JEFFREY BOSSERT CLARK
Acting Assistant Attorney General
AUGUST FLENTJE
Special Counsel to the Acting
Assistant Attorney General
ALEXANDER K. HAAS
Branch Director
DIANE KELLEHER
Assistant Branch Director
SERENA M. ORLOFF
MICHAEL DREZNER
STUART J. ROBINSON
Trial Attorneys
United States Department of Justice
Civil Division, Federal Programs Branch
Ben Franklin Station, P.O. Box No. 883
Washington, DC 20044
Phone: (202) 305-0167
Fax: (202) 616-8470
E-mail: serena.m.orloff@usdoj.gov
Counsel for Defendants

IN THE UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

U.S. WECHAT USERS ALLIANCE, *et al.*,

Plaintiffs,

v.

DONALD J. TRUMP, President of the United States, and WILBUR ROSS, Secretary of Commerce,

Defendants.

Case No. 3:20-cv-05910-LB

DECLARATION OF JOHN COSTELLO

DECLARATION OF JOHN COSTELLO

I, John Costello, declare as follows:

1. I am currently employed as the Deputy Assistant Secretary for Intelligence and Security.

2. I have served in this capacity since June 22, 2020. I am authorized to certify the truth and correctness of official records of the Department of Commerce ("Commerce"), and of other documents recorded or filed with Commerce.

3. The facts attested to herein are based on my personal knowledge or information made available to me in the course of my official duties. I make this declaration in support of the Government's motion to stay the Court's preliminary injunction.

4. Attached to my declaration are certain materials considered by the Secretary in Identification of Prohibited Transactions to Implement Executive Order 13943 and Address the Threat Posed by WeChat and the National Emergency with Respect to the Information and Communications Technology and Services Supply Chain. These are the prohibitions that the Court enjoined in its Order of September 19, 2020.

5. These materials include a decision memorandum and two supporting assessments, one by the Department of Homeland Security Cybersecurity and Infrastructure Security Agency ("DHS CISA") and the other by the Office of the Director of National Intelligence ("ODNI"). The ODNI assessment is classified and will be separately lodged with the Court. These materials are not a complete set of all the materials considered by the Secretary. Commerce is still in the process of collecting the relevant materials, and information that is classified, privileged or otherwise protected (including certain business-sensitive information received from third-parties) has been withheld.

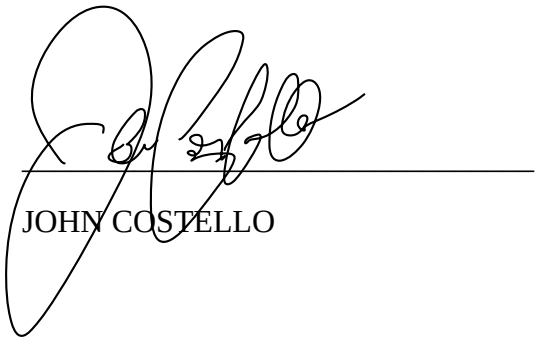
6. The Secretary made his final decision about which transactions related to WeChat/Tencent should be prohibited on Thursday, September 17, 2020. The prohibitions were publicly announced on Friday, September 18, 2020, and were published for inspection at the Government printing Office website later that morning.

7. The Commerce Department received authorization to submit the assessments from DHS CISA and ODNI to the Court as of September 24, 2020; such permissions are required by the Executive Order governing classified and otherwise sensitive information, as well as inter-agency procedures associated for the sharing of government reports.

I certify, pursuant to 28 U.S.C. § 1746, under penalty of perjury that the foregoing is true and

correct to the best of my knowledge, information, and belief.

Executed this 24th day of September 2020 in Washington, D.C.



JOHN COSTELLO

EXHIBIT A

FOR OFFICIAL USE ONLY

UNITED STATES DEPARTMENT OF COMMERCE
Office of Intelligence and Security
Deputy Assistant Secretary for Intelligence and Security
Washington, D.C. 20230

September 17, 2020

MEMORANDUM FOR THE SECRETARY

THROUGH: Rob Blair
Director
Office of Policy and Strategic Planning

FROM: John K. Costello
Deputy Assistant Secretary for Intelligence and Security
Office of Intelligence and Security

SUBJECT: Proposed Prohibited Transactions Related to WeChat Pursuant to Executive Order 13943

I. INTRODUCTION

On August 6, 2020, President Trump signed Executive Order ("EO") 13943, "Addressing the Threat Posed by WeChat, and Taking Additional Steps to Address the National Emergency With Respect to the Information and Communications Technology and Services Supply Chain" declaring that WeChat, a messaging, social media, and electronic payment application owned by the Chinese company Tencent Holdings Limited ("Tencent"), poses a threat to the national security, foreign policy, and economy of the United States. EO 13943 serves as an update to EO 13873, "Securing the Information and Communications Technology and Services Supply Chain." EO 13943 directs you to identify and prohibit transactions within 45 days. This memorandum serves to recommend a set of business-to-business transactions related to WeChat's operation in the United States that should be prohibited to address the national security threat posed by WeChat and to satisfy your obligation under the EO. The Department has carefully considered EO 13943 and other available information regarding WeChat's structure and operations. This includes consideration of publicly available reporting, classified or otherwise protected information, and information from parent company Tencent.

The President concluded that WeChat, a messaging and social media application owned by the Chinese company Tencent, poses a threat to the national security, foreign policy, and economy of the United States. This memorandum contains an additional, unclassified threat analysis sufficient to demonstrate the national security risk that Tencent and WeChat present to the United States. Assessments by the U.S. Intelligence Community ("USIC") and the Department of Homeland Security have reached concurrent and similar conclusions. Their assessments are included in Appendix A and B, and they contain classified, privileged, or otherwise protected information, respectively.

II. BACKGROUND

A. Background on Tencent

Tencent, headquartered in Shenzhen, China, is a multinational conglomerate listed on the Hong Kong Stock Exchange. Tencent's major services include communication and social networking, online PC and mobile games, content *(i.e.* news, videos, music, comics, and literature), utilities (*i.e.* email, application store, mobile security, and mobile browser), artificial intelligence ("AI"), cloud services, and financial technology. Founded in 1998 by Huateng ("Pony") Ma, Tencent found early success in 1999 with QQ messenger, a free instant messaging service provider making money from online advertising and membership fees. Capitalizing on its hundreds of millions of users, in 2011 Tencent launched WeChat, its popular mobile application, which became a gateway for expansions into third-party payment, advertising, social media, entertainment, and gaming businesses. Tencent was named a member of the PRC Government's AI "national team" in 2017, and Tencent has focused on developing a host of AI-empowered applications. It also provides cloud-computing services to different levels of the PRC Government. Tencent's market capitalization was around $417 billion in mid-September 2019. The firm has seen rapid revenue growth in recent years, with increases of 30% or more every year since 2014. In 2018, the firm generated $45.6 billion in total revenues. [1][2][3][4][5]

Aside from its WeChat messaging application, Tencent's most significant products are games that make up the biggest gaming franchise in the world. It has invested in game companies across the globe, including Epic Games, the developer of Fortnite; League of Legends creator of Riot Games; Supercell, the Finnish firm behind Clash Of Clans; Korea's CJ Games; and Glu Mobile. Tencent's gaming division has been an important part of its revenue stream, but regulatory hurdles in China are forcing the company to seek growth in other areas like cloud computing.[6] Tencent also maintains an investment portfolio that dwarfs those of its U.S. peers Facebook and Google. It has made more than 700 investments across the world, and in 400 of them, Tencent has taken board positions. Around 30-40 percent of the company's investments are outside China. Within China, Tencent has stakes in more than a quarter of Chinese "unicorns" (tech firms with a valuation of at least $1 billion).[7]

Tencent's North American operations span multiple industries, including automotive, consumer products and services, electronics, entertainment and education, financial and business services, information and communication technology ("ICT"), health, pharmaceutical, and biotechnology. Tencent has developed these operations through equity and non-equity activities, including acquisitions, greenfield investments, venture capital, patents, license agreements, research and development ("R&D") partnerships, event participation, and ties with management. Tencent established its first U.S. subsidiary in 2007, and since then has managed its North American operations from Palo Alto, CA in Silicon Valley. From 2000 to July 2019, Tencent announced 294 equity investments involving targets with locations in the United States or Canada, including 236 targets with U.S. headquarters and nine targets with Canadian headquarters. Tencent has completed investments worth $7.7 billion in these U.S.- and

