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–Appellants,

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–Appellees.

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

BRIEF FOR APPELLANTS

Of Counsel:

MICHAEL J. WALSH, JR.
Performing the Delegated Duties of the General Counsel

U.S. Department of Commerce

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 7260
U.S. Department of Justice
950 Pennsylvania Avenue NW
Washington, DC 20530
(202) 514-3388

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Cases: **Page(s)**

Statutes:

Executive and Administrative Materials:

Other Authorities:

INTRODUCTION

The district court improperly entered a preliminary injunction blocking recent action taken by the President and the Secretary of Commerce to respond to a serious threat to the Nation's security posed by the People's Republic of China (PRC) and the WeChat mobile app, a social-media app owned by Tencent Holdings, Ltd. (Tencent), a Chinese company. The Executive Branch has assessed that WeChat "poses a threat to the national security, foreign policy, and economy of the United States" because the PRC could "exploit[]" the app to "conduct espionage" and "build dossiers on millions of U.S. persons" for intelligence purposes. ER232, 243. The Executive Branch determined that WeChat collects vast amounts of American users' sensitive personal information, and that Tencent has cooperated extensively with the PRC and the Chinese Communist Party (CCP), including by tracking its users and allowing the data collected from their devices to be used to further the PRC's and CCP's surveillance and intelligence projects.

Pursuant to an Executive Order issued by the President, the Executive Branch has assessed that risk to national security as "immitigable" and "high," ER244-45, and the Secretary on that basis identified several prohibited business-to-business transactions related to WeChat. The Identification of Prohibited Transactions precludes mobile app stores from hosting the WeChat app for download in the United States, prevents various current commercial transactions related to optimizing and updating the app, and prohibits a number of potential future transactions that

could support the app or broaden the services provided to U.S. users. Plaintiffs in this case are all current U.S. users, but the restrictions do not prohibit such users from continuing to use the app.

Despite the clear and serious threat to national security identified by the President—and despite the government's measured response to that threat, based on a considered assessment by the Executive Branch—the district court entered a preliminary injunction preventing the restrictions from taking effect solely based on plaintiffs' claim that those regulations would violate their First Amendment rights. The court's acceptance of that argument rests on a series of mistaken premises about the role of the court, the scope of the First Amendment, and the effect of the prohibitions.

The district court fundamentally misunderstood the constitutional issues. The prohibited transactions do not restrict any speech at all; plaintiffs remain free to say whatever they like. Rather, the prohibitions simply limit the efficacy of one particular mobile app that poses a serious national-security threat. The Supreme Court has made clear that the First Amendment "does not prevent restrictions directed at commerce or conduct"—like those in the Identification—"from imposing incidental burdens on speech." *NIFLA v. Becerra*, 138 S. Ct. 2361, 2373 (2018) (quotation omitted). For that reason, the restrictions in the Identification do not implicate the First Amendment.

Even if the First Amendment were to apply, the prohibitions would easily pass muster, given their limited nature, the government's national-security interests, and

the comparatively minor burdens (if any) on plaintiffs' speech. In finding the Secretary's Identification insufficiently tailored, the district court improperly second-guessed the Executive Branch's judgment about what economic regulations are necessary to protect national security, despite repeated admonitions from this Court and the Supreme Court that such judgments are outside the judiciary's ken. *See Hernandez v. Mesa*, 140 S. Ct. 735, 749 (2020) ("Foreign policy and national security decisions are delicate, complex, and involve large elements of prophecy for which the Judiciary has neither aptitude, facilities, nor responsibility." (quotation omitted)).

Finally, even if plaintiffs had presented a valid claim on the merits, the district court abused its discretion in entering injunctive relief because the balance of the equities unquestionably favors the government's, and the public's, interests in preventing the PRC and the CCP from gaining access to vast amounts of Americans' sensitive personal information. The district court's contrary conclusion rests on a fundamental misunderstanding of the restrictions as an "effective ban of WeChat for all U.S. users," ER84, rather than a prohibition on commercial transactions that, at most, causes plaintiffs technological inconveniences that only incidentally burden their expressive activities. Plaintiffs' interests in continued use of the app free from regulations designed to prevent PRC espionage against Americans cannot outweigh the countervailing interests in the Nation's security.

This Court should vacate the preliminary injunction.

STATEMENT OF JURISDICTION

The district court had jurisdiction under 28 U.S.C. § 1331. ER443. The court entered a preliminary injunction on September 19, 2020. ER67. The government filed a timely notice of appeal on October 2, 2020. ER413. This Court has jurisdiction under 28 U.S.C. § 1292(a)(1).

STATEMENT OF THE ISSUE

Whether the district court improperly issued a preliminary injunction that prevents the Executive Branch from prohibiting particular business-to-business transactions with respect to the WeChat mobile app to protect national security, solely because of the potential, incidental burdens of that economic regulation on plaintiffs' expressive activity.

STATEMENT OF THE CASE

A. PRC Threats to National Security and the Executive Branch's Response

1. In recent decades, the United States has increasingly confronted serious national-security threats stemming from the PRC. The PRC seeks "to transform the international order to align with CCP interests and ideology," and its "expanding use of economic, political, and military power" to achieve that objective "harms vital American interests and undermines the sovereignty and dignity of countries and individuals around the world." ER268.

As part of its strategy to "transform the international order," ER268, the PRC harnesses "large China-based, -owned, or -influenced companies," particularly technology companies. U.S.-China Econ. & Sec. Review Comm'n, *The National Security Implications of Investments and Products from the People's Republic of China in the Telecommunications Sector* 7 (Jan. 2011), https://go.usa.gov/x72tG (Doc. 22-3, at 8). Those companies—referred to as China's "national champions"—play a "critical role" in its recent "technology push." ER379 (quotation omitted). The PRC plays a major role in those companies' growth, allowing them to "thriv[e] under light regulation," providing them with "unparalleled access to consumer data," and relying on them to make "large investments" in areas of strategic military and economic importance (such as artificial intelligence, financial technology, and semiconductors). ER379-80.

