

No. 20-16908

**IN THE UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT**

U.S. WECHAT USERS ALLIANCE, CHIHUO INC., BRENT COULTER, FANGYI DUAN,
JINNENG BAO, ELAINE PENG, XIAO ZHANG,

Plaintiffs-Appellees,

v.

DONALD J. TRUMP, in his official capacity as the President of the United States,
WILBUR ROSS, in his official capacity as Secretary of Commerce,

Defendants-Appellants.

On Appeal from the United States District Court
for the Northern District of California

**ADDENDUM TO EMERGENCY MOTION
FOR A STAY PENDING APPEAL**

JEFFREY BOSSERT CLARK
Acting Assistant Attorney General

DAVID L. ANDERSON
United States Attorney

H. THOMAS BYRON III
DENNIS FAN
SEAN JANDA

*Attorneys, Appellate Staff
Civil Division, Room 7213
U.S. Department of Justice
950 Pennsylvania Avenue NW
Washington, DC 20530
(202) 514-2494*

TABLE OF CONTENTS

DISTRICT COURT ORDER

Order Granting Motion for Preliminary Injunction (Sept. 19, 2020) (Doc. 59)	1
---	---

EXECUTIVE BRANCH DOCUMENTS

U.S. Department of Commerce, Press Release, Commerce Department Prohibits WeChat and TikTok Transactions to Protect the National Security of the United States (Sept. 18, 2020) (Doc. 45-1, at 15-20)	23
Office of the Secretary, U.S. Department of Commerce, 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 (Sept. 17, 2020) (Doc. 68-1, at 30-37)	31
Office of Intelligence and Security, U.S. Department of Commerce, Memorandum for the Secretary, Proposed Prohibited Transactions Related to WeChat Pursuant to Executive Order 13943 (Sept. 17, 2020) (Doc. 68-1, at 6-22)	37
Cyberscurity and Infrastructure Security Agency, U.S. Department of Homeland Security, Critical Infrastructure Security and Resilience Note (Sept. 2, 2020) (Doc. 68-1, at 24-28)	54
Executive Order 13943, 85 Fed. Reg. 48641 (Aug. 6, 2020) (Doc. 17-12, at 13-15)...	59
White House, United States Strategic Approach to the People's Republic of China (May 20, 2020) (Doc. 22-22, at 2-17)	52
U.S.-China Economic and Security Review Commission, 2019 Report to Congress, 116th Cong. (Nov. 2019) (Doc. 22-18, at 2-43)	78
Executive Order 13873, 84 Fed. Reg. 22,689 (May 15, 2019) (Doc. 17-12, at 17-20)	120

DECLARATIONS AND OTHER FILINGS

Declaration of John Costello (Sept. 24, 2020) (Doc. 68-1, at 1-4)	124
---	-----

Amended Complaint for Declaratory and Injunctive Relief (Sept. 18, 2020) (Doc. 49)	128
Declaration of Jinneng Bao (Aug. 26, 2020) (Doc. 17-1).....	165
Declaration of Ying Cao, Trustee of U.S. WeChat Users Alliance (Aug. 26, 2020) (Doc. 17-2).....	169
Declaration of Brent Coulter (Aug. 25, 2020) (Doc. 17-3).....	175
Declaration of Fangyi Duan (Aug. 26, 2020) (Doc. 17-4)	179
Declaration of Elaine Peng (Aug. 26, 2020) (Doc. 17-5)	186
Declaration of Xiao Zhang (Aug. 26, 2020) (Doc. 17-6)	192

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
San Francisco Division

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

Case No. 20-cv-05910-LB

Plaintiffs,

v.

**ORDER GRANTING MOTION FOR
PRELIMINARY INJUNCTION**

DONALD J. TRUMP, et al.,

Re: ECF No. 17 and 48

Defendants.

INTRODUCTION

The plaintiffs are persons in the United States who use WeChat, a messaging, social-media, and mobile-payment app.¹ In this lawsuit, they challenge the constitutionality of Executive Order 13943, which prohibits (without defining) “transactions” relating to WeChat (to protect national security), effective September 20, 2020. The Executive Order directs the Secretary of Commerce to “identify” the “transactions” that are prohibited. On September 18, 2020, the Secretary issued an “Identification of Prohibited Transactions to Implement Executive Order 13943,” identifying the prohibited transactions.

¹ Compl. – ECF No. 1; First Am. Complaint (“FAC”) – ECF No. 49. The plaintiffs are U.S. WeChat Users Alliance, a nonprofit formed to challenge the WeChat Executive Order, and individual and business users. *Id.* at 7–9 (¶¶ 19–25). Citations refer to material in the Electronic Case File (“ECF”); pinpoint citations are to the ECF-generated page numbers at the top of documents.

In relevant part, the Secretary’s Identification generally bans (1) app stores from distributing the WeChat app or updates to it, (2) internet-hosting, content-delivery, and other internet-transit services that enable the functioning or optimization of the WeChat app, (3) use of the app’s code, functions, or services in the functioning of software or services, and (4) services from allowing the transfer of funds via the app to or from parties in the United States. More colloquially, the result is that consumers in the U.S. cannot download or update the WeChat app, use it to send or receive money, and — because U.S. support for the app by data hosting and content caching will be eliminated — the app, while perhaps technically available to existing U.S. users, likely will be useless to them. In public comments on September 18th, the Secretary said that “[f]or all practical purposes, [WeChat] will be shut down in the U.S. . . . as of midnight Monday.”²

The plaintiffs claim that the ban (1) violates the First Amendment to the U.S. Constitution, (2) violates the Fifth Amendment, (3) violates the Religious Freedom Restoration Act, 42 U.S.C. § 2000bb(1)(a), (4) was not a lawful exercise of the President’s and the Secretary’s authority under the International Economic Emergency Powers Act (“IEEPA”) — which allows the President to prohibit “transactions” in the interest of national security — because the IEEPA, 50 U.S.C. § 1702(b)(1), does not allow them to regulate personal communications, and (5) violates the Administrative Procedures Act (“APA”) because the Secretary exceeded his authority under the IEEPA and should have promulgated the rule through the notice-and-comment rulemaking procedures in 5 U.S.C. § 553(b).³

The plaintiffs moved for a preliminary injunction and contend that they are likely to succeed, and have presented serious questions, on the merits of the First Amendment claim (and satisfied the other elements for preliminary-injunctive relief). First, they contend, effectively banning WeChat — which serves as a virtual public square for the Chinese-speaking and Chinese-

² Ana Swanson & David McCabe, *Trump to Ban TikTok and WeChat from U.S. App. Stores*, N.Y. TIMES, Sept. 18, 2020, <https://www.nytimes.com/2020/09/18/business/trump-tik-tok-wechat-ban.html> (last visited Sept. 18, 2020), Ex. C to Bien Decl. – ECF No. 45-1 at 23. At the September 18 and 19, 2020 hearings, the government did not contest that the court could consider — whether as a party admission or by judicial notice — the Secretary’s statement or other public officials’ statements.

³ FAC – ECF No. 49.

American community in the United States and is (as a practical matter) their only means of communication — forecloses meaningful access to communication in their community and thereby operates as a prior restraint on their right to free speech that does not survive strict scrutiny. Second, even if the prohibited transactions are content-neutral time-place-or-manner restrictions, they do not survive intermediate scrutiny because the complete ban is not narrowly tailored to address the government’s significant interest in national security.⁴ The plaintiffs also contend that they are likely to succeed on the merits of their claims that, by effectively shutting down U.S. users’ access to the WeChat app, (1) the President and the Secretary exceeded their authority under IEEPA, (2) the Secretary violated the APA, and (3) the Executive Order is void for vagueness (in part) because the government asserts conflicting interpretations of the prohibition’s effect.⁵ The government counters that the plaintiffs are not likely to succeed on the merits of their claims and have not established irreparable harm or that the balance of equities tips in their favor.⁶

The court grants the motion on the ground that the plaintiffs have shown serious questions going to the merits of the First Amendment claim, the balance of hardships tips in the plaintiffs’ favor, and the plaintiffs establish sufficiently the other elements for preliminary-injunctive relief.

STATEMENT

The next sections summarize (1) the plaintiffs’ (and the U.S. public’s) use of WeChat, (2) the relevant Executive Orders and agency action, and the plaintiffs’ contentions about the context of the action, (3) the government’s additional contentions about WeChat’s threat to national security, and (4) the case’s procedural history.⁷

⁴ *Id.* at 27–29 (¶¶ 78–86); *see* Mot. – ECF No. 17 at 29–39; Reply – ECF No. 28 at 18–22; Renewed Mot. – ECF No. 48 at 3–5.

⁵ Reply – ECF No. 28 at 17–23; *see id.* at 17–18 (narrowing the void-for-vagueness argument) (citing *Cty. of Santa Clara v. Trump*, 250 F. Supp. 3d 497, 534–35 (N.D. Cal. 2017)); Renewed Mot. – ECF No. 48 at 3–9; *see id.* at 8–9 (narrowing the void-for-vagueness argument further).

⁶ Opp’n – ECF No. 22 at 28–50; Opp’n – ECF No. 51 at 4–14.

⁷ Because this is a preliminary-injunction motion, the court overrules the government’s objections to the Alban and Chemerinsky declarations. Opp’n – ECF No. 22 at 51; *cf. Flynt Distrib. Co. v. Harvey*, 734 F.2d 1389, 1394 (9th Cir. 1984) (“The trial court may give even inadmissible evidence some weight, when to do so serves the purpose of preventing irreparable harm”).

1. WeChat

WeChat is a mobile app, developed by the Chinese company Tencent Holdings Ltd., with more than 1.2 billion users worldwide (including more than 100 million users outside of China and 19 million regular users in the U.S.).⁸ It allows its users to send messages, make video and audio calls, and send and receive money, and it also functions as a social-media platform.⁹

The plaintiffs' declarations establish that in the U.S., Chinese-American and Chinese-speaking WeChat users rely on the WeChat platforms to communicate, socialize, and engage in business, charitable, religious, medical-related, and political activities with family, friends, and colleagues (here in the U.S. and around the world).¹⁰ In the U.S., those in the Chinese-American, Chinese-speaking, and other communities rely on WeChat — as opposed to other platforms — as their “primary source of communication and commerce,” in part because western social-media platforms such as Facebook, WhatsApp, and Twitter are blocked in China, and WeChat often is the only way for its users to reach their networks in China.¹¹ In addition, WeChat provides content (such as the news) in Chinese, which is critical for the many U.S. WeChat users with limited proficiency in English.¹² WeChat also resonates culturally with its U.S.-based Chinese-speaking users because it integrates Chinese traditions into electronic transactions, such as sending gifts of money in “red envelopes.”¹³ Other platforms cannot practically replace WeChat because they lack the cultural relevance and practical interface with China and do not provide the integral connection

⁸ Cohen Decl. – ECF No. 17-9 at 3 (¶ 6); Sun Decl. – ECF No. 17-11 at 10 (¶ 13), 11 (¶ 16); Maya Tribbitt, *WeChat Users in the U.S. Fear Losing Family Links with Ban*, BLOOMBERG, Aug. 11, 2020, <https://www.bloomberquint.com/technology/wechat-users-in-the-u-s-fear-losing-family-links-with-ban>, Ex. TT to Bien Decl. – ECF No. 17-12 at 351.

⁹ Cohen Decl. – ECF No. 17-9 at 3 (¶ 6).

¹⁰ Sun Decl. – ECF No. 17-11 at 11 (¶ 17); Cao Decl. – ECF No. 17-2 at 3–4 (¶¶ 11–20); Peng Decl. – ECF No. 17-5 at 2–3 (¶¶ 1–4, 7–16); Duan Decl. – ECF No. 17-4 at 2 (¶¶ 6, 9), 3 (¶¶ 14, 16).

¹¹ Cohen Decl. – ECF No. 17-9 at 4 (¶ 6); Sun Decl. – ECF No. 17-11 at 9 (¶ 12).

¹² Sun Decl. – ECF No. 17-11 at 10–11 (¶¶ 15, 18); Jeung Decl. – ECF No. 17-10 at 8 (¶ 25) (“Four out of ten Chinese in the United States — and six out of ten of Chinese who are foreign-born — are limited English proficient. This high proportion of our community cannot access English social medial platforms and require WeChat for their communications”).

¹³ Sun Decl. – ECF No. 17-11 at 11 (¶ 16).

that WeChat provides to the Chinese community.¹⁴ In short, WeChat is irreplaceable for its users in the U.S., particularly in the Chinese-speaking and Chinese-American community.¹⁵

Plaintiff Elaine Peng illustrates these points when she describes her WeChat use for personal, political, and business communications, including running her nonprofit organization Mental Health Association for Chinese Communities, which provides mental-health education and services to the local Chinese community.¹⁶ WeChat is her primary tool for outreach and services.¹⁷ For example, she has two WeChat groups: one for internal communications with her 110 volunteers and one with 420 members (volunteers, recipients of services, and family members).¹⁸ Many of the Chinese community members are not fluent in English, and WeChat is the only online tool that they rely on.¹⁹ Most of her 400-plus service recipients are elderly, deficient in English, or both.²⁰ They suffer from mental-health issues that include depression, schizophrenia, bipolar disorder, and post-traumatic stress disorder.²¹ When she founded the nonprofit in 2013, she “went to great trouble” to teach the service recipients how to set up and use WeChat accounts, an effort that involved volunteers who expended “time, energy, and effort” to address the needs of clients who did not know how to use a smart phone.²² If her service recipients lose access to WeChat — “the only channel for them to receive services, educational material, and treatment resources” — it will be a “humanitarian crisis.”²³ In “the last month or so,” she has tried to shift

¹⁴ Cohen Decl. – ECF No. 17-9 at 7 (¶ 15); Sun Decl. – ECF No. 17-11 at 16–17 (¶¶ 32–33).

¹⁵ Cohen Decl. – ECF No. 17-9 at 7 (¶ 15); Sun Decl. – ECF No. 17-11 at 16 (¶ 32).

¹⁶ Peng Decl. – ECF No. 17-5 at 2–3 (¶¶ 1–4, 7–12); Peng Supp. Decl. – ECF No. 48-1 at 2 (¶ 3). The plaintiffs provide other examples too. *See supra* n.10 (collecting declarations).

¹⁷ Peng Supp. Decl. – ECF No. 48-1 at 2 (¶ 4).

¹⁸ *Id.*.

¹⁹ *Id.* (¶ 5).

²⁰ *Id.* (¶ 6).

²¹ *Id.* (¶ 7).

²² *Id.* (¶ 6).

²³ *Id.* (¶ 7).

1 them to other apps, but those apps are in English, and the language barriers and lack of technical
2 skills mean that most of the service recipients cannot be shifted to other apps.²⁴

3 Also, the nonprofit's data — including service recipients' names, addresses, other contact
4 information, and medical information — are stored on WeChat.²⁵ She sends out questionnaires to
5 the recipients via WeChat, staff members conduct one-on-one counseling via WeChat, chat history
6 helps staff members to evaluate and implement treatment, and she knows of no means to transfer
7 this information — housed in WeChat's "own system" — to another platform.²⁶ Losing access to
8 the platform means that she loses data and valuable information that took years to build and that
9 forms the foundation for her nonprofit.²⁷ As another example of WeChat's utility, her organization
10 used WeChat's real-time location-sharing technology to prevent a suicide.²⁸

11 She also uses WeChat to organize teams to disseminate Chinese-language materials —
12 educational information about the election and how to register to vote — to Chinese Americans
13 who mostly do not speak English and use WeChat as their only messaging and social-media app.²⁹
14

15 **2. Executive Orders and Agency Action**

16 **2.1 Executive Order 13873 (May 15, 2019)**

17 On May 15, 2019, the President issued an Executive Order finding that "foreign adversaries
18 are increasingly creating and exploiting vulnerabilities in information and communications
19 technology and services, which store and communicate vast amounts of sensitive information,
20 facilitate the digital economy, and support critical infrastructure and vital emergency services, in
21 order to commit malicious cyber-enabled actions, including economic and industrial espionage
22 against the United States and its people." Executive Order 13873, *Securing the Information and*
23

24 ²⁴ *Id.* (¶ 8).

25 ²⁵ *Id.* at 3 (¶ 9).

26 ²⁶ *Id.*

27 ²⁷ *Id.*

28 ²⁸ *Id.*

29 ²⁹ *Id.* (¶ 10).

1 *Communications Technology and Services Supply Chain*, 84 Fed. Reg. 22,689, 22,689 (the “ICTS
 2 Executive Order”). “The unrestricted acquisition or use in the United States of information and
 3 communications technology or services . . . supplied by persons owned by, controlled by, or
 4 subject to the jurisdiction or direction of foreign adversaries augments the ability of foreign
 5 adversaries to create and exploit vulnerabilities in information and communications technology or
 6 services, with potentially catastrophic effects, and thereby constitutes an unusual and
 7 extraordinary threat to the national security, foreign policy, and economy of the United States.” *Id.*
 8 The President invoked his authority under the “Constitution and laws of the United States,”
 9 including IEEPA and the National Emergencies Act (“NEA”), to declare a national emergency
 10 with respect to this threat. *Id.* He then prohibited transactions with foreign countries or foreign
 11 nationals that pose “an undue risk of sabotage to or subversion” of the “maintenance of
 12 information and communications technology or services in the United States” or “otherwise pose[]
 13 an unacceptable risk” to the national security. *Id.* at 22,690. He directed the Secretary of
 14 Commerce — “in consultation with” the Secretaries of the Treasury, State, Defense, and
 15 Homeland Security and the Attorney General, the U.S. Trade Representative, the Director of
 16 National Intelligence, the Chair of the FCC, and other appropriate officials — to identify
 17 transactions that pose an undue or unacceptable risk to the national security of the United States
 18 and to report to him about the threats from “foreign adversaries.” *Id.* at 22,690-92. The government
 19 references reports to the President from the Department of Homeland Security (mapping the
 20 vulnerabilities of the information-and-communications-technology framework “to assist
 21 identification of vulnerabilities”) and the Office of the Director of National Intelligence (in the
 22 form of a “classified initial threat assessment.”)³⁰

23 On May 13, 2020, the President renewed the declaration of emergency in the ICTS Executive
 24 Order. 85 Fed. Reg. 29,321. On May 20, 2020, he presented a report to Congress “outlining a set
 25 of broad strategies in relation to the U.S.’s foreign policy with China.”³¹

26 _____
 27 ³⁰ Opp’n – ECF No. 22 at 23.

28 ³¹ *Id.* at 23–24 (citing U.S. Strategic Approach to PRC (May 20, 2020), Ex. 22 to Orloff Decl. – ECF
 No. 22-22 at 2–17).

The plaintiffs do not challenge the ICTS Executive Order: “Plaintiffs are not challenging the validity of Executive Order 13873, the President’s May 15, 2019 declaration of a national emergency that is a necessary legal basis for the President to even issue the WeChat [Executive Order]; rather, Plaintiffs challenge the validity only of the *WeChat* [Executive Order].”³²

2.2 Executive Order 13943 (August 6, 2020)

On August 6, 2020, President Trump issued Executive Order 13943, “Addressing the Threat Posed by WeChat, and Taking Additional Steps to Address the National Emergency with Respect to the Information and Communication Technology and Services Supply Chain.” 85 Fed. Reg. 48,641 (the “WeChat Executive Order”). In it, he said that “additional steps must be taken to deal with the national emergency . . . declared in [the ICTS Executive Order]” because “the spread in the United States of mobile applications developed and owned by companies in the People’s Republic of China [] continues to threaten the national security, foreign policy, and economy of the United States.” *Id.* at 48,641. Further action was needed to address the threat that WeChat posed to the national security, foreign policy, and economy of the U.S. because WeChat’s “automatically captur[ing] vast swaths of information from its [over one billion] users” through its messaging, social-media, and electronic-payment applications “threatens to allow the Chinese Communist Party access to Americans’ personal and proprietary information.” *Id.* He cited a researcher’s reported discovery of “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.” *Id.* (The plaintiffs counter that an investigation revealed that this was a data breach.³³) He said that WeChat “reportedly censors content that the Chinese Communist Party deems politically sensitive” and may “be used for disinformation campaigns that benefit the Chinese Communist Party,” and he noted that other countries, including Australia and India, were beginning to restrict or ban the use of WeChat. *Id.* (The plaintiffs counter that Australia limited only its national-defense agency’s employees’ use of WeChat, and India’s restriction was tied to a border dispute

³² Reply – ECF No. 28 at 12–13 (emphasis in original).

³³ Mot. – ECF No. 17 at 20.

with China.³⁴) As a result, “[t]he United States must take aggressive action against the owner of WeChat [Tencent] to protect our national security.” *Id.*

In relevant part, the Order directed the following:

Section 1. (a) The following actions shall be prohibited beginning 45 days after the date of this order, to the extent permitted under applicable law: 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. . . . or any subsidiary of that entity, as identified by the Secretary of Commerce (Secretary) under section 1(c) of this order.

...

(c) 45 days after the date of this order, the Secretary [of Commerce] shall identify the transactions subject to subsection (a) of this section.

...

Section 3. For those persons who might have a constitutional presence in the United States, I [the President] find that because of the ability to transfer funds or other assets instantaneously, prior notice to such persons of measures to be taken pursuant to section 1 of this order would render those measures ineffectual. I therefore determine that for these measures to be effective in addressing the national emergency declared in Executive Order 13873, there need be no prior notice of an identification made pursuant to section 1(c) of this order.

Id. at 48,641–42. Thus, under the Order, effective September 20, 2020, transactions related to WeChat — as defined by the Secretary in the Identification of Prohibited Transactions — are banned.

2.3 The President’s Statements Before and After the WeChat Order

The plaintiffs point to the President’s anti-Chinese statements around the time he issued the WeChat Order, including his remarks about China’s responsibility for the COVID-19 pandemic (including calling it the “China virus,” the “China flu,” and similar names), his reference to China’s owning the United States if he is not reelected, and other mocking conduct that the plaintiffs characterize as showing racial animist and aimed at bolstering the President’s reelection campaign.³⁵

³⁴ *Id.* at 21.

³⁵ *Id.* at 21 (citing Interviews and Comments, Exs. E–P to Bien Decl. – ECF No. 17-12 at 30–100).

2.4 The Secretary of Commerce's Implementation of the WeChat Executive Order

On September 18, 2020, the Secretary issued the Identification of Prohibited Transactions, which set forth the following prohibited transactions:

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.³⁶

³⁶ Notice – ECF No. 28 at 2–3; Secretary's Identification of Prohibited Transactions, Ex. A to Bien Decl. – ECF No. 45-1 at 10–11.

The plaintiffs cite media reports, including the Secretary’s remarks (discussed above) that the prohibitions will effectively shut down WeChat for U.S. users.³⁷

3. The Government’s Additional Contentions About National Security

The government describes the threat to national security posed by China’s activities in the information-and-communications technology and services sectors.³⁸

For example, in 2010, bipartisan legislators wrote to the Chairman of the FCC asking for information about the security of U.S. telecommunication networks in the context of a proposed deal involving Sprint, Cricket, Huawei, and ZTE. In the letter, they observed that Huawei and ZTE — two companies with significant ties to the Chinese government — were “aggressively seeking to supply sensitive equipment for U.S. telecommunications infrastructure” and to service U.S. networks.³⁹ In 2011, the House Permanent Select Committee on Intelligence launched an investigation focused on Huawei and ZTE but expressed the broader concern that Chinese telecommunication companies with suspected ties to the Chinese government could provide opportunities for “espionage for a nation-state already well-known for perpetuating cyber-attacks and espionage on the United States” and could allow China to exert pressure or control over critical infrastructure or give it access to sensitive government and proprietary information, resulting in unfair diplomatic or commercial advantage over the U.S.⁴⁰ The government cites other contemporaneous reports regarding similar national-security concerns given the close ties that the so-called private companies maintained with the Chinese government.⁴¹

Then, the government identifies the risk that reliance on mobile technologies poses to national security, citing reports about the threat that results from China’s strategic insertion of its

³⁷ Response to Notice – ECF No. 45 at 2–3 (also characterizing the agency’s remarks as inconsistent).

³⁸ Opp’n – ECF No. 22 at 15–22.

³⁹ *Id.* at 15 (citing *Congressional Leaders Cite Telecommunications Concerns With Firms That Have Ties With Chinese Government* (Oct. 19, 2010), Ex. 1 to Orloff Decl. – ECF No. 22-1 at 3).

⁴⁰ *Id.* at 15–16 (citing Investigative Rep. on the U.S. Nat’l Sec. Issues Posed by Chinese Telecomms. Cos. Huawei and ZTE (Oct. 8, 2012), Ex. 2 to Orloff Decl. – ECF No. 22-2 at 6–8).

⁴¹ *Id.* at 16 (collecting reports).

companies and products into networks and markets outside of China.⁴² The government describes the vulnerabilities that result from, for example, 5G cellular networks.⁴³ It points to government-contracting decisions — embodied in the 2019 defense-appropriations bill — prohibiting government agencies and contractors from using telecommunications or video-surveillance equipment or services produced by ZTE, Huawei, and “other identified Chinese entities.”⁴⁴

Finally, the government cited reports identifying Tencent and WeChat as a growing threat and citing an Australian nonpartisan think tank’s report (1) discussing the Chinese government’s “highly strategic foreign policy” to become “the strongest voice in cyberspace,” (2) identifying Tencent as “one of a handful of Chinese companies ‘reported to have the highest proportion of internal [Chinese Communist Party committees] within the business sector,’” and (3) discussing the attendant risks for censorship in China, the dissemination of propaganda in the Chinese diaspora, and the potential to facilitate surveillance.⁴⁵ It cites other reports echoing these concerns.⁴⁶

4. Procedural History

The plaintiffs filed this lawsuit challenging the WeChat Executive Order on August 21, 2020, before the Secretary identified the prohibited transactions.⁴⁷ They moved for a preliminary injunction, advancing as a lead argument (refined in their reply brief) that the Executive Order was void for vagueness under the Fifth Amendment because (1) it did not define “transaction,” and (2) the Secretary’s definition would be issued on September 20, 2020, on the same day that the Order authorized enforcement, thereby denying them notice of prohibited criminal (and at least by

⁴² *Id.* at 16–17 (collecting and citing reports).

⁴³ *Id.* at 17 (collecting and citing reports).

⁴⁴ *Id.* at 18–19 (collecting and citing reports).

⁴⁵ *Id.* at 19–20 (citing and quoting *Mapping China’s Tech. Giants*, Australian Strategic Policy Inst., Ex. 14 to Orloff Decl. – ECF No. 22-14 at 18).

⁴⁶ *Id.* at 21–22 (collecting and citing reports).

⁴⁷ Compl. – ECF No. 1.

implication, civil) conduct.⁴⁸ They then made their First Amendment and IEEPA arguments.⁴⁹ The government opposed the motion on grounds that included prudential ripeness and justiciability because the Executive Order was not self-executing (and instead required the Secretary to define prohibited acts), and the Secretary had not identified the prohibited transactions yet.⁵⁰ Then, on September 16, 2020, the day before the preliminary-injunction hearing, the government said the following:

At present, activity involving the WeChat app is not prohibited. While the Department of Commerce continues to review a range of transactions, including those that could directly or indirectly impact use of the WeChat app, we can provide assurances that the Secretary does not intend to take actions that would target persons or groups whose only connection with WeChat is their use or downloading of the app to convey personal or business information between users, or otherwise define the relevant transactions in such a way that would impose criminal or civil liability on such users. In other words, while use of the app for such communications could be directly or indirectly impaired through measures targeted at other transactions, use and downloading of the app for this limited purpose will not be a defined transaction, and such users will not be targeted or subject to penalties.⁵¹

On September 18, 2020, the Secretary identified the prohibited transactions.⁵² The plaintiffs filed an amended complaint to address the Secretary's definitions and to add an APA claim, and they renewed their motion for a preliminary injunction.⁵³

The court held hearings on September 17, 18, and 19, 2020. All parties consented to the court's jurisdiction.⁵⁴

⁴⁸ Mot. – ECF No. 17 at 25–29; Reply – ECF No. 28 at 17–18 (narrowing the vagueness argument made in the motion).

⁴⁹ Mot. – ECF No. 17 at 29–43; Reply – ECF No. 28 at 18–23. The plaintiffs refined the First Amendment argument in the reply brief, contending that they raised serious questions on the merits and otherwise satisfied the other elements for injunctive relief. Reply – ECF No. 28 at 18–20, 23–26; Renewed Mot. – ECF No. 48 at 3–5. The government contends that the plaintiffs raised the “serious questions” argument for the first time in their renewed motion and that it is prejudiced by the short time that it had to respond. Opp’n – ECF No. 51 at 2–3. This is incorrect. The plaintiffs made the same argument in their reply brief. Reply – ECF No. 28 at 18–19.

⁵⁰ Opp’n – ECF No. 22 at 28–31.

⁵¹ Orloff Letter – ECF No. 31-1 at 2.

⁵² Order – ECF No. 39.

⁵³ FAC – ECF No. 49; Renewed Mot. – ECF No. 48.

⁵⁴ Consents – ECF Nos. 6, 8.

STATUTORY SCHEME

Two statutes provide the authority for Executive Orders: (1) the NEA, 50 U.S.C. §§ 1601–1651, and (2) the IEEPA, 50 U.S.C. §§ 1701–08.

The NEA, enacted in 1976, authorizes the President to declare a national emergency and provides for certain oversight authority. *Sierra Club v. Trump*, 379 F. Supp. 3d 883, 898 (N.D. Cal. 2019). The IEEPA, enacted in 1977, authorizes the President to exercise his authority during peacetime “to deal with any unusual or extraordinary threat, which has its source in whole or substantial part outside the United States, to the national security, foreign policy, or economy of the United States, if the President declares a national emergency with respect to such threat.” 50 U.S.C. § 1701(a). Relevantly to this case, the IEEPA limits the President’s emergency powers:

The authority granted to the President by this section does not include the authority to regulate or prohibit, directly or indirectly —

- (1) any postal, telegraphic, telephonic, or other personal communication, which does not involve a transfer of anything of value;
- (2) donations, by persons subject to the jurisdiction of the United States, of articles, such as food, clothing, and medicine, intended to be used to relieve human suffering, except to the extent that the President determines that such donations (A) would seriously impair his ability to deal with any national emergency declared under section 1701 of this title, (B) are in response to coercion against the proposed recipient or donor, or (C) would endanger Armed Forces of the United States which are engaged in hostilities or are in a situation where imminent involvement in hostilities is clearly indicated by the circumstances;
- (3) the importation from any country, or the exportation to any country, whether commercial or otherwise, regardless of format or medium of transmission, of any information or informational materials, including but not limited to, publications, films, posters, phonograph records, photographs, microfilms, microfiche, tapes, compact disks, CD ROMs, artworks, and news wire feeds. The exports exempted from regulation or prohibition by this paragraph do not include those which are otherwise controlled for export under section 4604 of this title, or under section 4605 of this title to the extent that such controls promote the nonproliferation or antiterrorism policies of the United States, or with respect to which acts are prohibited by chapter 37 of Title 18;
- (4) any transactions ordinarily incident to travel to or from any country, including importation of accompanied baggage for personal use, maintenance within any country including payment of living expenses and acquisition of goods or services for personal use, and arrangement or facilitation of such travel including nonscheduled air, sea, or land voyages.

Id. § 1702(b)(1)–(4).

STANDARD OF REVIEW

The standards for a TRO and a preliminary injunction are the same. *Stuhlbarg Int’l Sales Co. v. John D. Brush & Co., Inc.*, 240 F.3d 832, 839 n.7 (9th Cir. 2001). A movant must demonstrate (1) a likelihood of success on the merits, (2) a likelihood of irreparable harm that would result if an injunction were not issued, (3) the balance of equities tips in favor of the plaintiff, and (4) an injunction is in the public interest. *Winter v. Nat’l Res. Def. Council, Inc.*, 555 U.S. 7, 20 (2008). The irreparable injury must be both likely and immediate. *Id.* at 20–22. “[A] plaintiff must demonstrate immediate threatened injury as a prerequisite to preliminary injunctive relief.” *Caribbean Marine Serv. Co. v. Baldrige*, 844 F.2d 668, 674 (9th Cir. 1988).

Before *Winter*, the Ninth Circuit employed a “sliding scale” test that allowed a plaintiff to prove either “(1) a likelihood of success on the merits and the possibility of irreparable injury; or (2) serious questions going to the merits were raised and the balance of hardships tips sharply in its favor.” *Walczak v. EPL Prolong, Inc.*, 198 F.3d 725, 731 (9th Cir. 1999) (cleaned up). On this continuum, “the greater the relative hardship to [a movant], the less probability of success must be shown.” *Id.* After *Winter*, the Ninth Circuit held that although the Supreme Court invalidated one aspect of the sliding scale approach, the “serious questions” prong of the sliding scale survived if the plaintiff satisfied the other elements for preliminary relief. *Alliance for Wild Rockies v. Cottrell*, 632 F.3d 1127, 1131–32 (9th Cir. 2011). Thus, a preliminary injunction may be appropriate when a movant raises “serious questions going to the merits” of the case and the “balance of hardships tips sharply in the plaintiff’s favor,” provided that the other elements for relief are satisfied. *Id.* at 1134–35.

ANALYSIS

The plaintiffs contend that they are likely to succeed on the merits of their claims that — by effectively shutting down the WeChat app — (1) the government violated the First Amendment, and, at least, they have raised serious questions going to the merits of the claim, (2) the President and the Secretary of Commerce exceeded their authority under the IEEPA, (3) the Secretary

violated the APA, and (4) the executive action is void for vagueness.⁵⁵ The court grants the motion on the ground that the plaintiffs have shown serious questions going to the merits of the First Amendment claim, the balance of hardships tips in the plaintiffs' favor, and the plaintiffs establish sufficiently the other elements for preliminary-injunctive relief.

1. Likelihood of Success on the Merits: First Amendment

The plaintiffs contend that the prohibited transactions will result in shutting down WeChat, a public square for the Chinese-American and Chinese-speaking community in the U.S. that is effectively their only means of communication with their community. This, they say, is a prior restraint on their speech that does not survive strict scrutiny. Also, even if the effect of the prohibited transactions is a content-neutral time-place-or-manner restriction, it does not survive intermediate scrutiny because the effective ban on WeChat use is not narrowly tailored to address the government's significant interest in national security.⁵⁶ The government does not meaningfully contest through evidence that the effect of the prohibited transactions will be to shut down WeChat (perhaps because the Secretary conceded the point) and instead contends that its content-neutral restrictions are based on national-security concerns and survive intermediate scrutiny.⁵⁷

On this record, the plaintiffs have shown serious questions going to the merits of their First Amendment claim that the Secretary's prohibited transactions effectively eliminate the plaintiffs' key platform for communication, slow or eliminate discourse, and are the equivalent of censorship of speech or a prior restraint on it.⁵⁸ *Cf. City of Ladue v. Gilleo*, 512 U.S. 43, 54–59 (1994) (a city's barring all signs — except for signs identifying the residence, “for sale” signs, and signs warning of safety hazards — violated the city residents' right to free speech). The government — while recognizing that foreclosing “an entire medium of public expression” is constitutionally

⁵⁵ Mot. – ECF No. 17 at 29–42; Reply – ECF No. 28 at 17–23; Renewed Mot. – ECF No. 48 at 3–9.

⁵⁶ FAC – ECF No. 49 at 2–29 (¶¶ 78–86); *see* Mot. – ECF No. 17 at 29–39; Reply – ECF No. 28 at 18–22; Renewed Mot. – ECF No. 48 at 3–5.

⁵⁷ Opp'n – ECF No. 22 at 35–43; Opp'n – ECF No. 51 at 4–9.

⁵⁸ Reply – ECF No. 28 at 19.

1 problematic — makes the pragmatic argument that other substitute social-media apps permit
 2 communication.⁵⁹ But the plaintiffs establish through declarations that there are no viable
 3 substitute platforms or apps for the Chinese-speaking and Chinese-American community.⁶⁰ The
 4 government counters that shutting down WeChat does not foreclose communications for the
 5 plaintiffs, pointing to several declarations showing the plaintiffs’ efforts to switch to new
 6 platforms or apps.⁶¹ But the plaintiffs’ evidence reflects that WeChat is effectively the only means
 7 of communication for many in the community, not only because China bans other apps, but also
 8 because Chinese speakers with limited English proficiency have no options other than WeChat.⁶²

9 The plaintiffs also have shown serious questions going to the merits of the First Amendment
 10 claim even if — as the government contends — the Secretary’s identification of prohibited
 11 transactions (1) is a content-neutral regulation, (2) does not reflect the government’s preference or
 12 aversion to the speech, and (3) is subject to intermediate scrutiny. A content-neutral, time-place-
 13 or-manner restriction survives intermediate scrutiny if it (1) is narrowly tailored, (2) serves a
 14 significant governmental interest unrelated to the content of the speech, and (3) leaves open
 15 adequate channels for communication. *Ward v. Rock Against Racism*, 491 U.S. 781, 791 (1989);
 16 *Pac. Coast Horseshoeing Sch., Inc. v. Kirchmeyer*, 961 F.3d 1062, 1068 (9th Cir. 2020). To be
 17 narrowly tailored, the restriction must not “burden substantially more speech than is necessary to
 18 further the government’s legitimate interests.” *Ward*, 491 U.S. at 799. Unlike a content-based
 19 restriction of speech, it “need not be the least restrictive or least intrusive means of serving the
 20 governments interests. But the government still may not regulate expression in such a manner that
 21 a substantial portion of the burden on speech does not advance its goals.” *McCullen v. Coakley*,
 22 573 U.S. 464, 486 (2014) (cleaned up).

23
 24
 25 ⁵⁹ Opp’n – ECF No. 51 at 8 (quoting *G.K. Ltd. Travel v. City of Lake Oswego*, 436 F.3d 1064, 1074
 26 (9th Cir. 2006)).

27 ⁶⁰ See Statement, *supra*.

28 ⁶¹ Opp’n – ECF No. 22 at 42.

⁶² Sun Decl. – ECF No. 17-11 at 16–17 (¶¶ 32–34).

Certainly the government’s overarching national-security interest is significant. But on this record — while the government has established that China’s activities raise significant national-security concerns — it has put in scant little evidence that its effective ban of WeChat for all U.S. users addresses those concerns. And, as the plaintiffs point out, there are obvious alternatives to a complete ban, such as barring WeChat from government devices, as Australia has done, or taking other steps to address data security.⁶³

The government cited two cases to support its contention that “preventing or limiting” WeChat use advances the WeChat Executive Order’s essential purpose to reduce WeChat’s collection of data from U.S. users.⁶⁴ *See Trans Union Corp. v. FTC*, 267 F.3d 1138, 1142–43 (D.C. Cir. 2001) (upholding FCC’s ban on credit agency’s sale of consumers’ personal financial data because it was the only means of preventing the harm of disseminating personal data); *United States v. Elcom Ltd.*, 203 F. Supp. 2d 1111, 1132 (N.D. Cal. 2002) (upholding criminal charge under the Digital Millennium Copyright Act for selling a tool that allowed a user to remove copying restrictions from Adobe files and thereby engage in copyright infringement by duplicating eBooks; targeting tool sellers and banning tool sales was reasonably necessary to avoid copyright infringement and protect digital privacy). The speech interests at stake in these cases — a credit agency’s sale of consumer data and targeting unlawful copying — are not equivalent to the denial of speech that attends the complete ban of WeChat for the Chinese-American and Chinese-speaking U.S. users. On this limited record, the prohibited transactions burden substantially more speech than is necessary to serve the government’s significant interest in national security, especially given the lack of substitute channels for communication. *Ward*, 491 U.S. at 791.

