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

Fudan-Harvard China-U.S. Young Leaders 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. Data Legislation in Focus: Comparative Perspectives from the United States and Beyond

A. Introduction

In an era where data is ubiquitously generated and exponentially valuable, the necessity for a robust legal framework to govern its flow, usage, and protection is indisputable. This section provides a comprehensive overview and comparative analysis of data-related legislation in the United States and other principal regions of the world, mainly including the European Union and China. Through a thorough exploration of these distinct legal frameworks, the objective is to discern the variances that exist between these significant global players and to derive insights into the hallmarks of an effective legal policy on data governance.

B. United States

In the United States, there is no all-encompassing federal regulatory framework for data protection, unlike China and the European Union. The U.S. instead depends on a collection of specific federal laws, Executive Orders, and state-level regulations to oversee data protection.

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.

C. China & European Union

China and the European Union have emerged as influential leaders in the quest for stringent data privacy regulations, albeit with their own unique legislative frameworks.

As China has established itself as a major technology hub, it has progressively developed robust data privacy regulations. The evolution of China's data privacy landscape can be chronologically traced from a fragmented legal system to the formulation of the Personal Information Protection Law (PIPL) in 2021—a comprehensive regulation that closely mirrors aspects of the European Union's General Data Protection Regulation (GDPR). The PIPL notably extends its jurisdiction to both Chinese businesses and international entities operating with the personal information of individuals located in China, offering individuals rights highly reminiscent of those under the GDPR, such as access, rectification, erasure, and objection to automated decision-making. Additionally, PIPL imposes strict penalties for non-compliance, elevated to fines as sizeable as 50 million Yuan or 5% of annual revenue.

The EU, on the other hand, has long been at the forefront of data privacy, with the revolutionary GDPR coming into full force in March 2018. This extensive regulation harmonized preexisting data protection across member states while considerably enhancing individual rights and corporate obligations. Amongst the key features of the GDPR include granting EU citizens and residents extensive control over their personal data, recognizing property rights over data for individuals, and establishing enforcement mechanisms with significant financial penalties.

Both regions underscore the importance of informed consent, transparent data processing, and accountability for companies that handle personal data. However, there are distinctive attributes in each framework:

- China's PIPL specifically addresses the need for information provision before data collection and enforces local data storage for certain categories of data, mandating government consent for cross-border data transfers.

- The GDPR's enforcement is characterized by assigning supervisory authorities in each EU state to uphold compliance, which contrasts with China's omission of a unified enforcement agency—highlighting the need for further enhancement in its regulatory framework.

- Notably, the PIPL does not apply to government agencies in China, a limitation not present in the GDPR, indicating room for legislative expansion and refinement.

From an analytical perspective, the concurrent rise of China's PIPL and the EU's GDPR has significantly reshaped the global conversation on data privacy rights and regulations. Both have set benchmarks that

influence worldwide regulatory strategies, leading to a more harmonized approach to data privacy whilst recognizing the sovereignty of individual legislative environments. Being cognizant of these frameworks enables multinationals to navigate the complexities of compliance and foster trust with their global customer base. The convergence of principles between China and the EU reflects a growing consensus on the value of data privacy, presenting an opportunity to push for more coherent global standards in the digital era.

D. Comparative Analysis of AI Regulations between the three regions (United States, China & European Union)

The contrasting regulatory landscapes of China, the European Union, and the United States highlight the variations in how different regions are tackling challenges related to data privacy and protection.

As mentioned above, China's Personal Information Protection Law (PIPL) and the European Union's General Data Protection Regulation (GDPR) both signify comprehensive approaches to data protection law, focusing on informed consent, data minimization, and individuals' rights to control their personal data. These laws set forth stringent requirements and significant penalties for non-compliance, thereby emphasizing the significance each region places on data privacy as a priority.

