data protection and collection to states.

On the federal level, administrations have opted to utilize executive orders. Executive Order 14034 is a key policy governing the collection of U.S. consumers' data by foreign software or mobile applications. The order was issued in June 2021 by the Biden administration to clarify existing policies evaluating threats to Americans' privacy and data security posed by foreign apps and software. The order sets multiple standards for apps or software that violate or potentially violate Americans' privacy or pose a threat to national security to be enforced by current laws and agencies related to data protection (White House). The order is specifically targeted to protect Americans' data from apps or software owned or operated by groups in countries deemed "foreign adversaries." China is explicitly mentioned in this order (White House).

One factor this order establishes as a determinant for privacy and security threat is if the foreign-owned app or software is in any way connected to a foreign adversary's military or intelligence service, creating the risk that U.S. consumers' data is collected to inform adversary military or intelligence operations (White House). Another factor is if the foreign app or software collects sensitive information such as confidential data from government or business organizations or personal data from U.S. consumers (White House). A third factor is if the owner of the foreign app or software could be pressured by an adversary government into disclosing data collected about U.S. consumers (White House).

One more element of this order is to repeal Executive Orders 13942, 13943, and 13971 which were executive orders under the Trump administration specifically targeting Chinese apps; respectively TikTok, WeChat, and a range of others (Baker McKenzie). Each of those executive orders sought to restrict the operations of the aforementioned Chinese apps in the United States by allowing the Department of Commerce to restrict transactions between those under U.S. jurisdiction and the apps' parent companies (Baker McKenzie). Executive Order 14034 takes a broader approach to "adversaries" in general but still targets Chinese apps in the U.S. market.

In terms of federal legislation, the United States has relied on laws such as the Children's Online Privacy Protection Act, Gramm Leach Bliley Act, Health Insurance Portability and Accountability Act, Family Educational Rights and Privacy Act, and Privacy Act of 1974. These laws address specific sectors but do not provide a unified framework for data protection. More recently in 2018, however, the Foreign Investment Risk Review Modernization Act (FIRRMA) expanded the powers of the Committee on Foreign Investment in the United States (CFIU.S.) to review and take action against foreign investments in U.S. companies that may pose national

security concerns. This includes transactions involving mobile apps that could result in access to sensitive personal data of U.S. citizens.

The absence of comprehensive federal legislation impacts international data transfers. The U.S. does not have an adequacy decision from the EU, necessitating reliance on agreements like the Privacy Shield. However, the Privacy Shield has faced challenges, leading to uncertainties for companies dealing with cross-border data flows.

At the state level, all 50 states have some form of data breach notification laws, but California, Illinois, and Vermont have enacted more comprehensive data privacy regulations. The California Consumer Privacy Act (CCPA) is a notable example, providing consumers with rights like opting out of data collection and seeking damages for data breaches.

Also worth noting is the Commerce Department's "Clean Network Initiative." This initiative aimed to secure the U.S.'s assets from aggressive intrusions by malign actors, such as Chinese apps and cloud service providers. The program sought to establish guidelines and policies to protect sensitive personal information from exploitation by foreign adversaries.

In summary, the United States has implemented various policies to address concerns regarding data privacy and national security, particularly concerning foreign mobile apps, notably those from China. However, the measures range does not present a unified, cohesive policy, but rather represents a variety of different legal bases to act from.

China

China, a major technology hub, has undergone significant developments in data privacy regulations. Before the enactment of comprehensive legislation like the Personal Information Protection Law (PIPL) in 2021, China relied on a patchwork of laws to protect personal information. Early regulations included the 1982 Constitution and laws such as the General Principles of Civil Law of 1986, the Criminal Law, the Tort Liability Law of 2010, the Telecommunications and Internet Personal User Data Protection Regulation of 2013, and the Cybersecurity Law of 2016 (CSL).

The CSL was a pivotal step toward comprehensive data protection, applying primarily to companies within China. It required companies to make their data collection and use rules public and included principles like purpose specification, prohibiting data processing for purposes other than specified without consent. The CSL also allowed individuals to request data erasure in case of legal violations.