2. Likelihood of Success on the Merits: IEEPA

The plaintiffs contend that the President and the Secretary exceeded their authority under the IEEPA because the IEEPA does not give the President authority to regulate or prohibit “any

⁶³ Reply – ECF No. 28 at 21.

⁶⁴ Opp’n – ECF No. 22 at 39; Opp’n – ECF No. 51 at 7.

postal, telegraphic, telephonic, or other personal communication, which does not involve a transfer of anything of value.” 50 U.S.C. § 1702(b)(1)–(4). The record and the arguments do not allow the court to conclude at this juncture that the plaintiffs are likely to succeed on the merits of their claim that the elimination of support for the WeChat app — such as upgrades and throttling internet services — prohibits personal communication.

3. Likelihood of Success on the Merits: APA

To the extent that the APA claim rests on the argument that the Secretary of Commerce exceeded his authority under IEEPA, the plaintiffs are not likely to succeed on the merits of the claim for the reasons advanced in the last section.

To the extent that the claim rests on the Secretary’s failure to engage in the APA’s notice-and-comment rulemaking procedures, the briefing did not address the issue sufficiently for the court to evaluate its legal sufficiency. On this record, the court cannot conclude that the plaintiffs are likely to succeed on their claim.

4. Likelihood of Success on the Merits: Fifth Amendment

The plaintiffs contend that the WeChat Executive Order’s prohibited transactions — as identified by the Secretary — are void for vagueness because the government has provided conflicting interpretations of the effect of the prohibitions. The Secretary identified prohibited transactions understandably, and the plaintiffs are not likely to succeed on the claim to the extent that it is predicated on the lack of clarity of the prohibited transactions based on subsequent media reports. To the extent that the claim is predicated on the Secretary’s ability to identify future prohibited transactions (as set forth in prohibited transaction 7), the claim is not ripe.⁶⁵ *Bishop Paiute Tribe v. Inyo Cty.*, 863 F.3d 1144, 1154 (9th Cir. 2017).

⁶⁵ Opp’n – ECF No. 22 at 28–30 (discussing prudential ripeness).

5. Remaining *Winter* Elements

The remaining elements are a likelihood of irreparable harm if an injunction does not issue, the balance of equities tips in the plaintiff's favor, and an injunction is in the public interest. *Winter*, 555 U.S. at 20.

First, the plaintiffs have established irreparable harm. The immediate threat is the elimination of their platform for communication, which results in irreparable injury absent an injunction. *California v. Azar*, 911 F.3d 558, 581 (9th Cir. 2018); see *Elrod v. Burns*, 427 U.S. 347, 373 (1976) ("The loss of First Amendment freedoms, even for minimal periods of time, unquestionably constitutes irreparable injury.").

Second, the remaining elements — the balance of equities and whether an injunction is in the public interest — merge where the government is a party. *Azar*, 911 F.3d at 575. The balance of equities favors the plaintiffs: a stay maintains the status quo. Without a stay, at least on this record, a ban of WeChat eliminates all meaningful access to communication in the plaintiffs' community. The public interest favors the protection of the plaintiffs' constitutional rights. *Am. Beverage Ass'n v. City & Cty. of San Francisco*, 916 F.3d 749, 758 (9th Cir. 2019) ("it is always in the public interest to prevent the violation of a party's constitutional rights") (cleaned up).

The government contends that an injunction would "frustrate and displace the President's determination of how best to address threats to national security."⁶⁶ This is an important point, and the threats that the government has identified generally are significant. But while the general evidence about the threat to national security related to China (regarding technology and mobile technology) is considerable, the specific evidence about WeChat is modest. Also, on this record, the regulation — which eliminates a channel of communication without any apparent substitutes — burdens substantially more speech than is necessary to further the government's significant interest. *Ward*, 491 U.S. at 799. This affects the assessment of the public interest.

Finally, at the hearing, the government cited a *Washington Post* article contending that a ban of WeChat is a net positive for human rights: "WeChat it is a closed system that keeps its 1.2

⁶⁶ *Id.* at 50.

1 billion users in a parallel universe where they can communicate as long as they don't cross the
 2 lines, and banning it might eventually strengthen the voices of the Chinese diaspora.”⁶⁷ This is
 3 another important point: the federal government — based on its foreign-policy and national-
 4 security interests — may not want to countenance (or reward) the Chinese government's banning
 5 apps outside of the Chinese government's control and, more generally, censoring or punishing free
 6 speech in China or abroad. But as the President said recently in Executive Order 13925,

7 Free speech is the bedrock of American democracy. Our Founding Fathers protected this
 8 sacred right with the First Amendment to the Constitution. The freedom to express and
 9 debate ideas is the foundation for all of our rights as a free people.

10 ...

11 The growth of online platforms in recent years raises important questions about applying
 12 the ideals of the First Amendment to modern communications technology. Today, many
 13 Americans [including the plaintiffs and others in the U.S. WeChat community] follow the
 14 news, stay in touch with friends and family, and share their views on current events
 15 through social media and other online platforms. As a result, these platforms function in
 16 many ways as a 21st century equivalent of the public square.

17 85 Fed. Reg. 34,079 (May 28, 2020).

18 At this preliminary-injunction stage in the legal process, there are serious questions going to
 19 the merits of the First Amendment claim (even in the context of the significant national-security
 20 and foreign-policy concerns). In sum, the remaining *Winters* elements favor the plaintiffs.

21 **6. Scope of Relief**

22 The injunctive relief must remedy the harm. *E. Bay Sanctuary Covenant v. Trump*, 950 F.3d
 23 1242, 1282 (9th Cir. 2020). The plaintiffs live in four states, and the U.S. WeChat Users Alliance
 24 is comprised of WeChat Users throughout the United States.⁶⁸ WeChat is a network: limiting it to
 25 something less than the United States would not remedy the harm.

26 ⁶⁷ Tenzin Dorjee, *The WeChat ban is a difficult but necessary step toward openness in China*, WASH.
 27 POST, Sept. 18, 2020, <https://www.washingtonpost.com/opinions/2020/09/18/wechat-ban-is-difficult-necessary-step-toward-openness-china/> (last visited Sept. 19, 2020).

28 ⁶⁸ FAC – ECF No. 49 at 7–10 (¶¶ 19–25).

1 **CONCLUSION**

2 The court grants the plaintiffs' motion for a nationwide injunction against the implementation
3 of Executive Order 13,943 (limited to the Secretary of Commerce's Identification of Prohibited
4 Transactions 1 through 6).⁶⁹

5 Nothing in this order prevents the Secretary from reconsidering his decisions or from
6 identifying "any other transaction that is related to WeChat by any person, or with respect to any
7 property, subject to the jurisdiction of the United States, with Tencent Holdings Ltd., or any
8 subsidiary of that entity, as may be identified at a future date under the authority delegated under
9 Executive Order 13943."⁷⁰

10 This disposes of ECF Nos. 17 and 48.

11 **IT IS SO ORDERED.**

12 Dated: September 19, 2020.

13 

14 LAUREL BEELER
15 United States Magistrate Judge
16
17
18
19
20
21
22
23
24
25
26

27 ⁶⁹ Secretary's Identification of Prohibited Transactions, Ex. A to Bien Decl. – ECF No. 45-1 at 10–11.

28 ⁷⁰ *Id.* at 11.



An official website of the United States government
[Here's how you know we're official](#)

Coronavirus Updates for Department Employees



U.S. Department of Commerce

MENU

Search

All news

Press releases

Blog

Speeches

Fact sheets

Op-eds

Photos and videos

Livestreams

Archives

Media contacts

Was this page helpful?

Helpful

Not helpful

[Home](#) » [News](#) » [Press releases](#)

Was this page helpful?

Add.23

 **Helpful**

 **Not helpful**

Commerce Department Prohibits WeChat and TikTok Transactions to Protect the National Security of the United States

[Wilbur Ross](#)

In response to President Trump’s Executive Orders signed August 6, 2020, the Department of Commerce (Commerce) today announced prohibitions on transactions relating to mobile applications (apps) WeChat and TikTok to safeguard the national security of the United States. The Chinese Communist Party (CCP) has demonstrated the means and motives to use these apps to threaten the national security, foreign policy, and the economy of the U.S. Today’s announced prohibitions, when combined, protect users in the U.S. by eliminating access to these applications and significantly reducing their functionality.

FOR IMMEDIATE RELEASE
Friday, September 18, 2020

Office of Public Affairs

(202) 482-4883
publicaffairs@doc.gov

“Today’s actions prove once again that President Trump will do everything in his power to guarantee our national security and protect Americans from the threats of the Chinese Communist Party,” **said U.S. Department of Commerce Secretary Wilbur Ross.** “At the President’s direction, we have taken significant action to combat China’s malicious collection of American citizens’ personal data, while promoting our national values, democratic rules-based norms, and aggressive enforcement of U.S. laws and regulations.”

While the threats posed by WeChat and TikTok are not identical, they are similar. Each collects vast swaths of data from users, including network activity, location data, and browsing and search histories. Each is an active participant in China’s civil-military fusion and is subject to mandatory cooperation with the intelligence services of the CCP. This combination results in the use of WeChat and TikTok creating unacceptable risks to our national security.

Add.24

As of September 20, 2020, the following transactions are prohibited:

1. Any provision of service to distribute or maintain the **WeChat or TikTok** mobile applications, constituent code, or application updates through an online mobile application store in the U.S.;
2. Any provision of services through the **WeChat** mobile application for the purpose of transferring funds or processing payments within the U.S.

As of September 20, 2020, for WeChat and as of November 12, 2020, for TikTok, the following transactions are prohibited:

1. Any provision of internet hosting services enabling the functioning or optimization of the mobile application in the U.S.;
2. Any provision of content delivery network services enabling the functioning or optimization of the mobile application in the U.S.;
3. Any provision directly contracted or arranged internet transit or peering services enabling the function or optimization of the mobile application within the U.S.;
4. Any utilization of the mobile application's constituent code, functions, or services in the functioning of software or services developed and/or accessible within the U.S.

Any other prohibitive transaction relating to WeChat or TikTok may be identified at a future date. Should the U.S. Government determine that WeChat's or TikTok's illicit behavior is being replicated by another app somehow outside the scope of these executive orders, the President has the authority to consider whether additional orders may be appropriate to address such activities. The President has provided until November 12 for the national security concerns posed by TikTok to be resolved. If they are, the prohibitions in this order may be lifted.

The notices for these actions will be posted on the Federal Register at approximately 8:45AM EDT on Friday, September 18, 2020.

Background:

On August 6, 2020, President Trump signed Executive Orders (E.O.) 13942, Addressing the Threat Posed by TikTok, and E.O. 13943, Addressing the Threat Posed by WeChat. In the E.O.s, the President determined that the apps capture vast swaths of information from U.S. users, leaving the data vulnerable to CCP access for nefarious purposes. Commerce, at the Direction of the President, was required to identify transactions within 45 days to protect national security and the private data of millions of people across the country. Today's announced prohibitions fulfill the

President’s direction and mitigate national security risks.

LEADERSHIP
[Wilbur Ross](#)

TAGS
National security

Share this page



Explore

- [Issues](#)
- [News](#)
- [Data and reports](#)
- [Work with us](#)

About us

- [Our mission](#)
- [Strategic plan](#)
- [Bureaus and offices](#)
- [Privacy program](#)

Get in touch

[Contact us](#)

[Staff directory](#)

[Open government](#)

[FOIA](#)

Explore

[Issues](#)

[News](#)

[Data and reports](#)

[Work with us](#)

About us

[Our mission](#)

[Strategic plan](#)

[Bureaus and offices](#)

[Privacy program](#)

Get in touch

[Contact us](#)

[Staff directory](#)

[Open government](#)

Add.27

FOIA



U.S. Department of Commerce

1401 Constitution Ave NW
Washington, DC 20230



Sign up for email updates

To sign up for updates or to access your subscriber preferences, please enter your contact information below.

★Email Address

Subscribe

Archives • Accessibility • Agency Financial Report • Comment policy •
Digital strategy • Information quality • No Fear Act • Inspector General •
Plain language • Privacy policy • Payment Integrity • USA.gov •
Whistleblower Protection • WhiteHouse.gov

Add.28



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. Ténghùn 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]

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.

FOR OFFICIAL USE ONLY

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.¹²³⁴⁵

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>

FOR OFFICIAL USE ONLY

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 preferred over 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/#.Xz1G0n4pCUI>

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>

FOR OFFICIAL USE ONLY

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,²¹²²²³ 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>

FOR OFFICIAL USE ONLY

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&vwsr=0>

²⁹ Rich Barger, Chief Intelligence Officer of ThreatConnect, 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>

FOR OFFICIAL USE ONLY

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.⁴⁷⁴⁸ 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

⁴¹See <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/>

⁴⁴https://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>

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

FOR OFFICIAL USE ONLY

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.

FOR OFFICIAL USE ONLY

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.

FOR OFFICIAL USE ONLY

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)

(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)

(b) (4)

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)

(b) (4)

⁶⁸ https://www.wechat.com/en/privacy_policy.html

(b) (4)

FOR OFFICIAL USE ONLY

(b) (4)

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) (4)

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>

FOR OFFICIAL USE ONLY**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 Shenzhen, 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

FOR OFFICIAL USE ONLY

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>

FOR OFFICIAL USE ONLY

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.

FOR OFFICIAL USE ONLY

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) 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)

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;*

FOR OFFICIAL USE ONLY

Tencent contracts with (b) (4) content delivery network (“CDN”) providers⁸⁶ 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 agreements⁸⁷ (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.

FOR OFFICIAL USE ONLY

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.

Willbur Ross

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.



Cybersecurity and Infrastructure Security Agency

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,"³⁴ Any sale will likely have to go through a licensing procedure with the Chinese government, which recently updated its export restrictions list

(U) WARNING: This document is FOR OFFICIAL USE ONLY (FOUO). It is to be controlled, stored, handled, transmitted, distributed, and disposed of in accordance with DHS policy relating to FOUO information. This information shall not be distributed beyond the original addressees without prior authorization of the originator.

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.⁶⁷ 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.^{89 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.cnn.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.cnn.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.cnn.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

Presidential Documents

Executive Order 13943 of August 6, 2020

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

By the authority vested in me as President by the Constitution and the laws of the United States of America, including the International Emergency Economic Powers Act (50 U.S.C. 1701 *et seq.*) (IEEPA), the National Emergencies Act (50 U.S.C. 1601 *et seq.*), and section 301 of title 3, United States Code,

I, DONALD J. TRUMP, President of the United States of America, find that additional steps must be taken to deal with the national emergency with respect to the information and communications technology and services supply chain declared in Executive Order 13873 of May 15, 2019 (Securing the Information and Communications Technology and Services Supply Chain). As I explained in an Executive Order of August 6, 2020 (Addressing the Threat Posed by Tiktok, and Taking Additional Steps to Address the National Emergency With Respect to the Information and Communications Technology and Services Supply Chain), 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. To protect our Nation, I took action to address the threat posed by one mobile application, TikTok. Further action is needed to address a similar threat posed by another mobile application, WeChat.

WeChat, a messaging, social media, and electronic payment application owned by the Chinese company Tencent Holdings Ltd., reportedly has over one billion users worldwide, including users in the United States. Like TikTok, WeChat automatically captures vast swaths of information from its users. This data collection threatens to allow the Chinese Communist Party access to Americans' personal and proprietary information. In addition, the application captures the personal and proprietary information of Chinese nationals visiting the United States, thereby allowing the Chinese Communist Party a mechanism for keeping tabs on Chinese citizens who may be enjoying the benefits of a free society for the first time in their lives. For example, 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. WeChat, like TikTok, also reportedly censors content that the Chinese Communist Party deems politically sensitive and may also be used for disinformation campaigns that benefit the Chinese Communist Party. These risks have led other countries, including Australia and India, to begin restricting or banning the use of WeChat. The United States must take aggressive action against the owner of WeChat to protect our national security.

Accordingly, I hereby order:

Section 1. (a) The following actions shall be prohibited beginning 45 days after the date of this order, to the extent permitted under applicable law: 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. Ténghùn Kōnggǔ Yǒuxiàn Gōngsī), Shenzhen, China,

or any subsidiary of that entity, as identified by the Secretary of Commerce (Secretary) under section 1(c) of this order.

(b) The prohibition in subsection (a) of this section applies except to the extent provided by statutes, or in regulations, orders, directives, or licenses that may be issued pursuant to this order, and notwithstanding any contract entered into or any license or permit granted before the date of this order.

(c) 45 days after the date of this order, the Secretary shall identify the transactions subject to subsection (a) of this section.

Sec. 2. (a) Any transaction by a United States person or within the United States that evades or avoids, has the purpose of evading or avoiding, causes a violation of, or attempts to violate the prohibition set forth in this order is prohibited.

(b) Any conspiracy formed to violate any of the prohibitions set forth in this order is prohibited.

Sec. 3. For those persons who might have a constitutional presence in the United States, I find that because of the ability to transfer funds or other assets instantaneously, prior notice to such persons of measures to be taken pursuant to section 1 of this order would render those measures ineffectual. I therefore determine that for these measures to be effective in addressing the national emergency declared in Executive Order 13873, there need be no prior notice of an identification made pursuant to section 1(c) of this order.

Sec. 4. For the purposes of this order:

(a) the term “person” means an individual or entity;

(b) the term “entity” means a government or instrumentality of such government, partnership, association, trust, joint venture, corporation, group, subgroup, or other organization, including an international organization; and

(c) the term “United States person” means any United States citizen, permanent resident alien, entity organized under the laws of the United States or any jurisdiction within the United States (including foreign branches), or any person in the United States.

Sec. 5. The Secretary is hereby authorized to take such actions, including adopting rules and regulations, and to employ all powers granted to me by IEEPA as may be necessary to implement this order. The Secretary may, consistent with applicable law, redelegate any of these functions within the Department of Commerce. All departments and agencies of the United States shall take all appropriate measures within their authority to implement this order.

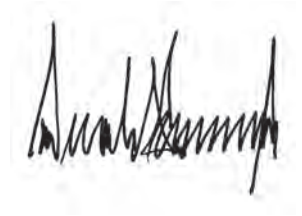
Sec. 6. General Provisions. (a) Nothing in this order shall be construed to impair or otherwise affect:

(i) the authority granted by law to an executive department, agency, or the head thereof; or

(ii) the functions of the Director of the Office of Management and Budget relating to budgetary, administrative, or legislative proposals.

(b) This order shall be implemented consistent with applicable law and subject to the availability of appropriations.

(c) This order is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.



THE WHITE HOUSE,
August 6, 2020.

[FR Doc. 2020-17700
Filed 8-10-20; 11:15 am]
Billing code 3295-F0-P



United States Strategic Approach to the People's Republic of China

Introduction

Since the United States and the People's Republic of China (PRC) established diplomatic relations in 1979, United States policy toward the PRC was largely premised on a hope that deepening engagement would spur fundamental economic and political opening in the PRC and lead to its emergence as a constructive and responsible global stakeholder, with a more open society. More than 40 years later, it has become evident that this approach underestimated the will of the Chinese Communist Party (CCP) to constrain the scope of economic and political reform in China. Over the past two decades, reforms have slowed, stalled, or reversed. The PRC's rapid economic development and increased engagement with the world did not lead to convergence with the citizen-centric, free and open order as the United States had hoped. The CCP has chosen instead to exploit the free and open rules-based order and attempt to reshape the international system in its favor. Beijing openly acknowledges that it seeks to transform the international order to align with CCP interests and ideology. The CCP's expanding use of economic, political, and military power to compel acquiescence from nation states harms vital American interests and undermines the sovereignty and dignity of countries and individuals around the world.

To respond to Beijing's challenge, the Administration has adopted a competitive approach to the PRC, based on a clear-eyed assessment of the CCP's intentions and actions, a reappraisal of the United States' many strategic advantages and shortfalls, and a tolerance of greater bilateral friction. Our approach is not premised on determining a particular end state for China. Rather, our goal is to protect United States vital national interests, as articulated in the four pillars of the 2017 *National Security Strategy of the United States of America* (NSS). We aim to: (1) protect the American people, homeland, and way of life; (2) promote American prosperity; (3) preserve peace through strength; and (4) advance American influence.

Our competitive approach to the PRC has two objectives: first, to improve the resiliency of our institutions, alliances, and partnerships to prevail against the challenges the PRC presents; and second, to compel Beijing to cease or reduce actions harmful to the United States' vital, national interests and those of our allies and partners. Even as we compete with the PRC, we welcome cooperation where our interests align. Competition need not lead to confrontation or conflict. The United States has a deep and abiding respect for the Chinese people and enjoys longstanding ties to the country. We do not seek to contain China's development, nor do we wish to disengage from the Chinese people. The United States expects to engage in fair competition with the PRC, whereby both of our nations, businesses, and individuals can enjoy security and prosperity.

Prevailing in strategic competition with the PRC requires cooperative engagement with multiple stakeholders, and the Administration is committed to building partnerships to

protect our shared interests and values. Vital partners of this Administration include the Congress, state and local governments, the private sector, civil society, and academia. The Congress has been speaking out through hearings, statements, and reports that shed light on the CCP's malign behavior. The Congress also provides legal authorities and resources for the United States Government to take the actions to achieve our strategic objectives. The Administration also recognizes the steps allies and partners have taken to develop more clear-eyed and robust approaches toward the PRC, including the European Union's publication in March 2019 of *EU-China: A Strategic Outlook*, among others.

The United States is also building cooperative partnerships and developing positive alternatives with foreign allies, partners, and international organizations to support the shared principles of a free and open order. Specific to the Indo-Pacific region, many of these initiatives are described in documents such as the Department of Defense June 2019 *Indo-Pacific Strategy Report* and the Department of State November 2019 report on *A Free and Open Indo-Pacific: Advancing a Shared Vision*. The United States is working in concert with mutually aligned visions and approaches such as the Association of Southeast Asian Nation's *Outlook on the Indo-Pacific*, Japan's free and open Indo-Pacific vision, India's Security and Growth for All in the Region policy, Australia's Indo-Pacific concept, the Republic of Korea's New Southern Policy, and Taiwan's New Southbound Policy.

This report does not attempt to detail the comprehensive range of actions and policy initiatives the Administration is carrying out across the globe as part of our strategic competition. Rather, this report focuses on the implementation of the NSS as it applies most directly to the PRC.

Challenges

The PRC today poses numerous challenges to United States national interests.

1. Economic Challenges

Beijing's poor record of following through on economic reform commitments and its extensive use of state-driven protectionist policies and practices harm United States companies and workers, distort global markets, violate international norms, and pollute the environment. When the PRC acceded to the World Trade Organization (WTO) in 2001, Beijing agreed to embrace the WTO's open market-oriented approach and embed these principles in its trading system and institutions. WTO members expected China to continue on its path of economic reform and transform itself into a market-oriented economy and trade regime.

These hopes were not realized. Beijing did not internalize the norms and practices of competition-based trade and investment, and instead exploited the benefits of WTO membership to become the world's largest exporter, while systematically protecting its domestic markets. Beijing's economic policies have led to massive industrial overcapacity that distorts global prices and allows China to expand global market share at the expense of

competitors operating without the unfair advantages that Beijing provides to its firms. The PRC retains its non-market economic structure and state-led, mercantilist approach to trade and investment. Political reforms have likewise atrophied and gone into reverse, and distinctions between the government and the party are eroding. General Secretary Xi's decision to remove presidential term limits, effectively extending his tenure indefinitely, epitomized these trends.

In his 2018 *Findings of the Investigation into China's Acts, Policies, and Practices Related to Technology Transfer, Intellectual Property, and Innovation under Section 301 of the Trade Act of 1974*, the United States Trade Representative (USTR) determined that numerous acts, policies, and practices of the PRC government were unreasonable or discriminatory, and burden or restrict United States commerce. Based on a rigorous investigation, USTR found that the PRC: (1) requires or pressures United States companies to transfer their technology to Chinese entities; (2) places substantial restrictions on United States companies' ability to license their technology on market terms; (3) directs and unfairly facilitates acquisition of United States companies and assets by domestic firms to obtain cutting edge technologies; and (4) conducts and supports unauthorized cyber intrusions into United States companies' networks to access sensitive information and trade secrets.

The list of Beijing's commitments to cease its predatory economic practices is littered with broken and empty promises. In 2015, Beijing promised that it would stop government-directed cyber-enabled theft of trade secrets for commercial gain, reiterating that same promise in 2017 and 2018. Later in 2018, the United States and a dozen other countries attributed global computer intrusion campaigns, targeting intellectual property and confidential business information, to operators affiliated with the PRC's Ministry of State Security – a contravention of Beijing's 2015 commitment. Since the 1980s, Beijing has signed multiple international agreements to protect intellectual property. Despite this, more than 63 percent of the world's counterfeits originate in China, inflicting hundreds of billions of dollars of damage on legitimate businesses around the world.

While Beijing acknowledges that China is now a “mature economy,” the PRC continues to argue in its dealings with international bodies, including the WTO, that it is still a “developing country.” Despite being the top importer of high technology products and ranking second only to the United States in terms of gross domestic product, defense spending, and outward investment, China self-designates as a developing country to justify policies and practices that systematically distort multiple sectors globally, harming the United States and other countries.

One Belt One Road (OBOR) is Beijing's umbrella term to describe a variety of initiatives, many of which appear designed to reshape international norms, standards, and networks to advance Beijing's global interests and vision, while also serving China's domestic economic requirements. Through OBOR and other initiatives, the PRC is expanding the use of Chinese industrial standards in key technology sectors, part of an effort to strengthen its own companies' position in the global marketplace at the expense of non-Chinese firms. Projects that Beijing has labeled OBOR include: transportation, information and communications technology and energy infrastructure; industrial parks; media collaboration; science and

technology exchanges; programs on culture and religion; and even military and security cooperation. Beijing is also seeking to arbitrate OBOR-related commercial disputes through its own specialized courts, which answer to the CCP. The United States welcomes contributions by China to sustainable, high-quality development that accords with international best practices, but OBOR projects frequently operate well outside of these standards and are characterized by poor quality, corruption, environmental degradation, a lack of public oversight or community involvement, opaque loans, and contracts generating or exacerbating governance and fiscal problems in host nations.

Given Beijing's increasing use of economic leverage to extract political concessions from or exact retribution against other countries, the United States judges that Beijing will attempt to convert OBOR projects into undue political influence and military access. Beijing uses a combination of threat and inducement to pressure governments, elites, corporations, think tanks, and others – often in an opaque manner – to toe the CCP line and censor free expression. Beijing has restricted trade and tourism with Australia, Canada, South Korea, Japan, Norway, the Philippines, and others, and has detained Canadian citizens, in an effort to interfere in these countries' internal political and judicial processes. After the Dalai Lama visited Mongolia in 2016, the PRC government imposed new tariffs on land-locked Mongolia's mineral exports passing through China, temporarily paralyzing Mongolia's economy.

Beijing seeks global recognition for its environmental efforts and claims to promote “green development.” China, however, has been the world's largest greenhouse gas emitter by a wide margin for more than a decade. Beijing has put forward vague and unenforceable emissions reduction commitments that allow China's emissions to keep growing until “around 2030.” China's planned growing emissions will outweigh the reductions from the rest of the world combined. Chinese firms also export polluting coal-fired power plants to developing countries by the hundreds. The PRC is also the world's largest source of marine plastic pollution, discharging over 3.5 million metric tons into the ocean each year. The PRC ranks first in the world for illegal, unreported, and unregulated fishing in coastal nations' waters around the world, threatening local economies and harming the marine environment. Chinese leaders' unwillingness to rein in these globally harmful practices does not match their rhetorical promises of environmental stewardship.

2. Challenges to Our Values

The CCP promotes globally a value proposition that challenges the bedrock American belief in the unalienable right of every person to life, liberty, and the pursuit of happiness. Under the current generation of leadership, the CCP has accelerated its efforts to portray its governance system as functioning better than those of what it refers to as “developed, western countries.” Beijing is clear that it sees itself as engaged in an ideological competition with the West. In 2013, General Secretary Xi called on the CCP to prepare for a “long-term period of cooperation and conflict” between two competing systems and declared that “capitalism is bound to die out and socialism is bound to win.”

The CCP aims to make China a “global leader in terms of comprehensive national power and international influence,” as General Secretary Xi expressed in 2017, by strengthening what it refers to as “the system of socialism with Chinese characteristics.” This system is rooted in Beijing’s interpretation of Marxist-Leninist ideology and combines a nationalistic, single-party dictatorship; a state-directed economy; deployment of science and technology in the service of the state; and the subordination of individual rights to serve CCP ends. This runs counter to principles shared by the United States and many likeminded countries of representative government, free enterprise, and the inherent dignity and worth of every individual.

Internationally, the CCP promotes General Secretary Xi’s vision for global governance under the banner of “building a community of common destiny for mankind.” Beijing’s efforts to compel ideological conformity at home, however, present an unsettling picture of what a CCP-led “community” looks like in practice: (1) an anticorruption campaign that has purged political opposition; (2) unjust prosecutions of bloggers, activists, and lawyers; (3) algorithmically determined arrests of ethnic and religious minorities; (4) stringent controls over and censorship of information, media, universities, businesses, and non-governmental organizations; (5) surveillance and social credit scoring of citizens, corporations, and organizations; and (6) and arbitrary detention, torture, and abuse of people perceived to be dissidents. In a stark example of domestic conformity, local officials publicized a book burning event at a community library to demonstrate their ideological alignment to “Xi Jinping Thought.”

One disastrous outgrowth of such an approach to governance is Beijing’s policies in Xinjiang, where since 2017, authorities have detained more than a million Uighurs and members of other ethnic and religious minority groups in indoctrination camps, where many endure forced labor, ideological indoctrination, and physical and psychological abuse. Outside these camps, the regime has instituted a police state employing emerging technologies such as artificial intelligence and biogenetics to monitor ethnic minorities’ activities to ensure allegiance to the CCP. Widespread religious persecution – of Christians, Tibetan Buddhists, Muslims, and members of Falun Gong – includes the demolition and desecration of places of worship, arrests of peaceful believers, forced renunciations of faith, and prohibitions on raising children in traditions of faith.

The CCP’s campaign to compel ideological conformity does not stop at China’s borders. In recent years, Beijing has intervened in sovereign nations’ internal affairs to engineer consent for its policies. PRC authorities have attempted to extend CCP influence over discourse and behavior around the world, with recent examples including companies and sports teams in the United States and the United Kingdom and politicians in Australia and Europe. PRC actors are exporting the tools of the CCP’s techno-authoritarian model to countries around the world, enabling authoritarian states to exert control over their citizens and surveil opposition, training foreign partners in propaganda and censorship techniques, and using bulk data collection to shape public sentiment.

China’s party-state controls the world’s most heavily resourced set of propaganda tools. Beijing communicates its narrative through state-run television, print, radio, and online

organizations whose presence is proliferating in the United States and around the world. The CCP often conceals its investments in foreign media entities. In 2015, China Radio International was revealed to control 33 radio stations in 14 countries via shell entities, and to subsidize multiple intermediaries through providing free, pro-Beijing content.

Beyond the media, the CCP uses a range of actors to advance its interests in the United States and other open democracies. CCP United Front organizations and agents target businesses, universities, think tanks, scholars, journalists, and local, state, and Federal officials in the United States and around the world, attempting to influence discourse and restrict external influence inside the PRC.

Beijing regularly attempts to compel or persuade Chinese nationals and others to undertake a range of malign behaviors that threaten United States national and economic security, and undermine academic freedom and the integrity of the United States research and development enterprise. These behaviors include misappropriation of technology and intellectual property, failure to appropriately disclose relationships with foreign government sponsored entities, breaches of contract and confidentiality, and manipulation of processes for fair and merit-based allocation of Federal research and development funding. Beijing also attempts to compel Chinese nationals to report on and threaten fellow Chinese students, protest against events that run counter to Beijing's political narrative, and otherwise restrict the academic freedom that is the hallmark and strength of the American education system.

PRC media entities, journalists, academics, and diplomats are free to operate in the United States, but Beijing denies reciprocal access to American counterpart institutions and officials. The PRC government routinely denies United States officials, including the United States Ambassador to the PRC, access to Department of State-funded American Cultural Centers, which are hosted in Chinese universities to share American culture with the Chinese people. Foreign reporters working in the PRC often face harassment and intimidation.

3. Security Challenges

As China has grown in strength, so has the willingness and capacity of the CCP to employ intimidation and coercion in its attempts to eliminate perceived threats to its interests and advance its strategic objectives globally. Beijing's actions belie Chinese leaders' proclamations that they oppose the threat or use of force, do not intervene in other countries' internal affairs, or are committed to resolving disputes through peaceful dialogue. Beijing contradicts its rhetoric and flouts its commitments to its neighbors by engaging in provocative and coercive military and paramilitary activities in the Yellow Sea, the East and South China Seas, the Taiwan Strait, and Sino-Indian border areas.

In May 2019, the Department of Defense issued its annual report to the Congress, *Military and Security Developments Involving the PRC*, assessing current and future trajectories of China's military-technological development, security and military strategies, and People's Liberation Army (PLA) organizational and operational concepts. In July 2019, the PRC

Minister of Defense publicly acknowledged that OBOR is linked to the PRC's aspirational expansion of PLA presence overseas, including locations such as the Pacific Islands and the Caribbean.

Beijing's military buildup threatens United States and allied national security interests and poses complex challenges for global commerce and supply chains. Beijing's Military-Civil Fusion (MCF) strategy gives the PLA unfettered access into civil entities developing and acquiring advanced technologies, including state-owned and private firms, universities, and research programs. Through non-transparent MCF linkages, United States and other foreign companies are unwittingly feeding dual-use technologies into PRC military research and development programs, strengthening the CCP's coercive ability to suppress domestic opposition and threaten foreign countries, including United States allies and partners.

The PRC's attempts to dominate the global information and communications technology industry through unfair practices is reflected in discriminatory regulations like the PRC National Cyber Security Law, which requires companies to comply with Chinese data localization measures that enable CCP access to foreign data. Other PRC laws compel companies like Huawei and ZTE to cooperate with Chinese security services, even when they do business abroad, creating security vulnerabilities for foreign countries and enterprises utilizing Chinese vendors' equipment and services.

Beijing refuses to honor its commitment to provide travel documents for Chinese citizens with orders of removal from the United States in a timely and consistent manner, effectively blocking their removals from our country and creating security risks for American communities. In addition, the PRC's violations of our bilateral consular treaty puts United States citizens at risk in China, with many Americans detrimentally affected by the PRC government's coercive exit bans and wrongful detentions.

Approach

The NSS demands that the United States "rethink the policies of the past two decades – policies based on the assumption that engagement with rivals and their inclusion in international institutions and global commerce would turn them into benign actors and trustworthy partners. For the most part, this premise turned out to be false. Rival actors use propaganda and other means to try to discredit democracy. They advance anti-Western views and spread false information to create divisions among ourselves, our allies, and our partners."

Guided by a return to principled realism, the United States is responding to the CCP's direct challenge by acknowledging that we are in a strategic competition and protecting our interests appropriately. The principles of the United States' approach to China are articulated both in the NSS and our vision for the Indo-Pacific region – sovereignty, freedom, openness, rule of law, fairness, and reciprocity. United States-China relations do not determine our Indo-Pacific strategy, but rather fall within that strategy and the overarching

NSS. By the same token, our vision of a free and open Indo-Pacific region does not exclude China.

The United States holds the PRC government to the same standards and principles that apply to all nations. We believe this is the treatment that the people of China want and deserve from their own government and from the international community. Given the strategic choices China's leadership is making, the United States now acknowledges and accepts the relationship with the PRC as the CCP has always framed it internally: one of great power competition.

United States policies are not premised on an attempt to change the PRC's domestic governance model, nor do they make concessions to the CCP's narratives of exceptionalism and victimhood. Rather, United States policies are designed to protect our interests and empower our institutions to withstand the CCP's malign behavior and collateral damage from the PRC's internal governance problems. Whether the PRC eventually converges with the principles of the free and open order can only be determined by the Chinese people themselves. We recognize that Beijing, not Washington, has agency over and responsibility for the PRC government's actions.

The United States rejects CCP attempts at false equivalency between rule of law and rule by law; between counterterrorism and oppression; between representative governance and autocracy; and between market-based competition and state-directed mercantilism. The United States will continue to challenge Beijing's propaganda and false narratives that distort the truth and attempt to demean American values and ideals.

Similarly, the United States does not and will not accommodate Beijing's actions that weaken a free, open, and rules-based international order. We will continue to refute the CCP's narrative that the United States is in strategic retreat or will shirk our international security commitments. The United States will work with our robust network of allies and like-minded partners to resist attacks on our shared norms and values, within our own governance institutions, around the world, and in international organizations.

The American people's generous contributions to China's development are a matter of historical record – just as the Chinese people's remarkable accomplishments in the era of Reform and Opening are undeniable. However, the negative trend lines of Beijing's policies and practices threaten the legacy of the Chinese people and their future position in the world.

Beijing has repeatedly demonstrated that it does not offer compromises in response to American displays of goodwill, and that its actions are not constrained by its prior commitments to respect our interests. As such, the United States responds to the PRC's actions rather than its stated commitments. Moreover, we do not cater to Beijing's demands to create a proper “atmosphere” or “conditions” for dialogue.

Likewise, the United States sees no value in engaging with Beijing for symbolism and pageantry; we instead demand tangible results and constructive outcomes. We acknowledge and respond in kind to Beijing's transactional approach with timely incentives and costs, or

credible threats thereof. When quiet diplomacy proves futile, the United States will increase public pressure on the PRC government and take action to protect United States interests by leveraging proportional costs when necessary.

The PRC government has fallen short of its commitments in many areas including: trade and investment; freedoms of expression and belief; political interference; freedoms of navigation and overflight; cyber and other types of espionage and theft; weapons proliferation; environmental protection; and global health. Agreements with Beijing must include stringent verification and enforcement mechanisms.

We speak candidly with the Chinese people and expect honesty from PRC leaders. In matters of diplomacy, the United States responds appropriately to the CCP's insincere or vague threats, and stands up alongside our allies and partners to resist coercion. Through our continuous and frank engagement, the United States welcomes cooperation by China to expand and work toward shared objectives in ways that benefit the peace, stability, and prosperity of the world. Our approach does not exclude the PRC. The United States stands ready to welcome China's positive contributions.

As the above tenets of our approach imply, competition necessarily includes engagement with the PRC, but our engagements are selective and results-oriented, with each advancing our national interests. We engage with the PRC to negotiate and enforce commitments to ensure fairness and reciprocity; clarify Beijing's intentions to avoid misunderstanding; and resolve disputes to prevent escalation. The United States is committed to maintaining open channels of communication with the PRC to reduce risks and manage crises. We expect the PRC to also keep these channels open and responsive.

Implementation

In accordance with the President's NSS, the political, economic, and security policies outlined in this report seek to protect the American people and homeland, promote American prosperity, preserve peace through strength, and advance a free and open vision abroad. During the first 3 years of the Administration, the United States has taken significant steps in implementing this strategy as it applies to China.

1. Protect the American People, the Homeland, and the American Way of Life

The United States Department of Justice (DOJ)'s China Initiative and Federal Bureau of Investigation are directing resources to identify and prosecute trade secrets theft, hacking, and economic espionage; and increasing efforts to protect against malign foreign investment in United States infrastructure, supply chain threats, and foreign agents seeking to influence American policy. For example, DOJ informed PRC state media company CGTN-America of its obligation to register as a foreign agent as specified under the Foreign Agents Registration Act (FARA), which obligates registrants to disclose their activities to Federal authorities and

appropriately label information materials they distribute. CGTN-America subsequently registered under FARA.