[1] https://www.foxbusiness.com/technology/tencent-stock-pony-ma-video-wechat
[2] Tencent Technology (Shenzhen) | QCC | https://www.qcc.com/creport/181e23a3c35a6fc18450f03cc13bb03b
[3] DOD report pdf – "Tencent Transactions in the US"
[4] ASPI – Mapping China's Tech Giants: https://chinatechmap.aspi.org.au/#/company/tencent
[5] DOD report pdf – "Tencent Transactions in the US"
[6] ASPI – Mapping China's Tech Giants: https://chinatechmap.aspi.org.au/#/company/tencent
[7] ASPI – Mapping China's Tech Giants: https://chinatechmap.aspi.org.au/#/company/tencent

Canadian-headquartered operations. The company has been an active participant in the U.S. economy through non-equity channels, including license agreements, R&D partnerships, and other ties.[8]

Tencent most frequently targets North American equity investments with a nexus to emerging technologies such as AI and machine learning, augmented reality and virtual reality, and autonomous cars. The company's non-equity activity has largely involved companies focused on AI and machine learning, gaming, and internet of things ("IoT") technologies.[9]

B. Background on the WeChat mobile application

Launched in 2011, WeChat is one of Tencent's best known products and one of China's most popular social media apps.[10] The app was first launched on Apple's iOS operating system and ported to the Android operating system shortly thereafter.[11] Tencent operates two versions of the application, the China-based "Weixin," which means "micro message," and the international version known as WeChat, which is available in the United States.[12] [13] Some features available on Weixin, like WeChat Pay, WeChat's payment processing platform, are not currently available in the United States. The separate systems are further bifurcated by a WeChat policy which treats the application differently if the user enrolls a Chinese mobile number rather than a non-Chinese mobile number.[14] Although WeChat's primary user base is in China, an estimated 100 to 200 million people outside of China use WeChat. Among them are millions of members of the Chinese diaspora in countries such as Canada, Australia, and the United States, but there is also broader expansion in much of Asia.[15] As of 2020, there are approximately 19 million active daily users in the United States.[16]

Weixin is one of the main ways people communicate within China, including for business communications. Similar services, such as Facebook, are blocked or inaccessible within China. Weixin has evolved beyond a messaging service and is often described as a "super app" and is even preferredover email. It has rapidly become a pervasive part of everyday life within China, as a key vector for communications, and is widely used for mobile payments, company branding and public relations, among other things.[17] It is estimated that a typical Chinese user utilizes the Weixin app ten times a day or more.[18]

---

[8] DOD report pdf – "Tencent Transactions in the US"
[9] DOD report pdf – "Tencent Transactions in the US"
[10] See https://www.reuters.com/article/us-usa-tencent-holdings-wechat-ban/wechat-us-ban-cuts-off-users-link-to-families-in-china-idUSKCN253339
[11] https://news.cgtn.com/news/30596a4e78677a6333566d54/share_p.html
[12] https://www.foxbusiness.com/technology/tencent-stock-pony-ma-video-wechat
[13] To distinguish the Chinese version of WeChat and the international version available in the United States (and the primary subject of this memorandum), this memorandum will refer to the former as "Weixin" and the latter as "WeChat".
[14] https://www.theverge.com/2019/11/25/20976964/chinese-americans-censorship-wechat-hong-kong-elections-tiktok
[15] https://www.japantimes.co.jp/opinion/2019/03/28/commentary/world-commentary/worried-huawei-take-closer-look-tencent/#.Xz1G0n4pCUl
[16] https://www.bloomberg.com/news/articles/2020-08-10/wechat-users-in-the-u-s-fear-losing-family-links-with-ban
[17] Everything you need to know about WeChat — China's billion-user messaging app | CNBC | https://www.cnbc.com/2019/02/04/what-is-wechat-china-biggest-messaging-app.html
[18] https://www.economist.com/business/2016/08/06/wechats-world

WeChat is currently operated by a Singaporean entity, but it is a wholly-owned subsidiary of Tencent. Approximately 2000 Tencent employees, the majority of which are located in the People's Republic of China ("PRC"), are dedicated to the operation of WeChat.

III. THE NATIONAL SECURITY FOREIGN POLICY, AND ECONOMIC RISK WECHAT POSES TO THE UNITED STATES

For the following reasons, we believe WeChat presents the following risks to the national security, foreign policy, and economy of the United States consistent with the President's determination in EO 13943.

A. Threat

1. The PRC presents a national security, foreign policy, and economic threat to the United States given its long-term effort to conduct espionage against the U.S. government, corporations, and persons.

The threats flowing to the United States from PRC espionage activities are well-recognized. For example, according to the U.S. Intelligence Community's ("USIC") 2019 Worldwide Threat Assessment, the PRC presents a persistent cyber espionage threat and a growing threat to our core military and critical infrastructure systems. Additionally, according to Federal Bureau of Investigation ("FBI") Director Christopher Wray, PRC intelligence and economic espionage presents the greatest long-term threat to U.S. national and economic security.[19] The PRC remains the most active strategic competitor responsible for cyber espionage against the U.S. Government ("USG") and U.S. corporations, allies, and persons. The USIC has assessed that PRC will continue to authorize cyber espionage against key U.S. technology sectors when doing so addresses a significant national security or economic goal not achievable through other means. Additionally, the USIC remains concerned about the potential for PRC intelligence and security services ("PRCISS") to use Chinese information technology firms as routine and systemic espionage platforms against the United States and its allies.[20] The PRC's continued use of traditional espionage, [21][22][23] intellectual property theft from U.S. corporations, and theft of personally identifiable information ("PII") illustrate the PRC's intention to use bulk data collection for economic and national security activities that are hostile to the economic and national security interests of the United States.[24]

The FBI notes that it is the PRC's and the Chinese Communist Party's ("CCPs") goal to introduce, understand, assimilate, and re-innovate foreign technology and knowledge to gain a technological edge. The PRC has demonstrated that it will achieve this goal by any means necessary, most notably through theft of foreign intellectual property.[25] The PRC government has engaged in data collection on a

[19] https://www.fbi.gov/news/speeches/the-threat-posed-by-the-chinese-government-and-the-chinese-communist-party-to-the-economic-and-national-security-of-the-united-states
[20] https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf, page 5
[21] https://www.justice.gov/opa/pr/former-cia-officer-arrested-and-charged-espionage
[22] https://www.justice.gov/opa/pr/northern-california-resident-charged-acting-illegal-agent
[23] https://www.justice.gov/opa/pr/former-intelligence-officer-convicted-attempted-espionage-sentenced-10-years-federal-prison
[24] See Appendix C for a list of Department of Justice cases that involve Chinese espionage.
[25] https://www.fbi.gov/file-repository/china-exec-summary-risk-to-corporate-america-2019.pdf/view

massive scale across multiple domains as a means of generating information to enhance state security—and the political security of the CCP.[26] A report from Australian think tank the Australian Strategic Policy Institute ("ASPI") describes the PRC Government's intent to use bulk data collection to support its efforts to shape, manage and control its global operating environment, and to generate cooperative and coercive tools of domestic control.[27] The data collected and used by the PRC to these ends comes in many forms, including text, images, video, and audio. Large data sets can reveal patterns and trends in human behavior, providing a "pattern of life" that can be used to facilitate intelligence and surveillance targeting, particularly when aggregated with other data sets. Bulk data, like images and voice data, can also be used to train algorithms for facial and voice recognition. [28]

According to U.S. officials and analysts, the PRC is building massive databases of Americans' personal information. Evidence suggests that the pattern of targeting large-scale databases is a tactic to further its intelligence-gathering and to understand more about who to target for espionage, whether electronically or via human recruitment. [29] Once harvested, the data can be used to glean details about key government personnel and potential spy recruits, or to gain information useful for intelligence targeting and surveillance.[30] [31]

Since 2012, more than 80% of the economic espionage cases brought by the Department of Justice's ("DOJ") National Security Division have implicated China and the frequency of cases continue to rise.[32,33] As reflected by recent DOJ indictments, the PRC continues to demonstrate an intent and capability to collect vast quantities of sensitive data, including corporate trade secrets related to U.S. military technology,[34] research related to COVID-19 vaccines, [35] and PII.[36,37,38] For example, in May of 2019, DOJ charged two Chinese nationals with conspiracy and intentional damage to a protected computer related to the hacking of Anthem, Inc., and stealing the sensitive personal data of approximately 78.8 million Americans in 2015.[39] In January of 2020, DOJ charged four members of the People's Liberation Army, the armed forces of the PRC, with conspiracy, fraud and espionage related to the hacking into protected computers of Equifax Inc. and stealing the sensitive personal information of 145 million Americans in 2017.[40] In August of 2017, DOJ charged a Chinese national with conspiracy