In return, the PRC expects those companies to "advance state interests" and "state objectives," and has subjected them to "stepped-up government scrutiny and increased pressure to align with [CCP] edicts." ER379, 381. For example, one such edict demands active cooperation with PRC intelligence and security services. Under Chinese law, companies must "comply with Chinese data localization measures that enable CCP access to foreign data" and "cooperate with Chinese security services, even when they do business abroad, creating security vulnerabilities for foreign countries and enterprises." ER274. And those companies must further keep that cooperation secret. *See id.*

2. The federal government has engaged in a concerted effort to combat those unique threats. Congress has recognized that the President must protect the "national security" in the United States' "long-term strategic competition with China" and must formulate policies that combat PRC "information operations" and "economic tools [that] gain access to sensitive United States industries." John S. McCain National Defense Authorization Act for Fiscal Year 2019, Pub. L. No. 115-232, § 1261, 132 Stat. 1636, 2060 (2018). And the Executive Branch has taken a range of actions to protect the Nation's security against those and other threats posed by the PRC and CCP.

The Director of National Intelligence—who oversees the intelligence community—has thus warned of the "potential for Chinese intelligence and security services to use Chinese information technology firms as routine and systemic espionage platforms against the United States and allies." Daniel R. Coats, Director of Nat'l Intelligence, *Worldwide Threat Assessment of the US Intelligence Community* 5 (2019), https://go.usa.gov/x7bcq. The Secretary of State has announced the nationwide need to "remove untrusted applications from U.S. mobile app stores" so as to keep "American[s'] most sensitive personal and business information" protected from "exploitation and theft for the CCP's benefit." Michael R. Pompeo, Sec'y of State, *Announcing the Expansion of the Clean Network to Safeguard America's Assets* (Aug. 5, 2020), https://go.usa.gov/x7cXJ. The multi-agency Committee on Foreign Investment in the United States has, in the past few years, assessed national-security risks arising

from acquisitions by Chinese companies of ownership interests in U.S. companies operating mobile apps and other software dealing in sensitive data—such as StayNTouch (hotel-management application and software). *See, e.g.*, 85 Fed. Reg. 13,719 (Mar. 10, 2020) (presidential order requiring divestment of Chinese acquirer's interests). And the Federal Communications Commission has designated as national-security threats still other PRC companies attempting to operate communications networks in the United States. *See, e.g.*, *In re China Mobile Int'l (USA) Inc.*, FCC 19-38, 2019 WL 2098511 (May 10, 2019) (denying China Mobile application to provide international telecommunications services in the United States); *In re Pacific Networks Corp. & ComNet (USA) LLC*, DA 20-450, 2020 WL 1977097 (Apr. 24, 2020) (directing Pacific Networks and ComNet to show cause why their authorizations to provide common-carrier communications services should not be revoked).

B. Statutory and Regulatory Background

At issue in this case are governmental countermeasures taken under the National Emergencies Act (NEA), Pub. L. No. 94-412, 90 Stat. 1255 (1976) (codified at 50 U.S.C. § 1601 *et seq.*), and International Emergency Economic Powers Act (IEEPA), Pub. L. No. 95-223, tit. II, 91 Stat. 1625, 1626 (1977) (codified at 50 U.S.C. § 1701 *et seq.*), two statutes that give the President broad powers to protect the national security of the United States from foreign actors. They empower the President to declare a national emergency with respect to "any unusual and 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." 50 U.S.C. § 1701(a); *see id.* § 1621(a). Once the President declares an emergency, he may exercise a number of emergency authorities to address the identified threat, including the authority to "regulate, direct and compel, nullify, void, prevent or prohibit, any … transactions involving[] any property in which any foreign country or a national thereof has any interest by any person, or with respect to any property, subject to the jurisdiction of the United States." *Id.* § 1702(a)(1)(B). Violations of those economic regulations or prohibitions are subject to civil or criminal penalties. *See id.* § 1705.

In 2019, the President declared a national emergency under the NEA and IEEPA, finding "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." Exec. Order No. 13,873, 84 Fed. Reg. 22,689, 22,689 (May 15, 2019) (ER393). Specifically, "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." *Id.* The President determined that those actions constitute "an unusual and extraordinary threat to the national security, foreign policy, and economy of the United States." *Id.*; *see* 85 Fed. Reg. 29,321 (May 13, 2020) (renewing the national emergency).

C. WeChat Executive Order and Identification

1. Tencent—one of China's "national champions," ER 379 (quotation omitted), and "one of the largest technology companies in China," ER252—owns the WeChat mobile app. *Id.* WeChat is one of the world's most popular mobile apps, "with a monthly user base of more than 1 billion people" worldwide and a daily active user base of more than 19 million people in the United States. ER446-47. WeChat allows users to engage in a variety of activities, including: communicating via text, voice, and video; posting content such as news stories or photographs; engaging with the content posted by other users; making and receiving certain payments; and using a number of other integrated services, such as video games and health-and-fitness features. *Id.* When users engage with those features, they provide WeChat with extensive access to data related to their activity both within and outside of the app. *See* ER240-41.

On August 6, 2020, the President issued an Executive Order finding "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 his 2019 Executive Order. *See* Exec. Order No. 13,943, 85 Fed. Reg. 48,641, 48,641

(Aug. 6, 2020) (ER262). The President further found that "the spread in the United States of mobile applications developed and owned by companies in the [PRC] continues to threaten the national security, foreign policy, and economy of the United States" and that WeChat posed such a threat. *Id.* The President explained that WeChat "automatically captures vast swaths of information from its users" and that such "data collection threatens to allow the [CCP] access to Americans' personal and proprietary information" and provides the PRC "a mechanism for keeping tabs on Chinese citizens" in the United States. *Id.* Therefore, the President determined, the "United States must take aggressive action against the owner of WeChat to protect our national security." *Id.* The President thus directed the Secretary of Commerce to "identify the transactions" in the United States relating to WeChat that should be prohibited and ordered that the identified transactions "shall be prohibited beginning 45 days after the date of this order" (on September 20, 2020). 85 Fed. Reg. at 48,641-42 (ER262-63).[1]

2. To implement that directive, the Secretary consulted with the Office of the Director of National Intelligence (ODNI) and the Cybersecurity and Infrastructure Security Agency (CISA) of the Department of Homeland Security (DHS). ER232.