The Administration is also responding to CCP propaganda in the United States by highlighting malign behavior, countering false narratives, and compelling transparency. United States officials, including those from the White House and the Departments of State, Defense, and Justice, are leading efforts to educate the American public about the PRC government's exploitation of our free and open society to push a CCP agenda inimical to United States interests and values. In an effort to achieve reciprocity of access, the Department of State has implemented a policy requiring Chinese diplomats to notify the United States Government before meeting with state and local government officials and academic institutions.

The Administration is raising awareness of and actively combatting Beijing's co-optation and coercion of its own citizens and others in United States academic institutions, beyond traditional espionage and influence efforts. We are working with universities to protect the rights of Chinese students on American campuses, provide information to counter CCP propaganda and disinformation, and ensure an understanding of ethical codes of conduct in an American academic environment.

Chinese students represent the largest cohort of foreign students in the United States today. The United States values the contributions of Chinese students and researchers. As of 2019, the number of Chinese students and researchers in the United States has reached an all-time high, while the number of student visa denials to Chinese applicants has steadily declined. The United States strongly supports the principles of open academic discourse and welcomes international students and researchers conducting legitimate academic pursuits; we are improving processes to screen out the small minority of Chinese applicants who attempt to enter the United States under false pretenses or with malign intent.

In the United States research community, Federal agencies such as the National Institutes of Health and the Department of Energy have updated or clarified regulations and procedures to ensure compliance with applicable standards of conduct and reporting, in order to improve transparency and prevent conflicts of interest. The National Science and Technology Council's Joint Committee on the Research Environment is developing standards for Federally-funded research, and best practices for United States research institutions. The Department of Defense is working to ensure grantees do not also have contracts with China's talent recruitment programs, while also continuing to welcome foreign researchers.

To prevent foreign malign actors from gaining access to United States information networks, the President issued the "Executive Order on Securing the Information and Communications Technology and Services Supply Chain" and the "Executive Order on Establishing the Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector." The implementation of these Executive Orders will prevent certain companies associated with or answering to the intelligence and security apparatus of foreign adversaries from, for example, readily accessing the private and sensitive information of the United States Government, the United States private sector, and

individual Americans. To ensure protection of our information worldwide, including sensitive military and intelligence data, the United States is actively engaging with our allies and partners, including in multilateral fora, to promote a set of common standards for secure, resilient, and trusted communications platforms that underpin the global information economy. To compel Beijing to adhere to norms of responsible state behavior, the United States is working with allies and like-minded partners to attribute and otherwise deter malicious cyber activities.

The Administration is implementing the Foreign Investment Risk Review Modernization Act to update and strengthen the capacity of the Committee on Foreign Investment in the United States (CFIUS) to address growing national security concerns over foreign exploitation of investment structures, which previously fell outside CFIUS jurisdiction. This includes preventing Chinese companies from exploiting access to United States innovation through minority investments in order to modernize the Chinese military. The United States has updated its export control regulations, particularly in light of Beijing's whole-of-society MCF strategy and its efforts to acquire advanced technologies related to hypersonics, quantum computing, artificial intelligence, biotechnology, and other emerging and foundational technologies. We are also engaging allies and partners to develop their own foreign investment screening mechanisms, and to update and implement export controls collaboratively through multilateral regimes and other forums.

The United States Government is also taking concrete actions to protect the American consumer from counterfeit and substandard products. Between 2017 and 2018, the United States Department of Homeland Security seized more than 59,000 shipments of counterfeit goods, produced in the PRC, valued at more than \$2.1 billion. This represents five times the total shipments and value seized from all other foreign countries combined.

In addition to falsely branded apparel, footwear, handbags, and watches, United States Customs and Border Protection intercepted three shipments containing 53,000 illegal Chinese gun parts and electronics that could have compromised the security and privacy of American businesses and consumers. United States law enforcement agencies are also targeting counterfeit pharmaceuticals and cosmetics originating from China, which have been found to contain high levels of contaminants, including bacteria and animal waste that pose a danger to American consumers.

The United States is working with Chinese authorities to stem the deadly flow of illicit Chinese fentanyl from the PRC to the United States. In December 2018, the President secured a commitment from his Chinese counterpart to control all forms of fentanyl in the PRC. With the Chinese regulatory regime in place since May 2019, United States and PRC law enforcement agencies are sharing intelligence and coordinating to set conditions for enforcement actions that will deter Chinese drug producers and traffickers. The United States is also working with China's postal agencies to improve tracking of small parcels for law enforcement purposes.

2. Promote American Prosperity

In response to the PRC's documented unfair and abusive trade practices and industrial policies, the Administration is taking strong actions to protect American businesses, workers, and farmers, and to put an end to Beijing's practices that have contributed to a hollowing-out of the United States manufacturing base. The United States is committed to rebalancing the United States-China economic relationship. Our whole-of-government approach supports fair trade and advances United States competitiveness, promotes United States exports, and breaks down unjust barriers to United States trade and investment. Having failed since 2003 to persuade Beijing to adhere to its economic commitments through regular, high-level dialogues, the United States is confronting China's market-distorting forced technology transfer and intellectual property practices by imposing costs in the form of tariffs levied on Chinese goods coming into the United States. Those tariffs will remain in place until a fair Phase Two trade deal is agreed to by the United States and the PRC.

In response to Beijing's repeated failure to reduce or eliminate its market-distorting subsidies and overcapacity, the United States imposed tariffs to protect our strategically important steel and aluminum industries. For those unfair Chinese trade practices that are subject to dispute settlement at the WTO, the United States continues to pursue and win multiple cases. Finally, to crack down on China's dumping and subsidies across a broad range of industries, the Department of Commerce is making greater utility of United States antidumping and countervailing duties laws than in past administrations.

In January 2020, the United States and the PRC signed Phase One of an economic and trade agreement that requires structural reforms and other changes to China's economic and trade regime, addressing several longstanding United States concerns. The agreement prohibits the PRC from forcing or pressuring foreign companies to transfer their technology as a condition for doing business in China; strengthens protection and enforcement of intellectual property in China in all key areas; creates new market opportunities in China for United States agriculture and financial services by addressing policy barriers; and addresses longstanding, unfair currency practices. The agreement also establishes a strong dispute resolution mechanism that ensures prompt and effective implementation and enforcement. By addressing structural barriers to trade and making the commitments fully enforceable, the Phase One agreement will expand United States exports to China. As part of this agreement, the PRC committed over the next 2 years to increase imports of United States goods and services by no less than \$200 billion in four broad categories: manufactured goods, agriculture, energy, and services. This agreement marks critical progress toward a more balanced trade relationship and a more level playing field for American workers and companies.

Domestically, the Administration is taking steps to strengthen the United States economy and promote economic sectors of the future, such as 5G technology, through tax reforms and a robust deregulatory agenda. The President's "Executive Order on Maintaining American Leadership in Artificial Intelligence" is an example of a United States Government initiative

to promote investment and collaboration to ensure the United States continues to lead in innovation and setting standards for a growing industry.

Together with other likeminded nations, the United States promotes an economic vision based on principles of sovereignty, free markets, and sustainable development. Alongside the European Union and Japan, the United States is engaged in a robust trilateral process to develop disciplines for state-owned enterprises, industrial subsidies, and forced technology transfers. We will also continue to work with our allies and partners to ensure that discriminatory industrial standards do not become global standards. As the world's most valuable consumer market, largest source of foreign direct investment, and leading wellspring of global technological innovation, the United States engages extensively with allies and partners to evaluate shared challenges and coordinate effective responses to ensure continued peace and prosperity. We work closely with United States companies to build their competitiveness at home and abroad while fostering sustainable development through programs such as Prosper Africa, *America Crece* in Latin America and the Caribbean, and Enhancing Development and Growth through Energy in the Indo-Pacific region.

3. Preserve Peace through Strength

The 2018 National Defense Strategy (NDS) prioritizes long-term competition with China and emphasizes modernization and partnerships to counter the PLA's technological advancements, force development, and growing international presence and assertiveness. As described in the Nuclear Posture Review, the Administration is prioritizing the modernization of the nuclear triad, including the development of supplementary capabilities designed to deter Beijing from using its weapons of mass destruction or conducting other strategic attacks. Meanwhile, the United States continues to urge China's leaders to come to the table and begin arms control and strategic risk reduction discussions as a nuclear power with a modern and growing nuclear arsenal and the world's largest collection of intermediate range delivery systems. The United States believes it is in the interest of all nations to improve Beijing's transparency, prevent miscalculations, and avoid costly arms buildups.

The Department of Defense is moving quickly to deploy hypersonic platforms, increasing investments in cyber and space capabilities, and developing more lethal fires based on resilient, adaptive, and cost-effective platforms. Together, these capabilities are intended to deter and counter Beijing's growing ambitions and the PLA's drive toward technological parity and superiority.

As part of our worldwide freedom of navigation operations program, the United States is pushing back on Beijing's hegemonic assertions and excessive claims. The United States military will continue to exercise the right to navigate and operate wherever international law allows, including in the South China Sea. We are speaking up for regional allies and partners, and providing security assistance to help them build capacity to withstand Beijing's attempts to use its military, paramilitary, and law enforcement forces to coerce and prevail in disputes. In 2018, the United States military withdrew the invitation for the PLA to

participate in the biennial Rim of the Pacific exercise due to Beijing's deployment of advanced missile systems onto manmade features in the South China Sea.

Stronger alliances and partnerships are a cornerstone of the NDS. The United States is building partner capacity and deepening interoperability to develop a combat-credible forward operating presence, fully integrated with allies and partners to deter and deny PRC aggression. The Administration's Conventional Arms Transfer policy aims to promote United States arms sales and accelerate the transformation of partner military capabilities in a strategic and complementary manner. In June 2019, the Department of Defense released its first *Indo-Pacific Strategy Report*, articulating the Department's implementation of the NDS and our whole-of-government strategy for the Indo-Pacific region.

The United States will continue to maintain strong unofficial relations with Taiwan in accordance with our "One China" policy, based on the Taiwan Relations Act and the three United States-PRC Joint Communiques. The United States maintains that any resolution of cross-Straits differences must be peaceful and according to the will of the people on both sides, without resorting to threat or coercion. Beijing's failure to honor its commitments under the communiques, as demonstrated by its massive military buildup, compels the United States to continue to assist the Taiwan military in maintaining a credible self-defense, which deters aggression and helps to ensure peace and stability in the region. In a 1982 memorandum, President Ronald Reagan insisted "that the quantity and quality of the arms provided Taiwan be conditioned entirely on the threat posed by the PRC." In 2019, the United States approved more than \$10 billion of arms sales to Taiwan.

The United States remains committed to maintaining a constructive, results-oriented relationship with the PRC. The United States conducts defense contacts and exchanges with the PRC to communicate strategic intent; prevent and manage crises; reduce the risks of miscalculation and misunderstanding that could escalate into conflict; and cooperate in areas of shared interest. The United States military engages with the PLA to develop effective crisis communication mechanisms, including responsive channels for de-escalation in unplanned scenarios.

4. Advance American Influence

For the past seven decades, the free and open international order has provided the stability to allow sovereign, independent states to flourish and contribute to unprecedented global economic growth. As a large, developed country and a major beneficiary of this order, the PRC should help guarantee freedom and openness for other nations around the globe. When Beijing instead promotes or abets authoritarianism, self-censorship, corruption, mercantilist economics, and intolerance of ethnic and religious diversity, the United States leads international efforts to resist and counter these malign activities.

In 2018 and 2019, the Secretary of State hosted the first two gatherings of the Ministerial to Advance Religious Freedom. Along with the President's unprecedented Global Call to Protect Religious Freedom during the United Nations General Assembly (UNGA) in September 2019, these events brought together global leaders to address religious persecution around the

world. During both ministerials, the United States and partner countries released joint statements calling on the PRC government to respect the rights of Uighur and other Turkic Muslims, Tibetan Buddhists, Christians, and Falun Gong adherents, all of whom face repression and persecution in China. In February 2020, the Department of State launched the first ever International Religious Freedom Alliance with 25 likeminded partners to defend the right of every person to worship without fear. The President met with Chinese dissidents and survivors on the margins of the 2019 Ministerial, and he shared the stage during UNGA with victims of religious persecution from China. The United States also continues to support human rights defenders and independent civil society working in or on China.

In October 2019 at the United Nations in New York, the United States joined likeminded nations in condemning Beijing's ongoing human rights violations and other repressive policies in Xinjiang that threaten international peace and security. The latter event followed United States Government actions to stop United States exports to select Chinese government agencies and surveillance technology companies complicit in the Xinjiang human rights abuses and to deny United States visas for Chinese officials, and their family members, responsible for violating Beijing's international human rights commitments. The United States has also begun actions to block imports of Chinese goods produced using forced labor in Xinjiang.

The United States will continue to take a principled stand against the use of our technology to support China's military and its technology-enabled authoritarianism, working in conjunction with likeminded allies and partners. In doing so, we will implement policies that keep pace with rapid technological change and PRC efforts to blend civil and military uses and compel companies to support China's security and intelligence services.

These efforts demonstrate United States commitment to the fundamental values and norms that have served as the foundation of the international system since the end of the Second World War. While the United States has no desire to interfere in the PRC's internal affairs, Washington will continue to be candid when Beijing strays from its international commitments and responsible behavior, especially when United States interests are at stake. For example, the United States has significant interests in the future of Hong Kong. Approximately 85,000 United States citizens and more than 1,300 United States businesses reside in Hong Kong. The President, the Vice President, and the Secretary of State have repeatedly called on Beijing to honor the 1984 Sino-British Joint Declaration and preserve Hong Kong's high degree of autonomy, rule of law, and democratic freedoms, which enable Hong Kong to remain a successful hub of international business and finance.

The United States is expanding its role as an Indo-Pacific nation that promotes free enterprise and democratic governance. In November 2019, the United States, Japan, and Australia launched the Blue Dot Network to promote transparently-financed, high quality infrastructure through private sector-led development around the world, which will add to the nearly 1 trillion dollars of United States direct investment in the Indo-Pacific region alone. At the same time, the Department of State issued a detailed progress report on the

implementation of our whole-of-government strategy for the Indo-Pacific region:
A Free and Open Indo-Pacific: Advancing a Shared Vision.

Conclusion

The Administration's approach to the PRC reflects a fundamental reevaluation of how the United States understands and responds to the leaders of the world's most populous country and second largest national economy. The United States recognizes the long-term strategic competition between our two systems. Through a whole-of-government approach and guided by a return to principled realism, as articulated by the NSS, the United States Government will continue to protect American interests and advance American influence. At the same time, we remain open to constructive, results-oriented engagement and cooperation from China where our interests align. We continue to engage with PRC leaders in a respectful yet clear-eyed manner, challenging Beijing to uphold its commitments.



2019

REPORT TO CONGRESS

of the

**U.S.-CHINA ECONOMIC AND
SECURITY REVIEW COMMISSION**

ONE HUNDRED SIXTEENTH CONGRESS
FIRST SESSION

NOVEMBER 2019

Printed for the use of the
U.S.-China Economic and Security Review Commission
Available online at: <https://www.uscc.gov>

U.S. GOVERNMENT PUBLISHING OFFICE
WASHINGTON : 2019

For sale by the Superintendent of Documents, U.S. Government Publishing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512-1800; DC area (202) 512-1800
Fax: (202) 512-2104 Mail: Stop IDCC, Washington, DC 20402-0001

Add.78



U.S.-CHINA ECONOMIC AND SECURITY REVIEW COMMISSION

CAROLYN BARTHOLOMEW, *Chairman*
ROBIN CLEVELAND, *Vice Chairman*

COMMISSIONERS

ANDREAS BORGEAS	KENNETH LEWIS
JEFFREY FIEDLER	MICHAEL A. MCDEVITT
Hon. CARTE P. GOODWIN	Hon. JAMES M. TALENT
ROY D. KAMPHAUSEN	MICHAEL R. WESSEL
THEA MEI LEE	LARRY M. WORTZEL

DANIEL W. PECK, *Executive Director*

The Commission was created on October 30, 2000 by the Floyd D. Spence National Defense Authorization Act of 2001, Pub. L. No. 106–398 (codified at 22 U.S.C. §7002), as amended by: The Treasury and General Government Appropriations Act, 2002, Pub. L. No. 107–67 (Nov. 12, 2001) (regarding employment status of staff and changing annual report due date from March to June); The Consolidated Appropriations Resolution, 2003, Pub. L. No. 108–7 (Feb. 20, 2003) (regarding Commission name change, terms of Commissioners, and responsibilities of the Commission); The Science, State, Justice, Commerce, and Related Agencies Appropriations Act, 2006, Pub. L. No. 109–108 (Nov. 22, 2005) (regarding responsibilities of the Commission and applicability of FACA); The Consolidated Appropriations Act, 2008, Pub. L. No. 110–161 (Dec. 26, 2007) (regarding submission of accounting reports; printing and binding; compensation for the executive director; changing annual report due date from June to December; and travel by members of the Commission and its staff); The Carl Levin and Howard P. “Buck” McKeon National Defense Authorization Act for Fiscal Year 2015, Pub. L. No. 113–291 (Dec. 19, 2014) (regarding responsibilities of the Commission). The Commission’s full charter and statutory mandate are available online at: <https://www.uscc.gov/about/uscc-charter>.

U.S.-CHINA ECONOMIC AND SECURITY REVIEW COMMISSION

NOVEMBER 14, 2019

The Honorable Chuck Grassley
 President Pro Tempore of the U.S. Senate, Washington, DC 20510
 The Honorable Nancy Pelosi
 Speaker of the U.S. House of Representatives, Washington, DC 20510

DEAR SENATOR GRASSLEY AND SPEAKER PELOSI:

On behalf of the U.S.-China Economic and Security Review Commission, we are pleased to transmit the Commission's 2019 Annual Report to Congress. This Report responds to our mandate "to monitor, investigate, and report to Congress on the national security implications of the bilateral trade and economic relationship between the United States and the People's Republic of China." The Commission reached a broad and bipartisan consensus on the contents of this Report, with all 12 members voting unanimously to approve and submit it to Congress.

In accordance with our mandate, this Report, which is current as of October 4, includes the results and recommendations of our hearings, research, travel, and review of the areas identified by Congress in our mandate, as defined in Public Law No. 106-398 (October 30, 2000), and amended by Public Laws No. 107-67 (November 12, 2001), No. 108-7 (February 20, 2003), 109-108 (November 22, 2005), No. 110-161 (December 26, 2007), and No. 113-291 (December 19, 2014). The Commission's charter, which includes the 11 directed research areas of our mandate, is included as Appendix I of the Report.

The Commission conducted eight public hearings, taking testimony from 77 expert witnesses from government, the private sector, academia, think tanks, research institutions, and other backgrounds. For each of these hearings, the Commission produced a transcript (posted on our website at <https://www.uscc.gov>). This year's hearings included:

- What Keeps Xi Up at Night: Beijing's Internal and External Challenges;
- Risks, Rewards, and Results: U.S. Companies in China and Chinese Companies in the United States;
- An Emerging China-Russia Axis? Implications for the United States in an Era of Strategic Competition;
- China in Space: A Strategic Competition?;
- Technology, Trade, and Military-Civil Fusion: China's Pursuit of Artificial Intelligence, New Materials, and New Energy;
- A "World-Class" Military: Assessing China's Global Military Ambitions;
- Exploring the Growing U.S. Reliance on China's Biotech and Pharmaceutical Products; and
- U.S.-China Relations in 2019: A Year in Review.

The Commission received a number of briefings by executive branch agencies and the Intelligence Community, including both unclassified and classified briefings on China's military modernization, the China-Russia relationship, U.S.-Hong Kong relations, China's ambitions in space, and U.S. strategy for responding to China's Belt and Road Initiative. The Commission is preparing a classified report to Congress on these and other topics. The Commission also received briefings by foreign diplomatic and military officials as well as U.S. and foreign nongovernmental experts.

Commissioners made official visits to Australia, Singapore, Hong Kong, and China to hear and discuss perspectives on China and its global and regional activities. In these visits, the Commission delegation met with U.S. diplomats, host government officials, business representatives, academics, journalists, and other experts.

The Commission also relied substantially on the work of our excellent professional staff and supported outside research (see Appendix IV) in accordance with our mandate (see Appendix I).

The Report includes 38 recommendations for congressional action. Our ten most important recommendations appear on page 24 at the conclusion of the Executive Summary.

We offer this Report to Congress in the hope that it will be useful for assessing progress and challenges in U.S.-China relations.

Thank you for the opportunity to serve. We look forward to continuing to work with Members of Congress in the upcoming year to address issues of concern in the U.S.-China relationship.

Yours truly,




Carolyn Bartholomew
Chairman



Robin Cleveland
Vice Chairman

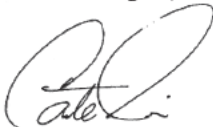
Commissioners Approving the 2019 Report



Carolyn Bartholomew, Chairman


Robin Cleveland, Vice Chairman


Andreas Borgeas, Commissioner


Jeffrey Fiedler, Commissioner

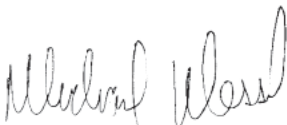

Carte P. Goodwin, Commissioner


Roy D. Kamphausen, Commissioner


Michael A. McDevitt, Commissioner


Kenneth Lewis, Commissioner


James M. Talent, Commissioner


Michael R. Wessel, Commissioner


Larry M. Wortzel, Commissioner

CONTENTS

	Page
TRANSMITTAL LETTER TO THE CONGRESS	iii
COMMISSIONERS APPROVING THE REPORT	v
EXECUTIVE SUMMARY	1
KEY RECOMMENDATIONS	24
INTRODUCTION	29

2019 REPORT TO CONGRESS OF THE
U.S.-CHINA ECONOMIC AND SECURITY REVIEW COMMISSION

Chapter 1: 2019 in Review	33
Section 1: Year in Review: Economics and Trade	33
Key Findings	33
Introduction	34
U.S.-China Trade	34
Bilateral Economic Tensions	38
Technological Conflict and Competition	46
China's Internal and External Economic Management	49
Section 2: Year in Review: Security, Politics, and Foreign Affairs	80
Key Findings	80
Introduction	81
A Year of Both Success and Setback	81
Chinese Diplomacy: Toward a China-Led World Order	89
Pressure on the Regional Balance	100
Tensions in U.S.-China Ties	104
Chapter 2: Beijing's Internal and External Challenges	119
Key Findings	119
Recommendations	120
Introduction	120
Internal Challenges to CCP Rule	121
China's Economic and Innovation Challenges	130
Resistance to Beijing's Ambitions Abroad: Economic, Military, and Political Challenges	136
Implications for the United States	153
Chapter 3: U.S.-China Competition	169
Section 1: U.S.-China Commercial Relations	169
Key Findings	169
Recommendations	170
Introduction	171
U.S.-China Economic Ties: An Unbalanced Relationship	171
Chinese Companies in the United States	172
U.S. Companies in China	182
Implications for the United States	191
Section 2: Emerging Technologies and Military-Civil Fusion: Artificial Intelligence, New Materials, and New Energy	205
Key Findings	205
Recommendations	206
Introduction	207

VIII

	Page
Military-Civil Fusion	208
Artificial Intelligence	214
New and Advanced Materials	220
Energy Storage	226
Civil Nuclear Power	229
Implications for the United States	230
Section 3: Growing U.S. Reliance on China’s Biotech and Pharmaceutical	
Products	248
Key Findings	248
Recommendations	249
Introduction	250
U.S. Reliance on Chinese Pharmaceutical and Medical Products	251
U.S. Government Oversight of Health Imports from China	257
China’s Pharmaceutical and Biotech Activities in the United States	261
U.S. Companies’ Access to Health Industries and Market Opportunities	
in China	265
U.S.-China Global Health Cooperation	269
Implications for the United States	269
Chapter 4: China’s Global Ambitions	283
Section 1: Beijing’s “World-Class” Military Goal	283
Key Findings	283
Recommendations	284
Introduction	285
A Military to Match Beijing’s Ambitions	285
Building a World-Class Military	288
A World-Class Military in Its Region and Beyond	296
Implications for the United States	303
Section 2: An Uneasy Entente: China- Russia Relations in a New Era of	
Strategic Competition with the United States	315
Key Findings	315
Recommendations	316
Introduction	316
A Deepening Entente	317
Mistrust and Power Asymmetry Limit Ties	327
Central Asia and Afghanistan, the Middle East, and the Arctic	335
Implications for the United States	343
Section 3: China’s Ambitions in Space: Contesting the Final Frontier	359
Key Findings	359
Recommendations	360
Introduction	361
National Rejuvenation and a “Space Dream”	362
Space Program Supports Geopolitical and Economic Goals	368
Space as the “Commanding Heights” of Future Military Conflict	379
Implications for the United States	383
Section 4: Changing Regional Dynamics: Oceania and Singapore	401
Key Findings	401
Recommendations	402
Introduction	402
Australia	403
Pacific Islands	418
Singapore	424
Implications for the United States	431
Chapter 5: Taiwan	445
Key Findings	445
Recommendations	446
Introduction	447
Cross-Strait Military and Security Issues	449
Taiwan’s External Relations	458
Economics and Trade	463
Implications for the United States	470

IX

	Page
Chapter 6: Hong Kong	481
Key Findings	481
Recommendations	482
Introduction	483
Proposed Extradition Bill Galvanizes Calls for Democracy	484
Hong Kong's Autonomy under Continued Attack	496
Hong Kong's Economic Relationship with Mainland China	505
Implications for the United States	513
Comprehensive List of the Commission's Recommendations	537
Appendices:	
Appendix I: Charter	547
Appendix II: Background of Commissioners	555
Appendix III: Public Hearings of the Commission During 2019	565
Appendix IIIA: List of Witnesses Testifying Before the Commission During 2019	569
Appendix IV: List of Research Material	573
Appendix V: Conflict of Interest and Lobbying Disclosure Reporting	577
Appendix VI: Acronyms and Abbreviations	579
2019 Commission Staff and Acknowledgements	581

EXECUTIVE SUMMARY

Chapter 1: 2019 in Review

Section 1: Year in Review: Economics and Trade

In 2019, the trade dispute between the United States and China entered its second year and remains mostly unresolved. The Chinese government's unwavering commitment to state management of its economy remains a major stumbling block. In response to decades of unfair economic practices, the United States wants the Chinese government to codify commitments to strengthen intellectual property protection, prohibit forced technology transfer, and remove industrial subsidies. But these practices are core features of China's economic system, and the Chinese government views U.S. demands as an attack on its national development. China continues to ignore the letter and the spirit of its World Trade Organization (WTO) commitments. The resulting impasse has led to multiple rounds of mutual tariff actions impacting more than \$500 billion in bilateral goods trade, and reducing trade between the two countries. In response to U.S. measures to address illegal activities of Chinese technology firms, China's government strengthened pursuit of technological self-reliance and its state-led approach to innovation, which uses licit and illicit means to achieve its goals. This will continue to pose a threat to U.S. economic competitiveness and national security.

Escalating trade tensions with the United States compounded China's domestic economic challenges, with the Chinese economy growing at its slowest pace in nearly 30 years in 2019. High debt levels constrain Beijing's ability to respond to the slowdown, and stimulus measures have so far been modest in comparison with past programs. The economic slowdown has disproportionately affected China's small and medium enterprises, which do not enjoy the same preferential treatment, access to credit, and government subsidies as state-owned or -supported enterprises. Meanwhile, regional banks have emerged as a key source of risk in China's financial system due to the high number of nonperforming loans on their balance sheets. China's government has also pursued limited market and financial system opening over the last year in an effort to attract foreign capital. These measures remain narrowly designed to address specific pressures facing China's economy and do not appear to herald a broader market liberalization of the kind that U.S. companies and policymakers have long advocated.

Key Findings

- On-and-off trade negotiations between the United States and China to resolve a years-long trade dispute have failed to produce a comprehensive agreement. The impasse in negotiations

(1)

underscores, in part, China's commitment to preserving the government's dominant role in determining economic outcomes.

- The United States is confronting China in response to decades of unfair Chinese economic policies and trade-distorting practices. The Chinese Communist Party (CCP) increasingly perceives U.S. actions as an attack on its vision for China's national development. China's government has intensified nationalist rhetoric criticizing the United States, applied pressure on U.S. companies, and targeted key U.S. export sectors with tariffs in response.
- U.S. measures to address illegal activities by Chinese technology companies are leading China's government to push harder on technological self-reliance. The reinvigoration of the state-driven approach to innovation will pose a sustained threat to U.S. global economic competitiveness and national security.
- A range of domestic factors and trade tensions with the United States have slowed China's economic growth. In response, China's government has deployed infrastructure spending, tax cuts, and targeted monetary stimulus. While the stimulus enabled a modest recovery during the first half of 2019, China's rate of growth continues to slow.
- China's government continues to falsify official economic statistics, obscuring the true extent of its current economic slowdown. Independent observers estimate that China's true growth rate is at least 0.5 percentage points—and possibly as much as 3 percentage points—lower than Beijing's published figures.
- Beijing's deleveraging campaign has succeeded in containing China's corporate debt growth, but local governments continue to borrow. Expanding household debt and a rapid increase in the value of nonperforming loans also pose significant risks to China's financial system and are a major challenge for Chinese policymakers.
- China's state sector is strengthening and private companies are struggling. The deleveraging campaign and related crackdown on shadow banking had the unintended effect of cutting off credit to the private sector, which traditionally relies on informal finance.
- China's government has taken limited market opening steps, including incremental liberalization of China's foreign investment regime and financial system. However, these measures have been pursued in terms favorable to the Chinese government as opposed to the market, underscoring that any changes in China's economic practices will continue to be controlled by the state.

Section 2: Year in Review: Security, Politics, and Foreign Affairs

In 2019, Beijing stepped up its efforts to promote itself as a global political and economic leader, offering the clearest evidence yet of its ambition to reshape the international order so it benefits Chinese interests and makes the world safe for the CCP. General Secretary of the CCP Xi Jinping continued to tout the CCP's model and "Chi-

nese wisdom” as solutions for the world’s problems and vowed to build a “community of common human destiny,” a CCP formulation for a China-led global governance regime. In the security realm, Beijing exhorted the People’s Liberation Army (PLA) to prepare itself for challenges in the years ahead while it continues its transformation into a “world-class” military able to conduct combat operations within and beyond the Indo-Pacific region. Meanwhile, as trade tensions between China and the United States deepened, General Secretary Xi declared that the CCP was now engaged in a “New Long March” and must prepare for a protracted, multidecade confrontation with Washington and its allies. At home, the CCP expanded its campaign of indoctrination and repression against Uyghurs, Tibetan Buddhists, Hui Muslims, Christians, and other religious groups and individuals the CCP considers to be politically unreliable.

Beijing also took new steps in 2019 to advance the aggressive approach to foreign and security policy it has taken in recent years. In the Indo-Pacific region, Beijing used displays of military force to intimidate its neighbors while applying informal economic sanctions against countries making decisions contrary to its interests. China also continued its efforts to influence or interfere with other countries’ political processes as well as global perceptions of its rise, including through United Front covert propaganda and co-optation activities, the targeting of U.S. and other foreign universities and media, arbitrary detentions of foreign citizens, and the export of censorship and surveillance technologies. Beijing also sought to shore up ties with key partners, such as North Korea and Iran, while growing its influence across the Western Hemisphere, Africa, and the Middle East.

The U.S.-China relationship deteriorated significantly over the past year as both sides blamed the other for issues such as the breakdown in trade negotiations and militarization of the South China Sea. Beijing’s views of the United States hardened as Chinese leaders took few meaningful steps to address issues of concern raised by Washington and Chinese state media intensified anti-U.S. propaganda. Meanwhile, the U.S. government increased its efforts to curb China’s influence and espionage activities in academic and commercial settings.

Key Findings

- In 2019, Beijing declared in unambiguous terms its intent to revise and reorder the international system in ways more befitting its national interests and repressive vision of governance. In a series of national addresses, Chinese leaders suggested the CCP viewed its “historic mission” as being not only to govern China, but also to profoundly influence global governance. The CCP took new steps to promote itself abroad as a model worthy of emulation, casting its political system and approach to economic development as superior alternatives to that of the United States and other democratic countries.
- Chinese leaders took a more strident tone in their discussion of military affairs, reinforcing a sense of urgency in the PLA’s preparations for a potential military conflict while indicating Beijing’s intent to position the PLA as a globally-oriented

military force. General Secretary Xi urged the PLA to make preparations for a possible conflict with the “powerful enemy adversary”—a phrase the CCP uses to refer to the United States—central to its modernization and training efforts.

- Despite signs of outward confidence, CCP leadership also revealed a growing unease over the mounting external resistance to its ambitions, which it viewed as threatening its objectives abroad and rule at home. In response to these challenges, the CCP deepened its control over the Chinese government and Chinese society and stepped up an ideological and nationalistic messaging campaign instructing key groups to “win the ideological war” against Western and other democratic countries.
- China continued its efforts to coerce or interfere in the domestic affairs of countries acting in ways contrary to its interests, detaining foreign citizens and carrying out an extensive influence campaign targeting foreign universities, media, and the Chinese diaspora. Beijing also expanded its global promotion of the Belt and Road Initiative (BRI), increasing military cooperation and exporting its censorship and surveillance technologies to countries under BRI auspices.
- In the Indo-Pacific region, China made new use of “gray zone” activities and military intimidation of its neighbors to secure its expansive sovereignty claims. Military tensions between China and Japan persisted in the East China Sea despite attempts by both countries to reset bilateral relations, while an annual poll of respondents in Southeast Asian countries found that fewer than one in ten saw China’s regional influence as benign.
- The U.S.-China relationship grew markedly more confrontational as tensions increased over political, economic, and security issues and polls reflected a significant drop in the U.S. public’s favorability toward China. Chinese leaders showed few signs of willingness to compromise on issues raised by Washington.

Chapter 2: Beijing’s Internal and External Challenges

The CCP faces a number of significant internal and external challenges as it seeks to ensure its hold on power while sustaining economic growth, maintaining control at home, and advancing its regional and increasingly global ambitions. Despite a lengthy campaign to clean up its ranks, the CCP has growing concerns over widespread corruption, weakened control and cohesion, and ideological decay. Chinese policymakers credit their state-led economic model for the country’s rapid growth, but the contradictions in China’s approach are increasingly apparent as it faces a struggling private sector, high debt levels, and a rapidly-aging population. China remains deeply dependent on foreign technology and vulnerable to supply chain disruption, but is pouring vast amounts of resources toward encouraging domestic innovation.

Externally, BRI has come under growing international skepticism over China’s opaque lending practices, accusations of corruption, and encroachment on host countries’ sovereignty. CCP leaders are also worried about the PLA’s lack of recent warfighting experience and

have long harbored concerns about the loyalty, capabilities, and responsiveness of their security forces. Furthermore, Beijing's military modernization efforts, coercion of its neighbors, and interference in other countries' internal affairs have generated global apprehension about its geopolitical ambitions.

China's leadership is acutely aware of these challenges and is making a concerted effort to overcome them. Ultimately, the extent to which Beijing can address these vulnerabilities affects its ability to contest U.S. leadership and carve out a place for its own model of global governance. In the economic realm, Beijing's commitment to its state-led economic model likely will prolong U.S.-China trade frictions and worsen China's domestic challenges. Chinese leaders' concerns over the PLA's readiness for war will continue to influence their willingness to initiate a conflict that could prompt the intervention of a modern, capable adversary such as the United States, at least in the near term. Finally, General Secretary Xi's consolidation of power has created a dangerous echo chamber for decision making, which could lead to domestic policy missteps and complicate U.S.-China relations during times of heightened tensions or crisis.

Key Findings

- The CCP is facing internal and external challenges as it attempts to maintain power at home and increase its influence abroad. China's leadership is acutely aware of these challenges and is making a concerted effort to overcome them.
- The CCP perceives Western values and democracy as weakening the ideological commitment to China's socialist system of Party cadres and the broader populace, which the Party views as a fundamental threat to its rule. General Secretary Xi has attempted to restore the CCP's belief in its founding values to further consolidate control over nearly all of China's government, economy, and society. His personal ascendancy within the CCP is in contrast to the previous consensus-based model established by his predecessors. Meanwhile, his signature anti-corruption campaign has contributed to bureaucratic confusion and paralysis while failing to resolve the endemic corruption plaguing China's governing system.
- China's current economic challenges include slowing economic growth, a struggling private sector, rising debt levels, and a rapidly-aging population. Beijing's deleveraging campaign has been a major drag on growth and disproportionately affects the private sector. Rather than attempt to energize China's economy through market reforms, the policy emphasis under General Secretary Xi has shifted markedly toward state control.
- Beijing views its dependence on foreign intellectual property as undermining its ambition to become a global power and a threat to its technological independence. China has accelerated its efforts to develop advanced technologies to move up the economic value chain and reduce its dependence on foreign technology, which it views as both a critical economic and security vulnerability.

- China's senior leaders are concerned over perceived shortfalls in the PLA's warfighting experience and capabilities and its failure to produce an officer corps that can plan and lead. These concerns undermine Chinese leaders' confidence in the PLA's ability to prevail against a highly-capable adversary. The CCP has also long harbored concerns over the loyalty and responsiveness of the PLA and internal security forces to Beijing and the potential for provincial officials to co-opt these forces to promote their own political ambitions.
- China's BRI faces growing skepticism due to concerns regarding corruption, opaque lending practices, and security threats. However, this criticism has not been followed by an outright rejection of BRI because significant infrastructure gaps persist globally and China has few competitors in infrastructure financing.
- Beijing's military modernization efforts, coercion of its neighbors, and interference in other countries' internal affairs have generated resistance to its geopolitical ambitions. Countries in the Indo-Pacific and outside the region are accelerating their military modernization programs, deepening cooperation, and increasing their military presence in the region in an attempt to deter Beijing from continuing its assertive behavior.

Chapter 3: U.S.-China Competition

Section 1: U.S.-China Commercial Relations

Chinese firms operate with far greater freedom in the United States than U.S. firms are permitted in China. The lack of reciprocity in market access, investment openness, regulatory treatment, and other areas have led to an environment where U.S. companies are disadvantaged in China's domestic market. Protected in their domestic market, Chinese companies are increasingly empowered to compete in third country markets. For this reason, many U.S. companies with operations in China, historically supportive of deepening engagement, have grown increasingly pessimistic about their ability to expand and participate in the Chinese market. The Chinese government's inbound foreign direct investment (FDI) regime has restricted foreign entry into some segments of the Chinese market, such as cloud computing and e-commerce. For high-priority sectors, China's government has made market entry conditional on transfer of technology and other concessions from U.S. and other foreign companies.

Much analysis has been done on Chinese FDI and capital raising in the United States, but little is known about Chinese companies' U.S. operations, governance, and impact on the broader U.S. economy. Chinese FDI in the United States peaked in 2016 and has subsequently fallen. By comparison, Chinese venture capital (VC) investment has not fallen as significantly. U.S. policymakers remain concerned about VC investment that might be directed by the Chinese government, as access to early-stage technologies could put U.S. national security and economic competitiveness at risk.

Beyond FDI, many Chinese companies raise capital on U.S. financial markets. Because Chinese companies frequently list in the United States using a variable interest entity, investments in U.S.-listed

Chinese companies are inherently risky, in part because the variable interest entity structure has been ruled unenforceable by China's legal system. The lack of disclosure by and oversight of U.S.-listed Chinese companies opens the door to adverse activities, such as insider trading, accounting fraud, and corporate governance concerns that could put U.S. investors, including pension funds, at risk.