---

[26] https://www.aspi.org.au/report/engineering-global-consent-chinese-communist-partys-data-driven-power-expansion
[27] https://s3-ap-southeast-2.amazonaws.com/ad-aspi/2019-10/Engineering%20global%20consent%20V2.pdf?eIvKpmwu2iVwZx4o1n8B5MAnncB75qbT
[28]http://webcache.googleusercontent.com/search?q=cache:HRPDTs985OIJ:https://www.technologyreview.com/2020/08/19/1006455/gtcom-samantha-hoffman-tiktok/&hl=en&gl=us&strip=1&vwsrc=0
[29] Rich Barger, Chief Intelligence Officer of ThreaetConnect, a Northern Virginia Cybersecurity Firm.
[30] https://www.washingtonpost.com/world/national-security/in-a-series-of-hacks-china-appears-to-building-a-database-on-americans/2015/06/05/d2af51fa-0ba3-11e5-95fd-d580f1c5d44e_story html
[31] See Appendix D for notable examples of Chinese government or government-affiliated groups targeting U.S. personally identifiable information.
[32] https://www.cnbc.com/2019/09/23/chinese-theft-of-trade-secrets-is-on-the-rise-us-doj-warns.html
[33] https://www.justice.gov/opa/information-about-department-justice-s-china-initiative-and-compilation-china-related
[34] https://www.justice.gov/opa/pr/two-chinese-hackers-working-ministry-state-security-charged-global-computer-intrusion
[35] https://www.justice.gov/opa/pr/two-chinese-hackers-working-ministry-state-security-charged-global-computer-intrusion
[36] https://www.justice.gov/opa/pr/member-sophisticated-china-based-hacking-group-indicted-series-computer-intrusions-including
[37] https://www.justice.gov/opa/pr/chinese-military-personnel-charged-computer-fraud-economic-espionage-and-wire-fraud-hacking
[38] https://www.cnn.com/2017/08/24/politics/fbi-arrests-chinese-national-in-opm-data-breach/index.html
[39] See https://www.politico.com/story/2019/05/09/chinese-hackers-anthem-data-breach-1421341
[40] See https://www.nytimes.com/2020/02/10/us/politics/equifax-hack-china.html

related to the Office of Personnel Management data breach, announced in 2015, where sensitive personal data of millions of current and former USG employees was stolen.[41] These are just a few of the numerous examples of the PRC's efforts to collect U.S. PII and sensitive personal data.

2. The CCP exerts influence over private Chinese companies such as Tencent and its employees through direct ties to personnel and corporate "Party Committees."

Corporate CCP Committees (*e.g.,* Party Committees) are a mechanism through which Beijing expands its authority and supervision over nominally private or non-governmental organizations, creating different nuances of corporate governance with PRC characteristics.[42] As of 2017, Party Committees existed in around 70 percent of 1.86 million private owned companies in China.[43] [44] [45] A Party Committee is formed by a group of senior CCP members who are given a leadership position inside public and private companies operating in China. The 2012 Constitution of the Communist Party of China provides the legal framework for this activity. Within private enterprises, the Party Committee implements CCP's policies and operates through the Trade Union and the Communist Youth League Organization.

According to press reporting, Party Committees have explicit roles even within foreign companies operating in the PRC, which has raised debates among investors involved in joint ventures (JVs) with PRC state-owned enterprises. Even if PRC law regulates the establishment of Party Committees in foreign invested enterprises (both JVs and fully owned) without requiring governance roles for their members, recent trends in officials' attitudes — which are oriented toward the demand for more power — indicate accelerating interference by the CCP in corporate activities in the PRC. This suggests that these positions on Party Committees are not merely symbolic, but rather an eventual source of political pressure in the boardroom. [46]

Tencent established a party organization as early as 2005, followed by a Party Committee in 2011 in which senior vice president Guo Kaitian served as party secretary. By 2013, it was one of the only Chinese tech firms to have publicly disclosed in English the existence of a Party Committee in the company. As of early 2017, the Party Committee boasted nine general branches, 89 party branches and 3,386 members.[47][48] Internally, Tencent has built an automated system within its human resources department for identifying CCP members. The company has led the way in "party building" among Internet companies. In 2016, it became the first Internet company to have a nationally recognized Party Committee. It was also the first Internet company to create a party propaganda magazine, *Tengxian*, and

---

[41] See https://federalnewsnetwork.com/workforce/2017/08/fbi-arrest-may-be-first-linked-to-opm-hack/

[42] https://www.chinabusinessreview.com/fact-sheet-communist-party-groups-in-foreign-companies-in-china/

[43] https://thediplomat.com/2019/12/politics-in-the-boardroom-the-role-of-chinese-communist-party-committees/

[44] https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwir3cKxo9DrAhUponIEHenaAIAQFjAAegQIAxAB&url=https%3A%2F%2Fwww.acga-asia.org%2Ffiles.php%3Faid%3D158%26id%3D1212&usg=AOvVaw0H3c8Zr4es4RXAJN2dMdA_, pg 42

[45] https://www.scmp.com/economy/china-economy/article/2174811/chinese-communist-party-needs-curtail-its-presence-private

[46] https://thediplomat.com/2019/12/politics-in-the-boardroom-the-role-of-chinese-communist-party-committees/

[47] https://chinatechmap.aspi.org.au/#/company/tencent

[48] https://sjc.bnu.edu.cn/djgk/zbjs/21149 html?fbclid=IwAR03V0YdiciNO393QcFfZ5uLQtQUYsVa7cZcnkVXHRo3NnRdF1_z0O17ZbM

also has a WeChat public account called, "Tencent Party Members' Home", to publicize its internal party building efforts.[49]

3. PRC Law Requires that Companies Subject to PRC Jurisdiction, such as Tencent, assist with PRCISS intelligence and surveillance efforts.

Over the last several years, the PRC government has actively worked to increase its influence over all Chinese companies and citizens, through new laws and regulations.[50] Of these laws, the 2017 National Intelligence Law is the most explicit in its requirements for PRC companies and citizens in complying with and assisting in intelligence and national security objectives. The National Intelligence Law obliges individuals, organizations, and institutions to assist Public Security and State Security officials in carrying out a wide array of intelligence work. Specifically, Article 7 provides that "[a]n organization or citizen shall support, assist in and cooperate in national intelligence work in accordance with the law and keep confidential the national intelligence work that it or he knows." Article 14 permits Chinese intelligence institutions to request citizens and organizations to provide necessary support, assistance, and cooperation. Furthermore, Article 17 allows Chinese intelligence agencies to take control of an organization's facilities, which includes communications equipment.

Though less explicit in their requirements, China maintains other laws under which Tencent also would be required to assist PRC State Security and Intelligence Services. The PRC's National Cybersecurity Law, passed in 2017, requires network operators to store select data within China and allows Chinese authorities to conduct spot-checks on a company's network operations. Article 28 of China's Cybersecurity Law states, "[n]etwork operators shall provide technical support and assistance to public security organs and national security organs that are safeguarding national security and investigating criminal activities in accordance with the law." [51] The PRC's National Security Law, passed in 2015, states, "All citizens of the People's Republic of China...shall have the responsibility and obligation to maintain national security."[52] According to press reporting, "[the law] includes elements that define criticism of the government as a form of subversion. It is very vague in defining what kind of specific actions would constitute a citizen endangering state security." [53]

As the recently passed Hong Kong Security Law demonstrates, the PRC now seeks to apply its security laws beyond the borders of mainland China. Article 38 of the Hong Kong Security Law specifically states the law is applicable to every individual including those outside of Hong Kong. Arguably, this would apply the Hong Kong Security Law to every person or company anywhere regardless of whether or not they are located in mainland China. Finally, Chinese companies that oppose requests from PRC intelligence or security services do not have adequate legal recourse to challenge such requests, given the PRC judiciary's lack of independence from the CCP. Though PRC

[49]https://chinatechmap.aspi.org.au/#/company/tencent

[50] See Appendix E for a description of 2015's National Security Law and 2017's Cybersecurity Law, which similarly compel companies and citizens to comply with government directives in furtherance of national security and intelligence objectives. It also contains a broader description of 2017's National Intelligence Law.

law purportedly requires that courts exercise judicial power independently, without outside interference.[54] Judges regularly receive political guidance on pending cases, including instructions on how to rule, from both the government and the CCP, particularly in politically sensitive cases.[55]

4. Tencent has complied with and assisted the PRC with its domestic and global monitoring, surveillance, and censorship efforts.