[1] The President issued a similar Executive Order against another mobile app—TikTok—that same day, *see* Exec. Order No. 13,942, 85 Fed. Reg. 48,637 (Aug. 6, 2020) (ER 265), and issued an additional presidential order pertaining to TikTok the following week, pursuant to the Defense Production Act, as amended. *See* 85 Fed. Reg. 51,297 (Aug. 14, 2020).

Both agencies provided assessments describing the national-security risks presented by WeChat. *Id.*; *see* ER259 (redacted ODNI assessment), 251 (CISA assessment).[2] In addition, the Secretary of Commerce prepared his own "additional, unclassified threat analysis sufficient to demonstrate the national security risk that Tencent and WeChat present to the United States." ER232. That analysis described the threat posed by Tencent, the vulnerabilities in the WeChat app, and the adverse consequences to national security.

a. Threat. The Secretary explained that PRC espionage activities present "well-recognized" threats to the United States, including "a persistent cyber espionage threat and a growing threat to our core military and critical infrastructure systems." ER235. Those threats stem from the PRC's ability to harness large technology firms (such as Tencent), which PRC intelligence services may use "as routine and systemic espionage platforms against the United States and its allies." *Id.*

The Secretary described the PRC's "use [of] bulk data collection for economic and national security activities that are hostile to the economic and national security interests of the United States." ER235. The PRC can use that data "to glean details about key government personnel and potential spy recruits, or to gain information useful for intelligence targeting and surveillance." ER236. "Large data sets" generated

[2] The government has submitted the full, classified ODNI assessment to the district court, and can upon request submit it to this Court ex parte and in camera pursuant to the statutory protections of IEEPA. *See* 50 U.S.C. § 1702(c).

by bulk collection "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." *Id.*

Those concerns are not theoretical. The PRC has targeted Americans' data in the past, as the Secretary found. In recent years, the Department of Justice has charged Chinese nationals with offenses related to: the hack on Anthem, Inc. (resulting in the theft of 78.8 million Americans' "sensitive personal data"); the hack on Equifax Inc. (resulting in the theft of 145 million Americans' "sensitive personal information"); and the Office of Personnel Management data breach (resulting in the theft of "sensitive personal data of millions of current and former" U.S. government employees). ER236-37. The PRC thus "continues to demonstrate an intent and capability to collect vast quantities of [Americans'] sensitive data" and "is building massive databases of Americans' personal information" by "targeting large-scale databases … [for] intelligence-gathering." ER236.

The Secretary was particularly concerned with Tencent's deep connections with the CCP. One mechanism that the CCP employs to wield "its authority and supervision over nominally private or non-governmental organizations" is a corporate Party Committee, a group formed by "senior CCP members who are given a leadership position inside" a given company and then are responsible for "implement[ing] CCP's policies" and exerting "political pressure in the boardroom." ER237. Tencent's Party Committee is "nationally recognized" and, as of 2017,

"boasted nine general branches, 89 party branches and 3,386 members." *Id.* And it actively recruits members; the company has created an automated internal system for identifying which employees are CCP members. *Id.*

Tencent's CEO—himself a member of the CCP—has "been transparent regarding the company's collaboration with the PRC." ER239. For example, the company has cooperated with PRC authorities to help prosecute dissidents based on social-media posts and to track individuals in Tibet. *Id.* Recent reporting has also "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." ER239; *see* ER288 (independent "technical experiments which reveal that WeChat communications conducted entirely among non-China-registered accounts are subject to pervasive content surveillance"). Tencent's extensive and routine cooperation with PRC authorities, as detailed by the Secretary, only confirmed the threat to data on U.S. persons. *See* ER256-57 (listing examples of cooperation with CCP and PRC intelligence services).

Even if Tencent wished to resist some of the PRC's surveillance demands, it would be required to comply under Chinese law. Under "the 2017 National Intelligence Law," Chinese companies are required to "support, assist in and cooperate in national intelligence work in accordance with the law"—and to "keep confidential the national intelligence work" they know about. ER238 (quotation

omitted). Moreover, Chinese legal authorities permit "Chinese intelligence agencies to take control of an organization's facilities, which includes communications equipment," and require "network operators to store select data within China." *Id.*

b. Vulnerability. The Secretary's memorandum further explained the vulnerabilities in the WeChat app. WeChat "collects and transmits sensitive personal information on U.S. persons, which is accessible to Tencent"—and, eventually, to "a range of third-parties, including regulators and judicial authorities and law enforcement agencies" of the PRC. ER240-41 (quotation omitted). That data includes geolocation information, chat histories, stored photos, health records, financial information, and other "sensitive personal information." *Id.* And WeChat may even, depending on a user's unwitting access permissions, be able to harvest that data when users are not using the app. *Id.* Although WeChat claims to only retain data for relatively short periods of time, those "stated privacy policies may contradict actual function." ER241. PRC authorities have in prior investigations used data that was, according to those written policies, supposed to have been deleted by Tencent. *Id.*

c. Consequence. The Secretary concluded that "WeChat presents an immitigable risk to the national security, foreign policy, and economy of the United States," and further assessed that risk to be "high." ER244-45. Specifically, "[o]ne of the foremost national security risks presented by" WeChat is the "possibility that the PRC government could, through lawful authority, extralegal influence," or PRC intelligence services, "compel Tencent to provide systemic access to U.S. user[s']

sensitive personal information." ER242. And the Secretary assessed that the PRC "would … use [WeChat] for foreign intelligence and surveillance." *Id.*

In sum, "[g]iven 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." ER243. The PRC has collected intelligence on millions of Americans in the past, and WeChat collects massive amounts of sensitive personal information from American users. *Id.* 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," and the PRC has the means to use this data as "a platform to enhance the PRC's ability to identify espionage targets for intelligence collection purposes." *Id.*

The Secretary considered alternative proposals that Tencent itself offered to mitigate the harms to national security. *See* ER562 (Under Seal) (Tencent proposal). Those proposals were technological measures that nonetheless permitted Tencent to "retain ownership" (and thus control) of WeChat and could not be implemented absent "a baseline level of trust" that could not be achieved because "Tencent maintains a deep relationship with the CCP and PRC," and has complied (and must continue to comply) with PRC intelligence services. ER244.

Based on that "immitigable risk," the assessment identified six "prohibitions on certain business-to-business transactions" that it recommended the government adopt

to "deny access to and reduce the functionality of the WeChat mobile app" within the United States "with the objective of preventing collection, transmission, and aggregation of U.S. user data by the WeChat app, Tencent, and [PRC intelligence services]." ER244. Those prohibitions, the assessment explained, are "necessary for the protection of U.S. national security." ER245.