Key Findings

- The nature of Chinese investment in the United States is changing. While Chinese FDI in the United States fell in 2018, VC investment in cutting-edge sectors has remained more stable. Broad trends in FDI from China mask VC investment. While lower than FDI, VC investment from Chinese entities could have more impact as it has prioritized potentially sensitive areas, including early-stage advanced technologies. This sustained Chinese investment raises concern for U.S. policymakers, as Beijing has accelerated its comprehensive effort to acquire a range of technologies to advance military and economic goals.
- U.S. laws, regulations, and practices afford Chinese companies certain advantages that U.S. companies do not enjoy. Chinese firms that raise capital on U.S. stock markets are subject to lower disclosure requirements than U.S. counterparts, raising risks for U.S. investors. The Chinese government continues to block the Public Company Accounting Oversight Board from inspecting auditors' work papers in China despite years of negotiations. As of September 2019, 172 Chinese firms were listed on major U.S. exchanges, with a total market capitalization of more than \$1 trillion.
- China's laws, regulations, and practices disadvantage U.S. companies relative to Chinese companies. China's foreign investment regime has restricted and conditioned U.S. companies' participation in the Chinese market to serve industrial policy aims. In addition, recent reports by the American and EU Chambers of Commerce in China suggest technology transfer requests have continued unabated. Technology transfer requests continue to compromise U.S. firms' operations.
- Chinese firms' U.S. operations may pose competitive challenges if they receive below-cost financing or subsidies from the Chinese state or if they can import inputs at less than fair value. There are serious gaps in the data that prevent a full assessment of the U.S.-China economic relationship. Analysis of Chinese companies' participation in the U.S. economy is constrained by the absence of empirical data on companies' operations, corporate governance, and legal compliance.

Section 2: Emerging Technologies and Military-Civil Fusion: Artificial Intelligence, New Materials, and New Energy

U.S. economic competitiveness and national security are under threat from the Chinese government's broad-based pursuit of leadership in artificial intelligence (AI), new materials, and new energy. Because these technologies underpin many other innovations, China's government has prioritized their development, aiming to en-

courage transfer of foreign technology and know-how, build national champions, and attain self-sufficiency. Beijing's enhanced program of military-civil fusion seeks to mobilize civilian technological advances in support of China's military modernization and spur broader economic growth and innovation by eliminating barriers between the commercial and defense sectors.

Chinese military planners view AI in particular as an advantage that could allow China to surpass U.S. military capabilities. In seeking to become the dominant manufacturer of new energy vehicles, Chinese firms have established control over substantial portions of the global lithium-ion battery supply chain. China's efforts to localize high-value industries that use new and advanced materials, particularly aerospace manufacturing, jeopardize critical U.S. exports and position China to develop and deploy commercial and military advances ahead of the United States.

Compared to past technological modernization efforts, China's current initiatives pose far greater challenges to U.S. interests. China's ability to capitalize on new technology has been enhanced by what it learned or stole from foreign firms. By creating complex and opaque ties between China's civilian institutions and its defense sector, military-civil fusion increases the risk that U.S. firms and universities may advance China's military capabilities while endangering future U.S. economic leadership.

China's industrial planners coordinate policy across China's economy to channel resources to targeted industries and spur demand for domestic products, harnessing the strengths of China's robust manufacturing base and a network of government-led investment funds, while disadvantaging foreign firms. Outside China's borders, the state is financing Chinese state-owned enterprises' acquisitions of leading foreign robotics, machine tooling, and other firms; promoting Chinese influence in international standards-setting bodies; and cultivating export markets for Chinese goods and services around the world.

Key Findings

- China's government has implemented a whole-of-society strategy to attain leadership in AI, new and advanced materials, and new energy technologies (e.g., energy storage and nuclear power). It is prioritizing these focus areas because they underpin advances in many other technologies and could lead to substantial scientific breakthroughs, economic disruption, enduring economic benefits, and rapid changes in military capabilities and tactics.
- The Chinese government's military-civil fusion policy aims to spur innovation and economic growth through an array of policies and other government-supported mechanisms, including venture capital funds, while leveraging the fruits of civilian innovation for China's defense sector. The breadth and opacity of military-civil fusion increase the chances civilian academic collaboration and business partnerships between the United States and China could aid China's military development.
- China's robust manufacturing base and government support for translating research breakthroughs into applications allow it

to commercialize new technologies more quickly than the United States and at a fraction of the cost. These advantages may enable China to outpace the United States in commercializing discoveries initially made in U.S. labs and funded by U.S. institutions for both mass market and military use.

- *Artificial intelligence:* Chinese firms and research institutes are advancing uses of AI that could undermine U.S. economic leadership and provide an asymmetrical advantage in warfare. Chinese military strategists see AI as a breakout technology that could enable China to rapidly modernize its military, surpassing overall U.S. capabilities and developing tactics that specifically target U.S. vulnerabilities.
- *New materials:* Chinese firms and universities are investing heavily in building up basic research capabilities and manufacturing capacity in new and advanced materials, including through acquisition of overseas firms, talent, and intellectual property. These efforts aim to close the technological gap with the United States and localize production of dual-use materials integral to high-value industries like aerospace. They could also enable China to surpass the United States in applying breakthrough discoveries to military hardware.
- *Energy storage:* China has quickly built up advanced production capacity in lithium-ion batteries and established control over a substantial portion of the global supply chain, exposing the United States to potential shortages in critical materials, battery components, and batteries. China's heavily subsidized expansion in lithium-ion batteries will likely lead to excess capacity and drive down global prices. If Chinese producers flood global markets with cheaper, technologically inferior batteries, it would jeopardize the economic viability of more innovative energy storage technologies currently under development in the United States.
- *Nuclear power:* China is positioning itself to become a leader in nuclear power through cultivating future nuclear export markets along the BRI, particularly in sub-Saharan Africa, and attracting advanced nuclear reactor designers to build prototypes in China.

Section 3: Growing U.S. Reliance on China's Biotech and Pharmaceutical Products

China is the largest producer of active pharmaceutical ingredients (APIs) in the world, and millions of U.S. consumers take life-saving drugs that contain ingredients made in China, even if the finished drugs themselves are not made in China. There are serious deficiencies in health and safety standards in China's pharmaceutical sector, and inconsistent and ineffective regulation by China's government. Nevertheless, U.S. imports of these health products—either directly from China or indirectly through companies in third countries—continue to increase. As the largest source of fentanyl, China also plays a key role in the ongoing U.S. opioid epidemic. Beijing's weak regulatory and enforcement regime allows chemical and pharmaceutical manufacturers to export dangerous controlled and uncontrolled substances.

U.S. consumers, including the U.S. military, are reliant on drugs or active ingredients sourced from China, which presents economic and national security risks, especially as China becomes more competitive in new and emerging therapies. The Chinese government is investing significant resources into the development of biotechnology products and genomics research, accumulating private and medical data on millions of U.S. persons in the process. The Chinese government also encourages mergers and acquisitions—as well as venture capital investments—in U.S. biotech and health firms, leading to technology transfer that has enabled the rapid development of China's domestic industry. U.S. health and biotech firms in China, meanwhile, continue to face regulatory and other market barriers. While the Chinese government has taken steps in recent years to streamline regulatory procedures and allow foreign medical products to enter the market more quickly, concerns remain over China's weak commitment to protecting intellectual property rights and willingness to favor domestic providers of health products.

Key Findings

- China is the world's largest producer of APIs. The United States is heavily dependent on drugs that are either sourced from China or include APIs sourced from China. This is especially true for generic drugs, which comprise most prescriptions filled in the United States. Drug companies are not required to list the API country of origin on their product labels; therefore, U.S. consumers may be unknowingly accepting risks associated with drugs originating from China.
- The Chinese government has designated biotechnology as a priority industry as a part of its 13th Five-Year Plan and the Made in China 2025 initiative. The development of China's pharmaceutical industry follows a pattern seen in some of its other industries, such as chemicals and telecommunications, where state support promotes domestic companies at the expense of foreign competitors.
- China's pharmaceutical industry is not effectively regulated by the Chinese government. China's regulatory apparatus is inadequately resourced to oversee thousands of Chinese drug manufacturers, even if Beijing made such oversight a greater priority. This has resulted in significant drug safety scandals.
- The U.S. Food and Drug Administration (FDA) struggles to guarantee the safety of drugs imported from China because of the small number of FDA inspectors in country, the large number of producers, the limited cooperation from Beijing, and the fraudulent tactics of many Chinese manufacturers. Because of U.S. dependency on China as a source of many critical drugs, banning certain imports due to contamination risks creating drug shortages in the United States.
- As a result of U.S. dependence on Chinese supply and the lack of effective health and safety regulation of Chinese producers, the American public, including its armed forces, are at risk of exposure to contaminated and dangerous medicines. Should Beijing opt to use U.S. dependence on China as an economic

weapon and cut supplies of critical drugs, it would have a serious effect on the health of U.S. consumers.

- Lack of data integrity in China presents challenges for U.S. and Chinese health regulators. In 2016, the China Food and Drug Administration investigated 1,622 drug clinical trial programs and canceled 80 percent of these drug applications after it found evidence of fraudulent data reporting and submissions of incomplete data, among other problems.
- China places great emphasis on genomic and other health-related data to enhance its biotech industry. Domestically, China established national and regional centers focused on big data in health and medicine. Investment and collaborations in the U.S. biotech sector give Chinese companies access to large volumes of U.S. medical and genomic data, but U.S. companies do not get reciprocal access.
- Foreign firms continue to face obstacles in China's health market. These obstacles include drug regulatory approval delays, drug pricing limitations, reimbursement controls, and intellectual property theft. U.S. companies must also compete with Chinese drug companies that introduce generic products or counterfeit drugs to the Chinese market shortly after a foreign patented drug is introduced.
- China is the largest source of fentanyl, a powerful synthetic opioid, in the United States. Although the Chinese government made multiple commitments to curtail the flow of illicit fentanyl to the United States, it has failed to carry out those commitments.

Chapter 4: China's Global Ambitions

Section 1: Beijing's "World-Class" Military Goal

In remarks before the CCP's 19th National Congress in October 2017, General Secretary Xi pledged to build the PLA into a "world-class" force by the middle of the 21st century. This milestone established a timeline for and helps define the goal of the CCP's sweeping ambition for growing China's military power—what General Secretary Xi declared shortly after assuming power in 2012 as China's "Strong Military Dream." This force would support the CCP's efforts to place China at the center of world affairs.

Beijing has instructed the PLA to remain primarily focused on a potential conflict with Taiwan, but has also directed the force to increase preparations for conflicts elsewhere around China's periphery, including with the United States, Japan, India, and other countries in the region. At the same time, it has given the PLA guidance to increase its operations beyond the Indo-Pacific region. One goal of this strategy is to defend China's overseas interests, which Beijing describes as being "crucial" and in recent years has elevated to a similar level of importance for the PLA as defending China's own territory. Another of Beijing's goals is to increase the difficulty the United States would face in intervening in a regional conflict.

Beijing's ambition to develop the PLA into a world-class force will create challenges for the United States and its allies and part-

ners. It would increase the confidence of Chinese leaders to employ the PLA to coerce China's neighbors into forfeiting their territorial claims and other sovereign interests. A military that is truly world-class in technology, training, and personnel would likely also allow China to prevail in a military conflict with any regional adversary. Moreover, Beijing could decide to initiate a military conflict even if it calculated the United States would intervene due to its confidence it would be able to effectively deter or defeat intervening U.S. military forces. Beyond armed conflict, a more robust overseas military presence will provide Beijing additional tools to support and influence countries around the world that pursue policies injurious to U.S. interests.

Key Findings

- In 2017, Beijing announced its goal to build the PLA into a world-class military, overcoming remaining shortfalls in the force's capabilities to establish China firmly among the ranks of the world's leading military powers. This objective is guided by CCP leaders' view that China is approaching the "world's center stage" and represents the military component of a multifaceted goal to establish China's leading global position in every important element of national power.
- Beijing views a world-class PLA as achieving parity in strength and prestige with the world's other leading militaries, especially with the U.S. armed forces, and being capable of preventing other countries from resisting China's pursuit of its national goals. Deterring outside intervention will be especially important in the Indo-Pacific region, where China aims to resolve territorial disputes with a number of important U.S. allies and partners—including through the use of military force if necessary—but will also extend to China's overseas interests.
- Once focused on territorial defense, China's military strategy has evolved in recent years to encompass a concept PLA strategists refer to as "forward defense," which would create greater strategic depth by extending China's defensive perimeter as far as possible from its own shores. China is developing key capabilities necessary for force projection centered on a sophisticated blue-water navy that Chinese naval leadership plans to use to combat the U.S. Navy in the far seas.
- To support this strategy, Beijing is expanding its military presence inside and beyond the Indo-Pacific, including by building a network of overseas "strategic strongpoints" consisting of military bases and commercial ports that can support military operations. China established its first permanent overseas military presence in Djibouti in 2017 and Argentina in 2018, and reportedly has reached an agreement for the PLA to operate from a naval base in Cambodia. The PLA is increasingly training and fielding capabilities for expeditionary operations, including by developing a third aircraft carrier and improving its amphibious assault capabilities.
- The PLA continues to prioritize the modernization of its maritime, air, information warfare, and long-range missile forces,

and is developing or has fielded cutting-edge capabilities in space, cyberspace, hypersonics, electronic warfare, and AI. Beijing is attempting to establish a leading position in the next global “revolution in military affairs” and is employing its “military-civil fusion” strategy to gain advantage in key emerging technologies. U.S. companies that partner with Chinese technology firms may be participants in this process.

- Notwithstanding its long-held policy of maintaining a “minimal nuclear deterrent,” Beijing is growing, modernizing, and diversifying its nuclear arsenal and delivery systems. China doubled the size of its nuclear arsenal over the last decade and U.S. officials estimate it will double it again in the next decade, while Beijing has increased the readiness and improved the accuracy of its nuclear forces.
- China continues to devote ample financial resources to its military modernization, with its officially-reported defense budget ranking second only to the United States since 2002. China’s overall defense spending has seen a nearly eight-fold increase over the past two decades, dwarfing the size and growth rate of other countries in the Indo-Pacific.

Section 2: An Uneasy Entente: China-Russia Relations in a New Era of Strategic Competition with the United States

China-Russia relations have strengthened considerably over the last decade in the face of what both countries perceive to be an increasingly threatening external environment. Beijing and Moscow believe the United States and the international liberal order pose a threat to their regime survival and national security. At the same time, they view the United States and other democracies as in decline and see an opportunity to expand their geopolitical influence at the expense of Washington and its allies. The two countries frame their relationship as the best it has ever been, but insist that it is not an alliance. However, China and Russia’s common expectation of diplomatic support in a dispute, shared antipathy to democratic values, opposition to the U.S. alliance system, and deepening diplomatic and military cooperation have already begun to challenge U.S. interests around the globe.

Nevertheless, Russia chafes at being a weaker partner in this relationship and fears becoming a mere “raw materials appendage” of China. Already scarred by historical enmity, the China-Russia relationship remains constrained by divergence over key national interests including differing stances on territorial disputes and partnerships with countries regarded as rivals by the other. Each country also harbors concerns over the potential military and geopolitical threat posed by the other. Finally, China’s growing influence in regions Russia perceives as its traditional sphere of influence—such as Central Asia and the Arctic—complicates the creation of a formal alliance.

Despite their differences, Moscow and Beijing work either independently or together to counter the United States and erode the values underpinning U.S. global leadership. China’s and Russia’s use of influence operations, cyberwarfare, and disinformation have the potential to destabilize the United States and democracies around the world. Moreover, coordinated Sino-Russian military activity has

created new security challenges for the United States and its allies. Russian sales of advanced military technology to China have bolstered PLA capabilities, while combined exercises have sought to improve interoperability. Coordinated military activity between both countries in a single theater or separate theaters could test the ability of the United States and its allies to respond. One country's success in pursuing its interests in opposition to the United States may also embolden the other to take similar actions.

Key Findings

- China and Russia both object to the current international order and the interests it promotes, including human rights, democracy, and a rules-based economic system that imposes on them obligations they wish to evade. Both countries see the values of that order as a threat to their authoritarian models and view the United States as the leader and primary defender, along with its alliance networks, of that order. Based on that common perception and their mutual interest in opposing the United States and its allies, an entente between China and Russia has emerged in recent years as the two have increased their diplomatic, military, and economic cooperation.
- China and Russia perceive threats to their regime security emanating from democracy movements—which they allege are “color revolutions” instigated by the United States—and from the free, open internet. Both countries seek to combat these challenges by interfering in democratic countries’ political processes and jointly championing the idea that the internet should be subject to sovereign states’ control. The two countries have also coordinated efforts to act as a counterweight to the United States by supporting rogue or authoritarian regimes and opposing U.S.-led votes in the UN Security Council. More broadly, China and Russia’s promotion of norms conducive to authoritarianism aims to subvert key elements of the international order.
- Beijing and Moscow’s view that the United States and its allies are in decline has emboldened both countries to take more assertive action in their regions in ways inimical to U.S. interests. These actions include military and paramilitary activities pursued separately by China and Russia that threaten the sovereignty of their neighbors as well as coordinated activity that creates new challenges for the United States and its allies in responding to combined Sino-Russian military operations.
- China and Russia’s trade in oil and gas is an important avenue by which both countries circumvent U.S. tariffs and international sanctions. Russia is China’s top source of imported oil, and is poised to become a major provider to China of natural gas over the next decade. Major energy deals and high-level contacts serve to soften the blow of sanctions and tariffs on both countries’ products, while signaling that China and Russia can rely on each other if alienated by the United States and other countries.
- Nonetheless, the China-Russia relationship remains scarred by historical enmity and constrained by Moscow’s concerns over its

increasingly subordinate role in the partnership. Divergence in key national interests, such as different stances on territorial disputes and support for regional rivals, further limits bilateral cooperation. Each country also harbors concerns over the potential military and geopolitical threat posed by the other. Moreover, China's growing influence in regions Russia perceives as its traditional sphere of influence—such as Central Asia and the Arctic—complicates the creation of a formal alliance.

Section 3: China's Ambitions in Space: Contesting the Final Frontier

China's government and military are determined to meet ambitious goals for space leadership, if not dominance, and China has connected its space program with its broader ambitions to become a terrestrial leader in political, economic, and military power. Beijing aims to establish a leading position in the future space-based economy and capture important sectors of the global commercial space industry, including promoting its space industry through partnerships under what it has termed the "Space Silk Road." Meanwhile, China has jumpstarted its domestic space industry by engaging in an extensive campaign of intellectual property theft, generous state support to commercial startups, and predatory pricing for Chinese space services in the global space market. Beijing has also used front companies to invest in U.S. space companies as part of its efforts to acquire U.S. technology by both licit and illicit means, while Chinese universities involved in developing space-related technology for the PLA have proactively pursued research collaboration with U.S. and other foreign universities.

China has aggressively pursued the development of counterspace weapons, which are inherently destabilizing. Chinese strategic writings on space warfare also appear to favor dangerously escalatory offensive tactics, raising concerns about whether it is possible to deter China from attacking U.S. space assets. China believes space is a "new commanding height in strategic competition" and views seizing dominance in space as a priority in a conflict. Beijing has also fought to promote its leadership role in international space governance institutions and indicated it may extend its vision of governance and sovereignty to outer space.

The United States retains many advantages in space, such as its international partnerships and its organizational and technical expertise, and China is in some ways attempting to follow in the footsteps of past U.S. achievements. Still, China's single-minded focus and national-level commitment to establishing itself as a global space leader harms other U.S. interests and threatens to undermine many of the advantages the United States has worked so long to establish. China is well-positioned to assume a commanding role in a future space-based economy, as its steps to dominate the global commercial launch and satellite sectors through generous subsidies and other advantages have already threatened to hollow out the U.S. space industrial base. Should the China Space Station proceed as planned and the International Space Station be retired, China may also replace the United States as many countries' default partner in human spaceflight.

Key Findings

- China's goal to establish a leading position in the economic and military use of outer space, or what Beijing calls its "space dream," is a core component of its aim to realize the "great rejuvenation of the Chinese nation." In pursuit of this goal, China has dedicated high-level attention and ample funding to catch up to and eventually surpass other spacefaring countries in terms of space-related industry, technology, diplomacy, and military power. If plans hold to launch its first long-term space station module in 2020, it will have matched the United States' nearly 40-year progression from first human spaceflight to first space station module in less than 20 years.
- China views space as critical to its future security and economic interests due to its vast strategic and economic potential. Moreover, Beijing has specific plans not merely to explore space, but to industrially dominate the space within the moon's orbit of Earth. China has invested significant resources in exploring the national security and economic value of this area, including its potential for space-based manufacturing, resource extraction, and power generation, although experts differ on the feasibility of some of these activities.
- Beijing uses its space program to advance its terrestrial geopolitical objectives, including cultivating customers for BRI, while also using diplomatic ties to advance its goals in space, such as by establishing an expanding network of overseas space ground stations. China's promotion of launch services, satellites, and the Beidou global navigation system under its Space Silk Road is deepening participants' reliance on China for space-based services.
- China is taking steps to establish a commanding position in the commercial launch and satellite sectors relying in part on aggressive state-backed financing that foreign market-driven companies cannot match. China has already succeeded in undercutting some U.S. and other foreign launch and satellite providers in the international market, threatening to hollow out these countries' space industrial bases.
- The emergence of China's indigenous space sector has been an early and notable success of Beijing's military-civil fusion strategy. The aggressive pursuit of foreign technology and talent gained through joint research and other means, especially from the United States and its allies and partners, continues to be central to this strategy and to China's space development goals in general.
- The Chinese government and military use Hong Kong-based companies to exploit legal loopholes and uneven enforcement in U.S. export controls to gain access to space capabilities which U.S. law prohibits Beijing from purchasing outright. Collaboration with foreign universities, including in the United States, is another important avenue in China's drive to acquire space technology. Chinese students enrolled in foreign science, technology, engineering, and mathematics programs are treated like

employees of China's defense industrial base, with defense enterprises regularly funding their studies in return for service commitments following graduation.

- China views space as a critical U.S. military and economic vulnerability, and has fielded an array of direct-ascent, cyber, electromagnetic, and co-orbital counterspace weapons capable of targeting nearly every class of U.S. space asset. The PLA has also developed doctrinal concepts for the use of these weapons encouraging escalatory attacks against an adversary's space systems early in a conflict, threatening to destabilize the space domain. It may be difficult for the United States to deter Beijing from using these weapons due to China's belief the United States has a greater vulnerability in space.

Section 4: Changing Regional Dynamics: Oceania and Singapore

China aims to replace the United States as a leading security and economic power in the Indo-Pacific region. While most countries in the region are aware of the risks posed by Beijing's increased assertiveness, they have struggled to effectively respond, due in part to a desire to continue benefiting from economic engagement with China.

Australia, a steadfast U.S. ally, maintains economic ties with China even as concern over Beijing's interference in its domestic politics has increased. As Australia's top trading partner, China wields significant economic leverage over Australia, which it has used during diplomatic disputes. Canberra has passed laws to address foreign political interference and economic espionage and is trying to address China's interference in Australian universities, but progress has been mixed. It has also taken measures to prevent Chinese investment in Australia's infrastructure that could harm Australia's national interest, while launching its largest military modernization effort since the Cold War to respond to China's growing military threat.

In recent years, Beijing has increased outreach to the Pacific Islands due to the region's strategic significance and voting power in the UN. Beijing's efforts have won it political support, including establishing diplomatic relations this year with the Solomon Islands and Kiribati, previously two of Taiwan's remaining diplomatic partners. Nevertheless, some South Pacific policymakers have grown concerned Chinese engagement could overwhelm these small countries and result in an excessive accumulation of debt to Beijing. China has also sought to raise its military profile in the Pacific Islands, while Australia and the United States have increased their engagement in the region in response to China's advances.

Singapore has pursued close relationships with both the United States and China while attempting to protect its autonomy in foreign affairs rather than side exclusively with either country. It remains dedicated to its relationship with the United States, as exemplified by its robust economic and security ties. At the same time, Beijing seeks a closer economic and military relationship with Singapore. Rhetorical commitment to greater security ties with China, as well as its role as a financial hub for China's BRI, demonstrates the challenges Singapore faces in hedging between the United States and China.

Beijing has benefited from popular conceptions that China is the most important economic partner to these Indo-Pacific countries, even as U.S. investment exceeds that from China. While Indo-Pacific countries understand the importance of the United States' continued presence, China's increasing influence threatens to alter the trajectory of U.S. relations with these countries absent strong U.S. involvement in the region.

Key Findings

- Beijing has used economic coercion, acquired strategically-significant assets, and interfered in the domestic politics of neighboring countries to advance its interests in the Indo-Pacific region. China seeks closer engagement with its neighbors not only for economic gain but also to gain influence over their decision making to eventually achieve regional dominance and replace the United States as a vital economic partner and preeminent regional security guarantor.
- Some targeted countries are becoming increasingly aware of these risks and are taking steps to respond to China's political interference and growing military strength. Still, countries have struggled to formulate comprehensive and effective responses.
- Australia wants to maintain positive economic ties with China, but is also wary of Beijing's increasing regional assertiveness and outright interference in Australia's political affairs. Its steps to mitigate the risks of engagement with China, including tightening foreign investment restrictions and cracking down on political interference, have had mixed success. The Australian business community still favors greater economic engagement with China while downplaying national security concerns.
- To address the growing military threat posed by China, Australia has launched its largest military modernization effort since the Cold War. Central to this effort are large-scale investments in new warships, submarines, and fighter aircraft. Australia is also standing up a new military unit dedicated to improving military coordination with Pacific Island countries and is working with the United States and Papua New Guinea to develop a naval base in the latter's territory, which will complement the already substantial U.S. military presence in Australia.
- China seeks engagement with the Pacific Islands to establish military access to the region, gain the benefit of these countries' voting power in the UN, undermine regional diplomatic support for Taiwan, and gain access to natural resources, among other goals. Pacific Island countries view China as a vital economic partner and source of infrastructure investment and aid, but some Pacific Island officials have expressed reservations about Beijing's increasing influence and presence in the region, particularly over growing indebtedness to China. As a result of China's growing inroads in the Pacific Islands, Australia has also increased its engagement in the region, though its efforts have also encountered some pushback.

- As a small country and regional economic hub, Singapore continues to work to maintain the balance between its relationships with the United States and China amid heightening U.S.-China tensions. Singapore is also concerned about China's attempts to undermine ASEAN's unity and its own ability to play a leading role in Southeast Asia. While Singapore remains a dedicated security partner of the United States, it also has close economic ties to China, including serving as an increasingly important financial and legal intermediary for BRI projects.

Chapter 5: Taiwan

The Taiwan Relations Act, which set the foundation for ties between the United States and Taiwan following the United States' severing of diplomatic ties with the Republic of China (Taiwan), celebrated its 40th anniversary in 2019. In the 40 years since the Taiwan Relations Act's signing, Taiwan has become a thriving multiparty democracy. Taiwan has a robust civil society and rule of law that protects universal human rights, open public discourse, and a free and independent media. The vibrancy of Taiwan's democratic system is on display in the ongoing campaigns for the 2020 presidential and legislative elections. In addition to being a model of a successful democracy for the Indo-Pacific region, Taiwan has become an increasingly important economic and geostrategic partner for the United States.

Meanwhile, throughout 2019 Beijing adopted a more coercive policy toward Taiwan, seeking to isolate and intimidate Taipei into unification on Beijing's terms. In January 2019, General Secretary Xi delivered a major speech on Beijing's Taiwan policy in which he claimed that Taiwan's unification with the People's Republic of China was inevitable and indicated that the "one country, two systems" model was the only acceptable arrangement for unification. That model has been roundly rejected by the Taiwan public and multiple Taiwan presidential administrations.

In implementing its more coercive approach, Beijing sharply escalated its military, diplomatic, and economic pressure against Taiwan, including interfering in Taiwan's media to shape public opinion on China and cross-Straits relations. In the Taiwan Strait area, the PLA carried out a series of provocative operations not seen in 20 years, while Beijing enticed two more of Taiwan's remaining 17 diplomatic partners to switch recognition to Beijing. It also severely curtailed cross-Straits tourism flows by suspending all approvals for individual tourists to visit Taiwan. Beijing's multipronged pressure campaign limits Taipei's ability to fully engage with the international community and diversify its economy away from deep reliance on China.

The people of Taiwan are now observing Beijing's unification model unfold in Hong Kong, where millions of people are fighting for their civil liberties against an unbending authoritarian regime. Should Beijing succeed in coercing Taiwan into submitting to a similar unification agreement, it not only would damage U.S. national security interests but also could undermine the progress of democratic values and institutions in the region.

Key Findings

- In 2019, General Secretary Xi made clear his increasingly uncompromising stance toward Taiwan's independent status and sense of urgency regarding unification. Beijing intensified its multipronged campaign to coerce and isolate Taiwan, including by supporting Taiwan politicians Beijing finds palatable, while opposing and seeking to discredit those it does not, particularly Taiwan's elected government headed by President Tsai Ing-wen. Guided by this policy, Beijing redoubled its efforts to bypass Taiwan's central government by conducting negotiations with unelected political parties, groups, and individuals.
- The deliberate crossing of the Taiwan Strait median line by Chinese fighter aircraft in March 2019 was the first such crossing in 20 years and marked a sharp escalation in the military pressure Beijing has increasingly applied against Taipei since General Secretary Xi assumed power in 2012. China signaled that its intensifying campaign of military coercion had become official policy in a key policy document released in July 2019, while the continued growth of the PLA's capabilities and budget threatened to overturn any remaining semblance of cross-Strait military balance.
- As Beijing escalated diplomatic, economic, cultural, and political warfare against Taiwan, evidence emerged that it sought to influence Taiwan's November 2018 local elections, including through traditional Taiwan media and disinformation spread through social media to exacerbate social divisions and undermine public confidence in the ruling Democratic Progressive Party government. Allegations that Beijing intervened on behalf of Taiwan presidential challenger Han Kuo-yu of the Nationalist Party (Kuomintang, or KMT) in his 2018 Kaohsiung mayoral campaign raised questions over whether it may be doing so again in the lead-up to Taiwan's presidential election in January 2020.
- The CCP adopted new tactics to leverage Taiwan media in support of its political goals, with evidence building that Beijing has shaped coverage of cross-Strait relations and potentially Taiwan's presidential election through direct partnerships with some major Taiwan media outlets. These partnerships have included China's Taiwan Affairs Office commissioning stories and giving instructions to editorial managers.
- Concerns in Taiwan over Beijing's desired "one country, two systems" unification model for Taiwan were amplified by 2019's massive protest movement in Hong Kong, which is governed by the same model and has seen the autonomy the model promises steadily erode. Presidential contenders from both major political parties in Taiwan assailed the "one country, two systems" model as unacceptable for any future sovereign agreement between the two sides.
- Taiwan took a series of steps to enhance its military capabilities and implement its new Overall Defense Concept. These measures included the island's largest increase in its defense budget

in more than a decade, breaking ground on the facility that will build Taiwan's indigenous submarines, allocating funding for the procurement of 60 new small fast-attack missile boats, and expediting production of new missile defense systems and mobile land-based antiship missile platforms.

- U.S.-Taiwan cooperation expanded into new areas as the United States took significant steps to support Taiwan, including the Trump Administration's approval of a landmark arms sale of new fighter aircraft to Taiwan, the first meeting between U.S. and Taiwan national security advisors since 1979, and a more assertive approach to U.S. Navy transits of the Taiwan Strait. However, talks under the Trade and Investment Framework Agreement have stalled since October 2016.

Chapter 6: Hong Kong

In 2019, the Hong Kong government's controversial bill that would allow for extradition to mainland China sparked a historic protest movement opposing the legislation and the Mainland's growing encroachment on the territory's autonomy. Millions of Hong Kong citizens participated in unprecedented mass demonstrations against the bill, causing its formal withdrawal, paralyzing the Hong Kong government, and dealing a major blow to Beijing. In the face of the Hong Kong authorities' intransigence and growing police violence against demonstrators, the movement's demands expanded while protesters strengthened their resolve to achieve Beijing's long-delayed promise of credible democratic elections. The protesters declared that democratic elections are essential to a truly representative government.

Instead of heeding the movement's calls for the preservation of Hong Kong's "high degree of autonomy," the CCP has used numerous tools to try to quell the demonstrations, including economic coercion, disinformation, and the apparent encouragement of pro-Beijing thugs to attack protesters. Meanwhile, the Hong Kong government, backed by Beijing, took new steps to erode the territory's freedom of expression, press freedom, rule of law, and freedom of assembly, making the territory more like any other Chinese city. These moves are having a harmful effect on Hong Kong's attractiveness as one of the world's preeminent trade and financial hubs. Hong Kong acts as a unique conduit for investment flows between mainland China and global financial markets, a role underpinned by international confidence in the strength of its institutions and the rule of law.

U.S. policy toward Hong Kong, as outlined in the U.S.-Hong Kong Policy Act of 1992, underscores U.S. support for Hong Kong's human rights and democratization, and is predicated on the territory retaining its autonomy under the "one country, two systems" framework. Beijing's growing encroachment on Hong Kong's autonomy in violation of its legal commitments has thus raised serious concerns for U.S. policymakers. The future direction of Hong Kong—and with it U.S.-Hong Kong policy—will rest upon the outcome of the anti-extradition bill protest movement and the extent to which the Hong Kong government and Beijing respect the aspirations of Hong Kong citizens.

Key Findings

- The Hong Kong government's proposal of a bill that would allow for extraditions to mainland China sparked the territory's worst political crisis since its 1997 handover to the Mainland from the United Kingdom. China's encroachment on Hong Kong's autonomy and its suppression of prodemocracy voices in recent years have fueled opposition, with many protesters now seeing the current demonstrations as Hong Kong's last stand to preserve its freedoms. Protesters voiced five demands: (1) formal withdrawal of the bill; (2) establishing an independent inquiry into police brutality; (3) removing the designation of the protests as "riots;" (4) releasing all those arrested during the movement; and (5) instituting universal suffrage.
- After unprecedented protests against the extradition bill, Hong Kong Chief Executive Carrie Lam suspended the measure in June 2019, dealing a blow to Beijing which had backed the legislation and crippling her political agenda. Her promise in September to formally withdraw the bill came after months of protests and escalation by the Hong Kong police seeking to quell demonstrations. The Hong Kong police used increasingly aggressive tactics against protesters, resulting in calls for an independent inquiry into police abuses.
- Despite millions of demonstrators—spanning ages, religions, and professions—taking to the streets in largely peaceful protest, the Lam Administration continues to align itself with Beijing and only conceded to one of the five protester demands. In an attempt to conflate the bolder actions of a few with the largely peaceful protests, Chinese officials have compared the movement to "terrorism" and a "color revolution," and have implicitly threatened to deploy its security forces from outside Hong Kong to suppress the demonstrations.
- In 2019, assessment of press freedom fell to its lowest point since the handover, while other civil liberties protected by the Basic Law (Hong Kong's mini constitution), including freedom of expression and assembly, faced increasing challenges.
- Throughout 2019, the CCP stepped up its efforts to intervene in Hong Kong's affairs, using an array of tools to increase its influence in the territory, most clearly by co-opting local media, political parties, and prominent individuals. Beijing also used overt and covert means to intervene in Hong Kong's affairs, such as conducting a disinformation campaign and using economic coercion in an attempt to discredit and intimidate the protest movement. These efforts included alleging without evidence that U.S. and other foreign "black hands" were fomenting the protests; directing and organizing pro-Beijing legislators, businesses, media, and other influential individuals against the movement; allegedly encouraging local gangs and mainland community groups to physically attack protesters and prodemocracy figures; and conducting apparent cyberattacks against Hong Kong protesters' communications and a prodemocracy media outlet.

- Hong Kong has a unique role as a conduit between Chinese companies and global financial markets. As Chinese companies are increasingly represented in key benchmark indices, analysts anticipate greater capital flows from the United States and other countries into Chinese companies through the stock and bond Connect platforms between mainland exchanges and Hong Kong. However, due to diminished confidence resulting from the extradition bill proposal and subsequent fallout, some foreign businesses are reportedly considering moving their operations away from Hong Kong.
- Hong Kong's status as a separate customs territory, distinct from mainland China, is under pressure. U.S. and Hong Kong officials cooperate on enforcing U.S. export controls of dual-use technologies, though U.S. officials continue to raise concerns about diversion of controlled items. Beijing's more assertive imposition of sovereign control over Hong Kong undermines the "high degree of autonomy" that underwrites trust in the Hong Kong government's ability to restrict sensitive U.S. technologies from being diverted to mainland China.

THE COMMISSION'S KEY RECOMMENDATIONS

The Commission considers 10 of its 38 recommendations to Congress to be of particular significance. The complete list of recommendations appears at the Report's conclusion on page 537.

The Commission recommends:

1. Congress enact legislation to preclude Chinese companies from issuing securities on U.S. stock exchanges if:
 - The Public Company Accounting Oversight Board is denied timely access to the audit work papers relating to the company's operations in China;
 - The company disclosure procedures are not consistent with best practices on U.S. and European exchanges;
 - The company utilizes a variable interest entity (VIE) structure;
 - The company does not comply with *Regulation Fair Disclosure*, which requires material information to be released to all investors at the same time.
2. Congress enact legislation stating that all provisions and the special status of Hong Kong included in the U.S.-Hong Kong Policy Act of 1992 will be suspended in the event that China's government deploys People's Liberation Army or People's Armed Police forces to engage in armed intervention in Hong Kong.
3. Congress enact legislation requiring the following information to be disclosed in all issuer initial public offering prospectuses and annual reports as material information to U.S. investors:
 - Financial support provided by the Chinese government, including: direct subsidies, grants, loans, below-market loans, loan guarantees, tax concessions, government procurement policies, and other forms of government support.
 - Conditions under which that support is provided, including but not limited to: export performance, input purchases manufactured locally from specific producers or using local intellectual property, or the assignment of Chinese Communist Party (CCP) or government personnel in corporate positions.
 - CCP committees established within any company, including: the establishment of a company Party committee, the standing of that Party committee within the company, which corporate personnel form that committee, and what role those personnel play.
 - Current company officers and directors of Chinese companies and U.S. subsidiaries or joint ventures in China who currently hold or have formerly held positions as CCP officials and/or Chinese government officials (central and local), including the position and location.
4. Congress hold hearings assessing the productive capacity of the U.S. pharmaceutical industry, U.S. dependence on Chinese pharmaceuticals and active pharmaceutical ingredients (APIs), and the ability of the U.S. Food and Drug Administration (FDA) to

guarantee the safety of such imports from China, with a view toward enacting legislation that would:

- Require the FDA to compile a list of all brand name and generic drugs and corresponding APIs that: (1) are not produced in the United States; (2) are deemed critical to the health and safety of U.S. consumers; and (3) are exclusively produced—or utilize APIs and ingredients produced—in China.
 - Require Medicare, Medicaid, the U.S. Department of Veterans Affairs, the U.S. Department of Defense, and other federally funded health systems to purchase their pharmaceuticals only from U.S. production facilities or from facilities that have been certified by the FDA to be in compliance with U.S. health and safety standards and that actively monitor, test, and assure the quality of the APIs and other components used in their drugs, unless the FDA finds the specific drug is unavailable in sufficient quantities from other sources.
 - Require the FDA, within six months, to investigate and certify to Congress whether the Chinese pharmaceutical industry is being regulated for safety, either by Chinese authorities or the FDA, to substantially the same degree as U.S. drug manufacturers and, if the FDA cannot so certify, forward to Congress a plan for protecting the American people from unsafe or contaminated drugs manufactured in China.
5. Congress require the relevant departments and agencies of jurisdiction—including the U.S. Department of the Treasury, the U.S. Department of Commerce, and the U.S. Securities and Exchange Commission—to prepare a report to Congress on the holdings of U.S. investors in Chinese bonds and other debt instruments. Such a report shall include information on the direct, indirect, and derivative ownership of any of these instruments.
 6. Congress direct the National Space Council to develop a strategy to ensure the United States remains the preeminent space power in the face of growing competition from China and Russia, including the production of an unclassified report with a classified annex containing the following:
 - A long-term economic space resource policy strategy, including an assessment of the viability of extraction of space-based precious minerals, onsite exploitation of space-based natural resources, and space-based solar power. It would also include a comparative assessment of China's programs related to these issues.
 - An assessment of U.S. strategic interests in or relating to cis-lunar space.
 - An assessment of the U.S. Department of Defense's current ability to guarantee the protection of commercial communications and navigation in space from China's growing counter-space capabilities, and any actions required to improve this capability.