Tencent's CEO, who is a member of the CCP, has been transparent regarding the company's collaboration with the PRC. For example, Tencent worked with the police in the city of Guangzhou to create an early warning system for tracking the movement of and predicting the size of crowds.[56]

According to press reporting, in May 2020, Liu Yanli was sentenced to four years imprisonment by the Dongbao District People's Court in Hubei's Jingmen city, which found her guilty of "picking quarrels and stirring up trouble," a public order charge frequently used to target peaceful critics of the regime. Liu was accused of criticizing the ruling party and Chinese leaders – "maliciously speculating on hot topics in current affairs" – based on social media posts from four years ago. Liu had repeatedly blogged about rights issues on multiple WeChat groups, campaigned in support of PLA veterans living in hardship, and called on officials to reveal details of their private wealth. She also posted comments about late supreme leader Mao Zedong, his premier Zhou Enlai, and current Chinese president Xi Jinping.[57]

According to press reporting, in March 2020, authorities in a Tibetan-populated county in Qinghai have begun closing chat groups on the popular social media platform Weixin, accusing users of disrupting social order by spreading false information on the spread of China's coronavirus. According to a report by the official Guinan News on March 4, 2020, over 75 groups were closed and another 223 placed under supervision following a sweep of 16 villages and five monasteries in Mangra (in Chinese, Guinan) county in the Tsolho (Hainan) Tibetan Autonomous Prefecture. The report also stated that "[t]he police will not tolerate and will investigate and punish illegal acts that fabricate and spread rumors and disrupt social order."[58] [59]

Both of the aforementioned examples along with those contained in Appendix F demonstrate how the WeChat or Weixin accounts of users in China are under constant surveillance by PRC authorities. Further, a report published by Citizen Lab in May 2020 revealed that WeChat communications conducted entirely among non-China-registered accounts are also subject to pervasive content surveillance that was previously thought to be exclusively reserved for China-registered accounts. Documents and images transmitted entirely among non-China-registered accounts undergo content surveillance wherein these files are analyzed for content that is politically sensitive in China. Files deemed politically sensitive are used to invisibly train and build WeChat's Chinese political

[54] See Dr. Christopher Ashely Ford, Assistant Sec'y of State for the U.S. Dep't of State Bureau of Int'l Security and Nonproliferation, Remarks at the Multilateral Action on Sensitive Techs. Conference (Sept. 11, 2019), https://www.state.gov/huawei-and-its-siblings-the-chinese-tech-giants-national-security-and-foreign-policy-implications/.
[55] See Ford Remarks.
[56] See https://www.wsj.com/articles/chinas-tech-giants-have-a-second-job-helping-the-government-see-everything-1512056284
[57] https://www.rfa.org/english/news/china/clerk-05062020112829.html?searchterm:utf8:ustring=%20wechat
[58] https://www.rfa.org/english/news/tibet/rumors-03052020145022 html?searchterm:utf8:ustring=%20wechat
[59] See Appendix F for examples of Tencent facilitating PRC monitoring, surveillance, and censorship.

censorship system.[60] In an analysis of WeChat's privacy agreements and policy documents, Citizen Lab found that Tencent and WeChat provide no clear reference or explanation of the content surveillance features and, therefore, absent performing their own technical experiments, users cannot determine if, and why, content surveillance was being applied.[61]

WeChat users running large group chats have received automated warnings about politically sensitive content. Some political activists say their WeChat accounts have been suspended or closed for posts critical of the government.[62] There are examples of U.S. citizens being censored from WeChat groups and having their accounts frozen. As a result, many U.S. users of WeChat choose to censor the messages and content they share with their contacts in China. WeChat is one of the limited options available to those who want to communicate with Chinese citizens and U.S. users may choose to self-censor their content rather than risk losing the ability to communicate through the app.[63][64]

B. Vulnerability

The WeChat mobile application collects and transmits sensitive personal information on U.S. persons, which is accessible to Tencent and stored in datacenters in China and Canada. (b) (4)

[redacted]

(b) (4)

WeChat user data is transmitted and stored in data centers owned by Tencent in Ontario, Canada and Hong Kong Special Administrative Region (SAR), People's Republic of China. (b) (4)

[redacted]

[60] https://citizenlab.ca/2020/05/we-chat-they-watch/
[61] https://citizenlab.ca/2020/05/we-chat-they-watch/
[62] https://www.wsj.com/articles/chinas-tech-giants-have-a-second-job-helping-the-government-see-everything-1512056284
[63] See Appendix A for the Office of the Director of National Intelligence's classified threat and counterintelligence assessments assessment which provides further support for the assessment contained herein.
[64] See Appendix G for examples of PRC censorship affecting U.S. WeChat users.
[65] Note that information provided by Tencent in response to our administrative subpoena is entitled to business confidential treatment and should not be disclosed publicly.
[66] (b) (4)

[redacted]

[68] https://www.wechat.com/en/privacy_policy html
(b) (4)

[redacted]

(b) (4) [redacted]

Additionally, WeChat states that it may share this data with a range of third-parties, including "regulators and judicial authorities and law enforcement agencies."[72] Data is purportedly retained according to a table found in the privacy policy based on the type of data, ranging from 120 hours after the relevant interaction for "non-persistent and semi-persistent communication between users" to until the account is deleted for data such as "Social Connect Information" that WeChat uses to link to other social media accounts.[73]

The WeChat application is largely built around a cloud-based application, with almost all features implemented through calls to centralized application programming interfaces located on servers controlled by WeChat or its related subsidiaries or designees. In order to be processed, data must be unencrypted across the internal platform. The data is necessarily concentrated on the WeChat servers. It is less clear exactly where those servers are, under whose jurisdiction they lie, and what internal and external access and controls exist for this data. Although WeChat's policy states that its servers are located in Canada and Hong Kong, it also acknowledges the possibility of data being accessed from locations around the world,[74] and the vulnerability therefore also exists in the access to unencrypted cloud-based data. This data may be accessible from unknown locations not specified by WeChat in its privacy policy.

WeChat users can also use "mini-programs," which can access a range of data, from medical records to location data. There has been some concern even inside China about lack of data security and controls around mini-program data access, although Tencent has recently attempted to address this with stronger internal data protection and policy.[75] However, the stated privacy policies may contradict actual function. For example, in 2018, a Chinese anti-corruption case illustrated that chat history data was used in investigations, in contrast to claims that chat histories are not stored by Tencent, even after user deletion.[76]

Finally, the accessibility of information available to WeChat on users' devices presents its own unique vulnerability. WeChat uses smart-phone features that allow access to users' stored photos, microphone for voice chat, and geolocation information. Although this access is mediated by the smartphone operating system's access control model, once the user does provide permission, it may be accessible even when users are not using the application, dependent on user permissions access on iOS or Android "splash screen request,", which may allow the application persistent permission to "always allow" access to this data.

(b) [redacted]

[72] https://www.wechat.com/en/privacy_policy html
[73] https://www.wechat.com/en/privacy_policy html
[74] ,https://www.wechat.com/en/privacy_policy html
[75] https://www.scmp.com/tech/apps-social/article/3065206/tencents-wechat-tightens-privacy-controls-third-party-apps-calls and https://www.thedrum.com/news/2020/04/13/wechats-new-privacy-controls-what-does-it-mean-users-and-advertisers
[76] https://www.scmp.com/news/china/policies-politics/article/2143920/growing-privacy-fears-china-after-cadres-punished-over

C. Consequence

1. Exploitation of WeChat user data imperils the privacy of U.S. citizens, the security of U.S. government personnel, and, at scale, directly threatens the economic security and national security of the United States.

One of the foremost national security risks presented by the WeChat mobile application in the United States is the possibility that the PRC government could, through lawful authority, extralegal influence ("Communist Party"), or PRCISS, compel Tencent to provide systemic access to U.S. user's sensitive personal information. A number of press reports clearly indicate the PRC Government has already compelled Tencent to assist them for domestic surveillance and law enforcement action within China, and their compliance is indicative of how they are likely to respond to intelligence requests on U.S. users. Given the bounty of information WeChat could offer on foreign users, as well as the aforementioned cyber tactics employed by the PRC, the Department of Commerce assesses the PRC and PRCISS would not limit their use of WeChat to domestic concerns and would instead use it for foreign intelligence and surveillance.

Tencent's assertion that its Hong Kong servers are "not subject to PRC law" is not entirely accurate and fails to capture the nuance of either the national security laws in question or PRC's governance of Hong Kong under the 'one country, two systems' arrangement. Tencent is headquartered in Shenzen, China, and is thus subject to PRC national security laws that require or compel the assistance of any Chinese citizen or entity in surveillance and intelligence operations. As Tencent is subject to PRC jurisdiction, PRC laws can compel cooperation from Tencent, regardless of whether Tencent's subsidiaries are located outside the territory of the PRC. Additionally, it is in Tencent's best interest to maintain positive relations with the CCP as any perception that the company is 'disloyal' or not conducting its business with the best interest of the party could jeopardize its standing and business interests in China. This dynamic presents significant *extra-legal* pressure on Tencent to comply with and actively assist in PRCISS intelligence collection and surveillance efforts.