Accompanying the CSL was the 2018 Specification, a non-binding rule that defined key terms and set standards for data controllers. It went further than the CSL by requiring data controllers to express data processing details to data subjects and ensuring the right to data portability.

In 2021, China implemented the PIPL, a comprehensive regulation modeled closely after the GDPR in the European Union. The PIPL applies to businesses within and outside China that handle the personal information of individuals within the country. Similar to the GDPR, the PIPL grants several rights to individuals, including access, rectification, erasure, consent withdrawal, account cancellation, obtaining copies, and the right to file complaints regarding significant impacts of automated decision-making.

The PIPL introduces new requirements, such as pre-collection information provision, applying to facial recognition, and mandating certain data to be stored on servers within China. It also regulates cross-border data transfers, requiring specific consent from the government. Notably, the PIPL distinguishes between personal information protection and the right to privacy.

The PIPL imposes stringent penalties, with fines of up to 50 million Yuan or 5% of annual revenue for violating companies. However, it does not apply to governmental agencies, a notable limitation. Some experts suggest improvements, emphasizing enhanced requirements for consent and disclosure, strengthened application of principles, the establishment of a unified enforcement agency, and improved private and public enforcement.

European Union

The European Union (EU) has been a pioneer in the realm of data privacy regulations, notably transitioning from prior regulations to the comprehensive General Data Protection Regulation (GDPR). The GDPR, enacted in March 2014 and fully effective from March 2018, represents a significant advancement in data privacy regulation and applies to businesses of all sizes operating in the EU. The key features of EU data privacy regulations include:

1. European Data Protection Directive (1995): The EU's early data privacy regulations, embodied in the European Data Protection Directive adopted in 1995, aimed to safeguard individuals concerning the processing of personal data by companies. The directive outlined seven main principles, emphasizing transparency, informed consent, data storage requirements, and the liability of companies for protecting personal information.

2. General Data Protection Regulation (GDPR): The GDPR, a comprehensive regulation, grants various rights to individuals, including EU citizens and anyone within the EU. Key rights include the right to be informed, the right to access, the right to portability, the

right to rectification, the right to erasure, the right to object, the right to restrict processing, and the right to object to automated decision-making. These rights empower individuals to control and manage their personal data, requiring companies to provide information, grant access to data, enable data portability, rectify inaccuracies, and more.

3. Government's Recognition of Property Rights: A notable theme in GDPR is the recognition of property rights related to data for the data subject rather than the collecting business. The regulation emphasizes individuals' control over their data and requires companies to respect individuals' decisions regarding their data.

4. Enforcement Measures: The GDPR includes enforcement measures, mandating each EU state to have at least one supervisory authority responsible for protecting individuals' rights concerning personal data. These authorities enforce compliance and have the authority to impose fines, which can be substantial, for violations.

Challenges associated with the GDPR implementation include the financial burden on companies, especially smaller ones, and a need for better understanding, as evidenced by the initial reactions and misinterpretations by some U.S. companies. Despite challenges, the GDPR represents a significant step in giving individuals greater control over their data and establishing a robust framework for data privacy within the EU.

B. Case Studies

To understand the tensions regarding data privacy more concretely, this paper examines two cases of the United States' restriction of Chinese apps: TikTok and WeChat. By examining these cases, the points of contention regarding bilateral relations between the United States and China can be better known, and we can provide more lucid recommendations on how to resolve them.

TikTok

TikTok is a popular social media and video-sharing app in the U.S. with more than 150 million U.S. users. However, a growing number of U.S. policymakers warn that TikTok poses a privacy and data security threat to Americans. The chief concerns stem from the fact that ByteDance, the Chinese company that owns TikTok, collects users' data and stores it on their servers. There is a concern that, because ByteDance is a Chinese company and thus subject to Chinese government regulations, they could leak U.S. users' data to the Chinese government if they were pressured to do so. This would compromise the privacy of TikTok's more than 150 million U.S. users and give the Chinese government access to a significant amount of data about

U.S. citizens. There is also a concern that the Chinese government could pressure ByteDance into harnessing TikTok as a tool to spread propaganda and misinformation in the U.S.