In contrast, the United States has a patchwork of laws and regulations, without a singular, comprehensive federal data privacy law. While the Biden administration and previous administrations have utilized executive orders to regulate specific aspects of data protection, such as with Executive Order 14034 specifically targeting foreign software applications, the U.S. approach is largely reactive and sector-specific. Federal policies such as the Health Insurance Portability and Accountability Act (HIPAA) and the Children’s Online Privacy Protection Act (COPPA) address specific concerns rather than offering an overarching regulatory framework like those found in China or the EU.

The sectoral approach within the U.S. can result in regulatory gaps and a complexity that may be challenging for companies to navigate effectively. However, it also offers a form of flexibility that can be advantageous to innovation, as regulations can be tailored to address particular industries or threats without imposing broad blanket policies.

The lack of a uniform standard in the U.S. also means there is a less predictable environment for international data transfers, especially with the invalidation of mechanisms such as the Privacy Shield, which aimed to ensure the secure transfer of personal data from the EU to the U.S. This contrasts with the harmonized regulations of the EU's GDPR, where data protection standards are consistent across all member states and clear mechanisms exist for data transfer outside the EU through adequacy decisions, standard contractual clauses, and other tools.

In light of recent developments, there is growing pressure for the U.S. to consider a more unified and comprehensive federal data privacy law, that could remedy the fragmented landscape and align more closely with global trends. The European Union and China's laws may serve as templates, but any U.S. regulation would need to account for American legal traditions and values, and balance between consumer data rights and the needs of various economic sectors.

Furthermore, States like California are pioneering a closer approximation to the GDPR's approach with the California Consumer Privacy Act (CCPA), which could pave the way for other states or even federal

legislators to consider adopting similar measures.

The convergence of data privacy principles among China, the EU, and the global community at large reflects an increasing trend toward recognizing the importance of personal data rights and protections. As multinational companies operate across these varied legal environments, they must be vigilant and nimble, keeping abreast of legal obligations in every region they operate within. With the digital economy's continued growth and the consequential rise in data breaches and privacy concerns, there is an ongoing opportunity to push for more standardized, global data protection regulations that could facilitate international commerce while also safeguarding individual privacy rights.

E. 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

a. Current Situation

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.

On March 7, 2024, the House Energy and Commerce Committee introduced the "Protecting Americans from Foreign Adversary Controlled Applications Act," aimed at forcing the separation of TikTok from its parent company ByteDance. This legislation is designed to address potential national security risks posed by applications controlled by foreign adversaries. According to the bill, if ByteDance, headquartered in China, does not divest control of TikTok, the app will effectively be banned in the United States. If enacted, ByteDance would have approximately six months to comply with the requirements of the bill.

On the afternoon of March 13, the separation bill passed the U.S. House of Representatives with 352 votes in favor and 65 against, and was sent to the Senate for a vote. President Biden has stated that if the bill passes both chambers of Congress and reaches his desk, he will sign it into law. However, the U.S. Senate has applied the brakes and proposed potential modifications to the bill, dashing hopes of swift passage and possibly providing breathing room for the popular short-video app. It's worth noting that this legislation targeting TikTok has garnered bipartisan support from the majority of members of Congress. Across party lines, there has been a trend of bipartisan, cross-organizational action against TikTok in the U.S. Congress, with condemnation of China increasingly becoming a shared stance among lawmakers.

Some senators have expressed caution, citing concerns that actions against TikTok could restrict freedom of speech and set unsettling precedents for political intervention in private enterprise. Additionally, there are concerns that the closure of TikTok could disenfranchise young voters who are enthusiastic users of the app. However, various strands, including those from the U.S. intelligence community, have expressed concerns about "Chinese social media intervention," "influence on U.S. societal discourse," and "threats to user data information security" represented by TikTok.

According to congressional aides and former intelligence officials familiar with the matter, the growing calls within Congress to ban TikTok do not stem from any new classified information but reflect the result of years of engagement between national security officials and lawmakers, who have long warned that the Chinese government could potentially exploit the app for nefarious purposes.

These aides and officials have noted that TikTok's success has heightened concerns among U.S. national security officials. Apart from worries about the app's potential for surreptitiously harvesting data, they also fear it could subtly influence public attitudes towards China or issues relevant to the Chinese Communist Party.

