PILLAR LEGAL

WOW vs TikTok – The New Data Wars

CHINA REGULATION WATCH & U.S. TECH LAW UPDATE[1]

January 12, 2023

By: Greg Pilarowski | Charles Yu | Ziwei Zhu | Alexandra Ashbrook | Magdalene Bedi

On January 23, 2023, the license agreement between Activision Blizzard, Inc. ("Activision Blizzard") and NetEase Inc. ("NetEase") with respect to the publication of multiple online games in mainland China will expire, ending a 14-year partnership between the two companies. On the expiration date, the companies will suspend the operations of multiple famous game titles in mainland China, including World of Warcraft ("WOW"), Starcraft II, Diablo III, Hearthstone, Heroes of the Storm and Overwatch. Although details of the failed license extension negotiations are not public, conflicts arising from China's new data localization laws may have substantially contributed to the partnership's dissolution.

Meanwhile, in the U.S. TikTok, Inc. ("TikTok"), publisher of the popular short-form video application of the same name, and wholly-owned subsidiary of Beijing ByteDance Technology Co. Ltd. ("ByteDance"), faces ongoing scrutiny from a national security perspective. U.S. government authorities are concerned that the Communist Party of China (the "CPC" or the "Party") might access TikTok collected U.S. personal data through the Party's authority over ByteDance, and use that data to support Party information campaigns in the U.S.[2] Although the U.S. does not have data localization laws and lacks a comprehensive national data privacy law, due to ByteDance's 2017 acquisition of Musical.ly, the Committee on Foreign Investment in the United States ("CFIUS") has the authority to address national security issues raised by TikTok's operations in the U.S.[3] TikTok has attempted to address these concerns by implementing its own data localization arrangements through a partnership with Oracle Corporation ("Oracle"), a cloud platform service, pursuant to which Oracle will host U.S. data separately from TikTok's own data servers in Singapore and Virginia.[4] If access to U.S. personal data by a hostile foreign power is a national security concern, the U.S. government does not have the legal tools that it needs to adequately address the issue, since the owners of most foreign mobile applications or internet based services that are available in the U.S. will not be subject to CFIUS jurisdiction if they have not previously completed a covered acquisition or investment transaction.

【博申律師事務所】

[1] This joint China Regulation Watch and U.S. Tech Law Update is provided by Pillar Legal, P.C. (the "Firm") as a service to clients and other readers. The information contained in this publication should not be construed as legal advice, and use of this memorandum does not create an attorney - client relationship between the reader and the Firm. In addition, the information has not been updated since the date first set forth above and may be required to be updated or customized for particular facts and circumstances. This joint China Regulation Watch and U.S. Tech Law Update may be considered "Attorney Advertising" under applicable law. Questions regarding the matters discussed in this publication may be directed to the Firm at the following contact details: +1-925-930-3932 (San Francisco Bay Area office), +86-21-5876-0206 (Shanghai office), email: info@pillarlegalpc.com. Firm website: www.pillarlegalpc.com.

[2] Lily Hay Newman, *It's Time to Get Real About TikTok's Risks*, WIRED (September 6, 2022).

[3] Greg Roumeliotis, Yingzhi Yang, Echo Wang, Alexandra Alper, *Exclusive: US opens national security investigation into TikTok*, REUTERS (November 1, 2019).

[4] Emily Baker-White, *Inside Project Texas, TikTok's Big Answer to US Lawmakers' China Fears*, BUZZFEED NEWS (March 11, 2022); *see also* Albert Calamug, *Delivering on our US data governance*, TIKTOK (June 17, 2022).

U.S. BAY AREA OFFICE 1990 NORTH CALIFORNIA BLVD. 8TH FLOOR | WALNUT CREEK, CA 94596 | T: +1 925 930 3932

SHANGHAI OFFICE KERRY PARKSIDE, 1155 FANGDIAN RD. 4TH FLOOR | PUDONG DISTRICT, SHANGHAI, CHINA 201204 | T: +86 21 5876 0206

WWW.PILLARLEGALPC.COM

This legal update discusses global data localization trends, how China's data localization rules might have driven Activision Blizzard and NetEase's failure to extend the WOW license, and how America's approach to TikTok reveals that the U.S. is not prepared to compete with China in the new data wars.

1. Data Localization

Dozens of countries have enacted or are considering policies to confine data within national borders through "data localization," which refers to rules requiring storage of data within national borders and restricting transfer of data across national borders. [5] The forms of data localization differ significantly across jurisdictions but can be broadly divided into two categories: hard localization[6] and soft localization.[7] Although data localization policies vary, a global trend towards soft data localization is emerging across geographic and political blocs. The contrasting approaches of the U.S. and China toward data localization outline the contours of the new data wars.

The case for data localization is rooted in data sovereignty, national security, and defensive cybersecurity. Some proponents of data localization believe data localization policies are a path towards "data sovereignty, meaning state control over data collected within a nation's borders, by preventing foreign technology companies from (a) circumventing government regulations and (b) withholding the economic benefits of data collection from the countries in which the data originated.[8] Increasingly, governments are also imposing data localization policies based on assertions that free-flowing data poses national security risks by providing hostile foreign governments access to exploitable personal data that could be used to disseminate misinformation, execute influence operations, and surveil citizens.[9] It's unclear whether data localization policies effectively address the national security concerns spurning their proliferation, but national security is nevertheless a common basis for broad, impactful data transfer restrictions.[10] Finally, some policymakers argue that data localization policies facilitate "defensive cybersecurity," or the ability of government agencies to detect, identify, respond, and recover from and ultimately protect against unauthorized, malignant access to data.[11] Whether data localization legitimately addresses cybersecurity risks is unclear; some evidence suggests

[5] As of June 24, 2022, the following countries have implemented data localization laws: Australia, Brazil, Bulgaria, Canada, China, Denmark, France, Germany, Hungary, Iceland, India, Indonesia, Jamaica, Japan, Kazakhstan, the Netherlands, New Zealand, Nigeria, Poland, Romania, Russian Federation, Slovakia, Sweden, Turkey, Uruguay, Vietnam.
[6] Hard localization refers to rules that require companies to store and process data on servers located within the country and prohibit cross-border data transfers. Anirudh Burman, Upasana Sharma, *How Would Data Localization Benefit India?* CARNEGIE ENDOWMENT FOR INTERNATIONAL PEACE (April 1, 2021).
[7] Soft localization rules require some form of local data storage but allow companies to transfer and process data outside a country's borders after meeting certain conditions, such as after obtaining the consent of users or conducting a privacy assessment with respect to the country to which the data will be transferred.
[8] Adrian Shahbaz, Allie Funk, Andrea Hackl, *User Privacy or Cyber Sovereignty? Assessing the human rights implications of data localization*, FREEDOM HOUSE (2022); see also David McCabe and Adam Satariano, *The Era of Borderless Data is Ending*, NEW YORK TIMES (May 23, 2022).
[9] Erol Yayboke, *The Real National Security Concerns over Data Localization*, CENTER FOR STRATEGIC AND INTERNATIONAL STUDIES (July 23, 2021).
[10] *Id*.
[11] Yayboke, *The Real National Security Concerns over Data Localization*.