- A plan to create a space commodities exchange to ensure the United States drives the creation of international standards for interoperable commercial space capabilities.
 - A plan to streamline and strengthen U.S. cooperation with allies and partners in space.
 - An interagency strategy to defend U.S. supply chains and manufacturing capacity critical to competitiveness in space.
7. Congress direct the U.S. Department of Justice to reestablish a higher education advisory board under the Federal Bureau of Investigation. In concert with the U.S. Department of Commerce's Bureau of Industry and Security, U.S. Department of Homeland Security, and U.S. Department of State, the higher education advisory board would convene semiannual meetings between university representatives and relevant federal agencies to review the adequacy of protections for sensitive technologies and research, identify patterns and early warning signs in academic espionage, assess training needs for university faculty and staff to comply with export controls and prevent unauthorized transfer of information, and share other areas of concern in protecting national security interests related to academic research.
 8. Congress direct the U.S. secretary of state to submit to Congress a report on actions that have been and will be taken by the United States to counter Beijing's attempts to isolate Taiwan's democratically-elected leaders and to strengthen support for Taiwan's engagement with the international community, including actions the Administration will take should Beijing increase its coercion against Taiwan. The report should:
 - List measures the U.S. government has taken and will take to expand interactions between U.S. and Taiwan government officials in accordance with the Taiwan Travel Act.
 - Formulate a strategy to expand development aid and security assistance to countries that maintain diplomatic ties with Taiwan.
 - Detail steps to expand multilateral collaboration involving Taiwan and other democracies to address global challenges, such as the Global Cooperation and Training Framework's workshops on epidemics, cybersecurity, and media literacy.
 9. Congress direct the Office of the Director for National Intelligence to prepare a National Intelligence Estimate of China's and Russia's approaches to competition with the United States and revision of the international order. The assessment would consider the influence of both countries' ideologies on their foreign policies, including areas both of overlap and of divergence; potential "wedge issues" the United States might exploit; and the implications for the North Atlantic Treaty Organization of a two-front conflict involving both China and Russia.
 10. Congress amend the U.S.-Hong Kong Policy Act of 1992 to direct the U.S. Department of State to develop a series of specific benchmarks for measuring Hong Kong's maintenance of a "high

degree of autonomy” from Beijing. Such benchmarks should employ both qualitative and quantitative measurements to evaluate the state of Hong Kong’s autonomy in the State Department’s annual *Hong Kong Policy Act Report*.

duce products with core competitiveness, and [we] won't be beaten in intensifying competition."¹⁰⁶

China's technology push under General Secretary Xi builds upon earlier efforts but differs in at least three key aspects: a greater emphasis on the strategic importance of reducing reliance on foreign core technologies, the critical role of private companies, and the mobilization of new funding channels.¹⁰⁷ According to Mr. Hirson, China's private technology companies* "rather than state-owned behemoths like China Telecom, represent China's 'national champions' in next generation areas."¹⁰⁸ China's major technology giants, including Baidu, Alibaba, and Tencent, have made large investments in AI and consumer internet and fintech industries.¹⁰⁹ Following the ZTE sanctions, Baidu, Alibaba, and Tencent each responded to Beijing's call for self-reliance by taking steps to support the development of the semiconductor industry in China.[†]¹¹⁰ In recent months, China's technology sector has faced stepped-up government scrutiny and increased pressure to align with Party edicts after years of thriving under light regulation‡—a trend some analysts caution may undermine Beijing's national strategy for innovation driven development.¹¹¹

Addressing Shortfalls in Defense Technology

Beijing is deeply concerned about its defense industry's capacity to independently innovate and develop the cutting-edge technologies it views as critical to what the CCP terms China's "core national power."¹¹² China has made great strides in key defense technologies related to cyber, space, advanced computing, and AI, and is a world leader in hypersonic weapons. Nevertheless, Beijing believes China is still lagging behind the United States, noting in its most recent defense white paper that China's military is "confronted by risks from technology surprise and a growing technological generation gap."¹¹³ General Secretary Xi has demonstrated particular concern over shortfalls in China's technological capabilities, which he has described as the "root cause of [China's] backwardness."¹¹⁴ China's defense industry continues to struggle to produce some high-end military components—such as advanced aircraft engines, guidance and control systems, and microprocessors—forcing Beijing to remain reliant on foreign technologies in these areas.¹¹⁵ China continues to rely in particular on foreign innovation systems from the United States and Japan for the core technologies and talent it views as necessary to its national security.¹¹⁶

*In China, direct ownership is not the primary determinant of the government's ability to control a company's decision making; in other words, private companies can also be directed to carry out government objectives. As described by Curtis J. Milhaupt and Wentong Zheng, "Large, successful [Chinese] firms—regardless of ownership—exhibit substantial similarities in areas commonly thought to distinguish SOEs from [private companies]: market dominance, receipt of state subsidies, proximity to state power, and execution of the state's policy objectives." Curtis J. Milhaupt and Wentong Zheng, "Beyond Ownership: State Capitalism and the Chinese Firm," *Georgetown Law Journal* 103 (2015): 665.

†For instance, in July 2018 Baidu unveiled its self-developed, high-end AI chip designed for autonomous vehicles and data centers. In September 2018, Alibaba established a semiconductor subsidiary to produce AI chips made for autonomous vehicles, smart cities, and smart logistics. Paul Triolo and Graham Webster, "China's Efforts to Build the Semiconductors at AI's Core," *New America*, December 7, 2018.

‡For example, in September 2019 Chinese state media reported that Hangzhou, a major technology hub in China, plans on assigning government officials to work with 100 local private companies, including Alibaba. Josh Horwitz, "China to Send State Officials to 100 Private Firms Including Alibaba," *Reuters*, September 23, 2019.

These plans and standards guidelines build on the progress of earlier policy initiatives to improve digital infrastructure. These initiatives have provided a technological foundation for quickly advancing AI subdomains.* For example, creating numerous cameras and sensors to monitor traffic conditions as part of China’s smart cities development program now provides the data for urban management systems like Alibaba’s City Brain in Hangzhou, which uses AI to monitor and redirect traffic to reduce congestion.⁶³

Industry Overview

China has emerged as a leader in several subdomains of AI, in particular computer vision, digital lifestyle products (e.g., ride hailing and delivery applications), robotics, and speech recognition.⁶⁴ China is ahead of or on par with the United States in technologies that are poised for transformational growth from the application of AI, such as commercial and military strike-capable drones incorporating autonomous navigation.⁶⁵ China trails the United States in autonomous vehicle (AV) technology but is rapidly catching up.⁶⁶

Many Chinese AI companies that appear most competitive vis-à-vis the United States are an outgrowth of the country’s broad adoption of mobile internet and use of mobile applications,† which gives China’s leading mobile platforms like Baidu, Alibaba, and Tencent unparalleled access to consumer data.⁶⁷ By contrast, China’s advances in industrial robotics have been driven by extensive government support and overseas acquisitions,‡ as well as some spillover from major international robot manufacturers locating production facilities in China.⁶⁸

Computer vision falls somewhere in between, with private funding responding to a demand created by government policy. Chinese image recognition startups outperform and are far better funded than international peers, but China’s Ministry of Public Security is a primary customer for facial recognition in surveillance systems and the National Development and Reform Commission, an economic planning agency, has issued policy encouraging use of AI in facial recognition.⁶⁹ China’s widespread use of surveillance applications of

*For instance, the white paper includes an appendix of ten applications of AI by Chinese companies to provide a template for different AI standards, but these technologies were in many cases supported by earlier industrial policies. In intelligent manufacturing, the white paper champions Haier’s COSMOplat, a customizable manufacturing execution and supply chain management system that was developed under Made in China 2025. Standards Administration of China and China Electronic Standardization Institute, *White Paper on Artificial Intelligence Standardization* (人工智能标准化白皮书), January 2018, 96–98. Translation.

†China’s mobile internet ecosystem developed with minimal competition from foreign firms due to mandated government monopolies in telecommunications, the Golden Shield Project (popularly known as the “Great Firewall”) which prohibits access to popular foreign sites like Google and Facebook from within mainland China’s borders, strict licensing requirements for provision of content over the internet, including via mobile applications, and increasingly demanding regulations on management of user data. Hugo Butcher Piat, “Navigating the Internet in China: Top Concerns for Foreign Businesses,” *China Briefing*, March 12, 2019; Ashwin Kaja and Eric Carlson, “China Issues New Rules for Mobile Apps,” *Inside Piracy*, July 1, 2016.

‡Chinese state-owned enterprises have concluded several major acquisitions of robotics and automation firms since Made in China 2025 encouraged closing China’s technological gap through acquiring foreign firms, including Chinese air conditioner and refrigerator manufacturer Midea Group’s acquisition of a majority stake in German robot maker Kuka AG, the world’s largest producer of robots used in auto factories. U.S.-China Economic and Security Review Commission, *Hearing on Technology, Trade, and Military-Civil Fusion*, written testimony of Dan Coughlin, June 7, 2019, 4; Sun Congying, “Midea, Kuka Chase Automation Dreams with \$1.6 Billion Park,” *Caixin*, March 29, 2018; Sun Yuyao, “Overseas Mergers and Acquisitions: Chinese Manufacturing Integrates into the Global Industrial System (海外并购并喷 中国制造融入全球产业体系),” *Advanced Manufacturing Daily*, December 29, 2012.

AI is driven in large part by the absence of privacy protections and by government repression of ethnic groups.⁷⁰ For example, law enforcement agencies across China are deploying facial recognition to identify and track Uyghurs, a Muslim minority from northwestern Xinjiang Province.⁷¹

Both the government and private sector are substantial investors in China's AI. In their AI development plans, the municipal governments of Shanghai and Tianjin each pledge to invest \$15 billion in AI, close to Google's parent Alphabet's \$16.6 billion in global R&D expenditure during 2017.^{*72} However, China's government guidance funds do not always raise or spend the money as planned due to a shortage of investors, inability to recruit qualified personnel to manage the funds, and lack of investment targets that meet the funds' investment criteria, among other reasons.⁷³ Nonetheless, in start-up funding, technology market research firm CB Insights estimates that Chinese companies (including Hong Kong-based companies) received 48 percent of global AI equity investment in 2017, ahead of the United States' 38 percent and up from 11 percent in 2016.⁷⁴ A handful of large foreign VC groups like Japanese conglomerate SoftBank and U.S. VC firm Sequoia are active investors in China's AI market.⁷⁵

China's AI "National Team"

In November 2017, China's Ministry of Science and Technology selected Baidu, Alibaba, and Tencent, as well as voice recognition firm iFlytek, to form a "National Team" charged with developing AI in a range of subdomains.^{†76} According to the government plan, Baidu is to focus on autonomous driving, Alibaba is to focus on cloud computing and smart cities, Tencent is to focus on AI-powered medical diagnosis, and iFlytek is to continue working on voice intelligence.⁷⁷ Hong Kong-based facial recognition start-up SenseTime was subsequently tapped to focus on intelligent vision.⁷⁸

In both design and execution, the national team approach differs from overt promotion of national champions.[‡] None of the firms are state-owned and all had established capabilities in their assigned subdomains before being selected.⁷⁹ In some respects,

*Alphabet's financial disclosures do not distinguish investments in AI from other capabilities and products, but it is likely the world's largest corporate spender on AI. Alphabet Inc., *Form 10-K for the Fiscal Year Ended December 31, 2017*, February 5, 2018, 36; *Economist*, "Google Leads in the Race to Dominate Artificial Intelligence," December 7, 2017.

†Chinese agencies have occasionally designated a "national team" of companies with pre-existing capabilities to focus on building up capacity in a particular field, such as the Ministry of Commerce's 2010 policy to support well-established brick and mortar retailers in developing e-commerce operations. Companies in a national team do not receive anticompetitive policy support to the extent of national champions and have more autonomy to pursue business avenues other than those directed by the government. U.S.-China Economic and Security Review Commission, *Hearing on Technology, Trade and Military-Civil Fusion*, written testimony of Jeffrey Ding, June 7, 2019, 8. Tencent Technology, "China's Ministry of Commerce's Support for Three Large Companies in the 'Ecommerce National Team' Revealed" (商务部扶持电子商务"国家队"三大企业曝光), *China Information Industry Network*, March 3, 2010. Translation.

‡National champions are large, often state-owned firms that advance state interests, whether to establish capacity in a new sector or become competitive internationally in a particular sector. Typically, they receive policy support to assist in advancing state objectives, including subsidies, tax credits, guaranteed market share or monopoly access in certain industries, and supportive regulation and financing to acquire or displace smaller competitors or vertically integrate within other functions of an industry.

These plans and standards guidelines build on the progress of earlier policy initiatives to improve digital infrastructure. These initiatives have provided a technological foundation for quickly advancing AI subdomains.* For example, creating numerous cameras and sensors to monitor traffic conditions as part of China's smart cities development program now provides the data for urban management systems like Alibaba's City Brain in Hangzhou, which uses AI to monitor and redirect traffic to reduce congestion.⁶³

Industry Overview

China has emerged as a leader in several subdomains of AI, in particular computer vision, digital lifestyle products (e.g., ride hailing and delivery applications), robotics, and speech recognition.⁶⁴ China is ahead of or on par with the United States in technologies that are poised for transformational growth from the application of AI, such as commercial and military strike-capable drones incorporating autonomous navigation.⁶⁵ China trails the United States in autonomous vehicle (AV) technology but is rapidly catching up.⁶⁶

Many Chinese AI companies that appear most competitive vis-à-vis the United States are an outgrowth of the country's broad adoption of mobile internet and use of mobile applications,† which gives China's leading mobile platforms like Baidu, Alibaba, and Tencent unparalleled access to consumer data.⁶⁷ By contrast, China's advances in industrial robotics have been driven by extensive government support and overseas acquisitions,‡ as well as some spillover from major international robot manufacturers locating production facilities in China.⁶⁸

Computer vision falls somewhere in between, with private funding responding to a demand created by government policy. Chinese image recognition startups outperform and are far better funded than international peers, but China's Ministry of Public Security is a primary customer for facial recognition in surveillance systems and the National Development and Reform Commission, an economic planning agency, has issued policy encouraging use of AI in facial recognition.⁶⁹ China's widespread use of surveillance applications of

*For instance, the white paper includes an appendix of ten applications of AI by Chinese companies to provide a template for different AI standards, but these technologies were in many cases supported by earlier industrial policies. In intelligent manufacturing, the white paper champions Haier's COSMOplat, a customizable manufacturing execution and supply chain management system that was developed under Made in China 2025. Standards Administration of China and China Electronic Standardization Institute, *White Paper on Artificial Intelligence Standardization* (人工智能标准化白皮书), January 2018, 96–98. Translation.

†China's mobile internet ecosystem developed with minimal competition from foreign firms due to mandated government monopolies in telecommunications, the Golden Shield Project (popularly known as the "Great Firewall") which prohibits access to popular foreign sites like Google and Facebook from within mainland China's borders, strict licensing requirements for provision of content over the internet, including via mobile applications, and increasingly demanding regulations on management of user data. Hugo Butcher Piat, "Navigating the Internet in China: Top Concerns for Foreign Businesses," *China Briefing*, March 12, 2019; Ashwin Kaja and Eric Carlson, "China Issues New Rules for Mobile Apps," *Inside Piracy*, July 1, 2016.

‡Chinese state-owned enterprises have concluded several major acquisitions of robotics and automation firms since Made in China 2025 encouraged closing China's technological gap through acquiring foreign firms, including Chinese air conditioner and refrigerator manufacturer Midea Group's acquisition of a majority stake in German robot maker Kuka AG, the world's largest producer of robots used in auto factories. U.S.-China Economic and Security Review Commission, *Hearing on Technology, Trade, and Military-Civil Fusion*, written testimony of Dan Coughlin, June 7, 2019, 4; Sun Congying, "Midea, Kuka Chase Automation Dreams with \$1.6 Billion Park," *Caixin*, March 29, 2018; Sun Yuyao, "Overseas Mergers and Acquisitions: Chinese Manufacturing Integrates into the Global Industrial System (海外并购并喷 中国制造融入全球产业体系)," *Advanced Manufacturing Daily*, December 29, 2012.

Addendum I: China’s Development of AI Technologies

AI Technology	Applications	Key Industrial Policies	China’s Current Capabilities	Key Companies
Machine Learning, which includes Deep Learning	Foundational for other areas of AI	Cultivating talent in advanced machine learning and leading in machine learning theory are cornerstones of China’s Strategy to dominate in global AI by 2030, unveiled in 2017. The National Development and Reform Commission has also tapped search engine giant Baidu to lead a nationwide online deep learning lab in coordination with Tsinghua and Beihang universities.	Chinese researchers have closed the gap with the United States in publication volume, but China lacks talent in the top echelon. Engineers focus mostly on commercial gains, not fundamental breakthroughs. China’s advantages in sheer volume of data are curtailed by its ability to label and analyze this data. China also lags in producing chips optimized for machine learning.	General: Alibaba, Tencent, Baidu; Chips: Cambricon (used in Huawei phones), Horizon Robotics
Natural Language Processing (NLP)	Speech/voice recognition, information retrieval/extraction, query answering, sentiment analysis	NLP is listed as one of eight “key common technologies” to be developed in China’s AI strategy. Chinese universities are partnering with companies to develop NLP applications, and several Chinese industry associations have launched respected conferences.	In research, China has been second behind the United States for five years. In industry, China is leading in chatbots and is developing machine translation for Chinese to languages in BRI countries. iFlytek is a leader in speech recognition for spoken Chinese.	Baidu, iFlytek; Microsoft, Research Asia is a major player for machine translation and chatbots.
Computer Vision and Biometrics	Facial and other image recognition, machine vision (analyzing images for inspection and process control)	China’s smart cities initiative promotes surveillance technology, and many companies have contracts with public security bureaus. Computer vision accounted for 35 percent of China’s AI market in 2017.	Numerous facial recognition companies, including many startups, are powering China’s surveillance state. In turn, internet giants like Huawei are integrating this tech into—and exporting—“Safe City” systems.	SenseTime, Yitu, Megvii (Face++), Xloong, Zoloz, DeepGlint, Huawei

Chinese voices [that are critical of Beijing] can be silenced in Australia,” Dr. Medcalf contends, “they can be silenced anywhere.”¹³

Responding to China’s Interference, Australia’s Progress Uncertain

Since 2016, following revelations of Australia’s vulnerability to CCP interference, Canberra has passed several new laws to counter foreign interference.* These new laws, which began to enter into force in 2018, target foreign interference in politics, economic espionage, and theft of trade secrets; establish a public register of foreign lobbyists; and require notification of political donations from those on the register or who disburse funds on behalf of a foreign principal.¹⁴ Canberra has also formed a new Department of Home Affairs to integrate certain intelligence, law enforcement, and policy responsibilities across the government and ordered the most significant review of its intelligence agencies in 40 years, which is still ongoing.¹⁵

Huang Xiangmo, a former Australian permanent resident and prolific political donor accused of acting as a proxy for Beijing, has been a primary focus of much of the public debate surrounding CCP interference in Australia.¹⁶ From 2014 to 2017, Mr. Huang was the president of the Australian Council for the Promotion of Peaceful Reunification of China, a political advocacy organization that frequently disguises the nature of its relationship to the Chinese government but is in fact directly subordinate to the CCP’s United Front Work Department.¹⁷ He received scrutiny for his donations to both major Australian political parties totaling \$1.5 million (AUD 2 million) since 2012, and he was accused of being a CCP “agent of influence” by an Australian senator who resigned due to public disclosure of his collaboration with Mr. Huang.[†]¹⁸ In February 2019, the Australian government revoked Mr. Huang’s permanent residency and denied his application for citizenship, citing concerns about his character.¹⁹

Australia’s new Foreign Influence Transparency Scheme, passed in 2018 and based on the U.S. Foreign Agents Registration Act, was intended to introduce transparency into foreign lobbying in Canberra, but registration and enforcement have so far been lackluster. Canberra has yet to prosecute any United Front-connected entities, such as Confucius Institutes and most Chinese state media, for not registering, despite the fact United Front activities were a primary focus of the law.²⁰ As of July 2019, only 18 Chinese foreign principals had registered, mostly comprising mineral, energy, and investment companies, as well as China Radio International and China Telecom, state-owned media and telecommunications companies, respectively.[‡]²¹ Only three former Cabinet ministers or designat-

*For more on the events leading to the passage of Australia’s new counter-foreign interference laws, see U.S.-China Economic and Security Review Commission, Chapter 3, Section 2, “China’s Relations with U.S. Allies and Partners,” in *2018 Annual Report to Congress*, November 2018, 304–339.

†Unless noted otherwise, this section uses the following exchange rate throughout: AUD 1 = \$0.68.

‡The United States Studies Center at the University of Sydney, which has an arrangement with the U.S. Department of State for “general political lobbying,” has registered. Australian Government Attorney-General’s Department, *United States Studies Center Foreign Influence Transparency Scheme Register Registration Record*, September 28, 2018.

ed position holders—a key type of lobbyist intended to be captured by the law—had registered as lobbyists for Chinese foreign principals by July 2019.^{*22} Notably, some of the most prominent former officials who became lobbyists for Beijing after their government service, such as former Minister of Trade and Investment Andrew Robb, former Foreign Minister Bob Carr, and former Premier of Victoria State John Brumby, left their lobbying positions before the law took effect, demonstrating some desire not to be perceived as working for Beijing.²³

Australia Struggles with Disinformation and Censorship in Chinese-Language Media

Disinformation is a serious concern for Australian media, particularly given the outsize influence of Chinese platforms, which are an important tool in Beijing's influence operations targeting the Chinese diaspora.²⁴ There are dozens of Chinese-language media outlets in Australia, and nearly all of them have been brought under the influence of Beijing to some degree. Over roughly the last ten years, the Chinese embassy and consulates in Australia have used coercion and threats to get these media to increasingly parrot the CCP's line.²⁵ For example, the Chinese consulate in Sydney repeatedly warned a local government† with a large ethnic Chinese population not to engage with one of the few remaining independent Australian Chinese-language media outlets, *Vision China Times*, including forcing its council to ban the paper from sponsoring a Lunar New Year celebration.²⁶ Beijing has long sought to pressure or coerce this newspaper into changing its coverage. *Vision China Times* general manager Maree Ma said in April 2019 that Chinese officials "don't like any media outlets that they cannot ... control."²⁷

Most Australian Mandarin-speakers access news through WeChat, a social media app now indispensable among many Chinese communities for communication and other purposes, raising concerns about Beijing's ability to target them with disinformation spread over the platform.‡²⁸ The use of the platform has spread beyond the Chinese Australian community, with about 3 million Australians using WeChat by 2017, according to Australia's Special Broadcast

* Designated position holders include Ministers, Members of Parliament, some Parliamentary staff, Agency heads and deputy heads (and equivalent offices), and Ambassadors or High Commissioners stationed outside Australia. As of July 2019, designated position holders registered under the Scheme included former Australian Senator Richard Allston, working on behalf of China Telecom (Australia); former Senator Nick Bolkus, working on behalf of Jiujiang Mining Australia; and former Ambassador to China Geoffrey Raby, working on behalf of Yancoal. Australian Government Attorney-General's Department, *Transparency Register: China*; U.S.-China Economic and Security Review Commission, *2018 Annual Report to Congress*, November 2018, 325.

† A local government is the third tier of government in Australia, below the state or territory level and the federal level. Its governing body is referred to as a council. Nick McKenzie, "China Pressured Sydney Council into Banning Media Company Critical of Communist Party," *Four Corners*, April 9, 2019; *Australian Collaboration*, "Democracy in Australia—Australia's Political System," May 3, 2013, via the Internet Archive Wayback Machine. <https://web.archive.org/web/20140127041502/http://www.australiancollaboration.com.au/pdf/Democracy/Australias-political-system.pdf>.

‡ Based on WeChat penetration in mainland China, which reaches 93 percent in tier 1 cities, media researcher Wanning Sun estimated almost the entire Mandarin-speaking community in Australia—approximately 597,000 people as of 2016, or 2 percent of Australia's population—used WeChat. Wanning Sun, "How Australia's Mandarin Speakers Get Their News," *Conversation*, November 22, 2018; Lucy Lv, "Who Are the Australians That Are Using China's WeChat?" *Special Broadcasting System*, November 3, 2017; Australia's Bureau of Statistics, *Census Reveals a Fast Changing, Culturally Diverse Nation*, June 27, 2017; Wanning Sun, "Chinese-Language Media in Australia: Developments, Challenges, and Opportunities," *Australia-China Relations Institute*, 2016, 45–46.

Federal Register

Vol. 84, No. 96

Friday, May 17, 2019

Presidential Documents

Title 3—

Executive Order 13873 of May 15, 2019

The President

Securing the Information and Communications Technology and Services Supply Chain

By the authority vested in me as President by the Constitution and the laws of the United States of America, including the International Emergency Economic Powers Act (50 U.S.C. 1701 *et seq.*) (IEEPA), the National Emergencies Act (50 U.S.C. 1601 *et seq.*), and section 301 of title 3, United States Code,

I, DONALD J. TRUMP, President of the United States of America, find that foreign adversaries are increasingly creating and exploiting vulnerabilities in information and communications technology and services, 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. I further find that the unrestricted acquisition or use in the United States of information and communications technology or services 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 information and communications technology or services, with potentially catastrophic effects, and thereby constitutes an unusual and extraordinary threat to the national security, foreign policy, and economy of the United States. This threat exists both in the case of individual acquisitions or uses of such technology or services, and when acquisitions or uses of such technologies are considered as a class. Although maintaining an open investment climate in information and communications technology, and in the United States economy more generally, is important for the overall growth and prosperity of the United States, such openness must be balanced by the need to protect our country against critical national security threats. To deal with this threat, additional steps are required to protect the security, integrity, and reliability of information and communications technology and services provided and used in the United States. In light of these findings, I hereby declare a national emergency with respect to this threat.

Accordingly, it is hereby ordered as follows:

Section 1. Implementation. (a) The following actions are prohibited: any acquisition, importation, transfer, installation, dealing in, or use of any information and communications technology or service (transaction) by any person, or with respect to any property, subject to the jurisdiction of the United States, where the transaction involves any property in which any foreign country or a national thereof has any interest (including through an interest in a contract for the provision of the technology or service), where the transaction was initiated, is pending, or will be completed after the date of this order, and where the Secretary of Commerce (Secretary), in consultation with the Secretary of the Treasury, the Secretary of State, the Secretary of Defense, the Attorney General, the Secretary of Homeland Security, the United States Trade Representative, the Director of National Intelligence, the Administrator of General Services, the Chairman of the Federal Communications Commission, and, as appropriate, the heads of other executive departments and agencies (agencies), has determined that:

(i) the transaction involves information and communications technology or services designed, developed, manufactured, or supplied, by persons owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary; and

(ii) the transaction:

(A) poses an undue risk of sabotage to or subversion of the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of information and communications technology or services in the United States;

(B) poses an undue risk of catastrophic effects on the security or resiliency of United States critical infrastructure or the digital economy of the United States; or

(C) otherwise poses an unacceptable risk to the national security of the United States or the security and safety of United States persons.

(b) The Secretary, in consultation with the heads of other agencies as appropriate, may at the Secretary's discretion design or negotiate measures to mitigate concerns identified under section 1(a) of this order. Such measures may serve as a precondition to the approval of a transaction or of a class of transactions that would otherwise be prohibited pursuant to this order.

(c) The prohibitions in subsection (a) of this section apply except to the extent provided by statutes, or in regulations, orders, directives, or licenses that may be issued pursuant to this order, and notwithstanding any contract entered into or any license or permit granted prior to the effective date of this order.

Sec. 2. Authorities. (a) The Secretary, in consultation with, or upon referral of a particular transaction from, the heads of other agencies as appropriate, is hereby authorized to take such actions, including directing the timing and manner of the cessation of transactions prohibited pursuant to section 1 of this order, adopting appropriate rules and regulations, and employing all other powers granted to the President by IEEPA, as may be necessary to implement this order. All agencies of the United States Government are directed to take all appropriate measures within their authority to carry out the provisions of this order.

(b) Rules and regulations issued pursuant to this order may, among other things, determine that particular countries or persons are foreign adversaries for the purposes of this order; identify persons owned by, controlled by, or subject to the jurisdiction or direction of foreign adversaries for the purposes of this order; identify particular technologies or countries with respect to which transactions involving information and communications technology or services warrant particular scrutiny under the provisions of this order; establish procedures to license transactions otherwise prohibited pursuant to this order; establish criteria, consistent with section 1 of this order, by which particular technologies or particular participants in the market for information and communications technology or services may be recognized as categorically included in or as categorically excluded from the prohibitions established by this order; and identify a mechanism and relevant factors for the negotiation of agreements to mitigate concerns raised in connection with subsection 1(a) of this order. Within 150 days of the date of this order, the Secretary, in consultation with the Secretary of the Treasury, Secretary of State, the Secretary of Defense, the Attorney General, the Secretary of Homeland Security, the United States Trade Representative, the Director of National Intelligence, the Administrator of General Services, the Chairman of the Federal Communications Commission and, as appropriate, the heads of other agencies, shall publish rules or regulations implementing the authorities delegated to the Secretary by this order.

(c) The Secretary may, consistent with applicable law, redelegate any of the authorities conferred on the Secretary pursuant to this section within the Department of Commerce.

Sec. 3. Definitions. For purposes of this order:

(a) the term “entity” means a partnership, association, trust, joint venture, corporation, group, subgroup, or other organization;

(b) the term “foreign adversary” means any foreign government or foreign non-government person engaged in a long-term pattern or serious instances of conduct significantly adverse to the national security of the United States or security and safety of United States persons;

(c) the term “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;

(d) the term “person” means an individual or entity; and

(e) the term “United States person” means any United States citizen, permanent resident alien, entity organized under the laws of the United States or any jurisdiction within the United States (including foreign branches), or any person in the United States.

Sec. 4. Recurring and Final Reports to the Congress. The Secretary, in consultation with the Secretary of State, is hereby authorized to submit recurring and final reports to the Congress on the national emergency declared in this order, consistent with section 401(c) of the NEA (50 U.S.C. 1641(c)) and section 204(c) of IEEPA (50 U.S.C. 1703(c)).

Sec. 5. Assessments and Reports. (a) The Director of National Intelligence shall continue to assess threats to the United States and its people from information and communications technology or services designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary. The Director of National Intelligence shall produce periodic written assessments of these threats in consultation with the heads of relevant agencies, and shall provide these assessments to the President, the Secretary for the Secretary’s use in connection with his responsibilities pursuant to this order, and the heads of other agencies as appropriate. An initial assessment shall be completed within 40 days of the date of this order, and further assessments shall be completed at least annually, and shall include analysis of:

(i) threats enabled by information and communications technologies or services designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction or direction of a foreign adversary; and

(ii) threats to the United States Government, United States critical infrastructure, and United States entities from information and communications technologies or services designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the influence of a foreign adversary.

(b) The Secretary of Homeland Security shall continue to assess and identify entities, hardware, software, and services that present vulnerabilities in the United States and that pose the greatest potential consequences to the national security of the United States. The Secretary of Homeland Security, in coordination with sector-specific agencies and coordinating councils as appropriate, shall produce a written assessment within 80 days of the date of this order, and annually thereafter. This assessment shall include an evaluation of hardware, software, or services that are relied upon by multiple information and communications technology or service providers, including the communication services relied upon by critical infrastructure entities identified pursuant to section 9 of Executive Order 13636 of February 12, 2013 (Improving Critical Infrastructure Cybersecurity).

(c) Within 1 year of the date of this order, and annually thereafter, the Secretary, in consultation as appropriate with the Secretary of the Treasury, the Secretary of Homeland Security, Secretary of State, the Secretary of Defense, the Attorney General, the United States Trade Representative, the

Director of National Intelligence, and the Chairman of the Federal Communications Commission, shall assess and report to the President whether the actions taken by the Secretary pursuant to this order are sufficient and continue to be necessary to mitigate the risks identified in, and pursuant to, this order.

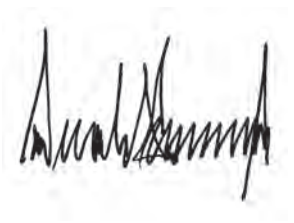
Sec. 6. General Provisions. (a) Nothing in this order shall be construed to impair or otherwise affect:

(i) the authority granted by law to an executive department or agency, or the head thereof; or

(ii) the functions of the Director of the Office of Management and Budget relating to budgetary, administrative, or legislative proposals.

(b) This order shall be implemented consistent with applicable law and subject to the availability of appropriations.

(c) This order is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.



THE WHITE HOUSE,
May 15, 2019.

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.

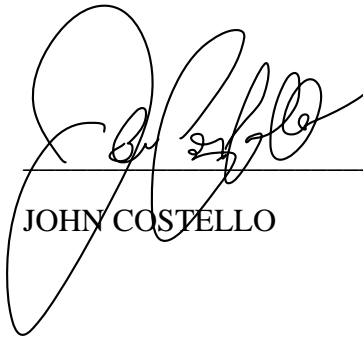
6. The Secretary made his final decision about which transactions related to WeChat/Tencent should be prohibited on Thursday, September 17, 2020. The prohibitions were publicly announced on Friday, September 18, 2020, and were published for inspection at the Government printing Office website later that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

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

1 MICHAEL W. BIEN – Cal. Bar No. 096891
VAN SWEARINGEN – Cal. Bar No. 259809
2 ALEXANDER GOURSE – Cal. Bar No. 321631
AMY XU – Cal. Bar No. 330707
3 ROSEN BIEN GALVAN & GRUNFELD LLP
101 Mission Street, Sixth Floor
4 San Francisco, California 94105-1738
Telephone: (415) 433-6830
5 Facsimile: (415) 433-7104
Email: mbien@rbgg.com
6 vswearingen@rbgg.com
agourse@rbgg.com
7 axu@rbgg.com

8 KELIANG (CLAY) ZHU – Cal. Bar No. 305509
DEHENG LAW OFFICES PC
9 7901 Stoneridge Drive #208
Pleasanton, California 94588
10 Telephone: (925) 399-5856
Facsimile: (925) 397-1976
11 Email: czhu@dehengsv.com

12 ANGUS F. NI – Wash. Bar No. 53828*
AFN LAW PLLC
13 502 Second Avenue, Suite 1400
Seattle, Washington 98104
14 Telephone: (773) 543-3223
Email: angus@afnlegal.com
15 * *Pro Hac Vice* application forthcoming

16 Attorneys for Plaintiffs

17
18 UNITED STATES DISTRICT COURT

19 NORTHERN DISTRICT OF CALIFORNIA, SAN FRANCISCO DIVISION

20 U.S. WECHAT USERS ALLIANCE,
CHIHUO INC., BRENT COULTER,
21 FANGYI DUAN, JINNENG BAO,
ELAINE PENG, and XIAO ZHANG,

22 Plaintiffs,

23 v.

24 DONALD J. TRUMP, in his official
capacity as President of the United States,
25 and WILBUR ROSS, in his official
capacity as Secretary of Commerce,

26 Defendants.
27
28

Case No. 3:20-cv-05910

**AMENDED COMPLAINT FOR
DECLARATORY AND INJUNCTIVE
RELIEF**

INTRODUCTION

1. Public space in the digital age is defined by platforms and users rather than physical places with geographic boundaries. Cyberspace, particularly social media, is one of “the most important places” to exchange views. *Packingham v. North Carolina*, 582 U.S. —, 137 S. Ct. 1730, 1735 (2017). Few digital public squares are as large as that found on WeChat. Released in 2011, WeChat is now one of the world’s most popular mobile telephone applications (“app”), with over 1 billion monthly active users.¹

2. Approximately 19 million users rely on the app in the United States, and it is the primary app Chinese-speakers in the U.S. use to participate in social life by connecting with loved ones, sharing special moments, arguing ideas, receiving up-to-the minute news, and participating in political discussions and advocacy.² As a “super-app,” WeChat users also rely on the app to make telephone calls, hold video conferences, upload documents, share photos, and make payments.³ It has become essential to the conduct of daily life for its users, many of whom regularly spend hours each day on the app.

3. WeChat is also used for numerous societally important purposes, including by public institutions. For example, as the coronavirus pandemic continues to separate people physically, WeChat has been used in the United States by police departments to inform the public about testing center locations, by volunteers to organize the delivery of medical supplies, and by families to stay in touch with isolated elderly relatives in nursing

¹ Rayna Hollander, *WeChat has hit 1 billion monthly active users*, BUSINESS INSIDER (Mar. 6, 2018, 11:59 a.m.), <https://www.businessinsider.com/wechat-has-hit-1-billion-monthly-active-users-2018-3>; Iris Deng and Celia Chen, *How WeChat became China’s everyday mobile app*, SOUTH CHINA MORNING POST (Aug. 16, 2018), <https://www.scmp.com/tech/article/2159831/how-wechat-became-chinas-everyday-mobile-app>.

² Rick Smith, *Crackdown on WeChat could hinder millions of US users who rely on social media tool*, WRAL TECHWIRE (Aug. 19, 2020), <https://www.wraltechwire.com/2020/08/19/crackdown-on-wechat-could-hinder-millions-of-us-users-who-rely-on-social-media-tool/>.

³ Bani Sapra, *This Chinese super-app is Apple’s biggest threat in China and could be a blueprint for Facebook’s future. Here’s what it’s like to use WeChat, which helps a billion users order food and hail rides*, BUSINESS INSIDER (Dec. 21, 2019), <https://www.businessinsider.com/chinese-superapp-wechat-best-feature-walkthrough-2019-12>.

homes. WeChat is also used by individuals and groups—including churches—for religious and cultural purposes: group prayer, organizing for holidays and events, taking care of the poor, sick and infirm, and education.

4. In the United States and across the world, national governments engage in dragnet surveillance of digital communications of ordinary people. Because governmental surveillance is all-pervasive and occurs at the network level, communications over WeChat, like communications on all other apps that run on our systematically surveilled internet infrastructure, are captured by this dragnet.

5. Despite widespread knowledge of these practices, hundreds of millions of people in this country voluntarily use surveilled devices and apps to participate in all facets of social and economic life every day. This is the case for WeChat users in the United States, where it is widespread knowledge amongst users that both the United States and Chinese governments monitor WeChat communications.⁴ WeChat users in the United States continue to use and rely on the app, knowing that Big Brother is watching.