One of the chief concerns of U.S. intelligence agencies is that due to the platform's opacity and the way its algorithms serve content to users, they may not necessarily detect Chinese influence operations even if they occur.

FBI Director Christopher Wray testified before Congress last week, stating that such operations are "very hard to detect, which is one of the reasons why national security concerns associated with TikTok are so significant."

Unfortunately, TikTok's response to this unexpected legislation has been somewhat counterproductive. TikTok has even sent pop-up messages to users encouraging them to contact their district's representatives—

providing ready-made evidence for supporters of the idea that "TikTok can effectively manipulate public opinion."

“Protecting Americans from Foreign Adversary Controlled Applications Act” may also affect other applications controlled by foreign companies, as entities covered by the bill must meet all four of the following criteria to be subject to this legislation: :

(i) permits a user to create an account or profile to generate, share, and view text, images, videos, real-time communications, or similar content;

(ii) has more than 1,000,000 monthly active users with respect to at least 2 of the 3 months preceding the date on which a relevant determination of the President is made pursuant to paragraph (3)(B);

(iii) enables 1 or more users to generate or distribute content that can be viewed by other users of the website, desktop application, mobile application, or augmented or immersive technology application; and

(iv) enables 1 or more users to view content generated by other users of the website, desktop application, mobile application, or augmented or immersive technology application.

Therefore, whether other Chinese companies/platforms expanding abroad will face similar restrictions remains to be seen.

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.

b. TikTok's reactions

lobbying behaviors

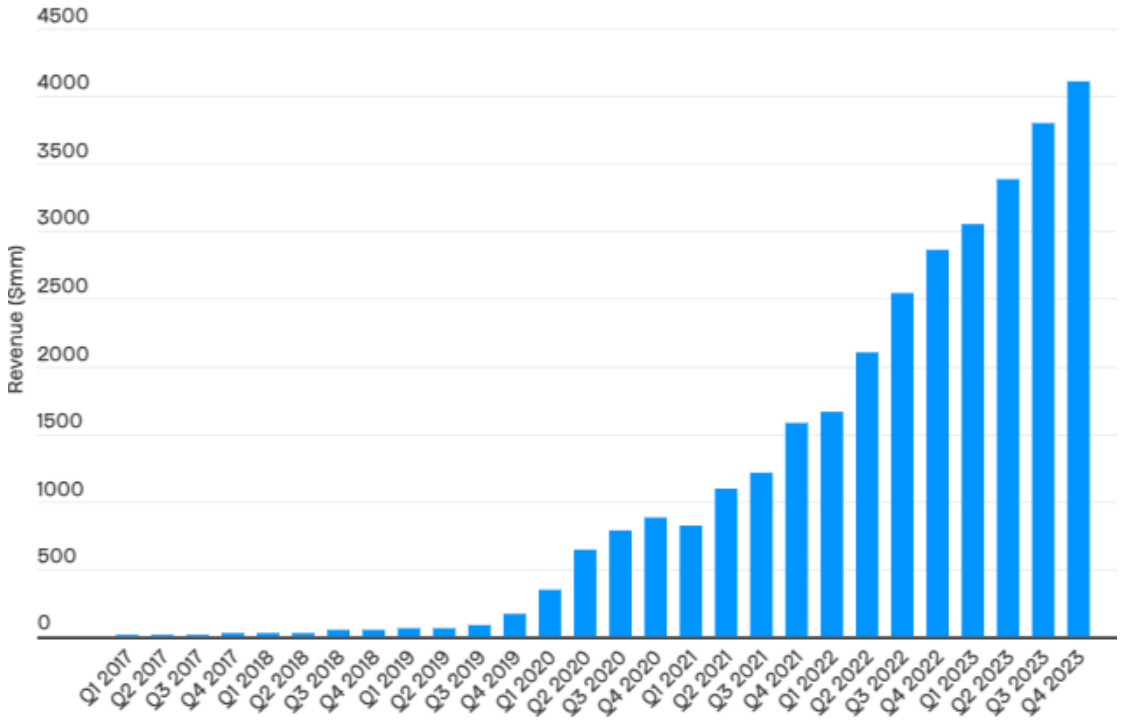
In 2020, Donald Trump planned to launch a ban on TikTok for security reasons.As a result, we can see a surge in TikTok lobbying from 2020. From figure 2, we can see the amount of money increase from 0.27 thousand dollars in 2019 to 1.85 million dollars in 2020.TikTok started to lobby the USA government since 2019. It is estimated that together with its parent company Bytedance, TikTok has spent over 13.4 million since 2019.