U.S. BAY AREA OFFICE 1990 NORTH CALIFORNIA BLVD. 8TH FLOOR | WALNUT CREEK, CA 94596 | T: +1 925 930 3932
SHANGHAI OFFICE KERRY PARKSIDE, 1155 FANGDIAN RD. 4TH FLOOR | PUDONG DISTRICT, SHANGHAI, CHINA 201204 | T: +86 21 5876 0206
WWW.PILLARLEGALPC.COM

that hard data localization may adversely impact cybersecurity defense.[12]

Although the recent global trend is toward more data localization, critics of these policies argue that territorializing data does more harm than good in multiple areas including cross-border law enforcement, human rights, and economic efficiency.[13] Critics of data localization assert that territorial-based restrictions on data access frustrate law enforcement authorities investigating within an already burdensome cross-border law enforcement cooperation framework, the impact of which is acutely felt by technology companies grappling to comply with, at times, conflicting requirements.[14] Further, those who advocate that a free, open, secure, and reliable internet supports the protection and enjoyment of human rights argue that data localization has contributed to an overall decline in internet freedom, since some domestic governments have leveraged locally stored data to enforce social and political control over citizens, such as by using geolocation data to monitor places of worship or public demonstrations.[15] Data localization mandates also introduce risk, complexity, and economic cost to companies' global operations by requiring companies to increase the number and geographical locations of data centers and localized operations that must be staffed and maintained.[16] For many technology companies, the increased costs could render global services impractical, resulting in companies exiting or foregoing entrance into markets.[17]

Perhaps reflecting attempts to balance the benefits and detriments of data localization, the global trend favors soft localization, with few countries adopting hard data localization mandates. Data localization policies generally apply extraterritorially, and often rely on some degree of government discretion. Additionally, national policies may establish different categories of personal data, such as "personal data," "sensitive personal data," and "critical personal data," and apply different restrictions to each. Overall, however, the trend is towards localizing data and restricting cross-border transfers.

The European Union (the "EU") enacted the General Data Protection Regulation (the "GDPR") in 2018, setting the global standard for comprehensive data protection regimes.[18] The GDPR imposes obligations onto companies extraterritorially, so long as they target or collect data related to people in the EU.[19] Under the GDPR, cross-border data transfers outside of the EU are permitted if the European Commission has issued an adequacy decision, meaning the destination country provides an adequate level of data protection based on the European Commission's assessment,[20] or, absent an adequacy decision, if certain safeguards are adopted to

---

[12] *Id.*; *see also* Peter Swire, DeBrae Kennedy-Mayo, *The Effects of Data Localization on Cybersecurity*, Georgia Tech Scheller College of Business Research Paper No. 4030905 (February 18, 2022).
[13] Jennifer Daskal, *Law Enforcement Access to Data cross Borders: The Evolving Security and Rights Issues* (October 2017).
[14] For example, while an increasing number of countries are adopting or considering data localization, some countries claim that their governments can unilaterally compel technology companies operating in their jurisdiction to produce any data collected by those companies, regardless of where that data is stored, and regardless of the location or nationality of the data subject. Technology companies are unable to comply with competing compliance demands, sometimes, and are forced to choose between the laws of nations seeking the disclosure of data and the laws of nations prohibiting such disclosure.
[15] Yayboke, *The Real National Security Concerns over Data Localization*.
[16] H. Jacqueline Brehmer, *Data Localization the Unintended Consequences of Privacy Litigation*, AMERICAN UNIVERSITY LAW REVIEW (2018).
[17] *Id.*
[18] Regulation (EU) 2016/679 (GDPR).
[19] *Id.*
[20] Art. 45 GDPR.

U.S. BAY AREA OFFICE 1990 NORTH CALIFORNIA BLVD. 8TH FLOOR | WALNUT CREEK, CA 94596 | T: +1 925 930 3932
SHANGHAI OFFICE KERRY PARKSIDE, 1155 FANGDIAN RD. 4TH FLOOR | PUDONG DISTRICT, SHANGHAI, CHINA 201204 | T: +86 21 5876 0206
WWW.PILLARLEGALPC.COM

protect the data.[21] For example, contractual clauses ensuring appropriate data protection safeguards can be used as grounds for data transfers from the EU to third countries, and to that end, the European Commission has pre-approved model contractual clauses ("Standard Contractual Clauses" or "SCCs").[22]

The United States addresses cross-border transfer of personal data through trade agreements. U.S. trade agreements related to cross-border data transfers generally oppose data localization, prioritizing instead open commerce and the free flow of data.[23] Further signaling U.S. opposition to restrictions on data flow, on January 27, 2022, a report released by the U.S. International Trade Commission detailing censorship and data localization policies and practices impacting U.S. businesses in China, Russia, Turkey, Vietnam, India, and Indonesia[24] was applauded by bipartisan U.S. Senate Finance Committee leaders, who called for the U.S. to use trade tools to combat "digital authoritarianism."[25]

China codified hard data localization requirements centered around data sovereignty and government control over data flow in the Personal Information Protection Law (个人信息保护法) ("PIPL")[26] and Cross-Border Data Transfer Security Assessment Measures (数据出境安全评估办法).[27] Under PIPL, certain forms of data, such as "personal information and important data," must be stored within China, and certain transfers of data out of China are only permitted after completing extensive security assessment by the Cyberspace Administration of China (国家互联网信息办公室) ("CAC"), which in practice amounts to a discretionary government approval.[28]

[21] Art. 46 GDPR.
[22] Commission Implementing Decision on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 (June 4, 2021).
[23] Agreement between the United States of America, the United Mexican States, and Canada (July 1, 2020).
[24] Foreign Censorship, Part 1: Policies and Practices Affecting U.S. Businesses (Investigation No. 332-585, USITC publication 5244, December 2021).
[25] U.S. Senate Committee on Finance, *Wyden and Crapo: U.S. Must Use Trade Tools To Fight Back Against Censorship and Digital Authoritarianism by China, Russia and Other Foreign Nations* (January 27, 2022); "Digital authoritarianism" is defined by the Center for Strategic and International Studies as "the use of the internet and related digital technologies by leaders with authoritarian tendencies to decrease trust in public institutions, increase social and political control, and/or undermine civil liberties." *See* Erol Yayboke, *Promote and Build: A Strategic Approach to Digital Authoritarianism*, Center for Strategic and International Studies (October 15, 2020).
[26] Personal Information Protection Law (个人信息保护法) (in English).
[27] Cross-Border Data Transfer Security Assessment Measures (数据出境安全评估办法) (in Chinese).
[28] Please find more information about CAC security assessment in our China Regulation Watch - Security Assessment for Cross-Border Data Transfers.

U.S. BAY AREA OFFICE 1990 NORTH CALIFORNIA BLVD. 8TH FLOOR | WALNUT CREEK, CA 94596 | T: +1 925 930 3932
SHANGHAI OFFICE KERRY PARKSIDE, 1155 FANGDIAN RD. 4TH FLOOR | PUDONG DISTRICT, SHANGHAI, CHINA 201204 | T: +86 21 5876 0206
WWW.PILLARLEGALPC.COM

Four leading emerging markets comprising Brazil, Russia,[29] India, and South Africa[30] have also implemented or have considered implementing data localization mandates. Notably, Brazil[31] and India,[32] contemplated hard data localization but withdrew the related proposals in favor of reliance on either vague government discretion or soft data localization, indicating that the trend towards data localization favors soft data localization.