6. On August 6, 2020, the President issued Executive Order 13943 entitled “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,” 85 FR 48641 (“the Executive Order”). Citing national security concerns, the Executive Order bans what appears to be all uses of WeChat by anyone within the United States as well as “U.S. persons” outside the United States. Section 1(a) of the Executive Order prohibits people and property subject to U.S. jurisdiction from carrying out “transactions” with WeChat after 45 days of the Executive Order’s issuance. Section 2(a) prohibits any transaction “by a United States person or

⁴ See Arjun Kharpal, *Chinese tech giant Tencent reportedly surveilled foreign users of WeChat to help censorship at home*, CNBC (May 8, 2020), <https://www.cnbc.com/2020/05/08/tencent-wechat-surveillance-help-censorship-in-china.html>; Tim Lau, *The Government Is Expanding Its Social Media Surveillance Capabilities*, BRENNAN CENTER FOR JUSTICE (May 22, 2019), <https://www.brennancenter.org/our-work/analysis-opinion/government-expanding-its-social-media-surveillance-capabilities>.

1 within the United States” that evades, avoids, or violates the uncertain prohibition in
 2 Section 1(a). Maddeningly, the Executive Order does not define what those transactions
 3 include, leaving individuals and companies at a loss as to whether they will risk civil
 4 and/or criminal prosecution and penalties if they do not fundamentally change the way
 5 they communicate or run their businesses. The vaguely worded Executive Order was
 6 issued without further explanation or a media briefing, and states that the Secretary of
 7 Commerce shall identify what transactions are prohibited after 45 days—in effect,
 8 delaying identification of what transactions are prohibited until after such transactions are
 9 already prohibited.⁵

10 7. Neither the Executive Order itself nor the White House provided concrete
 11 evidence to support the contention that using WeChat in the United States compromises
 12 national security. Notably, no other nation has implemented a comprehensive WeChat ban
 13 on the basis of any like-finding that WeChat is a threat to national security.⁶ The
 14 Executive Order was, however, issued in the midst of the 2020 election cycle, during a
 15 time when President Trump has made numerous anti-Chinese statements that have
 16 contributed to and incited racial animus against persons of Chinese descent⁷—all outside
 17 of the national security context.

18 8. In a stark violation of the First Amendment, the Executive Order targets and
 19

20 ⁵ Ana Swanson, *Trump’s Orders on WeChat and TikTok Are Uncertain. That May Be the*
 21 *Point.*, N.Y. TIMES (Aug. 7, 2020),
<https://www.nytimes.com/2020/08/07/business/economy/trump-executive-order-tiktok-wechat.html>.

22 ⁶ See Maria Abi-Habib, *India Bans Nearly 60 Chinese Apps, Including TikTok and*
 23 *WeChat*, N.Y. TIMES (June 29, 2020, updated on June 30, 2020),
<https://www.nytimes.com/2020/06/29/world/asia/tik-tok-banned-india-china.html> (stating
 24 that India’s ban is “part of the tit-for-tat retaliation after the Indian and Chinese militaries
 clashed earlier this month.”).

25 ⁷ See, e.g., Nadia Kim, *Asian Americans Suffer From Trump’s Racist Attacks Too*, PUBLIC
 26 SEMINAR (July 23, 2020), <https://publicseminar.org/essays/asian-americans-suffer-from-trumps-racist-attacks-too/>; Li Zhou, *Trump’s racist references to the coronavirus are his*
 27 *latest effort to stoke xenophobia*, VOX (June 23, 2020),
<https://www.vox.com/2020/6/23/21300332/trump-coronavirus-racism-asian-americans>;
 28 Matt Stevens, *How Asian-American Leaders Are Grappling With Xenophobia Amid*
Coronavirus, N.Y. TIMES (Mar. 29, 2020, updated on April 10, 2020),
<https://www.nytimes.com/2020/03/29/us/politics/coronavirus-asian-americans.html>.

1 silences WeChat users, the overwhelming majority of whom are members of the Chinese
 2 and Chinese-speaking communities. It regulates constitutionally protected speech,
 3 expression, and association and is not narrowly tailored to restrict only that speech which
 4 presents national security risks to the United States. Accordingly, it is unconstitutionally
 5 overbroad. Indeed, banning the use of WeChat in the United States has the effect of
 6 foreclosing all meaningful access to social media for members of the Chinese-speaking
 7 community, such as Plaintiffs, who rely on it to communicate and interact with others like
 8 themselves. The ban on WeChat, because it substantially burdens the free exercise of
 9 religion, also violates the Religious Freedom Restoration Act.

10 9. The Executive Order runs afoul of the Fifth Amendment’s Due Process
 11 Clause by failing to provide notice of the specific conduct that is prohibited; because of
 12 this uncertainty, WeChat users in the United States are justifiably fearful of using WeChat
 13 in any way and for any purpose—and also of losing access to WeChat. Since the
 14 Executive Order, numerous users, including Plaintiffs, have scrambled to seek alternatives
 15 without success. They are now afraid that by merely communicating with their families,
 16 they may violate the law and face sanctions.

17 10. WeChat is the only “super-app” with a natively Chinese interface designed
 18 for Chinese speakers. That is why it is the dominant social media and e-commerce
 19 application amongst the global Chinese diaspora, which include Chinese communities in
 20 the United States.⁸ These individuals, particularly those who do not speak English, are
 21 ***completely reliant*** on WeChat to communicate, socialize, and express themselves. As
 22 such, by prohibiting the use of only WeChat but not any similar applications (ones not
 23 made in China and without Chinese interfaces), the Executive Order singles out people of
 24 Chinese and Chinese-American ancestry and subjects them to disparate treatment on the
 25 basis of race, ethnicity, nationality, national origin, and alienage. In doing so, the
 26

27 ⁸ Thuy Ong, *Chinese social media platform WeChat reaches 1 billion accounts worldwide*,
 28 THE VERGE (Mar. 5, 2018), <https://www.theverge.com/2018/3/5/17080546/wechat-chinese-social-media-billion-users-china>.

Executive Order violates the Equal Protection Clause.

11. Finally, in issuing the Executive Order, the president acted beyond his authority provided by the International Emergency Economic Powers Act, which precludes the President from “*directly or indirectly*” regulating personal communications and the international exchange of information.

12. The U.S. WeChat Users Alliance (“USWUA”), Chihuo, Inc., Brent Coulter, Fangyi Duan, Jinneng Bao, Elaine Peng, and Xiao Zhang (collectively, “Plaintiffs”), bring this suit to challenge the Executive Order, which eviscerates an irreplaceable cultural bridge that connects Plaintiffs to family members, friends, business partners, customers, religious community members, and other individuals with common interests within the Chinese diaspora, located both in and outside of the United States. The Executive Order has already harmed Plaintiffs, who are plagued with fear for the loss of their beloved connections, whether it be with friends, family, community, customers, aid recipients of the charities they run, or even strangers whose ideas enrich their lives. They have been forced to divert time, energy, and money to seek alternative communication platforms, download and save irreplaceable digital histories, plan for business closures, find other sources of information, and try to obtain alternative contact information for those from whom they will soon be separated. Even if they succeed to some extent in their mitigation efforts, Plaintiffs will never be able to replace the full spectrum of the social interactivity that WeChat offers, nor will they be able to find any social networking platform with anything close to the same level of participation by the global Chinese diaspora—this is because WeChat’s network effects, generated by its 1 billion-plus daily users, is irreplaceable.

13. In short, the threatened displacement of these WeChat users from their public space is an irreparable harm that requires judicial intervention.

14. For these reasons, and those discussed below, the Court should (1) declare that the Executive Order and the Secretary of Commerce’s September 18, 2020, *Identification of Prohibited Transactions* are unlawful and unconstitutional; and (2) enjoin

1 Defendants from enforcing the Executive Order or the Secretary's *Identification* to prohibit
2 the use of WeChat in the United States, directly or indirectly.

3 JURISDICTION AND VENUE

4 15. The claims asserted herein arise under and pursuant to the Constitution and
5 laws of the United States. This Court has jurisdiction over the subject matter of this action
6 pursuant to 28 U.S.C. § 1331.

7 16. An actual, present, and justiciable controversy exists between the parties
8 within the meaning of 28 U.S.C. § 2201(a).

9 17. Plaintiffs' claims for declaratory and injunctive relief are authorized by 28
10 U.S.C. §§ 2201 and 2202, by Rules 57 and 65 of the Federal Rules of Civil Procedure, and
11 by the general legal and equitable powers of this Court.

12 18. Venue is proper in this District pursuant to 28 U.S.C. §§ 2201 and 1391
13 (e)(1) because Defendant are officers of the United States acting in their official capacities
14 and (1) at least one plaintiff resides in this district; and (2) a substantial part of the events
15 or omissions giving rise to the claim occurred in this district. For the same reason,
16 intradistrict assignment is proper in the San Francisco Division. *See* N.D. Cal. L.R. 3-2.

17 PARTIES

18 19. Plaintiff U.S. WeChat Users Alliance ("USWUA") is a New Jersey nonprofit
19 organization that is in the process of being registered under Internal Revenue Code section
20 501(c)(3), established by individuals in the United States for the purpose of opposing the
21 Executive Order. Plaintiff USWUA is made up of WeChat users located throughout the
22 United States who are not affiliated with WeChat, its parent company Tencent Holdings
23 Ltd. ("Tencent"), nor any political party or foreign government. Plaintiff USWUA runs on
24 public donations from WeChat users and organizes its efforts on WeChat. Plaintiff
25 USWUA is made up of individuals who want to continue using WeChat within the United
26 States and are currently suffering and will continue to suffer an injury based on the
27 Defendants' actions.

28 20. Plaintiff Elaine Peng is a United States citizen residing in Castro Valley,

1 California. Plaintiff Peng founded the Mental Health Association for Chinese
2 Communities (“MHACC”) in 2013 to provide mental health education, suicide prevention,
3 assistance, and other resources to her local Chinese community that is underserved by the
4 mental health profession due to language and cultural barriers. As president of MHACC,
5 Plaintiff Peng strives to make mental health programs available to those in need and has
6 received multiple awards for her work. Like much of the Chinese population in the United
7 States, Plaintiff Peng uses WeChat as her exclusive means to connect with her Chinese
8 families and friends, domestic or abroad. As most of the population MHACC serves relies
9 on WeChat to communicate, use of WeChat is also integral to MHACC’s mission to
10 provide mental health services and support to its members.

11 21. Plaintiff Brent Coulter is a United States citizen and WeChat user. Plaintiff
12 Coulter holds a Juris Doctor from the University of California, Hastings College of the
13 Law (“Hastings”), and lives in San Francisco, California. Plaintiff Coulter previously
14 lived in China for approximately five years, where he studied at Sichuan University and
15 worked in marketing. While in China, Plaintiff Coulter used WeChat as his main method
16 of communication to connect with friends and professional contacts. Now in the U.S., one
17 of Plaintiff Coulter’s professional goals is to bridge the gap between China and the U.S.
18 with regard to law and business. At Hastings, Plaintiff Coulter founded the Asian Law and
19 Business Association, through which he formed a partnership with the American Chamber
20 of Commerce (“AmCham”) in Southwest China. Each year, Plaintiff Coulter drafts two
21 chapters of AmCham’s annual white paper on U.S. business in China with his colleagues
22 in both countries. WeChat is central to Plaintiff Coulter’s annual collaboration and
23 remains the only way for him to connect with many of his professional contacts and
24 friends in China. Plaintiff Coulter relies on WeChat to build upon his professional career
25 which straddles law and business in the U.S. and China. Without WeChat, Plaintiff
26 Coulter would lose access to many of the relationships that he has built throughout his
27 studies and career.

28 22. Plaintiff Xiao Zhang is a Chinese citizen with a valid visa residing in

1 Houston, Texas. She is employed as an engineer and founded a nonprofit organization
2 known as Hita Education Foundation that supports underserved students at the high school
3 in her hometown in China. Plaintiff Zhang uses WeChat to speak with administrators,
4 teachers, parents of school children, and to help identify underserved Chinese students who
5 would benefit from the program. Plaintiff Zhang's nonprofit organization currently sends
6 donations of 300 yuan (approximately \$43 dollars) to seven students per month to pay for
7 meals and school supplies. Plaintiff Zhang also uses WeChat to transfer the funds to each
8 individual student, and WeChat is her exclusive means to connect with her Chinese-
9 speaking family members and friends, domestic or abroad.

10 23. Plaintiff Fangyi "Amy" Duan is a Chinese citizen with a valid visa, and
11 resides in Santa Clara, California. Plaintiff Duan is employed as the chief executive
12 officer of Plaintiff Chihuo, Inc. ("Chihuo"), a corporation that is dually registered in both
13 California and Delaware.

14 24. Plaintiff Chihuo is a media and online retailer that creates content regarding
15 Chinese restaurants and cuisine for people residing in the United States. Plaintiff Chihuo
16 provides U.S. based merchants an e-commerce platform for targeting Chinese-speaking
17 consumers. Plaintiff Chihuo serves its customers by providing targeted marketing and
18 advertising services online. Plaintiff Chihuo delivers its targeted advertising and
19 marketing services primarily on several WeChat official accounts through its various
20 functions, including WeChat Moments. Plaintiff Chihuo employs or contracts with
21 approximately thirty people as part of its business. Plaintiff Chihuo's WeChat accounts
22 cover 14 major metropolitan areas in the United States and are enjoyed by more than
23 640,000 readers.

24 25. Plaintiff Jinneng Bao is a United States permanent resident and lives in
25 Nassau County, New York. He is self-employed and runs several businesses including a
26 construction company primarily serving Chinese-speaking clients in New York. Plaintiff
27 Bao actively attends a Chinese church in New York and participates in Bible studies
28 regularly on WeChat. His Bible study group consists of mostly Chinese-speaking

members. Due to the pandemic, Plaintiff Bao’s Bible study group has stopped meeting in person, and WeChat is the only way the group currently maintains communications with one another.

26. Defendant Donald J. Trump (“President Trump”) is the President of the United States. He is sued in his official capacity. In that capacity, he issued the Executive Order challenged in this suit.

27. Defendant Wilbur Ross (“Secretary Ross”) is the United States Secretary of Commerce. He is sued in his official capacity. In the Executive Order, the Secretary is authorized to take actions, including adopting rules and regulations, to implement the Executive Order.

FACTUAL ALLEGATIONS

A. WeChat and App Capabilities

28. WeChat is one of the most popular messaging applications in the world, with a monthly user base of more than 1 billion people.⁹ Nearly every person in China with an online presence has at least one WeChat account, and over one-third of them spend four hours or more on the app every day—making WeChat an indispensable part of many peoples’ lives and work.¹⁰

29. Though WeChat began as a messaging service, it is now a “super-app” that serves a multitude of communicative needs, including making telephone calls, video conferencing, sharing photos, commenting on other users’ posts, making payments, and still other purposes.¹¹

⁹ Arjun Kharpal, Everything you need to know about WeChat—China’s billion-user messaging app, CNBC (Feb. 3, 2019), <https://www.cnbc.com/2019/02/04/what-is-wechat-china-biggest-messaging-app.html>.

¹⁰ Li Yuan, To Cover China, There’s No Substitute for WeChat, N.Y. TIMES (Jan. 9, 2019), <https://www.nytimes.com/2019/01/09/technology/personaltech/china-wechat.html>

¹¹ Bani Sapra, *This Chinese super-app is Apple’s biggest threat in China and could be a blueprint for Facebook’s future. Here’s what it’s like to use WeChat, which helps a billion users order food and hail rides*, BUSINESS INSIDER (Dec. 21, 2019), <https://www.businessinsider.com/chinese-superapp-wechat-best-feature-walkthrough-2019-12>.

30. One of WeChat's primary uses is the app's messaging capabilities, which include both text and voice messaging. Messaging through WeChat is the preferred method of communication in China, even when doing business. Through the app's messaging capabilities, users can have numerous ongoing conversations at one time, and can also set up group texts within a family, a business, or among friends, to communicate with the whole group simultaneously.

31. WeChat also has capabilities to make voice and video calls. WeChat users often choose to make voice calls within the app rather than through their cellular telephone provider because it is more convenient. Group voice conference calls and video chats—comparable to Zoom video group calls—can also be easily made on WeChat.

32. WeChat includes a feature called “Moments” through which users can upload photos, videos, share news articles, and compose text. WeChat users can comment or like the post, similar to the capabilities of apps like Facebook or Instagram.

33. WeChat also supports many integrated services, such as banking and ride-sharing, so that users do not need to use a separate app to get those services. Some companies have launched “mini-programs” within WeChat instead of standalone apps, making it more convenient for WeChat users to use their services.

34. WeChat has increasingly been adopted by older age groups in China, including a significant percentage of those over 60.¹² Even older users in their 70s use WeChat at high levels for messaging, voice calls, reading articles, and making payments.¹³

B. WeChat Usage Specifically in the United States

35. There are approximately 19 million daily active WeChat users in the United States.¹⁴ WeChat is very widely used within the Chinese-American community, which is

¹² Clark Boyd, *The Silver Lining: WeChat and China's Over-60s*, MEDIUM (Sept. 3, 2020), <https://medium.com/swlh/the-silver-lining-wechat-and-chinas-over-60s-168b193fb516>.

¹³ Mansoor Iqbal, *WeChat Revenue and Usage Statistics*, BUSINESS OF APPS (updated July 30, 2020), <https://www.businessofapps.com/data/wechat-statistics/>.

¹⁴ Krystal Hu, *WeChat U.S. ban cuts off users link to families in China*, REUTERS (Aug. 7, 2020), <https://www.reuters.com/article/us-usa-tencent-holdings-wechat-ban/wechat-us->

1 estimated to be four to five million people.¹⁵ WeChat is the dominant method for anyone
 2 in the United States who regularly communicates with people in China because it is free, is
 3 more convenient, and has better reception than traditional telephone calls. WeChat is used
 4 in the United States not only to keep in touch with friends and family, but also academics,
 5 professionals, and business people to discuss matters of professional importance. In the
 6 United States, the vast majority of the Chinese-speaking population is on WeChat, creating
 7 network-effects that encourage others to join and participate lest they be cut off entirely
 8 from family, friends, and business circles.¹⁶ Simply put, WeChat is irreplaceable because
 9 no other app has anywhere near the same number of users and engagement among the
 10 Chinese-speaking community in the United States.

11 36. WeChat users in the United States use the app to communicate within
 12 Chinese American communities in the United States and with Chinese speakers throughout
 13 the world. Without access to WeChat, users in the United States will be cut off from their
 14 cultural community in the U.S. and lose the main line of communication they have with
 15 the rest of their family thousands of miles away. Plaintiffs Peng, Zhang, Bao, and Fang all
 16 use WeChat while living in the United States to regularly communicate with their aging
 17 parents or other family members who reside in China.

18 37. The importance of WeChat to Chinese Americans cannot be overstated
 19 because a significant portion of these individuals speak little or no English. According to a
 20 study by the Pew Research Center, 41% of the Chinese population in the United States are
 21 not English proficient.¹⁷ Accordingly, a blanket prohibition on WeChat means that

22 _____
 23 [ban-cuts-off-users-link-to-families-in-china-
 idUSKCN253339#:~:text=In%20the%20past%20three%20months,according%20to%20an
 24 alytics%20firms%20Apptopia.](https://www.uskcn253339#:~:text=In%20the%20past%20three%20months,according%20to%20analytics%20firms%20Apptopia.)

25 ¹⁵ Gustavo Lopez, Neil G. Ruiz, and Eileen Patten, *Key facts about Asian Americans, a
 diverse and growing population*, PEW RESEARCH CENTER (Sept. 8, 2017),
<https://www.pewresearch.org/fact-tank/2017/09/08/key-facts-about-asian-americans/>.

26 ¹⁶ Mohit Mittal, *WeChat—The One App That Rules Them All*, HARVARD BUSINESS
 27 SCHOOL DIGITAL INITIATIVE (Aug. 25, 2017), [https://digital.hbs.edu/innovation-
 disruption/wechat%E2%80%8A-%E2%80%8Athe-one-app-rules/](https://digital.hbs.edu/innovation-disruption/wechat%E2%80%8A-%E2%80%8Athe-one-app-rules/).

28 ¹⁷ *English proficiency of Chinese population in the U.S.*, PEW RESEARCH CENTER (July 6,

millions of individuals in the United States will be unable to find a comparable substitute on apps such as Facebook, which are designed for English-speaking users and primarily have English-speaking user networks within the United States.

38. WeChat users in the United States use the app to engage in, organize, and publicize religious and cultural practices. For instance, various churches with primarily Chinese congregants have WeChat profiles and stream their services online.¹⁸ The Church of Jesus Christ of Latter-Day Saints uses WeChat to reach Chinese-American members and potential congregants within China.¹⁹ WeChat users in the United States attend and participate in religious services or events, such as funerals, weddings, or other gatherings through the app. Plaintiff Jinneng Bao relies on WeChat exclusively to attend regular Bible studies hosted by his Chinese church in New York. WeChat users in the United States organize and celebrate various religious and cultural holidays through their activity in WeChat groups. They post Moments about holidays such as the Chinese New Year, the Mid-Autumn Moon Festival, Ching Ming Festival (when Chinese people around the world visit the tombs of their departed loved ones), and the Duan Wu Festival (popularly known in the U.S. as the day when Chinese communities host dragon boat races). Because events, educational or celebratory, are frequently discussed and transmitted through social networks on WeChat, users rely on WeChat to learn about and celebrate religious and cultural events with their community members online.

2017), <https://www.pewsocialtrends.org/chart/english-proficiency-of-chinese-population-in-the-u-s/>.

¹⁸ Feng Long, *Leveraging Tech for Chinese Evangelism*, SIERRAPACIFIC (May 15, 2020), <https://www.undeniableblessing.org/blog/Leveraging-Tech-for-Chinese-Evangelism> (Oakland pastor who uses WeChat); MID-HUDSON CHINESE CHRISTIAN CHURCH (NY), <https://www.mhccc.org/> (last visited Aug. 20, 2020); BRENTWOOD BAPTIST CHURCH (TN), <https://brentwoodbaptist.com/chinese/> (last visited Aug. 20, 2020).

¹⁹ THE CHURCH OF JESUS CHRIST OF LATTER-DAY-SAINTS IN CHINA, <https://www.churchofjesuschrist.org/China> (last visited Aug. 20, 2020) (*see* Frequently Asked Questions by Church Leaders, Can Church leaders/members outside China keep in touch with Chinese members baptized in their brand/ward after those Chinese members return to China? Email? WeChat? Letters?); James Griffiths, *This US Church with Expansion in its DNA Wants to Open a Temple in China*, CNN (Hong Kong) (Jun. 11, 2020, <https://www.cnn.com/2020/06/06/asia/mormon-church-latter-day-saints-china-intl-hnk/index.html>).

39. In the United States, WeChat users organize around political causes through WeChat. For instance, many WeChat groups were used to organize, campaign, and raise funds in the 2016 presidential election, and users in the United States have similarly used WeChat to support candidates in the 2020 presidential election cycle.²⁰ Plaintiff Peng is an active member of several WeChat groups that discuss issues pertaining to the U.S. 2020 election and publish information on how to become a registered voter. Asian-Americans who organized to oppose a Democrat-backed ballot initiative in California, which would have reversed the state's ban on race-conscious admissions, did so primarily through WeChat.²¹ Organizations and causes wanting to reach Chinese-Americans use WeChat groups to raise awareness about demonstrations, spread voter education materials, and campaign for various candidates.

40. WeChat is integral for the spread of current events and news within Chinese communities. WeChat users use the app to read about current events and the news, including media from the United States, China, and around the world. Plaintiffs Zhang and Peng frequently use WeChat to read, share, and respond to news items that their WeChat contacts post to their Moments. Plaintiffs then comment, like, and share various news items that they receive from their WeChat contacts. Journalists who cover issues pertaining to China and Chinese communities rely on WeChat to investigate issues and communicate with people to interview. Large Chinese-language newspapers in the U.S., such as *Sing Tao Daily* and *World Journal*, publish news stories through their WeChat accounts.

41. Government entities in areas with significant numbers of Chinese immigrants or Chinese Americans use WeChat as a method of communicating with their

²⁰ See Wanning Sun, *Why Trump's WeChat ban does not make sense—and could actually cost him Chinese votes*, THE CONVERSATION (Aug. 10, 2020), <https://theconversation.com/why-trumps-wechat-ban-does-not-make-sense-and-could-actually-cost-him-chinese-votes-144207>.

²¹ Alia Wong, *The App at the Heart of the Movement to End Affirmative Action*, THE ATLANTIC (Nov. 20, 2018), <https://www.theatlantic.com/education/archive/2018/11/asian-americans-wechat-war-affirmative-action/576328/>.

1 constituents. For instance, the police department in Alhambra, California began using
 2 WeChat in 2015 to provide updates about local law enforcement efforts.²² The cities of
 3 Arcadia, San Gabriel, and Monterey Park in California have official WeChat accounts,
 4 which allow them to communicate with Chinese-speaking populations in their own
 5 language.²³ Local governments have used WeChat messaging as a way to send emergency
 6 notifications and provide public notice for local governance proposals.

7 42. During the COVID-19 pandemic, WeChat users have relied even more on
 8 the app to communicate and organize within their communities. In February 2020,
 9 volunteers in the Bay Area used WeChat to organize and send medical supplies to Wuhan,
 10 China at the start of the worldwide pandemic.²⁴ As travel restrictions emerged in the
 11 United States, WeChat users relied on the app in order to communicate with family
 12 members that they cannot visit in person in their home towns, in other areas of the United
 13 States, and around the world. People in the United States use the app to visit with elderly
 14 loved ones in nursing homes and hospitals, as well as with COVID-19 patients, who
 15 cannot be visited in person due to pandemic-related restrictions. Information about the
 16 pandemic, including regarding COVID-19 testing, prevention methods, and government
 17 responses to the pandemic, are broadly shared and discussed in the United States through
 18

19 ²² Ashley Fan, *Some San Gabriel Valley Communities Could Be Seriously Affected by*
 20 *Trump's WeChat Ban*, SAN GABRIEL VALLEY TRIB. (Aug. 10, 2020),
 21 <https://www.sgvtribune.com/2020/08/10/how-trumps-wechat-ban-could-disrupt-life-in-the-san-gabriel-valley/>; Josie Huang, *Alhambra Police Use WeChat as Bridge to Chinese*
 22 *Immigrants*, KPCC (Jan. 20, 2015),
 23 <https://www.scpr.org/blogs/multiamerican/2015/01/20/17819/alhambra-police-join-wechat-to-chinese/>.

24 ²³ Ashley Fan, *Some San Gabriel Valley Communities Could Be Seriously Affected by*
 25 *Trump's WeChat Ban*, SAN GABRIEL VALLEY TRIB. (Aug. 10, 2020),
 26 <https://www.sgvtribune.com/2020/08/10/how-trumps-wechat-ban-could-disrupt-life-in-the-san-gabriel-valley/>; Christopher Yee, *How this 32-year-old Interpreter Became*
 27 *Alhambra's Weibo, WeChat Guru*, SAN GABRIEL VALLEY TRIB. (Jul. 14, 2016, updated
 28 Aug. 30, 2017), <https://www.sgvtribune.com/2016/07/14/how-this-32-year-old-interpreter-became-alhambras-weibo-wechat-guru/>.

²⁴ Devin Katayama, Ericka Cruz Guevarra & Alan Montecillo, “‘That’s Where I Grew Up’: The Wuhan Natives Organizing Aid from the Bay, KQED (Feb. 19, 2020),
<https://www.kqed.org/news/11802206/thats-where-i-grew-up-the-wuhan-natives-organizing-aid-from-the-bay>.

WeChat groups and posts. For instance, a local police department in California posted information about times and locations for drive-up and walk-up COVID-19 testing on its WeChat profile. Similarly, doctors used WeChat extensively to spread information on the prevention of COVID-19 in the Chinese communities in Sacramento, California.²⁵ Organizations, such as Plaintiff Peng’s MHACC, make vital mental health programs available to their communities through WeChat, in a world where people are struggling with the long-term isolation associated with the pandemic.

PRESIDENT TRUMP’S EXECUTIVE ORDERS AND EMERGENCY DECLARATION

A. Executive Order 13873

43. Prior to the issuance of the Executive Order challenged by this lawsuit, on May 15, 2019, President Trump issued Executive Order 13873, titled “Securing the Information and Communications Technology Services Supply Chain.” 84 FR 22689 (May 15, 2019). Executive Order 13873 declares a national emergency with respect to the threat posed by unidentified “vulnerabilities in information and communications technology and services[.]”

44. According to this Order, these unidentified vulnerabilities constitute an “unusual and extraordinary threat to the national security, foreign policy, and economy of the United States,” due in part to the “unrestricted acquisition or use in the United States of information and communications technology or services designed, developed, manufactured, or supplied by persons owned by, controlled by, or subject to the jurisdiction of foreign adversaries[.]” The threat, according to the May 15, 2019 Order, “exists both in the case of individual acquisitions or uses of such technology or services, and when acquisitions or uses of such technologies are considered as a class.” Executive Order 13873 does not identify specific countries or companies that pose a national security

²⁵ Theodora Yu, *To Combat Coronavirus, These Doctors Are Helping Sacramento’s Chinese Community on WeChat*, SAC. BEE (Feb. 27, 2020), <https://www.sacbee.com/latest-news/article240662256.html>.

1 threat.

2 **B. Executive Order 13943**

3 45. More than fourteen months later, on August 6, 2020, President Trump issued
 4 Executive Order 13943, titled “Addressing the Threat Posed by WeChat, and Taking
 5 Additional Steps to Address the National Emergency with Respect to the Information and
 6 Communications Technology and Services Supply Chain.” 85 FR 48641 (Aug. 6, 2020).
 7 Executive Order 13943 states that WeChat “automatically captures vast swaths of
 8 information from its users,” and that the data collected by WeChat “threatens to allow the
 9 Chinese Communist Party access to Americans’ personal and proprietary information.”
 10 According to this Order, the data collected by WeChat also “captures the personal and
 11 proprietary information of Chinese nationals visiting the United states, thereby allowing
 12 the Chinese Communist Party a mechanism for keeping tabs on Chinese citizens who may
 13 be enjoying the benefits of a free society for the first time in their lives.”

14 46. Executive Order 13943 does not declare a new national emergency. Rather,
 15 it asserts that the “threat” posed by WeChat is “similar to” the threat posed by other
 16 Chinese-owned technology companies, such as TikTok, which the President took action
 17 against pursuant to his purported emergency powers under the International Emergency
 18 Economic Powers Act (“IEEPA”). *See* Executive Order 13942, 85 FR 48637 (Aug. 6,
 19 2020). The Executive Orders regulating WeChat and TikTok—both issued on the same
 20 day—rely on powers purportedly made available by the national emergency declared in
 21 Executive Order 13873, issued over a year earlier on May 15, 2019.

22 47. Several sections of Executive Order 13943 purport to alter the legal rights
 23 and obligations of private parties. Section 1(a) states that “any transaction that is related to
 24 WeChat by any person” will be “prohibited beginning 45 days after the date of this
 25 order[.]” Section 1(a) further prohibits, beginning 45 days from the date of the Order,
 26 transactions with Tencent, WeChat’s parent company, and any subsidiaries of Tencent that
 27 are “identified by the Secretary of Commerce[.]” Section 2(a) states that “[a]ny
 28 transaction ... that evades or avoids, has the purpose of evading or avoiding, causes a

1 violation of, or attempts to violate the prohibition set forth in this order is prohibited.”
2 Section 2(b) further prohibits “[a]ny conspiracy formed to violate any of the prohibitions
3 set forth in this order.” Section 3 purports to strip persons subject to the prohibitions in
4 Sections 1(a) and 2 of any right to notice of the specific conduct being prohibited.

5 48. Executive Order 13943, by its terms, may apply not only to WeChat, its
6 parent company Tencent, but also to the millions of American individuals, groups,
7 businesses, organizations, churches and government agencies, that use WeChat every day
8 to communicate, learn, speak, read, publish, organize, advertise, run a business, and meet
9 friends and family in their personal, professional and business lives. While “transaction”
10 is not defined in the Executive Order, it does make clear that it applies to “any United
11 States citizen, permanent resident alien, entity organized under the laws of the United
12 States or any jurisdiction within the United States (including foreign branches), or any
13 person in the United States.” *Id.* § 4(c). And “entity” is further defined to mean a
14 government or instrumentality of such government, partnership, association, trust, venture,
15 corporation, group, subgroup, or other organization, including an international
16 organization.” *Id.* § 4(b).

17 49. Two other sections of Executive Order 13943 direct the Secretary of
18 Commerce to take additional action: Section 1(c) directs the Secretary, within 45 days of
19 August 6, to “identify the transactions subject to subsection [1](a).” Section 5 authorizes
20 the Secretary to “take such actions, including adopting rules and regulations, and to
21 employ all powers granted to me by IEEPA as may be necessary to implement this order.”
22 The Executive Order specifically mentions the popular use of WeChat to pay for purchases
23 or to transfer money or to accept or make payments for their businesses from or to another
24 user, as the basis to relieve the Secretary of Commerce of any responsibility to give “prior
25 notice” to them “of measures to be taken” because advance notice “would render those
26 measures ineffectual.” *Id.* § 3. It is unclear whether this section permits the Secretary to
27 freeze or seize monies belonging to WeChat users in the U.S. without notice.

28 50. Under the Executive Order, WeChat users who engage in a prohibited

1 transaction may be prosecuted under the IEEPA, which provides for civil penalties of
2 \$250,000 or twice the amount of transaction, and criminal penalties of up to \$1 million
3 plus 20 years in prison. *See* 50 U.S.C. § 1705(b)-(c).

4 **C. The Secretary of Commerce Identifies the Transactions Prohibited by**
5 **EO 13943**

6 51. On September 18, 2020, the Commerce Department released its
7 “Identification of Prohibited Transactions to Implement Executive Order 13943” (the
8 “Identification”).

9 52. The Identification sets forth eleven defined terms and identifies seven
10 “transactions” to be prohibited pursuant to the Executive Order.

11 53. For example, the Identification defines “person” as “an individual or entity.”

12 54. It also defines “Transaction” to mean “any acquisition, importation, transfer,
13 installation, dealing in, or use of any information and communications technology or
14 service.”

15 55. It then states that the transactions prohibited by EO 13943 include, *inter alia*:

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

21 b. “Any provision of internet hosting services enabling the functioning
22 or optimization of the WeChat mobile application, within the land and maritime borders of
23 the United States and its territories.”

24 c. “Any provision of content delivery services enabling the functioning
25 or optimization of the WeChat mobile application, within the land and maritime borders of
26 the United States and its territories.”

27 d. “Any provision of content delivery services enabling the functioning
28 or optimization of the WeChat mobile application, within the land and maritime borders of

the United States and its territories.”

e. “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.”

56. In short, the Identification sets forth a de facto ban of WeChat.

57. On September 18, 2020, multiple Administration officials confirmed the purpose and intent of the Identification as being the eventual, complete prohibition of any use of WeChat in the United States.

58. For example, on September 18, 2020, Secretary of Commerce Wilbur Ross stated on Fox Business News that “WeChat is essentially a funds transfer and payment processing mechanism. For all practical purposes, it will be shut down in the U.S., but only in the U.S. as of midnight on Monday by the Commerce Department rule.”²⁶

59. Mr. Ross also stated that “WeChat is essentially a funds transfer and payment processing mechanism.” This is incorrect, as several of WeChat’s most important functions involve social networking and other communications, both in China and in the United States.

60. The Secretary’s mischaracterization demonstrates the government’s lack of investigation and understanding of the software that it has now banned.

61. In a televised interview on Friday, September 18, 2020, the Secretary of Commerce stated that it “is our *fear*” that WeChat is “taking data from the American public and sending it to China.” But the Secretary provided no examples of “data” being “sen[t] . . . to China” or how the mere transmission of “data” to China constitutes a national security threat.²⁷

62. Also on September 18, 2020, a separate statement from an anonymous

²⁶ Available at: <https://video.foxbusiness.com/v/6192199311001/#sp=show-clips>

²⁷ Available at: <https://video.foxbusiness.com/v/6192199311001/#sp=show-clips>.

1 “senior Commerce official” to a reporter for the technology publication CNET appears to
 2 confirm that the Administration has no evidence whatsoever of private data being
 3 harvested by WeChat in the United States. “Whether we have any evidence, domestically,
 4 of these particular apps taking data is missing the point, according to this official, because
 5 the Administration “know[s] what the Chinese government’s intent is here in the United
 6 States.”²⁸

7 63. On the same day, another anonymous government official in the Commerce
 8 Department stated to Reuters that “The U.S. Commerce Department[‘s] ... order ... will
 9 bar people in the United States from downloading Chinese-owned messaging app WeChat
 10 and video-sharing app TikTok starting on September 20.”²⁹

11 64. According to the official, the Commerce Department order will “deplatform”
 12 the two apps in the United States and bar Apple Inc’s app store, Alphabet Inc’s Google
 13 Play and others from offering the apps on any platform “that can be reached from within
 14 the United States.”³⁰

15 65. Journalists have likewise understood the Identification as a complete ban on
 16 the use of WeChat. On September 18, 2020, the New York Times reported under the
 17 headlined: “Trump Administration to Ban TikTok and WeChat From U.S. App Stores.”³¹
 18 The Wall Street Journal reported: “U.S. Bans Chinese Apps TikTok and WeChat, Citing
 19 Security Concerns.” CNBC reported: “Trump to block downloads of TikTok, WeChat on
 20

21
 22 ²⁸ September 18, 2020 CNET article titled “TickTok, WeChat downloads will be barred
 23 from US starting Sunday,” Available at: [https://www.cnet.com/news/tiktok-wechat-](https://www.cnet.com/news/tiktok-wechat-downloads-will-be-barred-from-us-starting-sunday)
[downloads-will-be-barred-from-us-starting-sunday](https://www.cnet.com/news/tiktok-wechat-downloads-will-be-barred-from-us-starting-sunday).

24 ²⁹ September 18, 2020 Reuters article titled “Officials: Trump to Block US Downloads of
 25 TikTok, WeChat on Sunday,” available at: [https://www.reuters.com/article/us-usa-tiktok-](https://www.reuters.com/article/us-usa-tiktok-ban-exclusive-idUSKBN2691QO)
[ban-exclusive-idUSKBN2691QO](https://www.reuters.com/article/us-usa-tiktok-ban-exclusive-idUSKBN2691QO).

26 ³⁰ September 18, 2020 CNET article titled “TickTok, WeChat downloads will be barred
 27 from US starting Sunday,” Available at: [https://www.cnet.com/news/tiktok-wechat-](https://www.cnet.com/news/tiktok-wechat-downloads-will-be-barred-from-us-starting-sunday)
[downloads-will-be-barred-from-us-starting-sunday](https://www.cnet.com/news/tiktok-wechat-downloads-will-be-barred-from-us-starting-sunday).

28 ³¹ September 18, 2020 New York Times article titled “Trump Administration to Ban
 TikTok and WeChat From U.S. App Stores,” available at:
<https://www.nytimes.com/2020/09/18/business/trump-tik-tok-wechat-ban.html>.

Sunday,” and noted that “WeChat is considered dead in the U.S.”³² And the Associated Press reported: “US bans WeChat, TikTok from app stores, threatens shutdowns,” saying that the move could “effectively wreck the operation of both ... services for U.S. users.”³³

D. Purported Authority for the Executive Order and Identification

66. Both Executive Order 13873 and Executive Order 13943 cite the National Emergencies Act (“NEA”) and the IEEPA as providing the legal authority for the President’s actions.

1. The National Emergencies Act

67. The NEA, Pub. L. No. 94-412, 90 Stat. 1255, codified at 50 U.S.C. §§ 1601-1651, was enacted by Congress in 1976 to rein in, rather than expand, the power of the president. The NEA was designed to “insure” that the president’s “extraordinary” emergency powers would “be utilized only when emergencies actually exist, and then, only under safeguards of congressional review.” S. Rep. No. 94-1168, at 2 (1976).