TikTok has taken several lobbying actions to prevent it from banned. For example. One of the lobbyists is David Urban, an adviser to Trump's re-election campaign. ByteDance paid $160,000 for Urban's American Continental Group to lobby on its behalf. The American Continental Group has seen its finances soar in the Trump era, in large part due to Urban's social proximity to the president.

In March 2023, Politico reported that TikTok hired SKDK to lobby amid a possible federal ban. SKDK is connected with Biden administration since most of the employees are formerly working for the Biden administration. For example, Anita Dunn, a founding partner, returned to the White House last May where she is senior adviser after a stint in the early part of the Biden administration and work on the 2020 campaign. However, after one month, in April, these two companies have ended their operations, which makes it harder for TikTok to approach the Biden administration. For TikTok, based on the fact that all federal devices are prohibited and some of the universities have banned its usage, it will not be easy to have better lobbying results in the near future.

Performance

While TikTok has been faced with great opposition from the USA government, it still has a dominant place in the market. The opposition has no effect on revenue and the number of users within the globe and United States. The revenue it generates seems to steadily increase. According to Sensor Tower, TikTok's revenue increased from 56 million dollars in 2019 to 41 billion dollars in 2023 Q4 worldwide. The revenue grew 73 times in 5 years. In the US market, the revenue increased from 2.1 billion in 2021 to 5.03 billion in 2022. Apart from the revenue, the number of users are increasing dramatically:its quarterly users have increased from 85 million to 1635 million in six years. Specifically in the United States, TikTok has 150 million monthly active users in February 2023, an increase from 100 million in August 2020 according to TikTok's report.



.

Revenue of TikTok from 2017 to 2023
Source: Sensor Tower

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) Comparative Analysis: Similarities and Differences

Similarities

Similarities are evident upon examination of the IPO regulation policies of the two nations.

Foremost, national security emerges as a shared concern for policymakers in both the US and China. Specifically, these concerns manifest in robust oversight to mitigate potential foreign interference and data leakage risks, exemplified by the enactment of the HFCAA in the US and heightened scrutiny on cybersecurity in China. The mutual emphasis on national security is not coincidental but rather expected. As data increasingly becomes a strategic asset, data security has rightfully assumed a prominent position within global national security agendas.

Additionally, both countries impose compliance requirements on companies seeking foreign listings. In the US, companies must adhere to US accounting principles, corporate governance standards, and legal obligations, primarily aimed at minimizing financial and security risks. Similarly, China has instituted comparable policies to ensure compliance with Chinese financial, cybersecurity, and national security laws for companies listing abroad.

Furthermore, regulatory frameworks for IPO regulation are relatively well-established in both countries. However, the evolving dynamics of the global market and international relations present ongoing challenges to the sustainability of these frameworks. Adjustments may be necessary to realign the expansion goals of corporations with strategic governmental interests in China, and to balance stringent requirements with market vitality in the US.

Differences

The policies of China and the United States regarding initial public offerings (IPOs) for foreign companies exhibit several key differences, primarily manifesting in the registration process, financial reporting and governance standards, regulatory attitudes towards foreign companies, and the emphasis on data security and national security:

Registration Process and Regulatory Review:

United States: The U.S. subjects foreign companies to a rigorous registration and review process through the Securities and Exchange Commission (SEC). This involves the submission of detailed registration documents and thorough scrutiny by the SEC to ensure that investors receive accurate and relevant information for making informed investment decisions.