2. World of Warcraft in China

When WOW and other Activision Blizzard games operated by NetEase suspend operations in January 2023, it will mark the end of an era for one of the most successful foreign game franchises in mainland China. In June 2005, upon the initial commercial launch of WOW in China, the game acquired 1.5 million active players within just one month.[33] In 2007, following the release of WOW's first expansion – *The Burning Crusade*, WOW achieved the milestone of one million concurrent players in China, and generated $170 million in revenue that year.[34] The popularity of WOW reached its peak in 2010 with 12 million subscribers worldwide.[35] Though that figure has since dropped, in 2016, *Warcraft*, the movie based on the game, grossed $156 million during its first five days in China, while the film had a less impressive opening weekend in the U.S. with just $24.4 million in box office receipts.[36]

[29] Federal Law No. 152-FZ of July 27 2006, as amended in 2014, on Personal Data (the "Law on Personal Data") mandates that data collected from Russian citizens be stored within Russia. Federal Law No. 152-FZ of July 27 2006 on Personal Data. Data may be mirrored on foreign servers, but may not be written directly to foreign servers and then mirrored to Russian servers. Blinov, *Encrypt your data to make GDPR and Russian Data Localization Law compatible*. This data localization mandate applies extraterritorially. On July 14, 2022, Russia amended the Law on Personal Data to impose pre-transfer requirements on cross-border data transfers, including a requirement that companies notify the government authority Roscomnadzor prior to conducting such transfers.[29]The amended Law on Personal Data also grants Roscomnadzor the discretionary authority to prohibit cross-border transfers within 10 business days of notification.Federal Law of 14 July 2022 No. 266-FZ on Amending the Federal Law on Personal Data (in Russian); *see also* Justin Sherman, *Russia is weaponizing its data laws against foreign organizations*, Brookings (September 27, 2022).

[30] South Africa's Protection of Personal Information Act permits cross-border transfers of data if certain conditions are met. No. 4 of 2013: Protection of Personal Information Act, 2013. The draft National Data and Cloud Policy requires that data considered "critical information infrastructure" be stored and processed within the country's borders, and that copies of data generated from South African natural resources be stored in South Africa for law enforcement purposes. Invitation to submit written submissions on the proposed National Data and Cloud Policy in terms of section 3(5) of the Electronic Communications Act, 2005 (Act No. 36 of 2005).

[31] Similar to the EU's GDPR, the General Personal Data Protection Law (Lei Geral de Proteção de Dados Pessoais, or "LGPD") allows cross-border data transfers only to countries that offer a level of protection of personal data[31] equivalent to the protection in LGPD, or under certain other enumerated bases. [31] In 2020, Brazil contemplated but did not enact an amendment to the LGPD that would have required that Brazilians' personal data be physically stored within Brazilian borders. Lara Haje, Ana Chalub, *Projeto determina que dados pessoais de brasileiros sejam armazenados no território nacional*, CÂMARA DOS DEPUTADOS (September 29, 2020).

[32] India's 2019 draft of India's Personal Data Protection bill segmented data into three categories requiring different forms of data localization, including hard data localization for critical personal data. Bill No. 373 of 2019, the Personal Data Protection Bill. However, on November 18, 2022, India's Ministry of Electronics and Information Technology published a new comprehensive data privacy draft proposal called the Digital Personal Data Protection Bill, 2022 that does not segment personal data based on the nature of the data, and which permits cross-border personal data transfer to and storage within "certain notified countries and territories," as to be determined by the central government. India hasn't yet issued guidance on which countries are included within "certain notified countries," only that such countries will be notified at the central government's discretion. The bill, if enacted into law, will apply extraterritorially. *See also* Ravin Nandle, *India's Digital Personal Data Protection Bill 2022: Does it overhaul the former PDPB?* IAPP (November 22, 2022).

[33] See World Of Warcraft® Reaches 1.5 Million Paying Customers In China, posted by GamesIndustry International on July 21, 2005.

[34] See "WoW achieves a million concurrent connections in China", posted by engadget on April 14, 2008.

[35] See "Latest World of Warcraft Player Count & Subscription Numbers" posted by Headphone Addict on December 2, 2022.

[36] See "Success of Warcraft in China helps US open door to audience of 1.4 billion" posted by The Observer on July 2, 2016.

U.S. BAY AREA OFFICE 1990 NORTH CALIFORNIA BLVD. 8TH FLOOR | WALNUT CREEK, CA 94596 | T: +1 925 930 3932

SHANGHAI OFFICE KERRY PARKSIDE, 1155 FANGDIAN RD. 4TH FLOOR | PUDONG DISTRICT, SHANGHAI, CHINA 201204 | T: +86 21 5876 0206

WWW.PILLARLEGALPC.COM

Notwithstanding the enduring popularity of WOW in China, Activision Blizzard indicated that the economic contribution from the licensed games in mainland China is relatively small, representing approximately 3% of their net revenues in 2021.[37] NetEase was less precise, stating that the licensed games contributed "a low-single-digital percentage" to their total net revenue in 2021 and the first nine months of 2022.[38] These low percentage numbers, however, translate into very large revenue dollar numbers—$8.8 billion for Activision Blizzard and $13.7 billion for NetEase for the full year of 2021.[39] Unsurprisingly, NetEase's Hong Kong-listed share price fell by over 9% on the first trading day after the companies announced their failure to extend the license agreement.[40] Activision Blizzard's stock price drop on the first day of trading after the announcement was less pronounced from $74.35 to $73.81, which may reflect its pending $68.7 billion all-cash acquisition by Microsoft (approximately $95 per share).[41]

Although Activision Blizzard indicated it is in talks with potential new partners to continue offering WOW in China, it is unclear whether a new partner would accept terms that NetEase rejected, and, if an agreement is reached, how quickly the game could be back online.[42] Given the real economic pain of the failure to extend the license agreement, there must have been an irreconcilable conflict between the parties. We believe that conflict arose from China's new data localization policy.

A. Who Controls WOW User Data in China?

Game development and game publishing are two different businesses. In much of the world an online game developer like Activision Blizzard can, if it chooses, also publish and operate its own online personal computer ("PC") games. In China, however, only domestic companies owned by domestic citizens can publish and operate online PC games within the country.[43] A foreign company like Activision Blizzard, therefore, can only bring a game like WOW to China by entering into a license agreement with a domestic company and granting that

[37] See "Quarterly report for quarter ended September 30, 2022," filed with the U.S. Securities and Exchanges Commission ("SEC") on November 7, 2022.
[38] NetEase stated in its 2021 annual report filed with SEC that the net revenues generated by games licensed from third-party developers accounted for in total 9.5% of NetEase's total net revenues in 2021. Such third-party developers include not only Blizzard but also other developers such as Mojang AB, licensor of Minecraft. We can only infer that the net revenue generated by Blizzard games is below 9.5%. However, NetEase further stated in its latest quarterly report that those games licensed from Blizzard only contributed a low-single-digit percentage to NetEase's total net revenue in 2021 and the first 9 months of 2022. See "网易公布 2022 年第三季度未经审计财务业绩" (English translation: NetEase Releases the Unaudited Financial Statements of the Third Quarter of 2022), posted by NetEase on its official website on November 17, 2022.
[39] Please find Blizzard 2021 annual report here and NetEase 2021 annual report here.
[40] See "NetEase's cooperation with Blizzard to end due to expiration of licenses" posted by Global Times on November 17, 2022.
[41] See "Microsoft to buy Activision in $68.7 billion all-cash deal" posted by CNBC on January 18, 2022.
[42] See "Blizzard talking with potential partners to continue offering World of Warcraft in China" posted by Reuters on December 13, 2022.
[43] Many China online game companies, including NetEase, use a variable interest entity ("VIE") structure to achieve apparent compliance with China's foreign investment restrictions that prohibit foreign investment into online game operating businesses while still having foreign shareholders through their U.S. public listing. Under such VIE structure, a domestic operating company that is qualified to operate in the restricted industry is controlled by a wholly owned subsidiary of the publicly listed entity through a series of contractual relationships. For more information about the VIE structure, please see our China Regulation Watch - China's Foreign Ownership Restrictions and the VIE Structure.