3. Following that recommendation, on September 17, 2020, the Secretary published his Identification of Prohibited Transactions pursuant to the WeChat Executive Order. As relevant here, the Secretary identified six transactions "that are prohibited, effective as of September 20, 2020." ER228.[3] Those prohibitions bar "[a]ny 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" and that involves any of the following:

> 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] In addition to the six prohibitions relevant here, the Identification also reserves the possibility of prohibiting other transactions "at a future date," ER229, but that reservation is not at issue here, ER88.

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 and maritime borders of the United States and its territories; [and]

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.

ER228-29.

Taken collectively, those prohibitions preclude mobile app stores from maintaining WeChat for download; prohibit various current economic transactions in the United States or involving U.S. persons between Tencent and certain businesses that would facilitate the functioning, optimization, or updating of the app; and prohibit—only "in the future," ER246—potential transactions providing WeChat with internet hosting services in the United States (WeChat is currently hosted abroad), a possibly forthcoming mobile-payment function, and any reconstitution of WeChat to circumvent the prohibitions.

The prohibitions do not, however, "require the removal of the app from user devices … where the app has been downloaded prior to the order." ER245. The

restrictions instead permit current U.S. users of WeChat to continue their "use of the WeChat app." *Id.* The Executive thus determined that the prohibitions would not result in the app becoming immediately unusable for current U.S. users, though the government hoped that users would transition to other apps, and the prohibitions "may ultimately make the application less effective over time" for current users. *Id.*

D. Prior Proceedings

On August 21, 2020, following the WeChat Executive Order but before the Identification, plaintiffs filed this action. Plaintiffs are a business and several individuals who are all current U.S. users of WeChat, along with the U.S. WeChat Users Alliance, an alleged organization of current U.S. users recently "founded … to respond to the Executive Order." ER482; *see* ER478, 488, 492, 499, 505 (declarations from plaintiffs confirming current use).

Before the Identification was published, plaintiffs moved in district court for a preliminary injunction, raising, among others, a claim that the forthcoming prohibitions would violate the First Amendment. *See* ER78-79. On September 18, while that motion was pending, the government notified the court of the Secretary's Identification. ER79. Later that day, the court ordered plaintiffs to file an amended complaint and a new motion for a preliminary injunction, and directed the parties to brief the new motion that evening. *See* ER520 (minute entry requiring 3:30 p.m. motion; 5 p.m. amended complaint; 6:30 p.m. opposition).

On September 19, the district court issued a preliminary injunction against the restrictions contained in the Identification. The court concluded that there were "serious questions" going to the merits of plaintiffs' First Amendment challenge. ER81-83 (quotation omitted). The court stated that, in its view, the restrictions failed intermediate scrutiny because they constituted an "effective ban of WeChat for all U.S. users." ER84. And the court addressed plaintiffs' 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," noting that this would be prohibited under the Supreme Court's intermediate-scrutiny precedents. ER82 (citing *City of Ladue v. Gilleo*, 512 U.S. 43 (1994)). By contrast, the court concluded either that plaintiffs were unlikely to succeed, or that the briefing was insufficient to allow the court to find a likelihood of success, on their remaining claims. ER84-85.

Because of the expedited timeframe for the preliminary injunction motion, the district court did not review the Secretary's decisional memorandum supporting the restrictions, which was only subsequently approved for release. *See* ER434. The court nonetheless declared that the government had "scant little evidence" that WeChat "raise[s] significant national-security concerns" "on this record." ER84. The court further stated that, "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." ER86. The court thus held that a

preliminary injunction was warranted to maintain "the status quo." *Id.* This Court and the district court both denied the government's request for a stay of that injunction pending appeal. *See* D.E. 24; ER1; *see also* ER527 (Under Seal).

SUMMARY OF ARGUMENT

Espionage by our foreign adversaries poses a significant threat to the security of the United States, and the WeChat mobile app provides the PRC and CCP with a powerful avenue to collect vast amounts of sensitive personal data that can then be used to the detriment of all Americans. The President and the Secretary of Commerce have acted following thorough deliberations, exercising a well-established statutory authority to protect the Nation's security from PRC efforts to collect intelligence on Americans on a massive scale through WeChat. The district court's preliminary injunction rests on legal errors, improperly hampers those efforts, and facilitates a foreign power's ability to threaten the security interests of the Nation—all in service of plaintiffs' bare preference for the full functionality of a single mobile app.

In issuing that injunction, the district court repeatedly misapprehended the facts and the law. Plaintiffs are unlikely to succeed on the merits of their First Amendment claims, they have failed to show any irreparable harm, and the balance of the equities decidedly favors the government's and the public's interests in safeguarding national security. The injunction should be vacated.

I. Plaintiffs have not shown that they are likely to succeed on their First Amendment claim. The President in promulgating the Executive Order, and the

Secretary in promulgating the Identification of Prohibited Transactions, prohibited only a limited set of commercial transactions with no expressive content. In doing so, they acted pursuant to broad statutory authority to address national emergencies involving inimical foreign actors. And they did so on the basis of the collective experience and judgment of the Executive Branch, which determined that WeChat's large-scale collection, retention, and aggregation of American users' sensitive personal information presents grave national-security risks.

Under well-established First Amendment principles, the restrictions here are not subject to First Amendment scrutiny at all because they are directed at commercial transactions and have (at most) only limited incidental effects on plaintiffs' speech. Any plaintiff, and any other current U.S. user of WeChat, can continue to use the app, and every American remains free to engage in unlimited expression on other platforms. And the general rule that such economic regulation does not implicate the First Amendment applies with particular force in this case, where the regulations are directed at stopping the malicious activity of Tencent and the PRC, both of which are foreign entities that enjoy no First Amendment protection in any event.

Even if the Identification were subject to First Amendment scrutiny, the prohibitions would constitute—at most—a limited, content-neutral time, place, and manner restriction on plaintiffs' speech that is subject to intermediate scrutiny. As the Secretary announced, the government took these steps with the explicitly content-

neutral "objective of preventing collection, transmission, and aggregation of U.S. user data." ER244.