China: While Chinese companies seeking foreign listings must also follow certain registration procedures, in recent years, China has intensified domestic regulation of these companies. This includes the introduction of new regulations requiring cybersecurity reviews and mandating that companies submit documents to the China Securities Regulatory Commission (CSRC) to ensure that these companies do not evade Chinese regulations through

overseas listings.

Financial Reporting and Governance Standards:

United States: Foreign issuers are generally required to adhere to U.S. Generally Accepted Accounting Principles (GAAP) or reconcile their financial statements accordingly, while also meeting corporate governance standards, including board composition and audit committee requirements.

China: China has implemented stricter management of data and financial information for companies listed overseas, particularly regarding data security and cross-border data flows. For example, the provisions of the "Cybersecurity Review Measures" introduced by China in 2021 stipulated that companies with data on more than 1 million users are subjected to cybersecurity reviews.

Regulatory Attitude Towards Foreign Companies:

United States: The U.S., through laws such as the Holding Foreign Companies Accountable Act (HFCAA), requires foreign companies listed in the U.S. to certify that they are not under the control of a foreign government and to allow the Public Company Accounting Oversight Board (PCAOB) to review their financial audits. This regulation has a significant impact on Chinese companies, given Chinese law restricts foreign inspection of audit documents for companies registered in China.

China: China's policies are more driven by considerations of national security and data sovereignty, focusing on strengthening the monitoring and review of Chinese companies listed overseas, especially those involving sensitive data and sectors.

Data Security and National Security Considerations:

United States: While the U.S. is concerned with data security and national security, adjustments are primarily made through market mechanisms and specific laws (like HFCAA), emphasizing transparency and investor protection.

China: China's approach to data security and national security is more direct and urgent, implementing new measures like cybersecurity reviews to exert more direct control and regulation over companies.

In summary, the United States' policy framework places more emphasis on market integrity, investor protection, and transparency, while China emphasizes control over companies, data security, and the protection of national security. These differences reflect the varying levels of emphasis on financial regulatory philosophy and national security considerations between the two countries.

c) 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

Despite fierce competition between China and USA, there is still negotiation between two countries. U.S.-China Track II Dialogue on the Digital Economy started in 2019 and was led by Admiral Dennis Blair, former director of national intelligence and a member of NCUSCR's Board of Directors. The leader from China side is Xu Liu, a former official with the National Development and Reform Confession. The Dialogue focuses on issues related to digital economy, such as data, AI and software. Up until now, the Dialogue hasn't achieved any practical results. Yet, there are four consensus agreements. The agreements analyzed the current relation between China and USA and shed light on principles both countries should obey in different areas. Moreover, suggestions are given to both governments on areas like data and financial service and semiconductors. All in all, the Dialogue is a sign that U.S.-China relations can go back to the norms. It shows both sides still hold the hope to cooperate in the future.

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

Alper, Alexandra. “U.S. accuses five firms in China of supporting Russia's military.” June 29, 2022. https://www.reuters.com/world/us-accuses-chinese-companies-supporting-russias-military-2022-06-28/

Alper, Alexandra and Maclean, William. “Factbox: Chinese companies added to U.S. entity list.” December 16, 2022. https://www.reuters.com/business/chinese-companies-added-us-entity-list-2022-12-15/

Cao, Ann. “Tech war: China’s chip imports slump 27 per cent in the first 2 months of 2023 as US sanctions bite.” March 7, 2023. https://www.scmp.com/tech/big-tech/article/3212677/tech-war-chinas-chip-imports-slump-27-cent-first-two-months-2023-us-sanctions-bite

“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.

“Chinese company BGI Group rejects rights accusation after US sanctions.” March 6, 2023. https://www.scmp.com/news/china/article/3212455/chinese-company-bgi-group-rejects-rights-accusation-after-us-sanctions

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.

Chris Devonshire-Ellis, “US Chip Sanctions on China: Analysis and Implications.” October 13, 2022. https://www.china-briefing.com/news/us-chip-sanctions-on-china-analysis-and-implications/

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.