As a result of these risks, there have been a number of proposals since the Trump administration to restrict or ban TikTok outright in the U.S. Currently, employees of the U.S. federal government and federal contractors are banned from having TikTok on phones used for work. In addition to this, 34 states have banned state employees from having TikTok on their phones. Montana is the only state to have banned all individuals from using TikTok.

To address concerns about privacy and data security, TikTok is implementing a series of data security measures called Project Texas. Project Texas would move all TikTok data collected on U.S. users to servers in the U.S. Access to data on these servers would be controlled by a subsidiary called U.S. Data Security, which reports to an independent board rather than ByteDance itself. U.S.DS would have full control over access to U.S. users' data and would not be obliged to provide data under the pressure of ByteDance. Third-party reviewing would be employed to ensure that these servers are secure and have no backdoors to access U.S. users' data. Third-party reviewing would also be employed to ensure that TikTok content displayed in the U.S. is free from foreign interference and that the company is complying with its policies.

Despite the Project Texas proposal, there is still scrutiny over TikTok. Potential outcomes for TikTok include reaching some sort of agreement with CFIU.S. that addresses concerns about privacy, data security, and access to the data of U.S. users; divestment of TikTok by selling it to a U.S. company; or even an outright ban on TikTok nationwide. Regardless of the final result, TikTok is a high-profile case of U.S. restrictions on a Chinese app, and analysis of potential solutions to the TikTok dilemma is warranted.

Within the United States, accusations against Chinese-origin social media platforms like TikTok focus on concerns such as "privacy infringement," "allowing the Chinese government access to U.S. data posing a threat to national security," and "addiction." Similar accusations have surfaced against Chinese e-commerce companies expanding overseas. For instance, in April (shortly after the release of the new cybersecurity strategy), SHEIN and Temu were singled out and criticized in a U.S. congressional report, accusing them of "stealing user data" and "violating privacy and security." Whether in the realm of social media or international e-commerce, Chinese-origin companies are currently facing ideological distrust and cybersecurity anxieties in the United States.

Despite concerns, Chinese apps continue to thrive in the U.S. market. For instance, Temu, a shopping app owned by China-based PDD Holdings, has rapidly gained popularity, reaching the number two spot on the Apple App Store among free apps. Other apps such as CapCut and TikTok, both owned by ByteDance, also remain widely used in the U.S.. Experts have pointed out that the scale of these apps' user bases significantly influences their potential cybersecurity

threat, highlighting the need for a comprehensive evaluation of the risks posed by different Chinese apps in the U.S. market. Concerns have been raised about the potential spread of harmful misinformation, with some advocating for the development of alternatives within the U.S. to mitigate the reliance on these Chinese apps.

In response to these concerns, some U.S. lawmakers have proposed bills, such as the RESTRICT Act, which would grant the Commerce Secretary the power to recommend barring technology from specific foreign adversary countries. However, there have been criticisms of the proposed bill's scope, as it could potentially have unintended consequences and restrict access to certain technologies beyond the intended targets. Some experts have emphasized the importance of fostering a competitive environment for U.S. and free-world alternatives to Chinese apps, thereby reducing the market dominance of these potentially risky apps. The ongoing debate underscores the need for a nuanced and strategic approach to address the challenges posed by Chinese apps in the U.S. market, balancing concerns of national security with consumer choice and technological innovation.

WeChat

The United States had a highly negative response to WeChat's entry into the U.S. market. WeChat's review mechanisms and the perceived "threat to U.S. national security" led the Trump administration to issue a ban on it, but this ban was temporarily halted by the federal court system in September 2020. In fact, according to data from App Annie, there are 2.3 million active WeChat users in the United States every week.

One major controversy surrounding WeChat is its "cross-border censorship system." WeChat accounts created within China are subject to ongoing scrutiny under Chinese mainland law, even if the account owners go abroad or settle in foreign countries. In 2020, a report by Citizenlab revealed that WeChat was monitoring overseas accounts to train algorithms for censoring Chinese information.

In June 2021, the Biden administration officially revoked the Trump-era bans on TikTok and WeChat. However, the controversy regarding the handling of WeChat user data outside of China has not ceased, and these disputes are often labeled as "national security" issues, particularly during periods of tension in U.S.-China relations.