Furthermore, Tencent cannot account for surveillance that may be conducted on its operations without its explicit knowledge or awareness at a corporate level. PRCISS are active in Hong Kong and possess the capability to surveil traffic incoming to or routed through mainland China. Chinese intelligence services could compromise the Hong Kong-based servers themselves or intercept Internet traffic coming to the server. Alternatively, they could compel the assistance of WeChat's core engineering team based in Guangzhou or other personnel involved in software development and engineering to directly compromise the app through routine app updates. Intelligence services could also compel the assistance of any third-party companies with whom Tencent contracts to service the WeChat application – including data management, software development, analytics, etc. These intelligence operations could ostensibly occur without Tencent's express knowledge or awareness at a corporate level.

Although WeChat's policy states its servers are located in Canada and Hong Kong,[77] modern cloud-based applications require complex and dynamic data flows, especially for AI-driven learning and automation for its user-base and geography of transiting data. Given the large user base in China, the

[77] https://www.wechat.com/en/privacy_policy html

overlap in some functionality between WeChat and Weixin, and the fact that data remains unencrypted across the internal platform, it is likely that some data would be processed and thus accessible inside China. Even certain mitigation measures such as modern access control, logs, and audits to minimize privacy harms would not protect against interference under certain national security laws and practices documented in China. Ultimately, like most cloud-based applications, physical, legal, or logical control of servers containing user data could allow complete compromise of confidentiality, integrity, and availability of unencrypted information. U.S.-based firms adopt transparent practices such as external audits to help reassure the global marketplace. Evidence for these practices at WeChat is minimal, limited to a privacy policy and submitting to a Payment Card Industry Data Security Standard audit.[78]

The consequence of WeChat's ability to host "mini-programs," grows exponentially given specific details of how information is potentially continually accessible even after deletion. This accessibility is a direct threat to U.S. persons' privacy and our national security. When mini-programs are used to access medical records for example, combined with the lack of transparency in Tencent's collection of data flowing across unencrypted cloud-based servers, U.S. users' medical information may be subject to manipulation and exploitation by adversaries. Similar to Russia's hacking of the World Anti-Doping Agency's database, foreign adversaries can and will use confidential medical information to their advantage.[79] [80] [81] Furthermore, medical information in the hands of our adversaries can lead to targeted efforts by our adversaries to identify and potentially exploit individuals in the USG or private sector with access to sensitive information or systems.

Given Tencent's history of cooperation with PRC officials, the extensive amount of sensitive personal data collected by their apps, both inside and outside of China, and their strong ties to the CCP and supporting its agenda, the WeChat app could expand the PRC's ability to conduct espionage on millions of U.S. persons. The PRC has stolen various types of sensitive data on millions of Americans to include health, financial, and other PII. Applications such as WeChat also collect other types of information, to include location data. The PRC could combine these various types of data, which they possess, and continue to collect, in order to build dossiers on millions of U.S. persons. Funneling all these various types of information into their AI apparatus could potentially create a platform to enhance the PRC's ability to identify espionage targets for intelligence collection purposes.

2. *Exploitation of WeChat for censorship or propaganda for U.S.-based users directly threatens U.S. national security by surreptitiously influencing U.S. public opinion to those that align with Chinese government objectives.*

Chinese companies, such as Tencent, must comply with the China Internet Security Law and the CCP exerts significant control of those entities, as described above.[82] Along these lines, Tencent's monitoring operations use computers to filter streamed videos, news feeds and other online platforms for thousands of words and phrases determined to be offensive. The censors at Chinese companies, such as Tencent, are also responsible for blocking news that portrays China negatively in addition to any

[78] https://www.wechat.com/en/privacy_policy html
[79] https://www healthcareitnews.com/news/medical-data-us-olympic-athletes-leaked-russian-hackers
[80] https://www.nytimes.com/2018/01/10/sports/olympics/russian-hackers-emails-doping.html
[81] https://nationalpost.com/sports/olympics/wada-claims-russian-hackers-leaked-fake-medical-records-in-effort-to-discredit-legitimate-use-of-banned-drugs
[82] See https://www.wsj.com/articles/chinas-tech-giants-have-a-second-job-helping-the-government-see-everything-1512056284

unfavorable references to the CCP and its senior leaders.[83] By severely limiting the dissemination of any content it deems controversial, the CCP is seeking to subversively influence the views of millions of U.S. WeChat users. As a result, WeChat offers a platform for the PRC that allows only pro-CCP propaganda and content to millions of U.S. users.

The CCP is dictating how millions of WeChat users in the U.S. handle politically sensitive information through the suspension and closure of U.S. citizens' accounts. Users outside of China, including millions of U.S. users, who share controversial material may initially receive warnings about the content they are sharing. There are many examples of U.S. citizens who continued to send material deemed to be offensive or disloyal to the CCP, resulting in their accounts being suspended. In order to continue using WeChat, U.S. citizens are forced to self-censor the content they share or jeopardize losing their preferred communication platform with their contacts in China. U.S. based users may choose to self-censor their content rather than risk losing the ability to communicate through WeChat.[84]

IV. RECOMMENDATION

Barring a complete divestiture of Tencent from the WeChat application, WeChat presents an immitigable risk to the national security, foreign policy, and economy of the United States. While WeChat has presented the Department of Commerce with a proposal to mitigate the concerns identified in EO 13943, we do not believe that this or any other mitigation proposal would be sufficient to address the aforementioned national security risk presented by WeChat under Tencent ownership.[85] Tencent's mitigation proposal specifically sought to create a new U.S. version of the app, deploy specific security measures to protect the new apps source code, partner with a U.S. cloud provider for user data storage, and manage the new app through a U.S.-based entity with a USG approved governance structure. Additionally, the Department considered additional mitigations to include escrow and review of WeChat's source code, regular compliance audits and notifications, and stringent approvals over management and personnel with access to user data.

However, all of these proposals still allowed Tencent to retain ownership of WeChat and would therefore not address our concerns regarding Tencent. Specifically, appropriately addressing national security concerns through mitigation requires a baseline level of trust in the entity subject to the mitigation terms. Given that WeChat remains under Tencent ownership, Tencent maintains a deep relationship with the CCP and PRC; PRC laws remain applicable to Tencent's operations outside of China, Tencent continues to support ongoing efforts to support PRC surveillance and censorship; and PRCISS's continue to engage in an ongoing pattern of espionage to collect U.S. person information. There is no way to create such a baseline of trust that would allow for effective mitigation without a complete divestiture from Tencent ownership.

The below prohibitions on certain business-to-business transactions deny access to and reduce the functionality of the WeChat mobile app within the land or maritime borders of the United States with the objective of preventing collection, transmission, and aggregation of U.S. user data by the WeChat app, Tencent, and PRCISS. Note that these transactions do not directly prohibit the

[83] See https://www.wsj.com/articles/chinas-tech-giants-have-a-second-job-helping-the-government-see-everything-1512056284
[84] See https://www.npr.org/2019/08/29/751116338/china-intercepts-wechat-texts-from-u-s-and-abroad-researcher-says
[85] See Appendix I for Tencent's mitigation proposal submitted to the Department of Commerce.

downloading or use of the WeChat app and are not directly targeted at users of the WeChat app. While these prohibitions may ultimately make the application less effective and may be challenging for U.S.-based WeChat users, but they are necessary for the protection of U.S. national security. We hope that other communications platforms may take its place.

We recommend that these prohibitions go into effect on September 20, 2020. While this offers a short timeframe for compliance, it should be noted that Tencent maintains a relatively small infrastructure in the United States to support the WeChat app. It maintains no data centers (b) (4) [redacted] under which the following prohibitions would apply. For these reasons, we judge the feasibility of compliance to be high. Given the national security risk in this case has been assessed to be high, and the costs and difficulty of compliance to be low, we recommend these prohibitions to go into effect in line with the timeline set by EO13943.

1. ***Any provision of services to distribute and maintain the WeChat mobile application, constituent code, or mobile application updates through an online mobile application store, or any online marketplace where mobile users may download or update applications for use on their mobile devices, accessible in the land or maritime borders of the United States and its territories;***

This prohibition would remove the WeChat app from U.S.-based mobile app stores, preventing mobile users from being able to download the app to their devices or receive updates. As scoped, this prohibition would only apply to app stores accessible in the United States, thus users would still be able to download the app while outside the United States. Additionally, the prohibition would not require the removal of the app from user devices, thus the app would remain on any device where the app has been downloaded prior to the order. However, these apps would no longer have the ability to be updated rendering them less effective and functional. This prohibit would limit availability of the app, but it alone would not prevent user data from being transmitted from user devices to WeChat data centers. Additional transactions below are necessary to minimize and reduce its use in the United States.