68. To this end, the NEA allows the President to utilize emergency powers authorized by Congress in other federal statutes only when there is a national emergency that has been declared in accordance with specific statutory requirements. 50 U.S.C. § 1621.

69. Among other actions required by the NEA, the President must specify the statutory powers he intends to invoke upon issuing a national emergency. 50 U.S.C. § 1631. He must also publish the declaration of a national emergency in the Federal Register and transmit it to Congress “immediately.” 50 U.S.C. § 1621(a). Every six months thereafter, for as long as the emergency remains in effect, the President must transmit to Congress “a report on the total expenditures incurred by the United States

³² September 18, 2020 CNBC article titled “Trump to block downloads of TikTok, WeChat on Sunday,” *available at*: <https://www.cnbc.com/2020/09/18/trump-to-block-us-downloads-of-tiktok-wechat-on-sunday-officials-tell-reuters.html>.

³³ September 18, 2020 Associated Press article titled “US Bans WeChat, TikTok From App Stores, Threatens Shutdowns,” *available at*: <https://www.usnews.com/news/business/articles/2020-09-18/us-banning-use-of-wechat-tiktok-for-national-security>.

Government during such six-month period which are directly attributable to the exercise of powers and authorities conferred by such declaration.” 50 U.S.C. § 1641(c). Each House of Congress, in turn, must meet at least once every six months following the declaration “to consider a vote on a joint resolution to determine whether that emergency shall be terminated.” 50 U.S.C. § 1622(b). Any national emergency declared by the President automatically terminates after one year unless the President publishes in the Federal Register and transmits to Congress a notice that the emergency “is to continue in effect after such anniversary.” 50 U.S.C. § 1622(d).

2. The International Economic Emergency Powers Act

70. The IEEPA grants the President limited emergency powers when the President has declared a national emergency, pursuant to the NEA, with regard to an “unusual and extraordinary threat, which has its source in whole or in substantial part outside the United States[.]” 50 U.S.C. § 1701(a). “Any exercise” of the powers granted by the IEEPA “to deal with any new threat shall be based on a new declaration of national emergency which must be with respect to such threat.” 50 U.S.C. § 1701(b).

71. The IEEPA does not grant the President unlimited powers during national emergencies. Rather, the statute includes specific limits on the emergency powers it authorizes. Section 1702(b) of the IEEPA states that “[t]he authority granted to the President by [the IEEPA] does not include the authority to regulate or prohibit, directly or indirectly ... (1) any postal, telegraphic, telephonic, or other personal communication, which does not involve a transfer of anything of value; (2) donations, by persons subject to the jurisdiction of the United States, of articles, such as food, clothing, and medicine, intended to be used to relieve human suffering ...; (3) the importation from any country, or the exportation to any country, whether commercial or otherwise, regardless of format or medium of transmission, of any information or informational materials ...; [or] (4) any transactions ordinarily incident to travel to or from any country[.]” 50 U.S.C. § 1702(b)(1)-(4). The IEEPA also requires that the President “consult with Congress before exercising any of the authorities granted by this chapter,” and that the President

1 “immediately transmit to Congress a report” containing certain additional information
 2 about the President’s reasons for exercising his emergency powers under the IEEPA and
 3 the specific actions he and his subordinates will take in exercising those powers. 50
 4 U.S.C. § 1703(a)-(b).

5 **E. Immediately Preceding the Executive Order, President Trump Targeted**
 6 **Denigrating Statements Against China And Chinese People**

7 72. In the months before the Executive Order was issued, President Trump made
 8 numerous anti-Chinese statements outside the context of national security that commenta-
 9 tors have described as inciting racial animus against persons of Chinese descent for
 10 political gain. Many of these inflammatory statements have been made in the context of
 11 the President blaming the coronavirus pandemic on China. Instead of using the official
 12 public health terms for the virus, such as the “novel coronavirus” and “COVID-19,”
 13 President Trump has repeatedly and intentionally referred to the virus causing the current
 14 pandemic as the “China virus,” “the Wuhan virus,” “China Flu,” and “Kung-Flu.”³⁴

15
 16 ³⁴ See, e.g., Remarks by President Trump in Press Briefing (July 23, 2020),
 17 <https://www.whitehouse.gov/briefings-statements/remarks-president-trump-press-briefing-072320/> (“We’ve had a tremendous week uniting the country in our fight against the
 18 **China virus**”); Donald J. Trump (@realDonaldTrump), TWITTER (Aug. 2, 2020),
 19 <https://twitter.com/realDonaldTrump/status/1289887533250351110> (“Big **China Virus**
 20 breakouts all over the World, including nations which were thought to have done a great
 21 job. The Fake News doesn’t report this. USA will be stronger than ever before, and
 22 soon!”); Donald J. Trump (@realDonaldTrump), TWITTER (Aug. 11, 2020),
 23 <https://twitter.com/realDonaldTrump/status/1293163704188645385> (“More Testing, which
 24 is a good thing (we have the most in the world), equals more Cases, which is Fake News
 25 Gold. They use Cases to demean the incredible job being done by the great men & women
 26 of the U.S. fighting the **China Plague!**”); Donald J. Trump (@realDonaldTrump),
 27 TWITTER (July 26, 2020),
 28 <https://twitter.com/realDonaldTrump/status/1287473812733341696> (“Because of my
 strong focus on the **China Virus**, including scheduled meetings on Vaccines, our economy
 and much else, I won’t be able to be in New York to throw out the opening pitch for the
 @Yankees on August 15th. We will make it later in the season!”); Donald J. Trump
 (@realDonaldTrump), TWITTER (Mar. 18, 2020),
<https://twitter.com/realDonaldTrump/status/1240243188708839424> (“I always treated the
Chinese Virus very seriously, and have done a very good job from the beginning,
 including my very early decision to close the “borders” from China - against the wishes of
 almost all. Many lives were saved. The Fake News new narrative is disgraceful & false!”);
 Li Zhou, *Trump’s Racist References to the Coronavirus Are His Latest Effort to Stoke*
Xenophobia, VOX (June 23, 2020), [https://www.vox.com/2020/6/23/21300332/trump-](https://www.vox.com/2020/6/23/21300332/trump-coronavirus-racism-asian-americans)
[coronavirus-racism-asian-americans](https://www.vox.com/2020/6/23/21300332/trump-coronavirus-racism-asian-americans); Colby Itkowitz, *Trump Again Uses Racially*

73. Facing criticism that these word choices were racist and unfairly subjected Chinese people—including Chinese Americans—to anger and hatred, the White House spokesperson has defended Trump’s dangerous and incendiary language.³⁵ The Anti-Defamation League has reported an increasing number of hate crimes, including racial slurs, spitting on, and physical assaults against Asian-Americans in the United States following the President’s use of these terms, and warned that “Statements by public officials referring to COVID-19 as the ‘Chinese virus,’ ‘Kung Flu’ or ‘Wuhan Flu’ may be exacerbating the scapegoating and targeting of the [Asian American and Pacific Islander] community.”³⁶ The incitement following the President’s statements reminded many in the Asian American community of the hatred and racial violence focused on persons of Asian descent after the success of the Japanese auto industry was blamed for major job losses in the American Rust Belt.³⁷

74. In addition to asserting that the United States’ incidence of COVID-19 is China’s fault, the President has exploited anti-Chinese sentiment as a rallying cry for his electoral campaign. For example, on August 11, 2020, President Trump stated that “[i]f I don’t win the election, China will own the United States. You’re going to have to learn to speak Chinese.”³⁸ President Trump has on numerous occasions mocked the accent of

Insensitive Term to Describe Coronavirus, WASH. POST (Jun. 23, 2020), https://www.washingtonpost.com/politics/trump-again-uses-kung-flu-to-describe-coronavirus/2020/06/23/0ab5a8d8-b5a9-11ea-aca5-ebb63d27e1ff_story.html.

³⁵ Andrew Restuccia, *White House Defends Trump Comments on ‘Kung Flu,’ Coronavirus Testing*, WALL ST. J. (Jun. 22, 2020), <https://www.wsj.com/articles/white-house-defends-trump-comments-on-kung-flu-coronavirus-testing-11592867688>.

³⁶ *Reports of Anti-Asian Assaults, Harassment and Hate Crimes Rise as Coronavirus Spreads*, ADL BLOG (Jun. 18, 2020), <https://www.adl.org/blog/reports-of-anti-asian-assaults-harassment-and-hate-crimes-rise-as-coronavirus-spreads>.

³⁷ Ali Rogin & Amna Nawaz, *‘We Have Been Through this Before.’ Why Anti-Asian Hate Crimes Are Rising Amid Coronavirus*, PBS NEWS HOUR (Jun. 25, 2020), <https://www.pbs.org/newshour/nation/we-have-been-through-this-before-why-anti-asian-hate-crimes-are-rising-amid-coronavirus>.

³⁸ Kevin Liptak, *Trump Says Americans Will Have to Learn Chinese if Biden Wins, but Offers Little Condemnation of Beijing*, CNN (Aug. 11, 2020), <https://www.cnn.com/2020/08/11/politics/trump-china-biden-learn-chinese/index.html>

Chinese and Asian-Americans, including those of prominent Asian leaders.³⁹

THE EXECUTIVE ORDER CAUSED MASS CONFUSION AND HAS ALREADY HARMED PLAINTIFFS

75. American law firms have been unable to advise their clients as to the scope of “transactions” that are banned under Executive Order 13943. Multiple prominent law firms in the United States have effectively conceded that they cannot provide guidance about the meaning of the Order, and have speculated that all uses of WeChat could be prohibited. One law firm recently informed its clients that the “extraordinary breadth and ambiguity” of the Executive Order has “left US companies and many others looking to the Trump Administration for additional clarity[.]”⁴⁰ Another firm speculated that WeChat “could be pulled out of the app stores and off of American phones Companies could be banned from interacting with the extensive interactive payment network used by WeChat.”⁴¹

76. Each plaintiff learned of the Executive Order at or near the time it was issued and has suffered harm as a result of the Executive Order’s sweeping prohibition on “any transaction that is related to WeChat by any person, or with respect to any property.” 85 FR 48641, at § 1(a). Plaintiff Duan, for example, experiences fear and worry on a daily basis that Chihuo, Inc.—the business she founded and for which she continues to serve as

³⁹ See, e.g., Laura Ma, *‘We want deal!’: Trump fakes Asian accent to mock Chinese and Japanese businessmen at US rally*, South China Morning Post (Aug. 26, 2015), <https://www.scmp.com/news/world/article/1852785/we-want-deal-trump-fakes-asian-accent-mock-chinese-japanese-businessmen>; Jennifer Gould and Emily Smith, *Trump cracks jokes about Equinox scandal, kamikaze pilots at Hamptons fundraiser*, N.Y. POST (Aug. 9, 2019), <https://nypost.com/2019/08/09/trump-cracks-jokes-about-rent-control-kamikaze-pilots-at-hamptons-fundraiser/> (reporting on Trump “mimicking Japanese and Korean accents”).

⁴⁰ Ambassador Charlene Barshefsky, David S. Cohen, Ronald I. Meltzer, David M. Horn & Semira Nikou, *New Executive Orders Target Chinese Apps*, WILMER HALE, (Aug. 10, 2020), <https://www.wilmerhale.com/en/insights/client-alerts/20200810-new-executive-orders-target-chinese-apps>.

⁴¹ David A. Kaufman, John Sandweg, David K. Cheng & Rachel S. Winkler, *Administration’s Attempt to Delete TikTok and WeChat: Latest Trade Tiff or New Battle*, NIXON PEABODY (Aug. 7, 2020), <https://www.nixonpeabody.com/en/ideas/articles/2020/08/07/administrations-attempt-to-delete-tiktok-and-wechat>.

CEO—will not survive if it cannot provide services to customers through WeChat. Plaintiff Peng fears that the non-profit organization she founded will not be able to continue providing services to Chinese speakers in the United States, and that she personally will be unable to maintain her social ties and communicate with other members of the Chinese community in the United States. Plaintiff Zhang worries that she will be unable to maintain social ties and communicate with other Chinese-speaking people—both in the United States and in China. She believes that the charity she founded—Hita Education Foundation—could not have been founded without WeChat and may not be able to survive without being able to connect with Chinese-speaking people through the app. Each individual plaintiff fears losing connection with close friends and family members.

77. All plaintiffs, moreover, have already been forced by the Executive Order to expend time and resources preserving their contacts and memories on WeChat and/or searching—without success—for an alternative platform that could sustain their businesses, charities, and/or social and family ties. Plaintiff Peng has received inquiries from Chinese families through MHACC, her mental health WeChat group, about where to go if WeChat is banned, but has been unable find a comparable substitute to replace WeChat. Plaintiff Chihuo has spent money attempting to redirect its business activities that currently depend on WeChat by establishing alternative social media channels on YouTube, Instagram and Facebook. These efforts to find a substitute for WeChat have not been and are unlikely to be successful. This is because alternative apps often do not offer a Chinese user interface. More importantly, alternative apps also do not provide access to WeChat’s vast network of Chinese-speaking users. Without mincing words, WeChat’s enormous network effect is *irreplaceable*, and any other platform would not provide the community that WeChat does.

FIRST CLAIM FOR RELIEF

(First Amendment Freedom of Speech)

78. Plaintiffs reallege and hereby incorporate by reference the allegations contained in the preceding paragraphs of this Complaint.

1 79. The First Amendment guarantees freedoms concerning religion, expression,
2 the press, assembly, and petitioning the government. Plaintiffs' use of WeChat are
3 exercises of all these freedoms.

4 80. WeChat is a mobile application that is broadly used by members of the
5 Chinese diaspora throughout the world, serving as a virtual public square where people
6 within the Chinese and Chinese-speaking communities can connect based on shared
7 interests. Plaintiffs and other WeChat users use the app to express themselves and
8 communicate by text, voice, and video messaging; attend religious services and cultural
9 events; organize political groups and causes; read and share information in the media,
10 among other protected First Amendment activities. These actions can reasonably be
11 understood to be included as "any transaction that is related to WeChat by any person, or
12 with respect to any property," as provided in the Executive Order.

13 81. Banning the use of WeChat in the United States has the effect of foreclosing
14 all meaningful access to social media for users, such as Plaintiffs, who wish to
15 communicate and interact with members of the Chinese and Chinese-speaking
16 communities.

17 82. The Executive Order discriminates against the ideas and viewpoints of
18 WeChat users. Under the Executive Order, only content on WeChat is prohibited; the
19 content on other comparable mobile applications is not regulated or prohibited, despite
20 also capturing personal and proprietary information from its users. Therefore, the
21 Executive Order targets speech by WeChat users, the majority of whom are members of
22 the Chinese and Chinese-speaking communities, and intends to silence viewpoints within
23 these communities.

24 83. The Executive Order is overly expansive and does not justify the supposed
25 risks that are presented by permitting WeChat to operate in the United States. There are
26 less restrictive ways to regulate the collection of personal and proprietary information on
27 the WeChat app and address potential national security concerns. Defendants cannot
28 proffer a justifiable reason for discriminating against the content of WeChat users, who

1 express viewpoints within the Chinese and Chinese-speaking communities.

2 84. The Executive Order is substantially overbroad in that it renders people who
3 conduct “any transaction that is related to WeChat” subject to incarceration and monetary
4 penalties, even though “any transaction” includes a wide range of protected expressive and
5 associative rights under the First Amendment.

6 85. Plaintiff and others similarly situated have been and will continue to be
7 chilled and burdened in the exercise of their First Amendment rights because of the threat
8 of penalties, including incarceration and other treatment, under the Executive Order that
9 arises in connection with “any transaction that is related to WeChat.”

10 86. Accordingly, the Executive Order violates Plaintiffs’ rights as guaranteed by
11 the First Amendment. Defendants’ violations inflict ongoing harm upon Plaintiffs.

12 **SECOND CLAIM FOR RELIEF**

13 **(Fifth Amendment – Equal Protection)**

14 87. Plaintiffs reallege and hereby incorporate by reference the allegations
15 contained in the preceding paragraphs of this Complaint.

16 88. The Due Process Clause of the Fifth Amendment prohibits the Federal
17 Government from denying equal protection of the laws, including on the basis of race,
18 ethnicity, nationality, national origin, and alienage.

19 89. WeChat is widely used and depended on by the Chinese community in the
20 United States to communicate with friends, family, customers, and other persons of
21 Chinese or Chinese American ancestry, including Chinese-language speakers.

22 90. Plaintiffs Peng, Duan, Zhang, and Bao are members of the Chinese
23 community in the United States. Plaintiff Brent Coulter uses WeChat to communicate
24 with people of Chinese and/or Chinese-American ancestry in the United States and abroad.
25 Plaintiffs USWUA and Chihuo are organizations or businesses whose members or
26 customers primarily consist of people of Chinese and/or Chinese American ancestry in the
27 United States, who use WeChat to communicate with others similar to them both in the
28 United States and abroad.

1 91. By prohibiting the use of WeChat but not other apps that are used primarily
2 by people who are not of Chinese or Chinese-American ancestry, Executive Order 13943
3 singles out people of Chinese and Chinese-American ancestry and subjects them and
4 people who communicate with them to disparate treatment on the basis of race, ethnicity,
5 nationality, national origin, and alienage.

6 92. This disparate treatment is motivated by Defendants' animus towards people
7 of Chinese and/or Chinese American ancestry, and has the purpose of discriminating
8 against people of Chinese and/or Chinese-American ancestry.

9 93. Defendants' issuance of Executive Order 13943 therefore violates Plaintiffs'
10 rights to equal protection guaranteed by the Fifth Amendment to the United States
11 Constitution. Defendants' violations inflict ongoing harm upon Plaintiffs.

12 **THIRD CLAIM FOR RELIEF**

13 **(Fifth Amendments – Due Process)**

14 94. Plaintiffs reallege and hereby incorporate by reference the allegations
15 contained in the preceding paragraphs of this Complaint.

16 95. Sections 1(a) and 2 of Executive Order 13943 alter the legal rights and
17 obligations of private parties, including Plaintiffs, independent of any action by the
18 Secretary of Commerce.

19 96. These sections include only a conclusory description of prohibited
20 "transactions related to WeChat," which provides no notice to WeChat users or anyone
21 else of the specific conduct that is prohibited.

22 97. In spite of the Executive Order's vagueness, violations of Sections 1(a) and 2
23 are punishable by incarceration and monetary penalties. 50 U.S.C. § 1705(b)-(c).

24 98. Plaintiffs, who use WeChat to communicate and share information with
25 friends, family, customers, and other persons both in the United States and abroad, do not
26 know which of their activities that involve WeChat are prohibited by the Executive Order.
27 Because of this uncertainty, they are justifiably fearful of using WeChat in any way and for
28 any purpose.

99. Sections 1(a) and 2 of Executive Order 13943 provide inadequate notice of the conduct they purport to penalize and are void for vagueness under the Fifth Amendment to the U.S. Constitution.

FOURTH CLAIM FOR RELIEF

(Ultra Vires (50 U.S.C. § 1702(b)))

100. Plaintiffs reallege and hereby incorporate by reference the allegations contained in the preceding paragraphs of this Complaint.

101. The IEEPA includes specific limits on Defendants’ authority to prohibit transactions related to WeChat. Section 1702(b) of the IEEPA states in relevant part that “[t]he authority granted to the President by [the IEEPA] does not include the authority to regulate or prohibit, directly or indirectly ... (1) any postal, telegraphic, telephonic, or other personal communication, which does not involve a transfer of anything of value; (2) donations, by persons subject to the jurisdiction of the United States, of articles, such as food, clothing, and medicine, intended to be used to relieve human suffering...[or] (3) the importation from any country, or the exportation to any country, whether commercial or otherwise, regardless of format or medium of transmission, of any information or informational materials[.]” 50 U.S.C. § 1702(b)(1)-(3).

102. Neither the President nor any other federal official can take an action that exceeds the scope of their constitutional and/or statutory authority. In Executive Order 13943, however, the President has nonetheless “prohibited” Plaintiffs from using WeChat in any manner, in direct contravention of the specific limits on Presidential authority contained in 50 U.S.C. § 1702(b).

103. The Secretary’s Identification likewise seeks to effectuate an outright ban of the WeChat platform—directly curtailing “communications” in the manner explicitly prohibited by the IEEPA.

104. Plaintiffs use WeChat for “personal communication[s]” that “do[] not involve a transfer of anything of value,” within the meaning of 50 U.S.C. § 1702(b)(1).

105. Plaintiffs use WeChat to coordinate and arrange for donations of “articles ...

intended to be used to relieve human suffering,” within the meaning of 50 U.S.C. § 1702(b)(2).

106. Plaintiffs use WeChat to import and/or export “information or information materials,” within the meaning of 50 U.S.C. § 1702(b)(3).

107. Defendants are acting *ultra vires* in prohibiting “personal communication[s],” that “do[] not involve a transfer of anything of value,” as well as the coordination of donations of “articles ... intended to be used to relieve human suffering” and the importation and/or exportation of “information or information materials.”

FIFTH CLAIM FOR RELIEF

(Ultra Vires (50 U.S.C. §§ 1621-22, 1641, 1703))

108. Plaintiffs reallege and hereby incorporate by reference the allegations contained in the preceding paragraphs of this Complaint.

109. On information and belief, Defendants did not immediately transmit to Congress the President’s declaration of a national emergency contained in Executive Order 13873, as required by 50 U.S.C. § 1621(a).

110. On information and belief, neither house of Congress has met, at the required six month intervals or otherwise, to consider a vote on a joint resolution to determine whether that emergency shall be terminated, as required by 50 U.S.C. § 1622(b).

111. On information and belief, the President has not transmitted to Congress any report on the total expenditures incurred by the United States government which are directly attributable to the exercise of powers and authorities conferred by the declaration of a national emergency in Executive Order 13873, as required by 50 U.S.C. § 1641(c).

112. On information and belief, the President did not consult with Congress, on the threat posed by WeChat or otherwise, before issuing Executive Order 13943, as required by 50 U.S.C. § 1703(a).

113. On information and belief, the President did not immediately transmit to the Congress a report specifying, among other information required in 50 U.S.C. § 1703(b), “the circumstances which necessitate such exercise of authority” and “the actions to be

1 taken in the exercise of those authorities[.]” Although the President did transmit a letter to
 2 the Speaker of the House of Representatives and the President of the Senate on the same
 3 day he issued Executive Order 13943, this letter merely repeats—often verbatim—the
 4 vague and conclusory language contained in the Executive Order. This limited
 5 information does not provide the Congress with sufficient information to exercise the kind
 6 of ongoing oversight of the President required by both the IEEPA and the NEA.

7 114. The President has acted *ultra vires* by exercising emergency powers
 8 purportedly authorized by the IEEPA without consulting with and reporting to Congress in
 9 the manner prescribed by 50 U.S.C. §§ 1621-22, 1641(c), and 1703.

10 **SIXTH CLAIM FOR RELIEF**

11 ***(Ultra Vires (50 U.S.C. § 1701))***

12 115. Plaintiffs reallege and hereby incorporate by reference the allegations
 13 contained in the preceding paragraphs of this Complaint.

14 116. 50 U.S.C. § 1701 conditions the President’s exercise of the emergency
 15 powers listed in Section 1702(a) on the President’s declaration of a national emergency
 16 with respect to an “unusual and extraordinary threat, which has its source in whole or
 17 substantial part outside the United States[.]” Section 1701 further requires that “[a]ny
 18 exercise” of the powers granted in Section 1702(a) “to deal with any new threat shall be
 19 based on a new declaration of national emergency which must be with respect to such
 20 threat.”

21 117. Executive Order 13943 cites the President’s declaration of a national
 22 emergency in Executive Order 13873 as the basis for his exercise of emergency powers
 23 purportedly granted by the IEEPA. Executive Order 13873, which was issued more than
 24 14 months before Executive Order 13943, does not mention WeChat and does not identify
 25 the app as a potential threat to the national security of the United States.

26 118. The threat purportedly posed by WeChat constitutes a “new threat” within
 27 the meaning of 50 U.S.C. § 1701(b), and thus requires a new declaration of national
 28 emergency before the President exercises any presidential powers authorized by the

1 IEEPA. The President has not issued such a new declaration of a national emergency with
2 respect to the threat posed by WeChat.

3 119. The President has acted *ultra vires* by exercising emergency powers
4 purportedly authorized by IEEPA that depend on the President having declared a national
5 emergency with respect to the threat posed by WeChat, in direct contravention of 50
6 U.S.C. § 1701(b).

7 **SEVENTH CLAIM FOR RELIEF**

8 **(Religious Freedom Restoration Act – 42 USC § 2000bb(1)(a))**

9 120. Plaintiffs reallege and hereby incorporate by reference the allegations
10 contained in the preceding paragraphs of this Complaint.

11 121. In 1993, Congress enacted the Religious Freedom Restoration Act (“RFRA”),
12 Pub. L. No. 103-31 (1993) (codified at 42 U.S.C. §§ 2000bb–2000bb-4).

13 122. RFRA prohibits the government from “substantially burden[ing] a person’s
14 exercise of religion even if the burden results from a rule of general applicability” unless
15 the government can demonstrate that the application of the burden to the person is: (1) in
16 furtherance of a compelling governmental interest; and (2) the least restrictive means of
17 furthering that compelling governmental interest. 42 U.S.C. § 2000bb-1.

18 123. WeChat users in the United States use WeChat to participate in the conduct
19 of religious worship and other practices in accordance with the tenets and practices of
20 various religions. WeChat users in the United States use WeChat to organize and
21 participate in religious activities with other members who similarly use WeChat regularly
22 in order to worship and/or practice their religion.

23 124. The Executive Order will result in substantial burdens upon the practice of
24 religion of WeChat users in the United States by forcing them to abstain from participating
25 in their practice of religion with other WeChat users or risk the threat of civil or criminal
26 sanctions and violates RFRA.

EIGHTH CLAIM FOR RELIEF

(Violation of the Administrative Procedure Act)

125. Plaintiffs hereby incorporate by reference the allegations contained in the preceding paragraphs of this Complaint.

126. The Secretary of Commerce published a document in the Federal Register on September 18, 2020 that identifies certain transactions related to WeChat” that are prohibited by EO 13943. The Secretary’s action constitutes “final agency action” within the meaning of 5 U.S.C. § 704.

127. . Under the Secretary’s definitions, the Executive Order prohibits, *inter alia*, “Any provision of services to distribute or maintain the WeChat mobile application, constituent code, or mobile application updates”; “Any provision of internet hosting services enabling the functioning or hosting of the WeChat mobile application”; and “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 United States and its territories.”

128. On September 18, 2020, the Secretary admitted , on national television, that his definitions of EO 13943 will “for all practical purposes” result in WeChat being “shut down in the U.S.” as soon as the President’s prohibition takes effect on September 20.

129. The Secretary’s definitions of the transactions prohibited by EO 13943 directly contravene Section 1702(b) by directly or indirectly regulating or prohibiting “personal communication[s],” that “do[] not involve a transfer of anything of value,” as well as the coordination of donations of “articles ... intended to be used to relieve human suffering” and the importation and/or exportation of “information or information materials.”

130. The definitions are therefore arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law, and in excess of statutory jurisdiction, authority, or limitations, or short of statutory right, within the meaning of 5 U.S.C. § 706(2).

131. Furthermore, the Identification was promulgated without notice and

comment rulemaking as required by the APA. 5 U.S.C. § 553(b), (c).

132. The Identification is therefore in direct contravention of the APA and must be vacated.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs and the Class pray for relief and judgment as follows:

1. Declaring that Executive Order 13943 is unconstitutional under the First Amendment;

2. Declaring that Executive Order 13943 is unconstitutional under the Fifth Amendment;

3. Declaring that Executive Order 13943 and the Identification do not comply with the limitations on presidential power in the National Emergency Act and the International Economic Emergency Powers Act, and is thus *ultra vires*;

4. Declaring that Executive Order 13943 violates the Religious Freedom Restoration Act;

5. Declaring that the Secretary's September 18, 2020 Identification of Prohibited Transactions violated the APA;

6. Preliminarily and permanently enjoining Defendants from enforcing the Executive Order and the Identification to prohibit the use of WeChat in the United States by individual users, businesses and groups;

7. Preliminarily and permanently staying the implementation date of any of the penalty provisions of Executive Order and the Identification; and

8. Granting such other and further relief as this Court may deem just and proper, including an award to Plaintiffs of the costs of this suit and reasonable attorneys' fees and litigation expenses under the Equal Access to Justice Act, 28 U.S.C. § 2412(d).

1 DATED: September 18, 2020

Respectfully submitted,

2 ROSEN BIEN GALVAN & GRUNFELD LLP

3 By: /s/ Michael W. Bien

4 Michael W. Bien

5 Attorneys for Plaintiffs

6 U.S. WECHAT USERS ALLIANCE, CHIHUO
7 INC., BRENT COULTER, FANGYI DUAN,
8 JINNENG BAO, ELAINE PENG, and XIAO
9 ZHANG

MICHAEL W. BIEN – Cal. Bar No. 096891
 VAN SWEARINGEN – Cal. Bar No. 259809
 ALEXANDER GOURSE – Cal. Bar No. 321631
 AMY XU – Cal. Bar No. 330707
 ROSEN BIEN GALVAN & GRUNFELD LLP
 101 Mission Street, Sixth Floor
 San Francisco, California 94105-1738
 Telephone: (415) 433-6830
 Facsimile: (415) 433-7104
 Email: mbien@rbgg.com
 vswearingen@rbgg.com
 agourse@rbgg.com
 axu@rbgg.com

KELIANG (CLAY) ZHU – Cal. Bar No. 305509
 DEHENG LAW OFFICES PC
 7901 Stoneridge Drive #208
 Pleasanton, California 94588
 Telephone: (925) 399-5856
 Facsimile: (925) 397-1976
 Email: czhu@dehengsv.com

ANGUS F. NI – Wash. Bar No. 53828*
 AFN LAW PLLC
 502 Second Avenue, Suite 1400
 Seattle, Washington 98104
 Telephone: (773) 543-3223
 Email: angus@afnlegal.com
 * *Pro Hac Vice* application forthcoming

Attorneys for Plaintiffs

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA, SAN FRANCISCO DIVISION

U.S. WECHAT USERS ALLIANCE,
 CHIHUO INC., BRENT COULTER,
 FANGYI DUAN, JINNENG BAO,
 ELAINE PENG, and XIAO ZHANG,

Plaintiffs,

v.

DONALD J. TRUMP, in his official
 capacity as President of the United States,
 and WILBUR ROSS, in his official
 capacity as Secretary of Commerce,

Defendants.

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

**DECLARATION OF JINNENG BAO
 IN SUPPORT OF PLAINTIFFS’
 MOTION FOR PRELIMINARY
 INJUNCTION**

Judge: Hon. Laurel Beeler
 Date: September 17, 2020
 Time: 9:30 a.m.
 Crtrm.: Remote

Trial Date: None Set

1 I, Jinneng Bao, declare:

2 1. I am a plaintiff in the above-entitled action (the “Action”). I have personal
3 knowledge of the matters set forth herein, and if called as a witness, I could and would
4 competently so testify.

5 2. I am a United States permanent resident residing in Nassau County, New
6 York. I have been living in the United States for thirteen years.

7 3. I was assisted in preparing this declaration in English. I primarily write and
8 speak in Chinese, and if called as a witness I would testify in Chinese.

9 4. I am self-employed and own several local businesses including construction
10 and trading businesses.

11 5. I first started using in WeChat in around 2012, and right now I have more
12 than 1,800 contacts in my WeChat, most of whom speak Chinese.

13 6. I have almost never used Facebook, Line, Telegram, WhatsApp, or other
14 similar apps to communicate with my contacts.

15 7. I talk to my mother and sister about twice a week and talk to my friends
16 back in China once a while, and the only means of communications is WeChat.

17 8. I constantly use WeChat for business purpose to talk to my employees,
18 partners, vendors, and customers, a majority of whom speak Chinese. WeChat is the
19 primary communications app for almost all of my Chinese-speaking customers because it
20 offers instant and convenient messaging and call functions.

21 9. I also use WeChat’s Moments to post pictures, videos, or text regarding my
22 daily life and recreational activities with my family in Long Island, New York. I
23 sometimes also post pictures or text about my business trips and projects in Upstate, New
24 York.

25 10. I am an active member of the New Life Chinese Alliance Church in New
26 York, and most of my fellow church members are Chinese Americans like me, whom are
27 not proficient in English. Our church members have WeChat groups to discuss church
28 activities. New Life Chinese Alliance Church in New York itself has two WeChat groups:

1 one for members in Flushing, Queens, and one for members in Brooklyn. Each group has
2 about 200 people. We discuss and study the Bible, and share our religious and life
3 experiences on a daily basis using WeChat. We also post information about the Church's
4 events. Due to the recent COVID-19 pandemic quarantine, we are unable to go to our
5 church to physically participate in mass. Most of our church members use Zoom remotely
6 for Sunday Mass and use WeChat for Bible Study.

7 11. I regularly attend Bible-study classes with other church members. Due to the
8 pandemic, our Bible-study classes have also stopped meeting in person. Right now, I
9 attend Bible-study classes only on WeChat, which are held on every Friday and Sunday
10 night. My Bible-study group has about 20 members of the church.

11 12. I learned about the Executive Order on WeChat from contacts sharing the
12 news with me, and from discussions in group chats and from media reports. I also read the
13 Executive Order itself, read news articles, and discussed with others to try to understand its
14 scope.

15 13. So far I have not fully understood, and no one can give me a definitive
16 answer, on the meaning of the words "transaction that is related to WeChat."

17 14. I understand that the Executive Order will take effect forty-five days after its
18 issuance, and that any violation of the Executive Order may subject a person to civil and
19 criminal sanctions.

20 15. I am not certain whether WeChat can still be used in the United States after
21 the Executive Order takes effect, or that if WeChat can be used, what uses will cause me to
22 violate the Executive Order and what uses will not. For example, I don't know if I will be
23 violating the Executive Order if I simply log onto WeChat, send a message to my church
24 members, make a voice or video call to my family or business partners, or download an
25 upgrade to WeChat. The possibility of being penalized or prosecuted for using WeChat
26 leaves me in fear of violating the law simply by communicating with people.

27 16. If WeChat is banned, it will be extremely difficult for me and my fellow
28 members to continue the Bible studies, and I fear that I will lose connections with my

1 church members as well as numerous other contacts on WeChat. I also don't know how I
2 will be able to run my business, because I depend on WeChat to communicate with my
3 employees and customers.

4 17. I have spent time studying on alternative apps so that I do not run afoul of
5 the law. Some of my friends are using an App called Line. My research shows that it is
6 difficult for me to switch to other apps such as Facebook, Line, or Telegram because they
7 are not designed for Chinese-speaking users, and very few of my WeChat contacts use
8 Facebook, Line, Telegram, or similar apps. I really do not what I will do if WeChat is
9 banned, but it worries me a lot.

10
11 I declare under penalty of perjury under the laws of the United States of America
12 that the foregoing is true and correct, and that this declaration is executed at Nassau
13 County, New York this 26 day of August, 2020.



14
15
16 Jinneng Bao

MICHAEL W. BIEN – Cal. Bar No. 096891
 VAN SWEARINGEN – Cal. Bar No. 259809
 ALEXANDER GOURSE – Cal. Bar No. 321631
 AMY XU – Cal. Bar No. 330707
 ROSEN BIEN GALVAN & GRUNFELD LLP
 101 Mission Street, Sixth Floor
 San Francisco, California 94105-1738
 Telephone: (415) 433-6830
 Facsimile: (415) 433-7104
 Email: mbien@rbgg.com
 vswearingen@rbgg.com
 agourse@rbgg.com
 axu@rbgg.com

KELIANG (CLAY) ZHU – Cal. Bar No. 305509
 DEHENG LAW OFFICES PC
 7901 Stoneridge Drive #208
 Pleasanton, California 94588
 Telephone: (925) 399-5856
 Facsimile: (925) 397-1976
 Email: czhu@dehengsv.com

ANGUS F. NI – Wash. Bar No. 53828*
 AFN LAW PLLC
 502 Second Avenue, Suite 1400
 Seattle, Washington 98104
 Telephone: (773) 543-3223
 Email: angus@afnlegal.com
 * *Pro Hac Vice* application forthcoming

Attorneys for Plaintiffs

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA, SAN FRANCISCO DIVISION

U.S. WECHAT USERS ALLIANCE,
 CHIHUO INC., BRENT COULTER,
 FANGYI DUAN, JINNENG BAO,
 ELAINE PENG, and XIAO ZHANG,

Plaintiffs,

v.

DONALD J. TRUMP, in his official
 capacity as President of the United States,
 and WILBUR ROSS, in his official
 capacity as Secretary of Commerce,

Defendants.

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

**DECLARATION OF YING CAO IN
 SUPPORT OF PLAINTIFFS' MOTION
 FOR PRELIMINARY INJUNCTION**

Judge: Hon. Laurel Beeler
 Date: September 17, 2020
 Time: 9:30 a.m.
 Crtrm.: Remote

Trial Date: None Set

1 I, Ying Cao, declare as follows:

2 1. I am one of three trustees of U.S. WeChat Users Alliance, (“USWUA”), a
3 Plaintiff in the above-captioned action (the “Action”). I have personal knowledge of the
4 matters stated herein and if called as a witness I would and could testify competently to
5 them.

6 2. I am an attorney and a member of the New York and New Jersey State Bar.

7 3. USWUA is incorporated in the State of New Jersey as a non-profit
8 organization.

9 4. My co-trustees and I founded USWUA solely to respond to the Executive
10 Order banning WeChat in the United States and to protect the lawful interests of average,
11 everyday WeChat users in the United States.

12 5. We founded USWUA ourselves. We do not have any connection with
13 representatives of WeChat, Tencent or any of their respective affiliates and are not
14 associated with WeChat, Tencent or any of their respective affiliates. We have not
15 solicited, nor, to my knowledge, have we received any donations or support from WeChat
16 or Tencent.

17 6. We do not represent the interests of, nor are we affiliated with, any political
18 party, government, or any governmental entity.

19 7. Our sole mission is to protect the lawful interests of WeChat users in the
20 United States. We rely exclusively on publicly raised donations in the United States.

21 8. WeChat is a multi-purpose messaging, social media, productivity, and utility
22 mobile app. At its heart, it is a social networking platform with numerous utility functions.

23 9. The social networking platform market is of a “winner-take-all” nature and is
24 thus dominated by a small number of major providers, with each enjoying near-monopoly
25 status in their own markets.

26 10. In China as well as among the global Chinese diaspora, WeChat has the
27 commanding, dominant position as a social media and messaging platform. It has a sticky
28 user base of over one billion monthly active users. By “sticky” I mean two things: (i) that

1 WeChat has a very powerful network effect that draws users to a social network found
2 nowhere else; and (ii) it is so useful and deeply integrated into users' daily lives that users
3 have become reliant on it for a variety of tasks and functions.

4 11. WeChat is often inseparable from its users' everyday habits. They use it to
5 order food, book rides, buy movie tickets, transfer money, and chat with friends and family
6 and business associates and clients, all without switching to other applications or webpages.
7 WeChat also integrates with essential public services, with Chinese-speaking Californians
8 even relying on it to receive live updates about the locations of wildfires currently raging
9 in California.

10 12. WeChat has become so central to its users that they click on the app icon
11 almost subconsciously whenever they use their smart phones.