The following is a general overview of the events surrounding WeChat's restrictions in the United States over the past few years：

1. In 2018, the U.S. Department of State announced that Chinese applications such as WeChat and Alipay were classified as "high-risk" applications and were prohibited from being used within U.S. government agencies as communication tools.

2. In 2019, the U.S. government imposed a series of sanctions and restrictions on Huawei, and WeChat was included. The U.S. Department of Commerce announced in May that Huawei and its subsidiaries were added to the "Entity List," which prohibits U.S. companies from providing technology services and components to Huawei. This effectively meant that Huawei's phones were no longer able to use Google services and apps, including the Android operating system and app store. WeChat was also affected by this restriction.

3. In August 2020, President Trump signed an executive order declaring a ban on the use or transaction of TikTok and WeChat-related applications through any means of cooperation with ByteDance, a Chinese company. This action sparked widespread controversy and legal disputes, but the related restriction measures were temporarily blocked by the court after a period of time.

4. In September of the same year, the U.S. Department of Commerce announced a ban on the downloading and updating of WeChat and TikTok in the United States. However, a temporary injunction was issued by the court shortly after, temporarily stopping the implementation of the ban.

III. Chinese Policies for IPOs in Foreign Listings

A. Laws and Regulations

In this section, this paper also reviews China and the United States' policies for IPOs in foreign listings to be more able to provide recommendations regarding balancing private enterprise and a state’s right to guarantee national security.

United States

The United States, through the Securities and Exchange Commission (SEC), has established a robust regulatory framework governing initial public offerings (IPOs) for both domestic and foreign companies. Their ultimate standing objectives seem to be to maintain market integrity, protect investors, and ensure transparency in the capital markets. The regulatory landscape encompasses several key dimensions, including the registration process, financial reporting, corporate governance, exchange listing requirements, legal liability, and ongoing reporting obligations. The most prominent and prevalent U.S. policies for IPOs in foreign Listings include the following.

Registration Process and SEC Review: Foreign companies seeking a listing on U.S. exchanges are required to register their securities with the SEC. This process involves the submission of a comprehensive registration statement, which undergoes meticulous review by the SEC. The scrutiny aims to guarantee that investors are provided with

accurate and relevant information for making well-informed investment decisions (SEC, 2020).

Financial Reporting and Governance Standards: To enhance comparability for U.S. investors, foreign issuers are often obligated to adhere to U.S. Generally Accepted Accounting Principles (GAAP) or reconcile their financial statements accordingly. Additionally, corporate governance standards are imposed, including requirements related to board composition and audit committees (SEC, 2020).

Exchange Listing Requirements: Foreign companies typically choose to list on renowned U.S. stock exchanges such as the New York Stock Exchange (NYSE) or NASDAQ. These exchanges have distinct listing requirements that issuers must satisfy, ensuring a certain level of financial stability and corporate governance (NYSE, 2021; NASDAQ, 2021).

Legal Liability and Enforcement: Foreign issuers are subject to U.S. securities laws, exposing them to legal liability for any violations. The SEC has the authority to enforce compliance, contributing to the overall regulatory enforcement mechanism (SEC, 2020).

Sarbanes-Oxley Act Compliance: The Sarbanes-Oxley Act mandates internal control assessments and CEO/CFO certifications for publicly traded companies in the U.S., and foreign issuers are no exception. This bolsters the corporate governance and accountability framework (SEC, 2002).

Ongoing Reporting Obligations: Post-IPO, foreign companies are required to fulfill ongoing reporting obligations, submitting periodic reports such as Form 10-K, Form 10-Q, and Form 8-K. This continuous disclosure ensures that investors remain apprised of material developments (SEC, 2020).

The U.S. Holding Foreign Companies Accountable Act (HFCAA): The HFCAA affects Chinese companies looking to list in the U.S. The act requires foreign companies listed on U.S. stock exchanges to declare they are not owned or controlled by a foreign government. Additionally, they must allow the Public Company Accounting Oversight Board (PCAOB) to review their financial audits. Since Chinese law restricts foreign inspection of audit documents for companies registered in China, this U.S. regulation has significantly impacted Chinese companies' ability to list in the U.S.