2. ***Any provision of Internet hosting services enabling the functioning or optimization of the WeChat mobile application, within the land and maritime borders of the United States and its territories;***

(b) (4) [redacted] his prohibition ensures that in the future, Tencent will be unable to host WeChat user data in the United States (in its data centers or through leased hosting services) or move WeChat's DNS host to the United States.

3. ***Any provision of content delivery services enabling the functioning or optimization of the WeChat mobile application, within the land and maritime borders of the United States and its territories;***

Tencent contracts with (b) (4) content delivery network ("CDN") providers[86] for the purposes of speeding delivery and optimizing service for users based in the United States. This prohibition would terminate those agreements and will likely reduce functionality and usability of the app for users within the United States.

4. ***Any provision of directly contracted or arranged Internet transit or peering services enabling the functioning or optimization of the WeChat mobile application, within the land and maritime borders of the United States and its territories;***

Tencent maintains peering agreements[87] (b) (4) for the purposes of speeding delivery and optimizing service for users based in the United States. This prohibition would terminate those agreements and likely reduce functionality and usability of the app for users within the United States.

5. ***Any provision of services through the WeChat mobile application for the purpose of transferring funds or processing payments to or from parties within the land or maritime borders of the United States and its territories; or***

Weixin's "WeChat Pay" functionality is not currently available in the United States. This prohibition ensures that, in the future, financial institutions will not be able to process payments or transfers of funds conducted through the WeChat app to or from parties in the United States, in the event that the service becomes available or a user manages to find an unauthorized method to use WeChat Pay in the United States.

6. ***Any utilization of the WeChat mobile application's constituent code, functions, or services in the functioning of software or services developed and/or accessible within the land and maritime borders of the United States and its territories.***

This prohibition serves to prevent any potential circumvention of the aforementioned prohibitions, as it would prohibit any method by which WeChat code, functions, or services could be serviced in a separately named and sold mobile app to which the aforementioned provisions would not apply. Additionally, it prevents interoperability with third-party apps that utilize WeChat functions and services, thus reducing any U.S. user data that could be collected incidentally and made accessible to Tencent.

We recommend that, consistent with your obligation under EO 13943, you prohibit these transactions effective September 20, 2020.

[86] Content delivery services are service that copy, save, and deliver content, for a fee, from geographically dispersed servers to end-users for the purposes of enabling faster delivery of content.
[87] Peering means a relationship between Internet service providers (ISP) where the parties directly interconnect to exchange Internet traffic, most often on a no-cost basis.

EXECUTIVE SECRETARIAT CLEARANCE:

_____ _____

Executive Secretariat Date

FOR OFFICIAL USE ONLY

Tracking Number: _____

DECISION FOR THE SECRETARY

Approval recommendation to prohibit transactions above in accordance with EO 13943.

 I approve the prohibitions outlined herein.

_____ I do not approve the prohibitions outlined herein.

_____ I approve as amended.

_____ I would like to discuss this issue.

EXHIBIT B

CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE NOTE

(U) September 2, 2020; XXXX EDT.

(U) TIKTOK AND WECHAT RISK ASSESSMENT

(U) KEY FINDINGS

- (U//FOUO) The Department of Homeland Security (DHS), Cybersecurity and Infrastructure Security Agency (CISA) assesses that TikTok and WeChat collect large amounts of information on users, have censored information deemed politically sensitive by the Chinese government, and would likely provide user and application data to the Chinese government upon request.

- (U//FOUO) The privacy and security concerns associated with the TikTok and WeChat applications (apps) could allow the Chinese government to gain persistent access to mobile devices, connected systems and networks, steal and exploit sensitive data, compromise device and or system integrity, and spread misinformation. These privacy and security concerns, the widespread use of these apps, the companies' ties to the Chinese government, and the legal structure of the Chinese government compelling Chinese entities to act as vestiges of the government create a level of risk resulting in national security concerns for the United States.

- (U//FOUO) To reduce the national security risks associated with these applications, the federal government can leverage the authorities noted in Executive Orders 13942 and 13943, including the prohibition of transactions with TikTok's and WeChat's parent organizations. CISA recommends the TikTok and WeChat applications not be permitted on the devices of State, Local, Tribal, and Territorial (SLTT) partners and critical infrastructure operators as they may provide malicious actors with access to mobile devices and sensitive data.

(U) SCOPE NOTE: CISA produced this risk assessment in response to a request for assistance from the Department of Commerce in implementing the August 6, 2020 Executive Orders concerning TikTok and WeChat. CISA's assessment leveraged fact patterns from publicly available indicators of threat, vulnerability, and consequence to make a risk determination of potential national security consequences stemming from the current usage of the TikTok and WeChat applications. A national security risk determination is a judgement around potential national security concerns. It is not meant to be definitive or predictive of future malicious activity that may or may not occur or future national security impact that may or may not be observed. However, it should be viewed as one, of multiple, pieces of relevant decision support to help inform risk management decisions being considered by policy makers.

(U) OVERVIEW

(U) TikTok is a social networking application allowing users to create and share short videos on their phones and post the content. TikTok is owned by ByteDance, a Beijing-based company founded in 2012 by Zhang Yiming.[1] As of August 2020, TikTok has approximately 100 million active monthly users in the U.S., an increase of roughly 800% since January 2018.[2]

- (U) ByteDance decided to partner with Oracle due to ongoing security concerns related to the application and Executive Order 13942, "Addressing the Threat Posed by TikTok." The ownership structure of TikTok under this deal is not clear as of the writing of this assessment, with Oracle describing itself as ByteDance's "trusted technology partner,"[3][4] Any sale will likely have to go through a licensing procedure with the Chinese government, which recently updated its export restrictions list

to include technologies for "recommendation of personalized information services based on data analysis."[5] If such a sale is approved by all governmental authorities in the U.S. and China, and becomes final, this risk assessment will be revisited to determine if this action substantially impacts the risks identified in this document.

(U) WeChat is a multi-purpose application for messaging, social media, and payments. It is the most popular app in China, with over 1 billion users worldwide and approximately 19 million users in the United States.[6][7] WeChat is owned by Tencent, which is based out of Shenzhen and is one of the largest technology companies in China.

(U//FOUO) TikTok and WeChat offer different services and require varying levels of information and accesses in order to be installed on mobile devices. As Chinese companies, they both may be compelled under the 2017 China Internet Security Law to provide that information to the Chinese government, such as source code and encryption keys.[8][9] [10]

(U) Chinese Government Strategic Intent

(U) The Office of the Director of National Intelligence (ODNI) stated in the 2019 worldwide threat assessment that China is "a persistent cyber espionage threat" that is the most active state involved in cyber espionage against the U.S. and "a growing attack threat to our core military and critical infrastructure systems." ODNI expressed concern that China would use Chinese technology firms "as routine and systemic espionage platforms against the United States and allies."[11] China has shown both intent and capability to hold U.S. companies at risk by stealing intellectual property, pursuing technically sophisticated campaigns (e.g. Cloudhopper and Equifax), and leveraging Chinese companies' market presence and technological reach to negatively impact the competitive market.

(U) ACTIVITY DEMONSTRATING CAPABILITY

(U//FOUO) We assess that TikTok and WeChat collect large amounts of information on users, have censored information deemed politically sensitive by the Chinese government, and could be compelled to provide user and application data to the Chinese government.

(U) TikTok reportedly censored content deemed politically sensitive by the Chinese government.[12] TikTok also collects large amounts of information on its users, including but not limited to location, device type, contacts and social network connections, and browsing and search histories.[13][14]

(U) TikTok Tracked User Data Using Tactic Banned by Google

(U) There have been credible public reports that, over a period of at least 15 months ending in November 2019, TikTok bypassed restrictions in the Android operating system to track user MAC addresses, which are unique identifiers found in all Internet-ready devices. This enabled TikTok to track application users over the long-term even if other identifiers, such as advertising ID and the user account, had been changed.[15]

(U) Tencent, the owner of WeChat, is one of the largest technology companies in China with a history of providing information to, and actively cooperating with, the Chinese government.[16][17][18] The application reportedly censors content that the Chinese Communist Party deems politically sensitive and provides captured personal information of users to the Chinese government when requested.