U.S. BAY AREA OFFICE 1990 NORTH CALIFORNIA BLVD. 8TH FLOOR | WALNUT CREEK, CA 94596 | T: +1 925 930 3932
SHANGHAI OFFICE KERRY PARKSIDE, 1155 FANGDIAN RD. 4TH FLOOR | PUDONG DISTRICT, SHANGHAI, CHINA 201204 | T: +86 21 5876 0206
WWW.PILLARLEGALPC.COM

domestic company the right to publish and operate the game in China.[44] This is how WOW entered the China market, first with The9 as its domestic publisher and later switching to NetEase as its domestic publisher.

When a game developer and a game publisher enter into a license agreement, they often divide data collected or generated within the game into various categories, with all of the data generally collected directly by the publisher but only some of the data shared by the publisher with the developer. User data, which often refers to a player's real name, identity card number, and contact information such as a mobile phone number, email address or WeChat account, is generally not shared by a publisher with the developer since control over the customer relationship is often regarded as a key publisher asset. Select game data, which often refers to the collection of database records that store permanent and persistent information about the state of play in the game, such as in-game items, game progress level, game log records, other game-play information and game analytical information, is often shared with developers to help identify and correct bugs, to detect bots or other in-game cheating programs and to improve the game.

China game license agreements generally follow this pattern, with the domestic publisher controlling all data collected or generated within the game, and only sharing select game data and analytical data with the foreign developer. User data is generally not shared with the foreign developer, which can make it very challenging for the foreign developer to transition to a new domestic operator at the end of a license agreement term if the original domestic publisher is not willing to cooperate with the transition.

In 2004, when Activision Blizzard first granted The9 a license to publish WOW in China, Activision Blizzard was in a very strong negotiating position, since the Warcraft series was already extremely popular outside of China and The9 was a relatively new and untested game publisher. Prior to the November 2004 initial launch of WOW in select countries outside of China, Activision Blizzard was already a premier developer and publisher of entertainment software renowned for creating many of the industry's most critically acclaimed games, including the Warcraft series, StarCraft, and the Diablo series.[45] Since its debut in 1994, the Warcraft series had won industry acclaim and had set sales records worldwide with over 14 million copies sold by 2004.[46] The9, however, was a relatively new game publisher with revenues of just $1.98 million in 2003.[47]

As a direct result of this unbalanced negotiating position, under the original WOW licensing agreement with The9, Activision Blizzard not only owned all game data and user data, but also controlled access to this critical data. If The9 wanted to access the game data or user data, that access was subject to Activision Blizzard's consent.[48] In 2009, when the original

[44] Please find more details about foreign ownership restrictions in game industry Pillar Legal's 6th edition Legal Primer: Regulation Of China's Digital Game Industry.
[45] See "Blizzard Entertainment Announces World Of Warcraft 'Street Date'" posted by Games Industry International on November 5, 2004. Note that the Word of Warcraft was developed by Blizzard Entertainment, a division of Vivendi Universal Games. In July 2008, Activision, Inc. merged with Vivendi Universal Games and formed Activision Blizzard.
[46] The Warcraft series released by 2004 include the *Warcraft: Orcs and Humans* (1994), *Warcraft II: Tides of Darkness* (1995), and *Warcraft III: Reign of Chaos* (2002).
[47] See The9's registration statement for its initial public offering filed with SEC in 2004 here.
[48] Please find more information in the WOW licensing agreement filed by The9 with the SEC here.

U.S. BAY AREA OFFICE 1990 NORTH CALIFORNIA BLVD. 8TH FLOOR | WALNUT CREEK, CA 94596 | T: +1 925 930 3932
SHANGHAI OFFICE KERRY PARKSIDE, 1155 FANGDIAN RD. 4TH FLOOR | PUDONG DISTRICT, SHANGHAI, CHINA 201204 | T: +86 21 5876 0206
WWW.PILLARLEGALPC.COM

license agreement with The9 expired and Activision Blizzard transitioned the China operation of WOW to NetEase, migration of user data didn't pose an obstacle due to the fact that Activision Blizzard already controlled all of that data.[49] If Activision Blizzard didn't control the data, the original users of the game in China might have lost their in-game items and achievements with the transition from The9 to NetEase, with many users perhaps losing interest in the game itself. Even if the contract specified a data transition process, it would have required a long legal battle with the then very hostile original publisher to compel compliance with those contractual obligations.[50]

Given how critical data control was to enable the transition from a then unhappy publishing relationship with The9 to the new publisher NetEase, and the immense popularity of WOW at the time of that transition,[51] it is unlikely that Activision Blizzard would have given up data control under its new license agreement with NetEase. Although the WOW license agreement with NetEase is not publicly available, due to the circumstances at the time, we believe that Activision Blizzard maintained control over all game and user data under that original 2009 agreement and its various extensions.

In addition, the privacy policy for WOW and other Activision Blizzard games operated by NetEase in China suggests that Activision Blizzard did retain access to user data.[52] Shanghai EaseNet Network Technology Co., Ltd. (上海网之易网络科技发展有限公司) ("Shanghai EaseNet"), the variable interest entity contractually controlled by a joint venture equally owed by NetEase and Activision Blizzard, [53] is the actual operator of WOW and other Activision Blizzard games in China and serves as the data controller for all of the personal information collected and generated by those games. Shanghai EaseNet discloses in its privacy policy that users' personal information may be shared with Activision Blizzard and its affiliates to improve user experience, including account security, combating cheating, or processing and analyzing data. In NetEase's general game privacy policy, however, NetEase indicates that all personal information collected

[49] See "魔兽玩家数据将被无缝转移 暴雪九城达成共识" (English translation: Blizzard and The9 reach the consensus of transferring World of Warcraft player data seamlessly to NetEase), posted by www.Chinanews.com on May 31, 2009. For additional background on the World of Warcraft transition saga, see the following articles by Greg Pilarowski at The Escapist: "China and the World of Tradecraft", posted on August 16, 2009, and "Mind the GAPP: Update on WoW in China", posted on November 6, 2009.

[50] The9 brought lawsuits against Blizzard in China's local courts for software copyright infringement, assets damage, and commercial defamation. See "The9 sues Blizzard in WoW China operation fallout" posted by endadget on June 2, 2009.

[51] According to China local media, right before Activision Blizzard changed local publisher from The9 to NetEase, WOW had about 5 million players in China. In the third quarter of 2009, The9's net revenue decreased 91% quarter over quarter and 94% year over year to $3.7 million, due to the expiration of the WOW license.

[52] Please find the privacy policy here, last updated on January 19, 2022. Only the Chinese version is available.

[53] Many China internet companies with foreign investors establish a variable interest entity ("VIE") structure to achieve apparent compliance with China's foreign investment restrictions that limit or prohibit foreign investment into certain telecommunication value added businesses such as online game operating companies. Under the VIE structure, the domestic operating company that holds the licenses required to operate in the restricted industry is controlled by the foreign invested company through a series of contractual relationships. Shanghai EaseNet is a domestic operating company, but unlike the traditional VIE structure with control exercised by a wholly owned subsidiary of the foreign invested company, Shanghai EaseNet is controlled by a joint venture with ownership equally divided between NetEase and Activision Blizzard. This unusual joint venture arrangement further demonstrates the strong bargaining position that Activision Blizzard had when it initially established its China publishing arrangements with NetEase. Please find more information about the VIE structure in our China Regulation Watch - China's Foreign Ownership Restrictions and the VIE Structure.