The restrictions are narrowly tailored to advance a significant government interest and they leave open ample alternative channels of communication. The identified national-security interests are of the highest order, and the Executive Branch has made a reasonable judgment that restricting the further growth of WeChat is a necessary step to protect those interests. In rejecting that judgment and speculating that other, narrower proposals could have protected the same interests, the district court improperly second-guessed the national-security determinations of the President and the Secretary. But as the Supreme Court has repeatedly cautioned, the "lack of competence on the part of the courts" to engage in such national-security assessments is "marked." *Trump v. Hawaii*, 138 S. Ct. 2392, 2419 (2018) (quotation omitted). Finally, the restrictions leave open ample alternative channels for communication because plaintiffs remain able to use not only every other app (save this one) but also other communication channels such as web-based applications, email, telephone, and postal mail.

II. Even aside from the district court's errors in evaluating the merits, the court also abused its discretion in granting a preliminary injunction. First, in determining that plaintiffs would suffer irreparable harm absent an injunction, the district court described the restrictions as an "effective ban." ER84. That characterization is wrong, and flatly belied by the record. In reality, plaintiffs will continue to be able to use the

platform for some time even after the prohibitions go into effect, and thus will suffer no irreparable or immediate harm. Second, in balancing the equities, the combination of that misapprehension and the court's inappropriate second-guessing of the Executive Branch's national-security judgment caused the court to elevate plaintiffs' alleged harms and undervalue the government's and the public's interests. When those misunderstandings are corrected, it is clear that the balance of the equities favors the government and the public, not the plaintiffs.

Finally, the equities are particularly out of alignment with respect to the injunction against the first prohibition, which prevents the app from being available in app stores for new downloads. In the near term, that would only negligibly affect plaintiffs, who already have installed the app, but it is the most critical of the prohibitions for protecting the national-security interests of the United States. Therefore, at an absolute minimum, the injunction should be vacated as to that prohibition.

STANDARD OF REVIEW

This Court reviews a preliminary injunction for abuse of discretion, with underlying "legal premises" reviewed de novo and factual findings reviewed for clear error. *Federal Trade Comm'n v. Enforma Nat. Prods., Inc.*, 362 F.3d 1204, 1211-12 (9th Cir. 2004). A plaintiff "must establish that he is likely to succeed on the merits, that he is likely to suffer irreparable harm in the absence of preliminary relief, that the balance of equities tips in his favor, and that an injunction is in the public interest." *Winter v.*

NRDC, Inc., 555 U.S. 7, 20 (2008). This Court treats a motions panel's decision on whether to stay an injunction as "persuasive, but not binding." *East Bay Sanctuary Covenant v. Trump*, 950 F.3d 1242, 1264-65 (9th Cir. 2020).

ARGUMENT

I. PLAINTIFFS HAVE NOT SHOWN A LIKELIHOOD OF SUCCESS ON THEIR FIRST AMENDMENT CHALLENGE TO THE EXECUTIVE BRANCH'S NATIONAL-SECURITY JUDGMENTS

The Secretary of Commerce's Identification of Prohibited Transactions blocks a number of commercial transactions relating to the WeChat mobile app, which provides the PRC with a powerful intelligence asset to collect Americans' sensitive personal data and harm American interests by increasing the potential effectiveness of foreign espionage. A preliminary injunction is "an extraordinary remedy" in all cases, but the one here is all the more so because it inhibits the Executive Branch's efforts to address "new and serious threats to our Nation and its people." *Winter v. NRDC, Inc.*, 555 U.S. 7, 24 (2008). (quotation omitted). In enjoining the Identification based on plaintiffs' First Amendment challenge, the district court erred in both: (A) assuming that the First Amendment applies to the Identification's national-security regulation of commercial transactions and (B) concluding, in any case, that the Identification was insufficiently tailored to withstand intermediate scrutiny.

A. The District Court Erred in Assuming that the First Amendment Applies to the Secretary's Regulation of Commercial Transactions to Protect National Security

It is well established that "[t]he First Amendment does not prevent restrictions directed at commerce or conduct from imposing incidental burdens on speech." *NIFLA v. Becerra*, 138 S. Ct. 2361, 2373 (2018) (quotation omitted); *see also, e.g.*, *Sorrell v. IMS Health, Inc.*, 564 U.S. 552, 567 (2011) (same); *44 Liquormart, Inc. v. Rhode Island*, 517 U.S. 484, 507 (1996) (plurality opinion) (viewing "direct regulation" limiting purchases as "not involv[ing] any restriction on speech"). In this case, the Secretary's Identification, which was promulgated pursuant to substantial national-security authorities to address foreign threats, does no more than regulate certain business-to-business transactions. For that reason, the district court erred in concluding that the restrictions were subject to First Amendment scrutiny at all.

1. The Executive Branch has addressed the national-security threats posed by WeChat solely through the regulation of economic activity. The President here acted pursuant to his "broad authority" under IEEPA "to act in times of national emergency with respect to property of a foreign country." *Dames & Moore v. Regan*, 453 U.S. 654, 677 (1981); *see Micei Int'l v. Department of Commerce*, 613 F.3d 1147, 1154 (D.C. Cir. 2010). Among the core provisions of IEEPA is the authority to "regulate, direct and compel, nullify, void, prevent or prohibit, any … transactions involving any[] property in which any foreign country or a national thereof has any interest by any person, or with respect to any property, subject to the jurisdiction of the United

States." 50 U.S.C. § 1702(a)(1)(B). Based on that statutory language, the Second Circuit has recently explained that "IEEPA authorizes the President to prohibit virtually any commercial transaction that, in his judgment, threatens national security." *United States v. Henry*, 888 F.3d 589, 598 (2d Cir. 2018), *cert. denied*, 139 S. Ct. 2615 (2019). IEEPA permits the President to bar transactions with all nationals and entire governments of a foreign nation, and that authority includes the power to regulate mobile apps susceptible to misuse by those foreign governments. *See Paradissiotis v. Rubin*, 171 F.3d 983, 988 (5th Cir. 1999) (barring "any transaction" with Government of Libya (quotation omitted)); *Consarc Corp. v. U.S. Treasury Dep't*, 71 F.3d 909, 911 (D.C. Cir. 1995) (upholding embargo restrictions on "all Iraqi interests in property within the United States").