12 13. WeChat has evolved from an instant messaging tool into an ecosystem. This
13 ecosystem includes WeChat instant messaging, WeChat Moments (an Instagram-like
14 social media "wall" functionality mainly used to share pictures with captions), WeChat
15 Official Accounts (a type of social media home page) and WeChat Mini Programs (a
16 feature that allows content creators and merchants to connect with and sell products to
17 customers through a customizable "mini-program" within the WeChat user interface).

18 14. WeChat also offers a digital payment function that serves various online-to-
19 offline services. For example, one can upload a credit or bank card to WeChat payments,
20 then scan a QR code at an establishment that accepts WeChat payments and pay that
21 establishment electronically through WeChat.

22 15. WeChat has revolutionized the way Chinese-speaking people communicate,
23 and has so entrenched itself amongst Chinese users that there is effectively no substitutes
24 for users that rely on it.

25 16. WeChat has a broad user base in the United States made up of Chinese-
26 Americans, Chinese citizens studying, working and living in the United States, as well as
27 other Americans in need of a convenient means of communication with people and
28 business in China.

1 17. For many of the WeChat users in the United States, WeChat's instant
2 messaging function is their main means of costless communication with family members
3 and business partners in China. For those without family in China but whose first
4 language is Chinese, WeChat is also a primary means of electronic communication
5 because other chat applications only provide English user interfaces.

6 18. Many users in the United States use WeChat in their work, whether as a
7 communication tool with colleagues, customers or suppliers, or as a tool to generate
8 business. For example, during the COVID-19 pandemic, many Chinese restaurants have
9 become heavily reliant on WeChat as a platform to advertise and promote their business
10 (for example on WeChat moments), solicit and process orders (for example on WeChat
11 mini-programs), and manage customer relationships (for example through their WeChat
12 homepages).

13 19. In short, for small businesses that cater primarily to a Chinese-speaking
14 clientele, WeChat has become a primary source of revenue. A WeChat ban will be
15 devastating to their businesses.

16 20. During the COVID-19 pandemic, more than 670 Chinese-Americans
17 grassroots organizations have raised over 15 million dollars and delivered millions of
18 personal protection equipment (PPE) to various hospitals, nursing homes, police
19 departments, firefighter stations, Volunteer First Aid Squad and other agencies. We
20 mainly use WeChat to organize this fundraising and donation efforts and communicate
21 news among the Chinese communities in the US.

22 21. I have read the Executive Order. As an attorney, I have received requests
23 from clients/potential clients for my assistance in interpreting whether/what uses of
24 WeChat is permitted under the Executive Order. Because the Executive Order does not
25 itself define the word "transaction," and delegates the Secretary of Commerce to identify
26 the "transactions" prohibited by the Executive Order almost at the same time when it takes
27 effect, we are yet unable to advise whether any particular use of WeChat will be allowed
28 after the Executive Order takes effect.

22. The vague language contained in the Executive Order has left WeChat users in the United States wondering how they will be affected. Enormous time has been spent researching the possible scope of coverage of the Executive Order. Uncertainty and fear of being subject to criminal penalties as a result of the Executive Order has caused distress, confusion and anxiety among WeChat users, myself included.

23. Since the Executive Order, WeChat users in the United States have been forced to explore other U.S. based social media platform options. But since WeChat is the most popular social media among the global Chinese population, many have found that there is no viable alternative. For example, users who use it as their primary means of international communication must now use the old and expensive international phone calls. Users who store important information on WeChat have no means of transferring that data other than to manually search, identify, and then type out or copy and paste such data onto other applications. The process is usually time-consuming, labor-intensive and mind-numbing.

24. Banning WeChat means effectively cutting off many people's primary means of communication with their business and social contacts, and will be highly disruptive to our way of life.

///

///

///

///

///

///

///

///

///

///

///

1 25. WeChat is used widely by millions in the United States to talk to families
2 and friends, to discuss and engage in political activities, to organize and participate in
3 charitable, religious and cultural programs, and to develop and communicate with business
4 clients across the world. The Executive Order has left WeChat users in the United States
5 in constant fear of becoming disconnected with families and friends in China and of being
6 cut off from political discussions, campaign participation, religious events such as group
7 prayers, and other social or cultural events.

8 I declare under penalty of perjury under the laws of the United States of America
9 that the foregoing is true and correct, and that this declaration is executed at

10 Short Hills, New Jersey this 26th day of August, 2020.

11 

12
13 _____
Ying Cao

1 MICHAEL W. BIEN – Cal. Bar No. 096891
 VAN SWEARINGEN – Cal. Bar No. 259809
 2 ALEXANDER GOURSE – Cal. Bar No. 321631
 AMY XU – Cal. Bar No. 330707
 3 ROSEN BIEN GALVAN & GRUNFELD LLP
 101 Mission Street, Sixth Floor
 4 San Francisco, California 94105-1738
 Telephone: (415) 433-6830
 5 Facsimile: (415) 433-7104
 Email: mbien@rbgg.com
 6 vswearingen@rbgg.com
 agourse@rbgg.com
 7 axu@rbgg.com

8 KELIANG (CLAY) ZHU – Cal. Bar No. 305509
 DEHENG LAW OFFICES PC
 9 7901 Stoneridge Drive #208
 Pleasanton, California 94588
 10 Telephone: (925) 399-5856
 Facsimile: (925) 397-1976
 11 Email: czhu@dehengsv.com

12 ANGUS F. NI – Wash. Bar No. 53828*
 AFN LAW PLLC
 13 502 Second Avenue, Suite 1400
 Seattle, Washington 98104
 14 Telephone: (773) 543-3223
 Email: angus@afnlegal.com
 15 * *Pro Hac Vice* application forthcoming

16 Attorneys for Plaintiffs

18 UNITED STATES DISTRICT COURT

19 NORTHERN DISTRICT OF CALIFORNIA, SAN FRANCISCO DIVISION

20 U.S. WECHAT USERS ALLIANCE,
 CHIHUO INC., BRENT COULTER,
 21 FANGYI DUAN, JINNENG BAO,
 ELAINE PENG, and XIAO ZHANG,

22 Plaintiffs,

23 v.

24 DONALD J. TRUMP, in his official
 capacity as President of the United States,
 25 and WILBUR ROSS, in his official
 capacity as Secretary of Commerce,

26 Defendants.

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

**DECLARATION OF BRENT
 COULTER IN SUPPORT OF
 PLAINTIFFS' MOTION FOR
 PRELIMINARY INJUNCTION**

Judge: Hon. Laurel Beeler
 Date: September 17, 2020
 Time: 9:30 a.m.
 Crtrm.: Remote

Trial Date: None Set

1 I, Brent Coulter, declare:

2 1. I am a plaintiff in the above-entitled action (the “Action”). I have personal
3 knowledge of the matters set forth herein, and if called as a witness, I could and would
4 competently so testify.

5 2. I am a United States citizen living in San Francisco, California.

6 3. I recently graduated from the University of California, Hastings College of
7 the Law with a Juris Doctor, and am now preparing for the California bar exam.

8 4. WeChat plays a central role in my life and it provides me the means to
9 communicate with my friends and family both in the U.S. and abroad. I have
10 approximately 1,617 contacts on WeChat right now.

11 5. I previously lived in China for approximately five years (2012-2017), where
12 I studied at Sichuan University in Chengdu, China and worked in marketing and policy.

13 6. While in China, I used WeChat as my main method of communication to
14 connect with my friends and professional contacts, because WeChat was and is the most
15 widely-used app in China. WeChat’s convenience and popularity gave my family members in
16 the U.S. a way to communicate with me from afar, in a multitude of ways (such as sharing
17 photos and comments) not provided by services such as Skype. Additionally, WeChat is not
18 only a social media platform and messaging application, but it also serves as necessary tool for
19 travel in China and allows consumers to purchase plane tickets and arrange ride shares like
20 Uber.

21 7. WeChat’s international platform remains vital in my everyday life because I
22 continue to use WeChat in the United States. WeChat is the only option I have to
23 communicate with everyone I met in China, from expats to close friends. I read my friends’
24 posts on WeChat Moments, learn about the world through their eyes, and they do the same
25 with me. Without WeChat, we will no longer be able to share our worlds with each other.

26 8. WeChat has helped me further U.S. interests in China. While in law school, I
27 established the Asian Law & Business Association (ALBA) with my peers. Through ALBA,
28 my colleagues and I worked together with Chinese representatives from the American

1 Chamber of Commerce to contribute chapters to its annual white paper on U.S. Business in
2 China. Without WeChat, this collaborative contribution would have never been possible.

3 9. I rely on WeChat to build upon my professional career straddling the U.S. and
4 China. I use WeChat to make new friendships and share my life others around the globe.
5 Banning it would effectively erase much of the hard work I and many other international
6 consumers put into learning about China. I greatly fear that I will lose the network that I have
7 built on WeChat if the WeChat ban becomes effective.

8 10. Shortly after hearing news of the ban, I was beyond disturbed by the
9 implications that it will have on the life. After years immersed in China tediously studying
10 Mandarin, putting time and effort into building relationships, and taking the risks it required to
11 achieve my bold dreams of building an international professional career, the WeChat ban
12 threatens to undermine all of this because it is my lifeline to China. The ban feels extremely
13 personal. Not only will the ban prevent me from sharing updates of my life with people, I get
14 emotional knowing that I could lose touch with beloved friends and the families who so
15 generously invited me into their homes. I firmly believe that trusting relationships serve as a
16 foundation for a constructive future with China. Without them, I am extremely worried about
17 the fate of my career and the fate of the people of our two nations. Any future travel to China
18 would be a logistical nightmare, from difficulty navigating, to organizing meetings and
19 networking. WeChat is simply that central to my interaction with China and its people.

20 11. I have anxiously scrambled to take action before the ban goes into effect.
21 Combing through my list of more than 1,600 friends to pick which people who are most
22 important has been stressful, depressing, and time consuming. I have had to message
23 friends and professionals for alternative contact information and had to post on my
24 WeChat Moments to let others know I may lose contact with them. For some contacts,
25 saving their Chinese phone number allows me to communicate with them via iMessage or
26 FaceTime, but that only works if both of us have an iPhone. In order to call or text those
27 who do not have an iPhone, I have to pay international calling or texting fees or contact
28 them via email, which is unreliable for communicating in China. I have yet to identify

1 another app that can replace WeChat.

2 12. Moreover, I will lose all of the tags or notes I have created for nearly all of
3 my contacts that allow me to efficiently group contacts, recall important details about
4 them, and share posts exclusively to each tag group. For example, I have added the tag
5 “Sichuan University” to my classmates which allows me to easily find them or share a post
6 exclusively for them to see and I have added notes such as “Lawyer met in Chengdu at
7 AGM” to specifically recall who a contact is and where we met. So, not only do I have the
8 difficult burden of finding alternative means to stay in touch, I now have to tediously
9 account for every important tag and note that I have created for each contact.

10
11 I declare under penalty of perjury under the laws of the United States of America
12 that the foregoing is true and correct, and that this declaration is executed at San Francisco,
13 California this 25 day of August, 2020.

14 

15 _____
16 Brent Coulter
17
18
19
20
21
22
23
24
25
26
27
28

MICHAEL W. BIEN – Cal. Bar No. 096891
 VAN SWEARINGEN – Cal. Bar No. 259809
 ALEXANDER GOURSE – Cal. Bar No. 321631
 AMY XU – Cal. Bar No. 330707
 ROSEN BIEN GALVAN & GRUNFELD LLP
 101 Mission Street, Sixth Floor
 San Francisco, California 94105-1738
 Telephone: (415) 433-6830
 Facsimile: (415) 433-7104
 Email: mbien@rbgg.com
 vswearingen@rbgg.com
 agourse@rbgg.com
 axu@rbgg.com

KELIANG (CLAY) ZHU – Cal. Bar No. 305509
 DEHENG LAW OFFICES PC
 7901 Stoneridge Drive #208
 Pleasanton, California 94588
 Telephone: (925) 399-5856
 Facsimile: (925) 397-1976
 Email: czhu@dehengsv.com

ANGUS F. NI – Wash. Bar No. 53828*
 AFN LAW PLLC
 502 Second Avenue, Suite 1400
 Seattle, Washington 98104
 Telephone: (773) 543-3223
 Email: angus@afnlegal.com
 * *Pro Hac Vice* application forthcoming

Attorneys for Plaintiffs

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA, SAN FRANCISCO DIVISION

U.S. WECHAT USERS ALLIANCE,
 CHIHUO INC., BRENT COULTER,
 FANGYI DUAN, JINNENG BAO,
 ELAINE PENG, and XIAO ZHANG,

Plaintiffs,

v.

DONALD J. TRUMP, in his official
 capacity as President of the United States,
 and WILBUR ROSS, in his official
 capacity as Secretary of Commerce,

Defendants.

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

**DECLARATION OF FANGYI DUAN
 IN SUPPORT OF PLAINTIFFS’
 MOTION FOR PRELIMINARY
 INJUNCTION**

Judge: Hon. Laurel Beeler
 Date: September 17, 2020
 Time: 9:30 a.m.
 Crtrm.: Remote

Trial Date: None Set

1 I, Fangyi Duan, declare as follows:

2 1. I am the CEO of Chihuo Inc., (“Chihuo”), a Plaintiff in the above-captioned
3 action (the “Action”). I have personal knowledge of the matters stated herein and if called
4 as a witness I would and could testify competently to them.

5 2. I was assisted in preparing this declaration in English. I primarily write and
6 speak in Chinese, and if called as a witness I would testify in Chinese.

7 3. I am a Chinese citizen residing in Santa Clara, California. I am in the process
8 of applying for a green card.

9 4. Chihuo is duly incorporated and existing under the laws of the State of
10 Delaware as a general corporation with its principal office in City of Industry, California.

11 5. I founded Chihuo with a mission of better connecting merchants with
12 customers within various Chinese communities in the United States.

13 6. We are in the business of providing digital marketing and advertising
14 services, first to restaurants, then extending broadly to clients in the food, travel,
15 technology and lifestyle services industries.

16 7. Since our founding, we have grown to be a leading content provider within
17 Chinese communities in the United States, our presence spans Los Angeles, the Bay area,
18 Seattle, Chicago, New York, Washington D.C., Boston, Atlanta, Houston, Philadelphia,
19 Dallas and Las Vegas.

20 8. We are a small business of approximately thirty employees, but our reach
21 goes well beyond the local communities that we live in. We have at least 740,000 active
22 followers on the WeChat homepages we maintain.

23 9. Through our WeChat network, we have built a thriving virtual community of
24 Chinese-language discussions, reviews, and advertising primarily focused on dining, food
25 products, and restaurants. We share content, such as restaurant reviews or recipes, on our
26 network of WeChat homepages. In return, our followers contribute to our content by their
27 commentary on our articles. They also strengthen our influence by sharing our content
28 within their own networks.

1 10. We rely heavily on social media platforms to distribute our content-based
2 marketing services. Since WeChat is the most widely used social media application of our
3 target audience (Chinese communities in the United States), we provide targeted marketing
4 and advertising services primarily on WeChat.

5 11. The success of our business is built upon WeChat's large user base within
6 the Chinese communities in the United States. Approximately 70% of our content
7 subscribers/viewers originate from WeChat.

8 12. We depend on the powerful WeChat network effects. Specifically, WeChat
9 has many users, our business has been successful at tapping that user base's interest in
10 restaurants, food products, and dining, and merchants are attracted to our marketing and
11 advertising services because we leverage WeChat and generate strong WeChat user traffic.

12 13. In particular, the instant messaging function of WeChat coupled with its
13 large user base enables us to deliver marketing and advertising to customers in a targeted
14 manner.

15 14. For example, utilizing WeChat's group chat functionality, our staff has
16 created more than 100 WeChat groups based on factors such as subscribers' personal taste
17 and geographical locations. These groups are populated by more than 50,000 active
18 WeChat users exchanging more than 7,000 messages in group conversations per day. This
19 enables our merchants to push relevant and valuable promotions directly to consumers in
20 an engaging and interactive manner.

21 15. The success of Chihuo's business on WeChat is also associated with
22 WeChat's additional unique social networking features. For example, through WeChat
23 Moments (a WeChat functionality allowing the sharing of pictures with short captions),
24 Chihuo is able to provide product display services in the form of graphics and video
25 advertising that WeChat users can interact with through "likes" and comments.

26 16. Chihuo has also established fourteen different WeChat homepages, each
27 providing geo-located, location-specific content targeting over 740,000 WeChat users in
28 fourteen different cities in the United States.

1 17. On these WeChat homepages, we generate an average of 65,000 visits per
2 day.

3 18. In addition, through WeChat Mini Programs (a feature within the WeChat
4 interface that connects content creators and merchants with viewers), we are able to
5 provide a one-stop mobile marketing solution which permits users to search, discover,
6 review, select, consult and reserve products and services of merchants with the touch of a
7 button.

8 19. Using these features that we offer through WeChat, merchants can reach
9 their most valuable target audience – interested customers – at the exact moment these
10 customers are looking for relevant products and services. These WeChat features are
11 especially beneficial to small enterprises with limited resources.

12 20. Our business model is fundamentally premised on free, continuous and
13 uninterrupted access to WeChat services in the United States. For example, approximately
14 70% of our \$2,500,000 annual revenue generated in the past year was generated from
15 providing services on WeChat.

16 21. I learned about the Executive Order on WeChat from contacts sharing the
17 news to me, from discussions in group chats and from media reports. Almost my entire
18 WeChat network was talking about it. I also read the Executive Order itself, read news
19 articles, and discussed with others to try to understand its scope. So far I have not fully
20 understood, and no one can give me a definitive answer, on the meaning of the words
21 “transaction that is related to WeChat”.

22 22. I understand that the Executive Order will take effect forty-five days after its
23 issuance, and that violation of the Executive Order may subject one to administrative, civil
24 or criminal liabilities.

25 23. I am not certain whether WeChat can still be used in the United States after
26 the Executive Order takes effect. Even if WeChat can still be used by then, I am not sure
27 what uses will cause me to violate the Executive Order and what uses will not. For
28 example, I don’t know if I will be violating the Executive Order if I simply log onto

1 WeChat, send a message to my employees, make a voice or video call with my business
2 partners, or post a promotion for a client. The possibility of being penalized for using
3 WeChat leaves me in constant fear of violating the law.

4 24. Since WeChat is the most popular social media among the global Chinese
5 population, we have found that it is commercially impracticable to seek alternative social
6 marketing solutions and still maintain our core business.

7 25. Since the Executive Order, we have received many client inquiries regarding
8 our operations. Some clients have suspended their business relationship with us while
9 other clients have ceased to renew their business relationship with us. In the past two
10 weeks, the Executive Order has cost us approximately US\$40,000 to US\$50,000 in lost
11 revenue. This is approximately 30% of our average monthly revenue. We are attempting to
12 mitigate the impact of the Executive Order, but a full out ban on WeChat will effectively
13 destroy our current business model.

14 26. Many of our employees have also expressed concerns about possible pay
15 cuts and losing their jobs. Our employees are suffering from low morale. In the worst
16 situation, only a quarter of the current employees will keep their jobs.

17 27. If access to WeChat is delayed, impaired or altogether denied to users
18 located in the United States as a result of the Executive Order, I do not know whether our
19 business will survive. I constantly fear that the Executive Order's prohibition on
20 transactions that are related to WeChat will cause me to lose my business, my employees,
21 my customers, and my professional relationships.

22 28. My ability to access the outside world, to maintain my own personal social
23 ties, and to communicate with my family members and friends in China and in the United
24 States will also be adversely affected. For example, I message my parents on WeChat
25 every few days. I am also subscribed to hundreds of WeChat homepages and rely on them
26 for information and news updates.

27 29. Faced with the threat of losing access to WeChat posed by the Executive
28 Order, we have been forced to expend our limited resources to explore switching to other

1 U.S. based social media platforms. However, we have not found any good alternatives.
 2 The thought of losing my company, which I built with my sweat and blood, as a result of
 3 the Executive Order, has caused me great anxiety.

4 30. Currently, we have multiple teams working on redesigning our website and
 5 opening new Chihuo accounts on other social media platforms. The website redesign
 6 project is expected to take at least 300 hours of work, adding two to three extra hours of
 7 work to the team members on top of their daily work. The content production team
 8 members are working five to ten extra hours a day to re-launch Chihuo on other platforms
 9 and to attract our followers there. Nonetheless, so far only a small percentage of our
 10 original followers have followed us to our new platforms. The fact that these efforts have
 11 been ineffective showcases the “stickiness” of WeChat’s network effects and its
 12 irreplaceability.

13 31. In short, because people use WeChat for its network effects, it is extremely
 14 difficult to attract them to other platforms that do not have the same networks.

15 32. Additionally, almost all of Chihuo’s business data is stored on WeChat. We
 16 store our promotion materials, business contacts, work communication and other vital
 17 information on WeChat. We grew and maintain our user base on WeChat. We share and
 18 interact with our followers on WeChat. Since WeChat is its own ecosystem, I am not
 19 aware of any method to transfer such data outside of WeChat in the same form and with
 20 the same content. Banning WeChat will mean erasing all this valuable data and destroying
 21 the informational foundations of Chihuo’s business that we built over the years.

22 ///

23 ///

24 ///

25 ///

26 ///

27 ///

28 ///

1 33. Despite the mitigation measures we have been forced to take, it is our sincere
2 belief that the harm caused by the Executive Order, if it is allowed to stand, cannot be fully
3 redressed. None of the alternatives that we are exploring can replace the functionality and
4 user base of WeChat.

5 I declare under penalty of perjury under the laws of the United States of America
6 that the foregoing is true and correct, and that this declaration is executed at Foster City,
7 California this 26th day of August, 2020.

8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28



Fangyi Duan

MICHAEL W. BIEN – Cal. Bar No. 096891
 VAN SWEARINGEN – Cal. Bar No. 259809
 ALEXANDER GOURSE – Cal. Bar No. 321631
 AMY XU – Cal. Bar No. 330707
 ROSEN BIEN GALVAN & GRUNFELD LLP
 101 Mission Street, Sixth Floor
 San Francisco, California 94105-1738
 Telephone: (415) 433-6830
 Facsimile: (415) 433-7104
 Email: mbien@rbgg.com
 vswearingen@rbgg.com
 agourse@rbgg.com
 axu@rbgg.com

KELIANG (CLAY) ZHU – Cal. Bar No. 305509
 DEHENG LAW OFFICES PC
 7901 Stoneridge Drive #208
 Pleasanton, California 94588
 Telephone: (925) 399-5856
 Facsimile: (925) 397-1976
 Email: czhu@dehengsv.com

ANGUS F. NI – Wash. Bar No. 53828*
 AFN LAW PLLC
 502 Second Avenue, Suite 1400
 Seattle, Washington 98104
 Telephone: (773) 543-3223
 Email: angus@afnlegal.com
 * *Pro Hac Vice* application forthcoming

Attorneys for Plaintiffs

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA, SAN FRANCISCO DIVISION

U.S. WECHAT USERS ALLIANCE,
 CHIHUO INC., BRENT COULTER,
 FANGYI DUAN, JINNENG BAO,
 ELAINE PENG, and XIAO ZHANG,

Plaintiffs,

v.

DONALD J. TRUMP, in his official
 capacity as President of the United States,
 and WILBUR ROSS, in his official
 capacity as Secretary of Commerce,

Defendants.

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

**DECLARATION OF ELAINE PENG
 IN SUPPORT OF PLAINTIFFS'
 MOTION FOR PRELIMINARY
 INJUNCTION**

Judge: Hon. Laurel Beeler
 Date: September 17, 2020
 Time: 9:30 a.m.
 Crtrm.: Remote

Trial Date: None Set

1 I, Elaine Peng, declare as follows:

2 1. I am a Plaintiff in the above-captioned action (the “Action”). I have personal
3 knowledge of the matters stated herein and if called as a witness I could and would testify
4 competently to them.

5 2. I was assisted in preparing this declaration in English. I primarily write and
6 speak in Chinese, and if called as a witness I would testify in Chinese.

7 3. I am a United States citizen residing in Castro Valley, California.

8 4. I founded the Mental Health Association for Chinese Communities
9 (“MHACC”), a nonprofit organization in 2013, with a mission of raising mental health
10 awareness within the Chinese community through advocacy, education, research, support,
11 and services to Chinese families and individuals afflicted by mental illness. MHACC is
12 subsequently registered as a 501(c)(3) nonprofit organization in the State of California in
13 2018.

14 5. As President and CEO of MHACC, I started multiple Chinese support
15 groups, developed and led numerous mental health programs, and developed the first
16 Chinese language website for the National Alliance on Mental Illness (“NAMI”).

17 6. Mine and MHACC’s mission is to provide mental health education to reduce
18 public prejudice against mental illness, decrease stigma among caregivers, promote mental
19 health and provide mental health programs and peer support to the underserved Chinese
20 community. I received the 2016 NAMI National’s Multicultural Outreach Award and the
21 2017 NAMI California’s Multicultural Outreach Award for my work in this field.

22 7. I first downloaded and used WeChat in 2014. Since then it has become the
23 exclusive means for me to communicate with Chinese family members and friends in both
24 China and in the United States on a daily basis. WeChat’s group chat function also allows
25 me to engage in discussions with a much wider network. I also receive news updates and
26 interact with my WeChat network through likes and comments.

27 8. I use the group chat function frequently for political discussions. I am a
28 member of multiple WeChat groups made up of WeChat users of similar political views

1 for the purpose of facilitating discussions relating to local, state or national politics.

2 9. I also use WeChat to further MHACC's mission. Since many of the Chinese
3 community members we serve are not fluent in English, WeChat is a much friendlier
4 application to them compared with other U.S. developed applications, which only have
5 English user interfaces.

6 10. WeChat is our primary communications tool with our service recipients. I
7 created two WeChat groups. One group consists of approximately 110 MHACC volunteers
8 for our use for internal communications. The second group has approximately 420
9 members, made up of both volunteers, service recipients and their family members.

10 11. In the larger WeChat group, people in similar mental-health situations can
11 share their experiences and organize to support one another. We also host lectures and
12 lessons at least weekly through WeChat using the group discussion function. We also
13 fundraise and share mental health lectures and other resources within these WeChat groups.

14 12. These WeChat groups have been a vital element of our work at MHACC.

15 13. MHACC has also created a WeChat homepage where we share mental health
16 resources on a monthly basis. The MHACC WeChat homepage currently has
17 approximately two hundred followers and has generated thousands of visits.

18 14. During the COVID-19 pandemics when physical mobility is seriously
19 impacted, WeChat has played a bigger role in my daily life and in MHACC's daily
20 operations. As cases of mental illness rise along with COVID-19, we have seen a dramatic
21 increase of the volume of discussion in the MHACC WeChat groups.

22 15. I have also noticed an uptick in the political discussions in my other WeChat
23 groups, since these can no longer take place in physical gatherings due to restrictions
24 requiring social distancing.

25 16. The daily operation of MHACC largely depends on the free, continuous and
26 uninterrupted access to WeChat services in the United States. MHACC provides, and
27 people in need of mental health assistance receive, a substantial amount of MHACC's
28 services on WeChat.

1 17. I learned about the Executive Order on WeChat from contacts sharing the
2 news to me, and from discussions in group chats and from media reports. I also read the
3 Executive Order itself, read news articles, and discussed with others to try to understand its
4 scope.

5 18. So far I have not fully understood, and no one can give me a definitive
6 answer, on the meaning of the words “transaction that is related to WeChat”.

7 19. I understand that the Executive Order will take effect forty-five days after its
8 issuance, and that violation of the Executive Order may subject one to administrative, civil
9 or criminal liabilities.

10 20. I am not certain whether WeChat can still be used in the United States after
11 the Executive Order takes effect, or that if WeChat can be used, what uses will cause me to
12 violate the Executive Order and what uses will not. For example, I don’t know if I will be
13 violating the Executive Order if I simply log onto WeChat, send a message to my service
14 recipients, make a voice or video call to my family, or share mental health resources with
15 my service recipients. The possibility of being penalized for using WeChat leaves me in
16 fear of violating the law simply by communicating with people.

17 21. To the extent access to WeChat is denied to users located in the United
18 States because of the Executive Order, the mission and operation of MHACC will be
19 negatively impacted in a very significant way. Since the Executive Order, we have
20 received hundreds of inquiries from our service recipients and their family members who
21 expressed serious concerns about not being able to get help from us if WeChat is banned.

22 22. I am concerned that, as a result of the Executive Order, MHACC will not be
23 able to serve its current users with much needed mental health services, and that I will lose
24 contact with the providers, care recipients, and family members with whom I am in regular
25 contact.

26 23. My ability to maintain my own social ties, and to communicate with other
27 Chinese community members in China and in the United States will also be adversely
28 affected. For example, I created a WeChat family group chat with all my thirty-eight

1 family members. I video chat with my elderly parents-in-law in China frequently on
2 WeChat to check on their health. Without WeChat, I will have to go back to the old way
3 of buying calling cards and making expensive international calls. I will also not be able to
4 reach all of my family members with one click. I will not be able to look at them through
5 video calls with my own eyes. Nor can they see that I am well with their own eyes.

6 24. Since WeChat is the most popular social media platform among Chinese
7 speakers in the U.S., it is practically impossible for me and MHACC to seek an alternative
8 social media platform that has the same or substantially similar reach.

9 25. Faced with the threats of losing access to WeChat posed by the Executive
10 Order, MHACC and I have been forced to expend our limited time, energy and resources
11 to explore other U.S. based social media platforms. However, we have not found a good
12 alternative.

13 26. We resorted to switching to Line (another, Korean-made social media
14 application) for our MHACC group sharing function as an imperfect temporary solution.
15 However, the process so far has been slow and ineffective and the solution problematic for
16 a number of reasons.

17 27. For example, the majority of our four hundred plus service recipients are
18 either elderly, or deficient in English, or both. When we first founded MHACC in 2013,
19 we went to great trouble just to instruct them on how to set up WeChat accounts, how to
20 use WeChat to message and share, as many of them do not know how to use a smart phone.
21 In some cases we had MHACC staff drive hours to recipients' homes, or recipients drive
22 hours to our office, just to have WeChat set up. The process took an enormous amount of
23 time and effort.

24 28. Since we started the project of switching to Line, we received countless
25 inquiries and requests for help with setting up Line. We now have no choice but to repeat
26 the same process as we did with WeChat set-up. The process this time is proving to be
27 more time and energy consuming, as Line only has an English user interface and is thus
28 unfriendly to our audience. I had to pull two MHACC staff from their routine work and

1 designated them to help with Line related inquiries specifically. Nonetheless, the process
2 has been slow and inefficient and only a small percentage of recipients have switched to
3 Line so far.


4 29. Additionally, almost all of MHACC's data is stored on WeChat. We store
5 our service recipients' names, addresses, contact information, and other vital information
6 on WeChat. We sent out intake questionnaires on WeChat for them to complete. Our staff
7 conducts one-on-one counselling with them on WeChat. We rely on the chat history to
8 evaluate their case and design their treatment, and then deliver it to them on WeChat. We
9 share articles on WeChat. In one case we even used the real-time location sharing function
10 on WeChat to prevent a suicide attempt.

11 30. Since WeChat is its own ecosystem, I am not aware of any method to
12 transfer this information outside of WeChat. Banning WeChat will mean erasing all this
13 valuable information and destroying the informational foundations that MHACC has
14 strived for years to build.

15 31. Further, we regularly invite guest speakers and mental health experts in
16 China to host lectures or lessons on WeChat in Chinese to our service recipients. This will
17 be impossible to do without WeChat.

18 32. Despite the mitigation measures we have been forced to take, it is my sincere
19 belief that the harm being caused by the Executive Order, if it is allowed to stand, cannot
20 be fully redressed.

21 I declare under penalty of perjury under the laws of the United States of America
22 that the foregoing is true and correct, and that this declaration is executed at Castro Valley,
23 California this 26th day of August, 2020.

24
25
26 
27 Elaine Peng
28

MICHAEL W. BIEN – Cal. Bar No. 096891
 VAN SWEARINGEN – Cal. Bar No. 259809
 ALEXANDER GOURSE – Cal. Bar No. 321631
 AMY XU – Cal. Bar No. 330707
 ROSEN BIEN GALVAN & GRUNFELD LLP
 101 Mission Street, Sixth Floor
 San Francisco, California 94105-1738
 Telephone: (415) 433-6830
 Facsimile: (415) 433-7104
 Email: mbien@rbgg.com
 vswearingen@rbgg.com
 agourse@rbgg.com
 axu@rbgg.com

KELIANG (CLAY) ZHU – Cal. Bar No. 305509
 DEHENG LAW OFFICES PC
 7901 Stoneridge Drive #208
 Pleasanton, California 94588
 Telephone: (925) 399-5856
 Facsimile: (925) 397-1976
 Email: czhu@dehengsv.com

ANGUS F. NI – Wash. Bar No. 53828*
 AFN LAW PLLC
 502 Second Avenue, Suite 1400
 Seattle, Washington 98104
 Telephone: (773) 543-3223
 Email: angus@afnlegal.com
 * *Pro Hac Vice* application forthcoming

Attorneys for Plaintiffs

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA, SAN FRANCISCO DIVISION

U.S. WECHAT USERS ALLIANCE,
 CHIHUO INC., BRENT COULTER,
 FANGYI DUAN, JINNENG BAO,
 ELAINE PENG, and XIAO ZHANG,

Plaintiffs,

v.

DONALD J. TRUMP, in his official
 capacity as President of the United States,
 and WILBUR ROSS, in his official
 capacity as Secretary of Commerce,

Defendants.

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

**DECLARATION OF XIAO ZHANG IN
 SUPPORT OF PLAINTIFFS' MOTION
 FOR PRELIMINARY INJUNCTION**

Judge: Hon. Laurel Beeler
 Date: September 17, 2020
 Time: 9:30 a.m.
 Crtrm.: Remote

Trial Date: None Set

1 I, Xiao Zhang, declare as follows:

2 1. I am a Plaintiff in the above-captioned action (the “Action”). I have personal
3 knowledge of the matters stated herein and if called as a witness I would and could testify
4 competently to them.

5 2. I was assisted in preparing this declaration in English. I primarily write and
6 speak in Chinese, and if called as a witness I would testify in Chinese.

7 3. I am a Chinese citizen residing in Sunnyvale, California. I have a visa that
8 permits me to live and work in the United States. I have lived in the United States since
9 2011.

10 4. I work as a Geomatics Specialist at Shell, a Fortune 500 oil and gas company.

11 5. In 2019 I founded a charity program, Hita Education Foundation (the
12 “Foundation”), to benefit disadvantaged students attending high school in my hometown in
13 China. The Foundation is incorporated in the State of Texas as a non-profit organization.

14 6. The Hita Foundation provides financial aid to students from poor families. It
15 is currently funding seven indigent students’ high school educations with monthly
16 donations of 300 yuan (approximately US\$43) to each for meals and school supplies.

17 7. I first downloaded and used WeChat around 2011 when it was launched.
18 Since then it has become the exclusive means for me to communicate with Chinese family
19 members and Chinese-speaking friends in both China and in the United States. I also use
20 WeChat for Foundation-related group chats, and for chatting with colleagues at Shell who
21 are also WeChat users. Further, I receive news updates and interact with my WeChat
22 network through WeChat’s numerous social-media functions.

23 8. I also use WeChat to further my Foundation’s mission. Since I am based in
24 the United States, I use WeChat to communicate with teachers at the high school where the
25 Foundation sponsors students.

26 9. WeChat is my primary means of receiving updates about the students the
27 Foundation is helping.

28 10. The Foundation also uses WeChat as the exclusive means of issuing monthly

1 grants to students. Through WeChat Pay (WeChat's digital payment function), I am able
2 to transfer the charitable funds I raise here to the students' bank accounts with just a few
3 clicks.

4 11. In fact, our fundraising efforts also depend on WeChat as we fundraise and
5 receive payments through WeChat Pay.

6 12. I also actively promote my Foundation through WeChat. In particular, we
7 share social media accounts about our charitable work with our WeChat network so that
8 they may share it with their networks, and so on.

9 13. I learned about the Executive Order on WeChat from contacts sharing the
10 news to me, from discussions in group chats. I also read the Executive Order itself, read
11 news articles, and discussed it with others to try to understand its scope. So far I have not
12 fully understood, and no one can give me a definitive answer, on the meaning of the words
13 "transaction that is related to WeChat".

14 14. I understand that the Executive Order will take effect forty-five days after its
15 issuance, and that violation of the Executive Order may subject one to administrative, civil
16 or criminal liabilities.

17 15. I am not certain whether WeChat can still be used in the United States after
18 the Executive Order takes effect, or that if WeChat can be used, what uses will cause me to
19 violate the Executive Order and what uses will not. For example, I don't know if I will be
20 violating the Executive Order if I simply log onto WeChat, send a message to my teachers,
21 make a voice or video call with my family, or make a transfer of charitable funds to the
22 indigent students we are trying to help. The possibility of being penalized for using
23 WeChat leaves me in a state of constant fear that I may be violating the law simply by
24 helping poor students go to school.

25 16. Since the Executive Order was issued, I keep worrying that I will no longer
26 be able to run my Foundation to support students from poor families. The daily operation
27 of my Foundation largely depends on the free, continuous and uninterrupted access to
28 WeChat in the United States. Without WeChat, our ability to raise awareness, raise funds,

1 and help our students will be severely compromised. The Executive Order has raised
2 concerns among our regular donors that they will be banned from donating to our
3 Foundation on WeChat.

4 17. If it was not for WeChat, I do not even think my Foundation could have been
5 founded in the first place.

6 18. My ability to maintain my social ties, and to communicate with other
7 Chinese speaking people in China and in the United States will also be adversely affected.

8 19. Since WeChat is the most popular social media platform among Chinese
9 speakers in the U.S., it is practically impossible for me and my Foundation to locate an
10 alternative platform that has the same or substantially similar reach. The possibility of
11 losing contact with my family, friends, donors, and social network generally has caused me
12 great anxiety.

13 20. Faced with the threats of losing access to WeChat posed by the Executive
14 Order, we have been forced to expend our limited time, energy and resources to explore
15 other U.S. based social media platforms. However, we have not found a good alternative.
16 The thought of losing the Foundation I built because of the Executive Order, and the
17 possibility that I may be found in violation of the Executive Order and subject to criminal
18 or civil penalties simply for using WeChat, has also caused me great anxiety.

19 21. We had to settle for backing up our WeChat data as a temporary solution.
20 However, there is no sophisticated backup solution and I had to manually type out contact
21 information of more than 500 WeChat contacts, search for and identify important data to
22 be transferred, such as profiles of the students we fund, and manually copy and paste them.


23 22. To ensure the continuous existence of the Foundation, we also had to build a
24 new website to receive donations. The website is still being prepared and has already
25 caused us hundreds of dollars in fees and dozens of hours and labor. We anticipate more
26 money, time and labor will be incurred for the website to launch.

27 23. Despite the mitigation measures we were forced to take, it is our sincere
28 belief that the harm caused by the Executive Order, if it is allowed to stand, cannot be fully

1 redressed. None of the alternatives that we are considering can replace the functionality
2 and ease of WeChat or the ability to communicate and receive support from a like-minded
3 community bound by our language and culture.

4 I declare under penalty of perjury under the laws of the United States of America
5 that the foregoing is true and correct, and that this declaration is executed at

6 summit California this 26 day of August, 2020.

7
8 
9 Xiao Zhang

CERTIFICATE OF SERVICE

I hereby certify that on October 2, 2020, I filed the foregoing addendum with the Clerk of the Court for the United States Court of Appeals for the Ninth Circuit by using the appellate CM/ECF system. All participants in the case are registered CM/ECF users and will be served by the appellate CM/ECF system.

/s/ Dennis Fan
DENNIS FAN