Ultimately, the relative strictness of U.S. IPO regulations compared to other jurisdictions is a subject of nuanced analysis. While the U.S. regulatory environment is often perceived as comprehensive and protective of investor interests, it is essential to recognize that varying regulatory landscapes globally may offer different balances between investor protection and market efficiency. Experts have engaged in dialogues regarding potential further enhancements

to U.S. IPO regulations; proposals include more frequent holistic reviews to ensure alignment with evolving market dynamics and facilitate increased streamlined processes without compromising regulatory objectives. Striking the right balance remains crucial to fostering an environment where companies are incentivized to access U.S. capital markets while maintaining the necessary safeguards (Bhagat & Welch, 2014). Furthermore, discussions on the global harmonization of regulatory standards have gained prominence. Advocates argue that harmonized regulations could reduce the compliance burden on foreign issuers and contribute to more seamless cross-border capital flows (La Porta et al., 2006). To conclude, the U.S. policies governing IPOs for foreign listings exhibit a prioritized commitment to investor protection and market integrity. Evaluating their strictness necessitates a contextual understanding of global regulatory diversity and considerations of ongoing dialogues aimed at refining these frameworks.

China

Chinese companies looking to go public in foreign markets have to navigate a complex regulatory framework that involves both domestic and international rules and oversight. The Chinese government has traditionally been cautious about allowing domestic companies to list abroad, mainly due to concerns about the potential loss of control over strategic assets, financial risks, and the exposure of sensitive data. The following is a summation of relevant laws and regulations:

Overseas Security Listing Regulations: For a long time, Chinese companies went public overseas through a structure known as a "variable interest entity" (VIE). The VIE structure allowed Chinese companies to list abroad even if the sector they operated in was closed to foreign investment, as it technically entailed a foreign shell company offering shares. However, in recent years, the Chinese government has tightened regulations on this practice.

Cybersecurity Reviews: In 2021, China introduced new regulations requiring companies with data on more than 1 million users to undergo a cybersecurity review before listing their shares overseas. This move followed the high-profile case of Didi Chuxing, the Chinese ride-hailing giant, which went public on the New York Stock Exchange, drawing immediate scrutiny from Chinese regulators who subsequently banned the company from registering new users, citing national security and the public interest.

The China Securities Regulatory Commission (CSRC): The CSRC introduced guidelines that require companies seeking a foreign listing to submit filings to the commission. These measures are intended to prevent firms from evading Chinese regulations through overseas listings and ensure that such listings are compliant with domestic securities laws. There are many roles of the CSRC, but some responsibilities include regulating the “application of technology in securities, futures, and fund markets, including setting up regulatory framework and policies,” “domestic companies issuing

and listing shares, depository receipts, convertible bonds, and other securities in overseas markets", and "drafting relevant laws and regulations, and putting forward suggestions for formulation and further revisions; and preparing relevant administrative rules and regulations" (CSRC, 2008). These policies make sure that Chinese companies wanting to have an IPO overseas (such as in the U.S.) are following the proper cybersecurity and national security laws to avoid risks and concerns that come with foreign listings (Yu, 2023).

These regulations have had a chilling effect on the rate of Chinese companies seeking IPOs in foreign markets. It has dampened some investor enthusiasm and led to heightened considerations of risk in investing in Chinese firms abroad. These regulations are seen as part of a broader effort by China to increase oversight of its tech giants and align their expansion with national security and data sovereignty priorities.

Furthermore, with escalating tensions between the U.S. and China, the regulatory environment concerning IPOs and listings has become an area of contention. For companies caught between the two, understanding and navigating the regulatory regimes of both countries is increasingly complex.

In summary, the Chinese policies on IPOs in foreign markets are evolving to address concerns over data security, financial stability, and overall oversight of Chinese companies' international expansion. This regulatory evolution illustrates how China is balancing its companies' globalization ambitions with domestic control, especially for industries deemed sensitive or strategic. Companies looking to execute an IPO outside of China now face a greater burden of compliance and must factor in the potential for regulatory headwinds, both domestically and in the host countries where they seek to list.