Faucon, Benoit and Lin, Liza “U.S. Weighs Sanctions for Chinese Companies Over Iran Surveillance Buildup.” February 4, 2023. https://www.wsj.com/articles/u-s-weighs-sanctions-for-chinese-companies-over-iran-surveillance-buildup-11675503914

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/.

He, Laura. “Wall Street is kicking out yet another big Chinese company.” March 1, 2022. https://edition.cnn.com/2021/03/01/investing/cnooc-nyse-delisting-intl-hnk/index.html

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/

Industry and Security Bureau. “Additions and Revisions to the Entity List and Conforming Removal From the Unverified List.” December 19, 2022. https://www.federalregister.gov/documents/2022/12/19/2022-27151/additions-and-revisions-to-the-entity-list-and-conforming-removal-from-the-unverified-list

Kastrenakes, Jacob. “Trump signs bill banning government use of Huawei and ZTE tech.” August 14, 2018. https://www.theverge.com/2018/8/13/17686310/huawei-zte-us-government-contractor-ban-trump

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.

MEAGHAN TOBIN, SIYI ZHAO. "What China Is Saying About the TikTok Furor in

Washington." March 18, 2024. https://cn.nytimes.com/china/20240318/china-tiktok-house-bill/
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.
Pan, Che. "China chip trade group warns US pact with Japan, Netherlands to tighten semiconductor export controls threatens global industry and free trade." February 15, 2023. https://www.scmp.com/tech/tech-war/article/3210333/china-semiconductor-trade-group-warns-us-pact-japan-netherlands-tighten-chip-export-controls
Psaledakis, Daphne and Nichols, Michelle. "U.S. sanctions China-based network accused of supplying Iran drone maker." March 10, 2023. https://www.reuters.com/world/us-targets-china-based-network-supporting-irans-drone-procurement-efforts-2023-03-09/
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/.
Rogin, Josh. "The State Department is wrong to play down China's bad actions." March 16, 2023. https://www.washingtonpost.com/opinions/2023/03/16/state-department-softening-china/
Sarah E. Needleman. "Why TikTok Could Be Banned and What Comes Next." March 18, 2024. https://cn.wsj.com/articles/%E5%85%B3%E4%BA%8Etiktok%E5%B0%81%E6%9D%80%E6%B3%95%E6%A1%88-%E4%BD%A0%E9%9C%80%E8%A6%81%E7%9F%A5%E9%81%93%E5%93%AA%E4%BA%9B-2433144d
Sheng, Yang and Kunyi, Yang. "US sanction on Chinese firms rebuked as 'long-arm jurisdiction'." https://www.globaltimes.cn/content/1180908.shtml
Shu, Catherine. "New defense bill bans the U.S. government from using Huawei and ZTE tech." August 14, 2018. https://techcrunch.com/2018/08/13/new-defense-bill-bans-the-u-s-government-from-

using-huawei-and-zte-tech/

Stu Woo & Georgia Wells & Raffaele Huang. "How TikTok Was Blindsided by U.S. Bill That Could Ban It." March 13, 2024. https://cn.wsj.com/articles/%E9%9D%A2%E5%AF%B9%E7%BE%8E%E5%9B%BD%E5%B0%81%E6%9D%80%E6%B3%95%E6%A1%88-tiktok%E4%B8%BA%E4%BD%95%E6%AF%AB%E6%97%A0%E9%98%B2%E5%A4%87-08172330

Swanson, Anna. "China's Economic Support for Russia Could Elicit More Sanctions." February 22, 2023. https://www.nytimes.com/2023/02/22/us/politics/china-russia-sanctions.html?smid=url-share

Tabeta, Shunsuke. "U.S. sanctions derail China chipmakers' expansion plans." February 15, 2023. https://asia.nikkei.com/Business/Tech/Semiconductors/U.S.-sanctions-derail-China-chipmakers-expansion-plans

Tellez, Anthony. "Here Are All The U.S. Sanctions Against China." February 8, 2023. https://www.forbes.com/sites/anthonytellez/2023/02/08/here-are-all-the-us-sanctions-against-china/?sh=6a58dea615b4