The President invoked that authority over economic transactions in the United States in determining 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, … in order to commit malicious cyber-enabled actions." Exec. Order No. 13,873, 84 Fed. Reg. at 22,689 (ER393). The WeChat Executive Order explains the specific threat that "WeChat automatically captures vast swaths of information from its users," and that this "data collection threatens to allow the [CCP] access to" U.S. users' "personal and proprietary information." Exec. Order No. 13,943, 85 Fed. Reg. at 48,641 (ER262). To combat that threat, the President directed the Secretary of Commerce to identify

economic transactions that are necessary to prohibit to protect national security. *Id.* at 48,641-42.

To appropriately identify the necessary prohibited transactions, the Secretary first consulted with other agencies with national-security and intelligence expertise, including ODNI and DHS CISA. The Secretary then determined that WeChat poses a "high" risk to national security, that the PRC "would … use [WeChat] for foreign intelligence and surveillance," and that Tencent is "likely to respond to intelligence requests on U.S. users." ER242, 245.

In discussing those conclusions, the Secretary explained that WeChat collects an "extensive amount of sensitive personal data" on U.S. users, including geolocation data, chat histories, stored photos, health records, financial information, and other "sensitive personal information." ER240-41, 243. That data collection enables the PRC "to build dossiers on millions of U.S. persons" and "to identify espionage targets for intelligence collection purposes." ER243. And collecting that "bulk data" further permits the PRC "to glean details about key government personnel and potential spy recruits, or to gain information useful for intelligence targeting and surveillance." ER236. The Secretary further concluded that the national-security risk was heightened in this case because of Tencent's deep entanglement, and "history of cooperation," with PRC officials and the CCP—and that, even if Tencent were potentially to resist cooperation, the PRC had the legal ability to compel that cooperation anyway. ER242-43.

Based on those assessments, the Executive determined that WeChat's operation in the United States presents serious and novel threats to national security, particularly given Beijing's broader efforts "to reshape the international system in its favor" at the expense of "vital American interests." ER268. To address that threat, the Executive identified a targeted set of economic prohibitions that were "necessary for the protection of U.S. national security." ER245. Those restrictions prohibit mobile app stores from carrying the WeChat app for download in the United States, thus protecting new U.S. users and limiting the relentless flow of sensitive data subject to PRC intelligence collection. In addition, the restrictions prevent app stores from offering software updates to the WeChat app and constrain businesses that facilitate the app's functioning, in order to diminish WeChat's capabilities and encourage current U.S. users to find alternatives to WeChat. *See* ER245-46. The restrictions do not, however, prohibit individuals from continuing to use the platform, even if the effect of the restrictions may be that the app's performance degrades over time as users are unable to update it. *See* ER245.

2. The district court erred in basing its preliminary injunction on plaintiffs' First Amendment challenge, because the Identification—which does not prohibit any plaintiff or current U.S. user from using WeChat or from engaging in the same expression on any other platform—does not implicate the First Amendment at all.

As the Supreme Court has repeatedly confirmed, regulations governing conduct are generally not subject to any First Amendment scrutiny, even when they

also impose incidental burdens on speech. *See, e.g.*, *NIFLA*, 138 S. Ct. at 2373. For example, the Supreme Court has explained that a trespass rule forbidding the reentry of any person with prior civil violations into an otherwise open public forum does not have "anything to do with the First Amendment," even as applied to the entry of persons who wish to engage in expressive activity in the forum. *See Virginia v. Hicks*, 539 U.S. 113, 123 (2003). The Supreme Court explained that barring such a violator from a public forum "no more implicates the First Amendment than would the punishment of a person who has (pursuant to a lawful regulation) been banned from a public park after vandalizing it, and who ignores the ban in order to take part in a political demonstration." *Id.* Similarly, the Court has concluded that "the First Amendment is not implicated" by the government's attempt to apply a general law permitting the closure of public-health nuisances to a bookstore, even though the bookstore indisputably facilitated First Amendment activity. *Arcara v. Cloud Books, Inc.*, 478 U.S. 697, 706-07 (1986).

So too here. The Identification merely applies general national-security laws and regulations to prohibit a variety of commercial transactions related to WeChat, with the purpose of counteracting the PRC's wholesale collection and retention of Americans' sensitive data. And that application of general national-security laws to a mobile app no more implicates the First Amendment than does the application of general trespass laws to protestors or public-health laws to bookstores. Indeed, if anything, the Identification presents an even more straightforward case of economic

regulation than do *Hicks* and *Cloud Books* because current users may continue their "use of the WeChat app," at least in the short term. ER245. At all events, it cannot be that the First Amendment protects an app that threatens national security simply because the app happens to provide users with communicative functionality. In short, the alleged burdens on plaintiffs' speech are purely incidental, and "the First Amendment does not prevent restrictions directed at commerce or conduct"—like those here—"from imposing incidental burdens on speech." *Sorrell*, 564 U.S. at 567.

To be sure, such regulation of commerce or conduct may be subject to First Amendment scrutiny when the regulated conduct itself contains a "significant expressive element," *Cloud Books*, 478 U.S. at 706—as, for example, in the case of a prohibition on burning one's draft card, *see United States v. O'Brien*, 391 U.S. 367 (1968). Or First Amendment scrutiny may apply when the regulation "has the inevitable effect of singling out those engaged in expressive activity"—as, for example, in the case of a "tax imposed on the sale of large quantities of newsprint and ink," *Cloud Books*, 478 U.S. at 704, 706-07; *see Minneapolis Star & Tribune Co. v. Minnesota Comm'r of Revenue*, 460 U.S. 575 (1983). *See also HomeAway.com, Inc. v. City of Santa Monica*, 918 F.3d 676, 685 (9th Cir. 2019) (reiterating the *Cloud Books* framework). Neither is applicable here.