B. Case Study

The most relevant case study on the issue of IPOs for foreign listings in the case of Didi Chuxing, detailed below:

Didi Chuxing

Founded in 2012, Didi Chuxing is China's leading mobile transportation company that is headquartered in Beijing (Zhong & Yuan, 2021). Their services include taxi hailing, social ride-sharing, on-demand delivery services, and more, such as the global ride-sharing app, Uber (Ciaccia, 2022). Didi Chuxing went public via an initial public offering (IPO) in June 2021 on the New York Stock Exchange (Ciaccia, 2022). However, the company delisted from its American shares in December 2022 due to pressure from the Chinese government following an examination of its cybersecurity practices and the failure of their drivers and vehicles to meet local security mandates (Zhong & Yuan, 2021, Ciaccia, 2022).

Prior to filing the IPO, the company recognized that its business could plummet if its data security and private practices were not to the standards in China (Zhong & Yuan, 2021, Ciaccia, 2022). Beijing had concerns about a large company with such data and influence on citizens going public in American stock exchanges (Zhong & Yuan, 2021). Further, reports indicate that China was concerned with the amount of data Didi Chuxing actually held and made public, such as the publication of a graph detailing the working times of various government ministries. China has set a series of restrictions on disorganized corporate expansions, which also ensures that companies aren't dodging certain aspects related to local security and information (Zhong & Yuan, 2021). China wants major tech companies to protect their data, but also store it locally and refrain from collecting extra and unnecessary user information (Zhong & Yuan, 2021). Data security and privacy impact trust and communication between countries, especially the U.S. and China, this emphasizes the importance for countries to liaise and be clear with their expectations and policies to protect data and people.

The question for policymakers is if China's policies regarding IPOs are too prohibitive and arbitrary. Should China amend its policies to make a clearer outline of when companies would be subject to delisting and other punitive measures? Or should the government retain the right to punish companies on a case-by-case basis as they appear to threaten national security and privacy rights?

IV. Recommendations

A. U.S. Policies on Mobile Apps Data Collection

After carefully analyzing the various policies of nations regarding mobile app data collection and understanding the points of contention between the U.S. and China on the issue, our team recommends that the U.S. adopt the following policy changes:

1. Federal Data Protection Standards

One step the United States can take to address the hurdles technology companies from China and other foreign countries face when trying to introduce their apps into the U.S. market is creating a uniform set of standards governing data collection across all 50 states. The current patchwork of state laws governing consumer data protection creates headaches and legal risks for technology companies in both the U.S. and abroad when it comes to collecting data. Moreover, it allows individual states to ban entirely some foreign apps, such as Montana's attempt to ban TikTok. To address this issue, Congress should create a set of national standards that supersede individual state laws governing digital privacy and data security. These standards should adequately protect consumers from misuse of their data and address national security concerns, erring on the side of being more restrictive rather than less. Such federal standards could be

based on existing comprehensive data privacy regulations in some states, such as the CCPA in California.

2. Cross-Agency Standardization

Linked to the policy recommendation above, another step the United States can take to address issues foreign companies face when introducing apps in the U.S. is standardizing data protection regulations at the federal level. The patchwork of data protection regulations set by individual agencies should be replaced by a comprehensive set of national standards, as mentioned above. These standards would apply across the jurisdictions of the various regulatory agencies which currently have their own set of regulations, replacing the need for individual agencies to regulate data collection in certain areas. However, any set of comprehensive national data protection regulations should be informed by the current policies of agencies with regulations in this space.

3. Domestic Data Storage for Foreign Apps

Another policy recommendation to reconcile U.S. national security concerns with the desire of Chinese technology companies to access the U.S. market is to require apps with potential ties to foreign governments, as determined by CFIU.S., to store data collected on U.S. consumers in servers located in and regulated by the United States. This would allow foreign technology companies to market apps to U.S. consumers while ensuring that the data of U.S. citizens cannot reach the governments or intelligence services of other countries. Such a law could use TikTok's Project Texas, which has TikTok storing all data collected on U.S. consumers on servers in the U.S., as a model for what projects under this law could look like.