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

U.S.-China track II dialogue on the Digital Economy. NCUSCR. (2024, January 3). https://www.ncuscr.org/program/us-china-track-ii-dialogue-digital-economy/

U.S. Department of the Treasury. "Treasury Sanctions Individuals for Undermining Hong Kong's Autonomy." August 7, 2020. https://home.treasury.gov/news/press-releases/sm1088

"US sanctions Chinese individual Luo Dingwen and three Chinese firms for supporting Iran missile programme." February 26, 2020. https://www.scmp.com/news/world/united-states-canada/article/3052339/us-sanctions-chinese-individual-luo-dingwen-and

"U.S. sanctions foreign entities over Iran's missile program." February 26, 2020. https://www.tehrantimes.com/news/445595/U-S-sanctions-foreign-entities-over-Iran-s-missile-program

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-nee

d-to-know.

Woo, Ryan. “China says US should change attitude or risk conflict.” March 8, 2023. https://www.reuters.com/world/china/china-says-if-us-does-not-change-path-towards-it-there-will-surely-be-conflict-2023-03-07/

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.

118th Congress (2023-2024). "H.R.7521 - Protecting Americans from Foreign Adversary Controlled Applications Act." Accessed March 18, 2024. https://www.congress.gov/bill/118th-congress/house-bill/7521/text

Biden Jr, J. R. (2020). Why American Must Lead Again: Recusing US Foreign Policy after Trump. *Foreign Aff.*, *99*, 64.

Clausius, M. (2022). The Banning of TikTok, and the Ban of Foreign Software for National Security Purposes. *Wash. U. Global Stud. L. Rev.*, *21*, 273.

Ehrlich, Sean D., 'What Are Access Points and What Are Their Effects?', *Access Points: An Institutional Theory of Policy Bias and Policy Complexity* (2011; online edn, Oxford Academic, 19 Jan. 2012), https://doi.org/10.1093/acprof:oso/9780199737536.003.0002, accessed 16 June 2023.

Garten, J. E. (1997). Business and foreign policy. *Foreign Aff.*, *76*, 67.

Gray, J. E. (2021). The geopolitics of platforms: The TikTok challenge. *Internet policy review*, *10*(2), 1-26.

Hansen, John Mark. *Gaining access: Congress and the farm lobby, 1919-1981*. University of Chicago Press, 1991.

Hojnacki, M., & Kimball, D. C. (1998). Organized interests and the decision of whom to lobby in Congress. *American Political Science Review*, *92*(4), 775-790.

Kim, I. S., & Milner, H. V. (2019). Multinational corporations and their influence through lobbying on foreign policy. *Multinational Corporations in a Changing Global Economy*, 497-536.

Klüver, H., Mahoney, C., & Opper, M. (2015). Framing in context: how interest groups employ framing to lobby the European Commission. *Journal of European Public Policy*, *22*(4), 481-498.

Landers, S. H., & Sehgal, A. R. (2000). How do physicians lobby their members of Congress?. *Archives of Internal Medicine*, *160*(21), 3248-3251.

Mearsheimer, J. J., & Walt, S. M. (2006). The Israel lobby and US foreign policy.

Miao, W., Huang, D., & Huang, Y. (2023). More than business: The de-politicisation and re-

politicisation of TikTok in the media discourses of China, America and India (2017–2020). *Media International Australia*, *186*(1), 97-114.

Newhouse, J. (2009). Diplomacy, Inc.: The influence of lobbies on US foreign policy. *Foreign Affairs*, 73-92.

Sitaraman, G. (2022). The regulation of foreign platforms. Stanford Law Review, 74, 1073.

Su, C. W., Song, Y., Tao, R., & Hao, L. N. (2020). Does political conflict affect bilateral trade or vice versa? Evidence from Sino-US relations. Economic research-Ekonomska istraživanja, 33(1), 3238-3257.

Zarifian, J. (2014). The Armenian-American lobby and its impact on US foreign policy. *Society, 51*(5), 503-512.

Zhu, Q., & Long, K. (2019). How will artificial intelligence impact Sino–US relations?. China International Strategy Review, 1, 139-151.