U.S. BAY AREA OFFICE 1990 NORTH CALIFORNIA BLVD. 8TH FLOOR | WALNUT CREEK, CA 94596 | T: +1 925 930 3932

SHANGHAI OFFICE KERRY PARKSIDE, 1155 FANGDIAN RD. 4TH FLOOR | PUDONG DISTRICT, SHANGHAI, CHINA 201204 | T: +86 21 5876 0206

WWW.PILLARLEGALPC.COM

from games is saved in China, and that NetEase will obtain a separate consent from users before transferring any personal information out of China. [54]

B. China Data Localization Requirements

When China's PIPL came into effect on November 1, 2021, the rules governing the collection, use and sharing of data from games like WOW changed in meaningful ways. Many elements of China's PIPL are modeled on Europe's GDPR, including the very broad definition of personal information. In other areas, such as data localization requirements, China's PIPL far exceeds the requirements of GDPR.

Similar to the GDPR, PIPL defines personal information as any kind of information recorded electronically or in other forms that is related to an identified or identifiable natural person, excluding information that has been anonymized.[55] Under this definition, all user data and a large amount of game data, such as information about a player's in-game items, game progress level and game log records, fall within the definition of personal information.[56] Aggregate analytical game data that cannot be connected to an identified person is, however, regarded as anonymized data, and thus is not subject to PIPL's requirements.[57]

China's data localization requirements, however, go well beyond what Europe requires. GDPR, with its focus on protecting the privacy of Europeans, allows the transfer of personal data to countries outside of Europe where the European Commission has determined that local laws provide adequate privacy protection or pursuant to other appropriate safeguards such as Standard Contractual Clauses.[58] PIPL, with its focus on data sovereignty, conditions cross-border data transfers by large data controllers upon completion of an extensive security assessment with the Cyberspace Administration of China (国家互联网信息办公室) ("CAC"), thus making cross-border data transfers out of China subject to government discretion.[59]

[54] Please find NetEase's general game privacy policy here, last updated on November 8, 2022. Only Chinese version is available. NetEase's general game privacy policy applies to games operated by Hangzhou NetEase Leihuo Technology Co., Ltd. (杭州网易雷火科技有限公司), Guangzhou NetEase Computer System Co., Ltd. (广州网易计算机系统有限公司), and Shanghai EaseNet Minecraft Network Technology Co., Ltd. (上海网之易吾世界网络科技有限公司).

[55] See Article 4 of PIPL.

[56] According to the Guidelines for Internet Data Classification and Grading (网络数据分类分级指引) issued in December 2021, there are two approaches to identify personal information: (1) "from information to individual," and (2) "from individual to information." Under the "from information to individual" approach, any information that can identify a specific natural person, independently or in combination with other information, should be regarded as personal information. Information such as name, national identity number, email address, mobile phone number, and bank account number can independently identify a specific natural person, and thus are classified as personal information. Similarly, information like gender, birth date, profession, marital status, and education background is also classified as personal information, because this information can be used in combination with other information to identify a specific natural person. Under the "from individual to information" approach, a natural person's inherent characteristics such as nationality, personal biometric information, and any information generated during such natural person's activities such as personal location information, personal communication information, web browsing records is also classified as personal information.

[57] According to Article 73 of PIPL, "anonymization" refers to the process in which any personal information is processed to the extent that it cannot identify a specific natural person and cannot be restored to its original state.

[58] See Article 44, 45 and 46 of GDPR.

[59] See Article 38, 39, and 40 of PIPL.

U.S. BAY AREA OFFICE 1990 NORTH CALIFORNIA BLVD. 8TH FLOOR | WALNUT CREEK, CA 94596 | T: +1 925 930 3932

SHANGHAI OFFICE KERRY PARKSIDE, 1155 FANGDIAN RD. 4TH FLOOR | PUDONG DISTRICT, SHANGHAI, CHINA 201204 | T: +86 21 5876 0206

WWW.PILLARLEGALPC.COM

According to China's various data localization rules,[60] any company that processes personal information of one million or more individuals must complete a security assessment conducted by the CAC[61] before providing any personal information to an overseas recipient.[62] Providing personal information to an overseas recipient refers not only to transferring personal information to an overseas recipient or entrusting an overseas recipient to process personal information, but also includes allowing an overseas entity, organization or individual to access personal information that is collected and stored within China.[63]

NetEase, which is China's second largest game company and generated $13.7 billion of revenue in 2021, clearly has over one million users.[64] As a result, on March 1, 2023, when the cross-border security assessment rules become effective with respect to pre-existing cooperation arrangements, NetEase would have needed to pass a security assessment with CAC before providing any additional personal information to Activision Blizzard outside of China's borders.[65] The security assessment submission materials include an application form, a detailed self-assessment report, an interparty data processing agreement and other relevant documents. As this process is new, it is uncertain what criteria CAC will use to determine whether to approve a security assessment application for cross-border data transfers.

Taken together, China's broad definition of personal information and strict cross-border data transfer requirements mean that foreign game developers, including Activision Blizzard, will no longer be able to freely access data that is critical to the game from outside China or easily persuade their domestic publishers to transfer data to them outside of China.

C. CAC Security Assessment or Data Localization?

There are two paths that Activision Blizzard and NetEase could have taken to comply with PIPL while maintaining Activision Blizzard's presumed access to player personal information. The first path is for NetEase to complete a CAC security assessment to transfer

---

[60] China's data localization rules are contained in various provisions of PIPL, along with regulations and guidelines released after PIPL become effective in November 2021, such as Article 38, 39, 40, 53 and 55 of PIPL; the Cross-Border Data Transfer Security Assessment Measures (数据出境安全评估办法) (the "Security Assessment Measures") issued by CAC on July 7, 2022, and effective on September 1, 2022; the draft Personal Information Cross-Border Transfer Standard Contract Provisions (个人信息出境标准合同规定) issued by CAC on June 30, 2022 for public comments; the Guide to the Application for Security Assessment of Outbound Data Transfers (First Edition) (数据出境安全评估申报指南(第一版)) (the "Application Guide") issued by CAC on August 31, 2022; and the Cross-Border Personal Information Processing Security Certification Specifications Version 2.0 (个人信息跨境处理活动安全认证规范 V2.0) issued by the National Information Security Standard Technology Committee (全国信息安全标准化技术委员会) on December 16, 2022.

[61] According to Article 4 of the Cross-Border Data Transfer Security Assessment Measures (数据出境安全评估办法) issued by CAC on July 7, 2022, the cross-border security assessment will apply in the following situations: (i) transferring any important data out of China; (ii) transferring any personal information out of China by a critical information infrastructure operator or a data processor that processes the personal information of more than 1,000,000 individuals; or (iii) transferring any personal information out of China by a data processor that provides personal information of more than 100,000 individuals or provides sensitive personal information of more than 10,000 individuals to overseas recipients as of January 1 of the previous year.

[62] See Article 40 of PIPL.

[63] According to the Application Guide (defined above), allowing any overseas entity, organization or individual to **access**, retrieve, download or export any data that is collected and stored within China constitutes an outbound data transfer.

[64] See "Annual revenue of leading Chinese gaming enterprises in 2021" published by statista on August 11, 2022.

[65] Pursuant to Article 20 of the Security Assessment Measures, for cross-border data transfers already carried out prior to September 1, 2022, which is the effective date of the Security Assessment Measures, the relevant transferor company has a compliance grace period of six months.