4. Implement a Personal Data Protection Law Modeled on European Union GDPR

In response to the growing concerns over data privacy and security in the United States, we believe that the U.S. should implement a comprehensive personal data protection law modeled on the European Union's General Data Protection Regulation (GDPR). The GDPR is a gold standard for data protection globally and provides a robust framework that empowers individuals with control over their personal data. By adopting similar legislation, the U.S. can better safeguard the sensitive information of its citizens from intrusive practices by both domestic and foreign software companies. This approach would establish clear guidelines regarding the collection, processing, and storage of personal data, ensuring that individuals have greater transparency and control over how their information is used. Key elements of the GDPR, such as granting individuals control over their data usage, determining who has access to their data, and the right to request deletion of their data should be incorporated into the proposed

legislation. These provisions would offer U.S. citizens stronger privacy protections and mitigate the risks associated with unauthorized data access and exploitation. By giving individuals more agency over their personal information, the U.S. can foster trust in the digital ecosystem and encourage responsible data-handling practices among businesses and organizations.

Additionally, adopting a GDPR-inspired personal data protection law would not only enhance privacy rights but also bolster national security efforts. With the increasing frequency and sophistication of cyber threats, protecting sensitive data from unauthorized access is critical to safeguarding infrastructure and intellectual property. By strengthening data protection laws, the U.S. can mitigate the risks of data breaches and cyberattacks, therefore strengthening its resilience against malicious actors. Implementing stringent data protection measures can also provide significant economic benefits: Improved data privacy regulations can enhance consumer confidence in digital services and e-commerce platforms, leading to increased participation in online activities and transactions. By instilling trust in the digital marketplace, businesses can better utilize data-driven strategies to innovate and grow their operations. Additionally, harmonizing U.S. data protection laws with international standards, such as the GDPR, can facilitate cross-border data flows and promote cooperation in the global digital economy, fostering innovation.

B. China Policies for IPOs in Foreign Listings

China's policies regarding initial public offerings (IPOs) in foreign listings can significantly impact both domestic and international markets. Chinese policymakers can help facilitate the listing of Chinese companies in foreign markets responsibly and sustainably while protecting the interests of investors and maintaining the integrity of the financial system. China's policies ensure that companies wanting to have an IPO overseas are following the appropriate cybersecurity measures and national security laws to prevent safety concerns and other potential risks in foreign listings (Yu, 2023). Although work is being done by the China Securities Regulatory Commission (CSRC, 2008), some recommendations can be encouraged to strengthen bilateral relations and foster economic growth. To enhance Chinese policies regarding IPOs in foreign listings, policymakers should focus on promoting transparency, regulatory oversight, and increased corporate governance standards. This can be done by implementing robust disclosure requirements aligned with international accounting standards, strengthening regulatory oversight to ensure compliance, and encouraging improved corporate governance practices such as the appointment of independent directors and transparent decision-making processes. Additionally, policymakers should prioritize investor education and protection, streamline approval processes, foster international cooperation, and encourage long-term sustainability among Chinese companies seeking foreign listings. By implementing these recommendations, Chinese authorities can enable the listing of Chinese companies abroad while safeguarding investor interests and promoting the stability and integrity of the economy.

Furthermore, increasing communication between the United States and China is crucial for making a stronger relationship concerning IPOs in foreign listings. Both nations should establish regular channels of dialogue and collaboration, including regular meetings between regulatory authorities and industry stakeholders. These discussions should focus on sharing best practices, addressing regulatory concerns, and exploring opportunities for mutual understanding and cooperation. Furthermore, the creation of joint working groups or committees dedicated to IPO-related issues could facilitate ongoing communication and problem-solving, such as the China Securities Regulatory Commission (CSRC). By fostering an environment of open and constructive dialogue, the United States and China can work together to build trust, promote transparency, and create a more conducive environment for Chinese companies seeking listings in U.S. markets, ultimately strengthening bilateral ties and promoting economic growth and stability.