The Identification regulates a set of business-to-business transactions that facilitate WeChat's ability to collect and retain sensitive data. A business's choice to engage in a commercial transaction with another business does not involve

"significant expressive elements." That is why, for example, entering into a contract, even with a media company, does not implicate the First Amendment. *See Cohen v. Cowles Media Co.*, 501 U.S. 663, 672 (1991) (rejecting as "incidental, and constitutionally insignificant" for First Amendment purposes, the application of contract law to enforce "certain kinds of promises"). Likewise, the restrictions do not "single out" individuals who may be engaged in expression. Just as closing a bookstore for public-health reasons does not single out readers generally, or even readers who rely on the bookstore specifically, regulating a mobile app for national-security reasons does not single out its users who are engaged in communicative activities. *See generally Cloud Books*, 478 U.S. at 704-07. Indeed, the Identification imposes commercial restrictions that would equally burden those who use the platform to engage in nonexpressive activity, such as playing video games or using WeChat's e-commerce or health-and-fitness features. Therefore, at most, the burden of the regulation here falls only secondarily on app users engaging in a range of expressive and nonexpressive activity, making this a far cry from the situation where the "burden of [a] tax *inevitably* fell disproportionately—in fact, almost *exclusively*—upon the shoulders of newspapers exercising the constitutionally protected freedom of the press." *Cloud Books*, 478 U.S. at 704 (emphases added).

B. Even Assuming the First Amendment Applies, the District Court Erred in Concluding that the Identification's Restrictions Do Not Withstand Intermediate Scrutiny

Even if the Secretary's Identification implicates the First Amendment, the regulations here easily pass muster under intermediate scrutiny, because they are content neutral, are "narrowly tailored to serve a significant governmental interest," and "leave open ample alternative channels for communication of the information." *Lone Star Sec. & Video, Inc. v. City of Los Angeles*, 827 F.3d 1192, 1197 (9th Cir. 2016) (quoting *Clark v. Community for Creative Non-Violence*, 468 U.S. 288, 293 (1984)).

1. The prohibitions are content neutral

As even the district court seemed to recognize, the Identification is content-neutral because it does not "target speech" of U.S. users "based on its communicative content." *Reed v. Town of Gilbert*, 576 U.S. 155, 163 (2015); *see* ER16-17; *see also* ER38:19-21 (recognizing the issue is whether "content neutral regulations … survive intermediate scrutiny" under narrow tailoring). Instead, the Executive designed each of the targeted commercial prohibitions with the explicitly content-neutral "objective of preventing collection, transmission, and aggregation of U.S. user data by the WeChat app, Tencent, and [PRC intelligence services]." ER244. That objective is independent of the *content* of any WeChat user's speech—including plaintiffs' speech in particular. And of course the prohibitions do not prevent plaintiffs, or anybody else, from communicating their ideas in other ways, including through the full panoply of social-media platforms and other technologies that remain available.

Plaintiffs have urged that the prohibitions restrict the speech of U.S. users based on content, simply because the Executive observed that the PRC could use the app to spread disinformation and propaganda. But although the Secretary briefly discussed PRC disinformation and propaganda efforts related to WeChat in the context of explaining CCP strategic goals, ER243-44, he additionally made clear that "*the* objective" of the regulations was to prevent WeChat's data collection, not to target any content shared on the platform, ER244 (emphasis added).

At all events, the prevalence of CCP disinformation and censorship has nothing to do with the content of any speech by plaintiffs. Plaintiffs do not claim that *they* are engaging in CCP disinformation and censorship. The PRC (a foreign state) and Tencent (a "foreign organization[] operating abroad") also have "no First Amendment rights," and "plaintiffs cannot export their own First Amendment rights to shield foreign organizations." *Agency for Int'l Dev. v. Alliance for Open Soc'y Int'l, Inc.*, 140 S. Ct. 2082, 2088 (2020); *see id.* (explaining that plaintiffs' "prefer[ence]" for affiliating with particular foreign organizations is not enough to subject regulations to First Amendment scrutiny). And even viewed from the perspective of plaintiffs and their ability to interact with the content provided by Tencent or the PRC (or other foreign actors), the Supreme Court has "limited [its] review" of such claims of Americans' "right to receive information" from abroad "to whether the Executive gave a 'facially legitimate and bona fide' reason for its action." *Trump v. Hawaii*, 138 S. Ct. 2392, 2419 (2018) (quoting *Kleindienst v. Mandel*, 408 U.S. 753, 764-65, 769 (1972)).

The national-security concerns identified by the President and the Secretary related to Tencent's collection and retention of Americans' sensitive personal information easily satisfy that deferential standard.

The prohibitions at issue here thus are in no way directed at *plaintiffs*, or the content of their speech, and it is black-letter law that a plaintiff may not ordinarily "rest his claim to relief on the legal rights or interests of third parties." *Kowalski v. Tesmer*, 543 U.S. 125, 129 (2004). That principle applies with special force in this context, where foreign adversaries may seek to turn the Constitution's freedoms against Americans, using First Amendment arguments to cripple the United States' authority to address a serious national-security threat. The PRC's repressive regime has leveraged Chinese companies such as WeChat to engage in widespread surveillance and censorship that are anathema to freedoms recognized in the United States. Just because those efforts have now reached Americans does not mean that the United States' effort to halt the PRC's advances violates the First Amendment rights of Americans generally, let alone plaintiffs specifically.

Plaintiffs have also incorrectly compared the Identification to a prior restraint on speech—a particular form of content restriction. *See* ER68-69. The Supreme Court has explained that the First Amendment affords "special protection" against those laws that "prohibit the publication or broadcast of particular information or commentary"—that is, laws "that impose a 'previous' or 'prior' restraint on speech." *Nebraska Press Ass'n v. Stuart*, 427 U.S. 539, 556 (1976). For example, a court generally

may not enjoin a newspaper from publishing future issues because it has previously published malicious or scandalous material, nor may a municipal theatre refuse to allow the performance of a particular musical because the theatre objects to the content of the show. *See Near v. Minnesota ex rel. Olson*, 283 U.S. 697 (1931) (newspaper injunction); *Southeastern Promotions, Ltd. v. Conrad*, 420 U.S. 546 (1975) (municipal theatre). Because the prohibitions are content-neutral, however, they categorically are outside of the prior-restraint framework. *See Thomas v. Chicago Park Dist.*, 534 U.S. 316 (2002) (explaining that a content-neutral permitting scheme requiring government approval before conducting large-scale events is not a prior restraint). But even setting that aside, the restrictions do not prohibit plaintiffs from engaging in the "publication or broadcast of particular information or commentary" at all, *Nebraska Press Ass'n*, 427 U.S. at 556, much less require plaintiffs to obtain government pre-approval before saying particular things. *Cf. Alexander v. United States*, 509 U.S. 544, 550-51 (1993) (explaining that a forfeiture order entered against an individual who sells obscene material imposes "no prior restraint on" his "ability to engage in any expressive activity he chooses," even if it makes it harder for him to do so).