U.S. BAY AREA OFFICE 1990 NORTH CALIFORNIA BLVD. 8TH FLOOR | WALNUT CREEK, CA 94596 | T: +1 925 930 3932

SHANGHAI OFFICE KERRY PARKSIDE, 1155 FANGDIAN RD. 4TH FLOOR | PUDONG DISTRICT, SHANGHAI, CHINA 201204 | T: +86 21 5876 0206

WWW.PILLARLEGALPC.COM

player personal information to Activision Blizzard overseas. The second path is for Activision Blizzard to localize all player personal information within China, establishing a local team for game operations support in China and excluding any involvement from Activision Blizzard's global team that requires access to player personal information. A third solution path, which Activision Blizzard presumably would not accept for the reasons discussed above, would be to reduce or eliminate Activision Blizzard's access to player personal information.

From Activision Blizzard's perspective, completing a CAC security assessment would be the best approach since this path would allow the parties to maintain the existing arrangement, in which we presume Activision Blizzard has both access from outside China to, and the ability to transfer outside China, player personal information. However, NetEase would have been reluctant to apply for the CAC security assessment given the material uncertainty involved with this new process and the sensitivity of its arrangements with Activision Blizzard. For example, it might be difficult for NetEase to justify the necessity of transferring personal information from millions of WOW players to Activision Blizzard, especially since China's minor anti-fatigue and real name registration rules require NetEase to collect sensitive personal information, such as players' real names, ages and identity card numbers. The security assessment process might also draw government attention to other details of the business arrangement between NetEase and Activision Blizzard, such as who controls access to player personal information, NetEase's internal data compliance practices, Activision Blizzard games' operation workflows and the parties' unusual VIE joint venture arrangement. In addition, PIPL requires the local China data controller to take sufficient and necessary security measures to ensure that the foreign data recipient complies with PIPL.[66] Although the parties could have negotiated contractual obligations and indemnification provisions to address this PIPL compliance risk, the heavy penalty of up to five percent of annual revenue for PIPL violations, along with potential reputational damage, would still cause concern for NetEase.[67] The recent negative example provided by Didi, a China ride sharing company that was recently fined $1.2 billion for violating China cyber security laws, data security laws, and data privacy laws, would likely have also prompted NetEase to be more cautious on data privacy issues.[68]

From NetEase's perspective, complete localization of all player personal information in China would be the best approach since this path would allow the parties to avoid the CAC security assessment requirement for cross-border data transfers, thereby reducing government scrutiny of their joint operations in China. Activision Blizzard, however, would have resisted this path as it would likely require material reorganization of how it manages its China game operations. Complete data localization would prohibit Activision Blizzard's overseas personnel from accessing or processing China player data, which would require Activision Blizzard to rent servers in China, establish local teams in China to support its games and use local China vendors for any necessary third party services that involve access to player personal information. Although the parties could have negotiated how to allocate these incremental additional costs

[66] According to Article 38 of PIPL, a personal information processor (a data controller using GDPR terminology) shall take any necessary measure to ensure that the processing activities carried out by overseas recipients meets the protection standards and requirements of PIPL.

[67] Fines imposed on a China data controller can be up to the greater of fifty million Renminbi or five percent of an organization's annual revenue. Moreover, PIPL also imposes personal liability on responsible persons within China data controllers, and individuals can be fined up to one million Renminbi for violating PIPL.

[68] See "China fines Didi $1.2 billion for violating cybersecurity and data laws" posted by CNN Business on July 21, 2022.

U.S. BAY AREA OFFICE 1990 NORTH CALIFORNIA BLVD. 8TH FLOOR | WALNUT CREEK, CA 94596 | T: +1 925 930 3932

SHANGHAI OFFICE KERRY PARKSIDE, 1155 FANGDIAN RD. 4TH FLOOR | PUDONG DISTRICT, SHANGHAI, CHINA 201204 | T: +86 21 5876 0206

WWW.PILLARLEGALPC.COM

among themselves, establishing the new arrangement would nonetheless require significant effort. In addition, it is not clear whether Activision Blizzard would have been able to achieve complete data localization by the March 1, 2023 deadline.

Given the above barriers to compromise, we believe that China's new data localization requirements greatly contributed to the dissolution of Activision Blizzard and NetEase's longstanding partnership.

3. TikTok in America

TikTok is one of the fastest growing apps in the world with over a billion monthly active users, 100 million of which are in the United States.[69] Its meteoric rise and cultural impact coupled with ownership by China based ByteDance, has attracted increased scrutiny from U.S. regulators. In August 2020, this scrutiny culminated in former U.S. President Donald Trump's executive order that would have effectively banned TikTok unless ByteDance sold its U.S. operations.[70]

Although President Trump's executive order was invalidated by U.S. federal courts, [71] U.S. government authorities continue to be concerned that the Communist Party of China might access TikTok collected U.S. personal data through the Party's authority over ByteDance, and use that data to support Party information campaigns in the U.S. Although the U.S. does not have any laws that require data localization, and lacks a comprehensive national data privacy law, due to ByteDance's 2017 acquisition of Musical.ly, the Committee on Foreign Investment in the United States has the authority to address national security issues raised by TikTok's operations in the U.S.

TikTok has attempted to address these concerns by implementing its own data localization arrangements through a partnership with Oracle, pursuant to which Oracle will host U.S. data separately from TikTok's own data servers. It is unclear whether the Oracle data localization agreements will satisfy CFIUS national security concerns, but it is clear that CFIUS' jurisdiction over TikTok was simply a matter of historic chance. If ByteDance had not acquired Musical.ly, then CFIUS would not have the authority to require TikTok to implement data localization arrangements to address U.S. national security concerns.

If access to U.S. personal data by a hostile foreign power such as China is a national security concern, the U.S. government does not have the legal tools that it needs to adequately address the issue, since the owners of most foreign mobile applications and internet based services that are available in the U.S. will not be subject to CFIUS jurisdiction if they have not previously completed a covered acquisition or investment transaction.

[69] Drew Harwell, *How TikTok ate the internet*, WASHINGTON POST (October 14, 2022).
[70] Executive Order 13942 of August 6, 2020.
[71] *See TikTok Inc. v. Trump*, 490 F. Supp. 3d 73 (D.D.C. 2020); *see also Marland v. Trump*, 498 F. Supp. 3d 624 (E.D. Pa. 2020).

U.S. BAY AREA OFFICE 1990 NORTH CALIFORNIA BLVD. 8TH FLOOR | WALNUT CREEK, CA 94596 | T: +1 925 930 3932
SHANGHAI OFFICE KERRY PARKSIDE, 1155 FANGDIAN RD. 4TH FLOOR | PUDONG DISTRICT, SHANGHAI, CHINA 201204 | T: +86 21 5876 0206
WWW.PILLARLEGALPC.COM

A. U.S. Federal Approach to Data Privacy

Currently, the U.S. does not have a comprehensive federal data privacy law. Targeted federal data privacy laws do exist, such as the Health Insurance Portability and Accountability Act, commonly known as HIPAA,[72] the Family Educational Rights and Privacy Act, the Children's Online Privacy Protection Act, commonly known as COPPA,[73] and the Gramm-Leach-Bliley Act, commonly known as GLBA.[74]

Congress has considered several draft comprehensive privacy laws, one of the most recent of which is the bipartisan American Data Privacy Protection Act ("ADPPA"), introduced in June 2022.[75] If signed into law, ADPPA would give U.S. citizens many of the data privacy rights covered by Europe's GDPR, such as rights regarding correction, deletion, access, and portability of covered personal data.[76] ADPPA does not, however, include restrictions on cross-border data transfers, require data localization or provide other restrictions that would limit transfers of U.S. citizen personal data to countries that are hostile to the United States.[77]