Works Cited

"China's Appetite for U.S. IPOs Shows Little Sign of Roaring Back - Nikkei Asia." Accessed February 26, 2024. https://asia.nikkei.com/Business/Markets/China-s-appetite-for-U.S.-IPOs-shows-little-sign-of-roaring-back.

Chorzempa, Martin. "U.S. Security Scrutiny of Foreign Investment Rises, but so Does Foreign Investment | PIIE," September 1, 2022. https://www.piie.com/blogs/realtime-economic-issues-watch/us-security-scrutiny-foreign-investment-rises-so-does-foreign.

Council on Foreign Relations. "The U.S. Government Banned TikTok From Federal Devices. What's Next?" Accessed February 26, 2024. https://www.cfr.org/in-brief/us-government-banned-tiktok-federal-devices-whats-next.

"DiDi Chuxing: The Chinese Ride-Sharing Giant." Accessed February 26, 2024. https://www.investopedia.com/articles/small-business/012517/didi-chuxing.asp.

Federal Register. "Addressing the Threat Posed by TikTok, and Taking Additional Steps To Address the National Emergency With Respect to the Information and Communications Technology and Services Supply Chain," August 11, 2020. https://www.federalregister.gov/documents/2020/08/11/2020-17699/addressing-the-threat-posed-by-tiktok-and-taking-additional-steps-to-address-the-national-emergency.

Feiner, Lauren. "Chinese Apps Remain Hugely Popular in the U.S. despite Efforts to Ban TikTok." CNBC, May 29, 2023. https://www.cnbc.com/2023/05/29/chinese-apps-remain-popular-in-the-us-despite-efforts-to-ban-tiktok.html.

Fisher Phillips. "What Federal Contractors Need to Know about the TikTok Ban for Government Devices: Your 5-Step Compliance Plan." Accessed February 26, 2024. https://www.fisherphillips.com/en/news-insights/what-federal-contractors-tiktok-ban-for-government-devices.html.

Fultonberg, Lorne. "Research: Transparency Improves IPO Process." Daniels College of Business, August 8, 2023. https://daniels.du.edu/blog/research-transparency-improves-ipo-process/.

House, The White. "Executive Order on Protecting Americans' Sensitive Data from Foreign Adversaries." The White House, June 9, 2021.

https://www.whitehouse.gov/briefing-room/presidential-actions/2021/06/09/executive-order-on-protecting-americans-sensitive-data-from-foreign-adversaries/.

Kelly, Charlsey A. “Data Privacy Regulations in the United States, China, and the European Union,” n.d.

Kelly, Nikki Carvajal, Caroline. “Trump Issues Orders Banning TikTok and WeChat from Operating in 45 Days If They Are Not Sold by Chinese Parent Companies | CNN Politics.” CNN, August 7, 2020. https://www.cnn.com/2020/08/06/politics/trump-executive-order-tiktok/index.html.

“OICV-IOSCO - Iosco.Org.” Accessed February 26, 2024. https://www.iosco.org/.

“Overview.” Accessed February 26, 2024. http://www.csrc.gov.cn/csrc_en/c102023/common_zcnr.shtml?channelid=e9958c689bef4d468d81dc93c8d3479f.

Poitras, Terence Gilroy, Alexandre (Alex) Lamy, Ryan. “Biden Administration Revokes Executive Orders Banning Certain Chinese Software Applications.” Global Sanctions and Export Controls Blog, June 15, 2021. https://sanctionsnews.bakermckenzie.com/biden-administration-revokes-executive-orders-banning-certain-chinese-software-applications/.

TikTok. “About Project Texas,” January 25, 2023. https://usds.tiktok.com/usds-about/.

United States Department of State. “The Clean Network.” Accessed February 26, 2024. https://2017-2021.state.gov/the-clean-network/.

WhatIs. “TikTok Bans Explained: Everything You Need to Know.” Accessed February 26, 2024. https://www.techtarget.com/whatis/feature/TikTok-bans-explained-Everything-you-need-to-know.

Zhong, Raymond, and Li Yuan. “The Rise and Fall of the World’s Ride-Hailing Giant.” *The New York Times*, August 27, 2021, sec. Technology. https://www.nytimes.com/2021/08/27/technology/china-didi-crackdown.html.