- (U) As stated in Executive Order 13943, "in March 2019, a researcher reportedly discovered a Chinese database containing billions of WeChat messages sent from users in not only China but also the United States, Taiwan, South Korea, and Australia."[19]

(U) POTENTIAL CONSEQUENCES OF TIKTOK AND WECHAT USE

(U//FOUO) The privacy and security concerns associated with the TikTok and WeChat applications could allow the Chinese government to gain persistent access to mobile devices and connected systems and networks, steal and exploit sensitive data, and spread misinformation. These privacy and security concerns, the widespread use of these apps, the companies' ties to the Chinese government, and the legal structure of the Chinese government compelling Chinese entities to act as vestiges of the government create a level of risk resulting in national security concerns for the United States.

(U) Persistent System Access

(U) The inadvertent or malicious insertion of vulnerabilities within applications that the developer marks as legitimate through digital signatures are nearly impossible to detect. This can provide malicious actors with persistent access to the device on which the app is installed and the capability to intercept data that routes through this device. Poorly or maliciously developed applications make proper network management nearly impossible and can lead to the compromise of other connected network devices.

(U//FOUO) Malicious code, if inserted through TikTok or WeChat, could allow the Chinese government or other malicious actors to compromise the device on which the application is installed, affecting the confidentiality, integrity, and availability of any data traversing the device. The compromised device could also act as a jumping-off point into connected devices and networks, creating the potential for larger impacts to organizations with devices that have these applications installed.

(U) System Access Example

(U//FOUO) A cyber actor could use a mobile Man-In-The-Middle (MiTM) attack to intercept data between an application and a network device to steal sensitive data like usernames and passwords. Once a cyber actor has access to network credentials, they can leverage them as a jumping-off point to gain additional access within the network. Due in part to the growth of man-in-the-middle attacks across North America and Asia, network attacks increased 4% in 2019 and mobile apps are used in nearly 80% of attacks targeting mobile devices.[20]

(U) Data Theft and Exploitation

(U//FOUO) Mobile devices and technologies deliver numerous services to the public and store personal and sensitive data which makes mobile apps an attractive target for cyber actors. This can include, as in the case of TikTok and WeChat, precise location information, contact details, and photos and messages. The increasing use of mobile apps to support functions and services is leading to apps replacing operating systems as the most prominent avenue of cyberattack.[21]

(U//FOUO) The use of TikTok and WeChat applications could expose sensitive data to theft. Data exfiltrated from mobile devices containing these applications could be used for a variety of purposes by the Chinese government. For example, personal data could be used for future exploitation, such as the future development of spear-phishing emails. Usernames and passwords, if not properly protected, could provide malicious actors further access to additional systems and networks, putting sensitive data on those systems and networks at risk. Use of TikTok and WeChat on mobile devices used by government or critical infrastructure personnel could allow the Chinese government to access information on these devices, including potentially sensitive information about assets and operations.

(U) Geolocation Tracking

(U//FOUO) The use by a malicious actor of location data within TikTok and WeChat can reveal details about the number of users in a location, their movements and daily routines, and otherwise unknown associations between users and locations. TikTok and WeChat request permission for location and other resources that are not needed for their function and may collect, aggregate, and transmit information to the Chinese government that exposes a user's location.[22] Even if GPS and cellular data are unavailable or not permitted

by the user, a mobile device calculates location using Wi-Fi or Bluetooth. Apps may also use other sensor data (that does not require user permission) and web browser information to obtain or infer location information.

(U) Misinformation and Censorship

(U//FOUO) WeChat and TikTok may be used for disinformation campaigns that benefit the Chinese government. While China likely uses other social media content to collect information, WeChat and TikTok are beholden to Chinese intelligence and national security laws which puts pressure on the companies to comply with surveillance requests and curate or censor content. In 2020, TikTok videos spread debunked conspiracy theories about the origins of the 2019 Novel Coronavirus.[23] Misinformation on coronavirus in the U.S. has also been spread on WeChat, and WeChat already surveils foreign users of the application in order to improve its ability to censor content.[24][25] The Chinese government could use WeChat and TikTok to censor unfavorable content and promote pro-Chinese government content in an attempt to sway public opinion and sow discord. Exploitation of WeChat and TikTok for censorship or propaganda for U.S. based users deprives U.S. citizens of their civil rights and directly threatens U.S. national security.

(U) RISK MITIGATION

(U//FOUO) To reduce the national security risks associated with these applications, the federal government can leverage the authorities noted in Executive Orders 13942 and 13943, including the prohibition of transactions with TikTok's and WeChat's parent organizations. CISA recommends the TikTok and WeChat applications not be permitted on the devices of State, Local, Tribal, and Territorial (SLTT) partners and critical infrastructure operators as they may provide malicious actors with access to mobile devices and sensitive data.

(U) Further steps are available to limit location data exposure, including disabling location services settings on the device, disabling radio signals such as Bluetooth and Wi-Fi when they are not actively in use, giving apps as few permissions as possible, and disabling advertising permissions to the greatest extent possible.[26]

(U) The National Risk Management Center (NRMC), Cybersecurity and Infrastructure Security Agency (CISA), is the planning, analysis, and collaboration center working in close coordination with the critical infrastructure community to Identify; Analyze; Prioritize; and Manage the most strategic risks to National Critical Functions. These are the functions of government and the private sector so vital to the United States that their disruption, corruption, or dysfunction would have a debilitating impact on security, national economic security, national public health or safety, or any combination thereof. NRMC products are visible to authorized users at HSIN-CI and Intelink. For more information, contact NRMC@hq.dhs.gov or visit https://www.cisa.gov/national-risk-management.

(U) Prepared By: (Style: Date)

(U) PDM20142

[1] (U) https://www.bloomberg.com/profile/company/1439927D:CH
[2] (U) https://www.cnbc.com/2020/08/31/tiktok-sale-bytedance-says-it-will-abide-by-amended-china-export-rules.html
[3] (U) https://www.nytimes.com/2020/09/13/technology/tiktok-microsoft-oracle-bytedance.html
[4] (U) https://www.cnn.com/2020/09/13/tech/microsoft-tiktok-bytedance/index.html
[5] (U) https://www.cnbc.com/2020/08/31/tiktok-sale-bytedance-says-it-will-abide-by-amended-china-export-rules.html
[6] (U) https://www.whitehouse.gov/presidential-actions/executive-order-addressing-threat-posed-wechat/
[7] (U) https://www.bloombergquint.com/technology/wechat-users-in-the-u-s-fear-losing-family-links-with-ban
[8] (U) https://www.uscc.gov/sites/default/files/Research/How%20Chinese%20Companies%20Facilitate%20Tech%20Transfer%20from%20the%20US.pdf
[9] (U) https://thediplomat.com/2017/06/chinas-cybersecurity-law-what-you-need-to-know/
[10] (U) https://thediplomat.com/2017/06/chinas-cybersecurity-law-what-you-need-to-know/
[11] (U) https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf
[12] (U) 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
[13] (U) 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
[14] (U) https://www.washingtonpost.com/technology/2020/07/13/tiktok-privacy/
[15] (U) https://www.wsj.com/articles/tiktok-tracked-user-data-using-tactic-banned-by-google-11597176738?redirect=amp#click=https://t.co/UDXi4EI4Wv
[16] (U) https://www.state.gov/huawei-and-its-siblings-the-chinese-tech-giants-national-security-and-foreign-policy-implications/
[17] (U) https://www.wsj.com/articles/chinas-tech-giants-have-a-second-job-helping-the-government-see-everything-1512056284
[18] (U) https://www.cnbc.com/2020/05/08/tencent-wechat-surveillance-help-censorship-in-china.html
[19] (U) https://www.federalregister.gov/documents/2020/08/11/2020-17700/addressing-the-threat-posed-by-wechat-and-taking-additional-steps-to-address-the-national-emergency
[20] (U) https://www.darkreading.com/mobile/apps-remain-favorite-mobile-attack-vector/d/d-id/1337043
[21] (U) https://www.dhs.gov/science-and-technology/cybersecurity-mobile-app-security
[22] (U) https://media.defense.gov/2020/Aug/04/2002469874/-1/-1/0/CSI_LIMITING_LOCATION_DATA_EXPOSURE_FINAL.PDF
[23] (U) https://www.whitehouse.gov/presidential-actions/executive-order-addressing-threat-posed-tiktok/
[24] (U) https://www.nbcnews.com/news/asian-america/how-chinese-language-media-u-s-are-debunking-wechat-coronavirus-n1156621
[25] (U) https://www.wsj.com/articles/chinas-wechat-monitors-foreign-users-to-refine-censorship-at-home-11588852802
[26] (U) https://media.defense.gov/2020/Aug/04/2002469874/-1/-1/0/CSI_LIMITING_LOCATION_DATA_EXPOSURE_FINAL.PDF

EXHIBIT C

Billing Code: 351020

DEPARTMENT OF COMMERCE

15 CFR Chapter VII

[Docket Number 200917-0248]

RIN: 0605-XD010

Identification of Prohibited Transactions to Implement Executive Order 13943 and Address the Threat Posed by WeChat and the National Emergency with Respect to the Information and Communications Technology and Services Supply Chain

AGENCY: Office of the Secretary, U.S. Department of Commerce.