B. Cross-Border Data Transfers

In the U.S., cross-border transfer of personal data is largely addressed through international trade agreements. Current U.S. trade policy seeks to balance the need for cross-border data flows with national security and data privacy concerns. The United States-Mexico-Canada agreement ("USMCA"), signed on January 29, 2020, includes rules on privacy, cross border data flows, and cybersecurity.[78] The digital trade chapter (a) ensures that data can be transferred cross-border, and (b) puts limits on where data can be stored and how such data can be processed.[79] In particular, the USMCA recognizes the Asia-Pacific Economic Cooperation (APEC) Cross-Border Privacy Rules ("CBPR") System as a valid cross-border transfer mechanism and requires that any new restrictions on the cross-border transfer of data be based on a "legitimate public policy objective."[80] The U.S.-Japan Digital Trade Agreement is another notable agreement addressing cross-border data transfers, covering rules on digital aspects of international commerce.[81] Like the USMCA, this agreement requires both countries to have a legal framework to protect personal information and places limits on the ability to restrict cross-border transfers of data.[82]

[72] *HIPAA Privacy Rule*, THE HIPAA JOURNAL; see also Tatum Hunter, Jeremy B. Merrill, *Health apps share your concerns with advertisers. HIPAA can't stop it*, WASHINGTON POST (September 22, 2022).
[73] *Children's Privacy*, ELECTRONIC INFORMATION PRIVACY INFORMATION CENTER; Josh Fruhlinger, *COPPA explained: How this law protects children's privacy,* CSO (February 8, 2021).
[74] Katie Liu, *Guide to the Gramm–Leach–Bliley Act*, IAPP.
[75] H.R. 8152 (ADPPA).
[76] *Id*.
[77] *Id*.
[78] *UNITED STATES–MEXICO–CANADA TRADE FACT SHEET Modernizing NAFTA into a 21st Century Trade Agreement*, Office of the US Trade Representative.
[79] *Id*.
[80] *What is the Cross-Border Privacy Rules System*, APEC.
[81] U.S.-Japan Digital Trade Agreement Text.
[82] *Id*.

U.S. BAY AREA OFFICE 1990 NORTH CALIFORNIA BLVD. 8TH FLOOR | WALNUT CREEK, CA 94596 | T: +1 925 930 3932
SHANGHAI OFFICE KERRY PARKSIDE, 1155 FANGDIAN RD. 4TH FLOOR | PUDONG DISTRICT, SHANGHAI, CHINA 201204 | T: +86 21 5876 0206
WWW.PILLARLEGALPC.COM

California, Colorado, Connecticut, Utah and Virginia adopted comprehensive data privacy laws, but none of these state level statutes address cross-border data transfers.[83] The state based laws generally avoid rules addressing international commerce, such as cross-border data transfer restriction, due to provisions of the U.S. Constitution that grant Congress the power to regulate commerce with foreign nations and between states.[84] Because digital commerce includes the trade and sale of data, Congress, as opposed to the states, has the authority to regulate cross-border data flows between the U.S. and foreign nations, as well as between states. As a result, any attempt to regulate U.S. cross-border data transfers would need to be implemented at the federal level.

C. The Limited Role of CFIUS

In part because of the United States does not have a comprehensive legal framework for data privacy, the U.S. government is currently addressing the national security issues raised by TikTok's U.S. operations through CFIUS jurisdiction over ByteDance's 2017 acquisition of Musical.ly. Other attempts to address the same issues, such as a Presidential executive order, were blocked by the U.S. courts.

The President is authorized to review transactions by or with any foreign person that could result in the foreign person having the power to directly or indirectly determine, direct, or decide important matters affecting a "U.S. Business," meaning any entity engaged in interstate commerce in the U.S.[85] The President is assisted and advised by CFIUS, an interagency committee comprised of nine cabinet-level Executive agencies, although various other offices observe and, sometimes, participate in CFIUS's activities.[86] The President, as advised by CFIUS, may suspend or prohibit any "covered transaction" when, in the President's judgment, there is credible evidence that the foreign person exercising control over a U.S. Business might take action that threatens to impair national security.[87] Thus, CFIUS's authority is limited to issues of national security connected to "covered transactions."

When first established over forty-five years ago, CFIUS was a monitoring and reporting committee charged with studying foreign investment in the United States.[88] In 1988, anxiety around proposed purchases of U.S.-based companies by Japan-based companies prompted Congress to pass the Exon-Florio Amendment, which granted CFIUS the authority to review foreign acquisitions, mergers, or takeovers of U.S. businesses by foreign purchasers from a national security perspective.[89] In 2018, spurred by the ongoing trade war with China, President Trump signed into law the Foreign Investment Risk Review Modernization Act ("FIRRMA") as part of the National Defense Authorization Act for Fiscal Year 2019, which sought to close gaps

[83] *State Laws Related to Digital Privacy*, NATIONAL CONFERENCE OF STATE LEGISLATURES (June 7, 2022).
[84] Jennifer Huddleston, *Are States the Appropriate Policy Playground When It Comes to Privacy?* JAMES MADISON INSTITUTE (April 10, 2019).
[85] 31 CFR 800; 31 CFR § 800.252.
[86] Executive Order 11858.
[87] 50 U.S. Code § 4565.
[88] Amy Deen Westbrook, *Securing the Nation or Entrenching the Board? The Evolution of CFIUS Review of Corporate Acquisitions*, MARQUETTE LAW REVIEW (February 2, 2020).
[89] *Id*.

U.S. BAY AREA OFFICE 1990 NORTH CALIFORNIA BLVD. 8TH FLOOR | WALNUT CREEK, CA 94596 | T: +1 925 930 3932
SHANGHAI OFFICE KERRY PARKSIDE, 1155 FANGDIAN RD. 4TH FLOOR | PUDONG DISTRICT, SHANGHAI, CHINA 201204 | T: +86 21 5876 0206
WWW.PILLARLEGALPC.COM

in CFIUS's scope by expanding the definition of "covered transactions" to include minority foreign investments in U.S. business that do not amount to foreign control.[90]

Under FIRRMA, "Covered Transactions" refers to both transactions which could result in foreign control of a U.S. Business and additional types of transactions, including all "other investments" by a foreign person in any unaffiliated U.S. Business which deals with (i) "critical infrastructure,"[91] (ii) "critical technology,"[92] or (iii) "sensitive personal data" of U.S. citizens that may be exploited in a manner that threatens national security.[93] Here, "Other Investment" refers to a direct or indirect investment by a foreign person in a U.S. Business that affords the foreign person (i) access to material nonpublic technological information, (ii) membership, observer rights, nomination rights on the board of directors or equivalent governing body, or (iii) any involvement, other than through voting shares, in substantive decision making in a U.S. business in connection with critical infrastructure, critical technologies, or the "sensitive personal data" of a U.S Citizen (also referred to as "TID businesses").[94] The definition of "Sensitive Personal Data" refers to identifiable data that is maintained or collected by a U.S. Business that (i) targets or tailors products or services to any U.S. executive branch agency or military department with intelligence or national security responsibilities, or to personnel and contractors thereof; (ii) has maintained or collected identifiable data within one or more enumerated categories[95] on greater than one million individuals at any point over the twelve months prior to the transaction at issue, or has demonstrated a business objective to maintain or collect any identifiable data within the enumerated categories on greater than one million individuals; and (iii) the results of an individual's genetic tests.[96]

Parties that believe they may be engaged in a Covered Transaction may notify CFIUS of their transaction through a "Notice," meaning a joint voluntary filing, the contents of which describe the transaction, the parties to the transaction, and additional background into the parties' respective business activities.[97] Once a Notice is filed, CFIUS conducts a 30-day assessment of

[90] H.R.5841, Foreign Investment Risk Review Modernization Act of 2018.
[91] "Critical Infrastructure" means systems and assets, whether physical or virtual, so vital to the U.S. that their incapacity or destruction would have a debilitating impact on national security. FIRRMA, Sec. 1703(a)(5).
[92] "Critical Technologies" means (i) defense articles or defense services included on the U.S. Munitions list, (ii) items included on the Commerce Control List and controlled pursuant to multilateral regimes or for reasons relating to regional stability or surreptitious listening, (iii) specially designed and prepared nuclear equipment, parts, and components, materials, software and technology regulated in relation to assistance to foreign atomic energy activities, (iv) Nuclear facilities, equipment, and materials regulated in connection with the import and export of nuclear equipment and material, (v) select agents and toxins, and (vi) "emerging and foundational technologies" subject to U.S. export controls. FIRRMA, Sec. 1703(a)(6) and Sec. 1755.
[93] FIRRMA, Sec. 1703(a)(4)(B)(iii).
[94] FIRRMA, Sec. 1703(a)(4)(D).
[95] Such enumerated categories include (i) financial data that could be used to analyze or determine an individual's financial distress or hardship; (ii) the set of data in a consumer report; (iii) the set of data in an application for health insurance, long-term care insurance, professional liability insurance, mortgage insurance, or life insurance; (iv) data relating to the physical, mental, or psychological health condition of an individual; (v) non-public electronic communications, including email, messaging, or chat communications, between or among users of a U.S. business's products or services if a primary purpose of such product or service is to facilitate third-party user communications; (vi) geolocation data collected using positioning systems, cell phone towers, or WiFi access points such as via a mobile application, vehicle GPS, other onboard mapping tool, or wearable electronic device; (vii) biometric enrollment data including facial, voice, retina/iris, and palm/fingerprint templates; (viii) data stored and processed for generating a state or federal government identification card; (ix) data concerning U.S. Government personnel security clearance status; and (x) the set of data in an application for a U.S. Government personnel security clearance or an application for employment in a position of public trust. 31 CFR § 800.241(a)(1)(ii).
[96] 31 CFR § 800.241.
[97] 31 C.F.R. § 800.502.

U.S. Bay Area Office 1990 North California Blvd. 8th Floor | Walnut Creek, CA 94596 | T: +1 925 930 3932
Shanghai Office Kerry Parkside, 1155 Fangdian Rd. 4th Floor | Pudong District, Shanghai, China 201204 | T: +86 21 5876 0206
www.pillarlegalpc.com

the transaction to identify national security concerns.[98] If CFIUS identifies national security concerns during the initial assessment period, then CFIUS will commence a 45-day investigation.[99] After the investigation period, CFIUS will either approve the transaction or impose mitigation measures on the parties that the parties must undertake before the transaction may move forward.[100] CFIUS may also refer a transaction to the President with a request for the President's decision if (i) CFIUS recommends a prohibition or suspension of the transaction, (ii) CFIUS is unable to reach a decision, or (iii) CFIUS exercises its discretion to make such request. Within 15-days, the President will either approve, disapprove, or approve with conditions the proposed transaction.[101] Once CFIUS approves a transaction, absent false, incomplete, or misleading information, such transaction will not be subject to further government scrutiny.[102] However, failure to file for CFIUS review of Covered Transactions grants CFIUS the authority to unilaterally initiate a review of such transactions at any time, including after the transaction has closed.[103]

When ByteDance acquired TikTok's predecessor, Musical.ly, in 2017, the parties did not file a Notice with CFIUS.[104] Although ByteDance and Musical.ly were both China based businesses, Musical.ly was engaged in interstate commerce in the U.S., constituting a U.S. Business within CFIUS's jurisdiction.[105] If ByteDance had not acquired Musical.ly, the U.S. might not have the authority to require TikTok to localize its data, absent an act of Congress establishing new data privacy laws or other data localization requirements. That the U.S. is able to impose a data localization mandate on TikTok is coincidental, and likely not repeatable in most situations implicating U.S. personal data. If foreign access to U.S. personal data is a sincere national security concern, then the U.S. does not currently have the legal tools to address that concern.

Many businesses with operations in the U.S. transfer the personal data of U.S. citizens across international borders, including to entities in China. For example, PayPal, a U.S. business based in Palo Alto, shares customer names, addresses, transaction details, and device identifiers with Cheetah Mobile and Money Swap Exchange Limited, both of which are China-based companies, to process payments and target advertisements.[106] Unlike PayPal, which identified its third-party servers pursuant to Luxembourg banking law, many businesses with operations in the U.S. are not subject to data privacy laws that require transparent disclose of their data collection, processing and sharing practices.[107]

[98] 31 CFR § 800.507.
[99] 31 C.F.R.§ 800.505, § 802.505.
[100] 31 CFR § 800.508.
[101] *Id.*
[102] *Id.*
[103] *Id.*
[104] Greg Roumeliotis, Yingzhi Yang, Echo Wang, Alexandra Alper, *Exclusive: U.S. opens national security investigation into TikTok*, REUTERS (November 1, 2019).
[105] Murray Newlands, *The Origin and Future of America's Hottest New App: musical.ly*, Forbes (June 10, 2016).
[106] List of Third Parties (other than PayPal Customers) with Whom Personal Information May be Shared (effective January 3, 2023).
[107] Caitlin Chen, *U.S. Digital Privacy Troubles Do Not Start or End with TikTok*, CENTER FOR STRATEGIC AND INTERNATIONAL STUDIES (October 6, 2022).

U.S. BAY AREA OFFICE 1990 NORTH CALIFORNIA BLVD. 8TH FLOOR | WALNUT CREEK, CA 94596 | T: +1 925 930 3932
SHANGHAI OFFICE KERRY PARKSIDE, 1155 FANGDIAN RD. 4TH FLOOR | PUDONG DISTRICT, SHANGHAI, CHINA 201204 | T: +86 21 5876 0206
WWW.PILLARLEGALPC.COM

In addition, hostile foreign powers could simply purchase the personal data of U.S. citizens through data brokers, which are businesses that compile user information from multiple mobile apps and other sources to sell to both domestic and foreign buyers.[108] Some large U.S. data brokers, such as Acxiom, Epsilon, and Oracle disclose that they sell information to government agencies, but other data brokers do not provide this type of disclosure.[109] Without a comprehensive data privacy law, the U.S. has no way of knowing the size of the data brokerage industry, the granularity of the data collected, and to whom the data is sold.

China's comprehensive data protection framework, broad definition of personal data, and stringent data localization rules will, in many instances, prevent foreign companies from accessing local data from outside of China. The U.S., by contrast, struggles to mitigate access to U.S. data held by a single company. If data localization requirements are what dissolved Activision Blizzard's partnership with NetEase, then the ongoing travails of WOW in China are a testament to the impact of China's data policies. TikTok in America exposes the lack of legal tools that the U.S. has given itself to address data protection and any related national security concerns. If there is a new data war between China and the U.S., then China clearly has the advantage.

[108] *Id.*; *see also* *Data Brokers*, ELECTRONIC PRIVACY INFORMATION CENTER.
[109] Chen, *U.S. Digital Privacy Troubles Do Not Start or End with TikTok*.

U.S. BAY AREA OFFICE 1990 NORTH CALIFORNIA BLVD. 8TH FLOOR | WALNUT CREEK, CA 94596 | T: +1 925 930 3932
SHANGHAI OFFICE KERRY PARKSIDE, 1155 FANGDIAN RD. 4TH FLOOR | PUDONG DISTRICT, SHANGHAI, CHINA 201204 | T: +86 21 5876 0206
WWW.PILLARLEGALPC.COM