ACTION: Identification of prohibited transactions.

SUMMARY: Pursuant to Executive Order 13943, the Secretary of Commerce is publishing this Identification of Prohibited Transactions related to WeChat by any person, or with respect to any property, subject to the jurisdiction of the United States, with Tencent Holdings Ltd. (a.k.a. Téngxùn Kònggǔ Yǒuxiàn Gōngsī), Shenzhen, China, or any subsidiary of that entity, to address the national emergency with respect to the information and communications technology and services supply chain declared in Executive Order 13873, May 15, 2019 (Securing the Information and Communications Technology and Services Supply Chain), and particularly to address the threat identified in Executive Order 13943 posed by mobile application WeChat.

DATES: Identification of prohibited transactions is effective as of September 20, 2020, as set forth in Executive Order 13943.

FOR FURTHER INFORMATION CONTACT:

Kathy Smith, U.S. Department of Commerce, 1401 Constitution Avenue NW, Washington, DC 20230; telephone: (202) 482-1859.

For media inquiries: Meghan Burris, Director, Office of Public Affairs, U.S. Department of Commerce, 1401 Constitution Avenue NW, Washington, DC 20230; telephone: (202) 482-4883.

SUPPLEMENTARY INFORMATION:

In Executive Order 13873 of May 15, 2019 (Securing the Information and Communications Technology and Services Supply Chain), the President found that foreign adversaries are increasingly creating and exploiting vulnerabilities in information and communications technology and services (ICTS), which store and communicate vast amounts of sensitive information, facilitate the digital economy, and support critical infrastructure and vital emergency services, in order to commit malicious cyber-enabled actions, including economic and industrial espionage against the United States and its people. The President found that the unrestricted acquisition or use in the United States of ICTS designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of foreign adversaries augments the ability of foreign adversaries to create and exploit vulnerabilities in ICTS, with potentially catastrophic effects, and thereby constitutes an unusual and extraordinary threat to the national security, foreign policy, and economy of the United States, and declared a national emergency with respect to this threat. The President directed that additional steps are required to protect the security, integrity, and reliability of ICTS provided and used in the United States.

On August 6, 2020, in Executive Order 13943 (Addressing the Threat Posed by WeChat, and Taking Additional Steps To Address the National Emergency With Respect to the Information and Communications Technology and Services Supply Chain), the President found that the spread in the United States of mobile applications developed and owned by companies in the People's Republic of China (China) continues to threaten the national security, foreign policy, and economy of the United States. The President directed that action must be taken to address the threat posed by the mobile application WeChat.

Pursuant to Executive Order 13943, any transaction that is related to WeChat by any person, or with respect to any property, subject to the jurisdiction of the United States, with Tencent Holdings Ltd. (a.k.a. Téngxùn Kònggǔ Yǒuxiàn Gōngsī), Shenzhen, China, or any subsidiary of that entity, as identified by the Secretary of Commerce (Secretary) within 45 days from the date of the order, shall be prohibited, to the extent permitted under applicable law. This Identification of Prohibited Transactions implements that directive by the President.

Identifying Prohibited Transactions

Definitions

Content delivery service means a service that copies, saves, and delivers content, for a fee, from geographically dispersed servers to end-users for the purposes of enabling faster delivery of content.

Entity means a government or instrumentality of such government, partnership, association, trust, joint venture, corporation, group, subgroup, or other organization, including an international organization.

Information and communications technology or services means any hardware, software, or other product or service primarily intended to fulfill or enable the function of information or data processing, storage, retrieval, or communication by electronic means, including transmission, storage, and display.

Internet hosting service means a service through which storage and computing resources are provided to an individual or organization for the accommodation and maintenance of one or more websites or Internet services. Services may include but are not limited to file hosting, domain name server hosting, cloud hosting, and virtual private server hosting, among others.

Internet transit service means a service where a network operator provides connectivity, transport and routing for another network, enabling them to reach broader portions of the Internet. A transit provider's routers also announce to other networks that they can carry traffic to the network that has purchased transit.

Mobile application means a software application designed to run on a mobile device such as a phone, tablet, or watch.

Mobile application store means any online marketplace where users can download, or update, and install software applications to a mobile device.

Peering means a relationship between Internet service providers (ISP) where the parties directly interconnect to exchange Internet traffic, most often on a no-cost basis.

Person means an individual or entity.

Subsidiary means a company that is owned or controlled by a parent or holding company.

Transaction means any acquisition, importation, transfer, installation, dealing in, or use of any information and communications technology or service.

Identification of Prohibited Transactions

Pursuant to the International Emergency Economic Powers Act, 50 U.S.C. 1701, *et seq*, Executive Order 13873 (84 FR 22689, May 15, 2019), and as set forth and provided for in Executive Order 13943 (85 FR 48641, August 6, 2020), the Secretary identifies the following transactions that are prohibited, effective as of September 20, 2020:

Any transaction that is related to WeChat by any person, or with respect to any property, subject to the jurisdiction of the United States, with Tencent Holdings Ltd. (a.k.a. Téngxùn Kònggǔ Yǒuxiàn Gōngsī), Shenzhen, China, or any subsidiary of that entity, involving:

1. Any provision of services to distribute or maintain the WeChat mobile application, constituent code, or mobile application updates through an online mobile application store, or any online marketplace where mobile users within the land or maritime borders of the United States and its territories may download or update applications for use on their mobile devices;

2. Any provision of internet hosting services enabling the functioning or optimization of the WeChat mobile application, within the land and maritime borders of the United States and its territories;

3. Any provision of content delivery services enabling the functioning or optimization of the WeChat mobile application, within the land and maritime borders of the United States and its territories;

4. Any provision of directly contracted or arranged internet transit or peering services enabling the functioning or optimization of the WeChat mobile application, within the land and maritime borders of the United States and its territories;

5. Any provision of services through the WeChat mobile application for the purpose of transferring funds or processing payments to or from parties within the land or maritime borders of the United States and its territories;

6. Any utilization of the WeChat mobile application's constituent code, functions, or services in the functioning of software or services developed and/or accessible within the land and maritime borders of the United States and its territories; or

7. Any other transaction that is related to WeChat by any person, or with respect to any property, subject to the jurisdiction of the United States, with Tencent Holdings Ltd., or any subsidiary of that entity, as may be identified at a future date under the authority delegated under Executive Order 13943.

The identified prohibitions herein only apply to the parties to business-to-business transactions, and apply except to the extent provided by statutes, or in regulations, orders, directives, or licenses that may be issued pursuant to Executive Order 13943, and notwithstanding any contract entered into or any license or permit granted before the date of Executive Order 13943. Any other transaction with Tencent Holdings Ltd. or its subsidiaries is permitted under Executive Order 13943, as implemented by the Secretary, unless identified as prohibited or otherwise contrary to law.

These identified prohibitions do not apply to:

(1) Payment of wages, salaries, and benefit packages to employees or contractors;

(2) The exchange between or among WeChat mobile application users of personal or business information using the WeChat mobile application, to include the transferring and receiving of funds;

(3) Activities related to mobile applications intended for distribution, installation or use outside of the United States by any person, including but not limited to any person subject to U.S. jurisdiction, and all ancillary activities, including activities performed by any U.S. person, which are ordinarily incident to, and necessary for, the distribution, installation, and use of mobile applications outside of the United States; or

(4) The storing of WeChat mobile application user data in the United States.

AUTHORITY

International Emergency Economic Powers Act, 50 U.S.C. 1701, *et seq.*; National Emergencies Act, 50 U.S.C. 1601 *et seq.*; Executive Order 13943, Addressing the Threat Posed by WeChat, August 6, 2020; Executive Order 13873, Securing the Information and Communications Technology and Services Supply Chain, May 15, 2019.

Dated: September 17, 2020.

This document of the Department of Commerce was signed on September 17, by Wilbur Ross, Secretary of Commerce. That document with the original signature and date is maintained by the Department of Commerce. For administrative purposes only, and in compliance with requirements of the Office of the Federal Register, the undersigned Department of Commerce Federal Register Liaison Officer has been authorized to sign and submit the document in electronic format for publication, as an official document of the Department of Commerce. This administrative process in no way alters the legal effect of this document upon publication in the Federal Register.

Signed in Washington, DC, on September 17, 2020.

Asha Mathew,

Federal Register Liaison Officer, U.S. Department of Commerce.

[FR Doc. 2020-20921 Filed: 9/18/2020 8:45 am; Publication Date: 9/22/2020]