2. The prohibitions narrowly target specific commercial transactions in aid of national security

The district court erred in holding that the Secretary's restrictions are not narrowly tailored to serve the interests of national security. The national-security interest here is significant. *See Haig v. Agee*, 453 U.S. 280, 307 (1981) (finding it

"'obvious and unarguable' that no governmental interest is more compelling than the security of the Nation"). Yet the court both (a) impermissibly discounted those interests and (b) improperly faulted the Secretary's judgment regarding what transactions were necessary to prohibit based on those interests.

a. The district court gave little consideration to the actual national-security bases underlying the prohibitions. The Supreme Court has made clear that the district court's disregard for those interests is erroneous. Even in constitutional challenges under the First Amendment, the Constitution demands "respect for the Government's conclusions" in "collecting evidence and drawing factual inferences" in matters of "national security and foreign relations." *Holder v. Humanitarian Law Project*, 561 U.S. 1, 34 (2010). The Executive Branch is "uniquely positioned to make principled distinctions" when acting in the national-security realm, including where those distinctions carry constitutional significance, and courts must give significant weight to the Executive's "careful balancing of interests." *Id.* at 35-36.

As the Supreme Court has admonished, when evaluating the strength of the record on "questions of national security, the lack of competence on the part of the courts is marked." *Hawaii*, 138 S. Ct. at 2419 (quotation omitted); *see Boumediene v. Bush*, 553 U.S. 723, 797 (2008) (cautioning that "federal judges" do not "begin the day with briefings that may describe new and serious threats to our Nation and its people"). For that reason, the Supreme Court has repeatedly rejected "plaintiffs' request[s] for a searching inquiry into the persuasiveness of the President's

justifications" where national-security judgments are concerned. *Hawaii*, 138 S. Ct. at 2409; *see Department of the Navy v. Egan*, 484 U.S. 518, 530 (1988) ("[C]ourts traditionally have been reluctant to intrude upon the authority of the Executive in … national security affairs.").

The district court erred, then, in treating plaintiffs' constitutional challenge like one arising in a much less sensitive context and failing to recognize the deference due to the Executive's unique expertise in national security. In so doing, the court concluded merely that it believed there was "scant little evidence" of national-security harms connected to WeChat's operation. ER84.[4] That conclusion improperly disregards the Secretary's careful consultation with other expert agencies including ODNI and DHS CISA. And it ignores the Secretary's own assessment that WeChat poses a "high" national security risk because the PRC could "exploit[]" WeChat "for foreign intelligence and surveillance" and because Tencent is "likely to respond to intelligence requests on U.S. users." ER242, 245.

The district court further erred in demanding "specific evidence" linking WeChat in particular ways to the unique national-security threats posed by the PRC. ER86. That holding is irreconcilable with the Supreme Court's rejection of the

[4] The district court arrived at that conclusion despite not having reviewed much of the material supporting the Secretary's Identification, including his decision memo and the threat assessments prepared by DHS CISA and ODNI. After reviewing those materials in connection with the government's stay motion, the court did not alter its ultimate conclusion but allowed that the evidence in fact "illuminates the threat that Tencent (through WeChat) poses to national security." ER16.

demand for "'specific evidence'" as "a dangerous requirement" that would inhibit "preventive measure[s]" based on the Executive Branch's "informed judgment." *Humanitarian Law Project*, 561 U.S. at 34-35. The Supreme Court thus has emphasized that national-security actions often "confront evolving threats in an area where information can be difficult to obtain and the impact of certain conduct difficult to assess." *Id.* at 34. By necessity, the prohibitions here are in part a preventive measure, seeking to thwart the PRC's bulk collection and aggregation of Americans' sensitive personal information, even assuming Beijing has yet to act on that information in the most egregious ways harmful to American interests. Were the United States required to wait for that widespread espionage against American interests to bear fruit in the most dangerous and palpable ways before acting, it would be far too late. Thus, when the Executive Branch takes such "preventive measure[s]," its "conclusions must often be based on informed judgment rather than concrete evidence" of the type that the district court seemingly demanded. *Id.* at 34-35. And in such a circumstance, the government "is not required to conclusively link all the pieces in the puzzle before [the Judiciary] grant[s] weight to its empirical conclusions." *Id.* at 35.

At bottom, the district court's injunction is undergirded by a manifestly erroneous second-guessing of the Executive Branch's informed judgments about serious threats to national security. Without considering the actual balance that the Executive determined "necessary" to protect national security, the court blocked the prohibitions from proceeding based on plaintiffs' assertion that the Constitution

protects their preference for the unbridled usage of a mobile app. As the Supreme Court has warned, for plaintiffs to establish a likelihood of success on the merits, it is not enough that they "simply disagree with the considered judgment" of national-security officials. *Humanitarian Law Project*, 561 U.S. at 36. Those officials are under "no constitutional mandate to abandon their considered professional judgment" in the face of plaintiffs' contrary views. *Goldman v. Weinberger*, 475 U.S. 503, 509 (1986) (deferring, even in the face of expert testimony to the contrary, to military officials' judgment about the deleterious effects of accommodating plaintiff's request for a religious exemption to a military policy). The district court was wrong here to accept plaintiffs' assertion rather than deferring to the considered judgment of Executive Branch officials charged with protecting national security.

b. The only question is whether the prohibitions in the Identification are sufficiently tailored to address those significant national-security threats. They are. When, as here, the regulations "seek[] to prevent imminent harms in the context of international affairs and national security," the government "'must of necessity paint with a brush broader than it customarily wields in domestic areas.'" *Humanitarian Law Project*, 561 U.S. at 35 (quoting *Zemel v. Rusk*, 381 U.S. 1, 17 (1965)). The Executive is "uniquely positioned to make principled distinctions between activities." *Id.* And the restrictions must be upheld if the Executive has "adequately substantiated [its] determination that, to serve the Government's interest in [national security], it was necessary to prohibit" the particular commercial transactions. *Id.* at 36.

Here, the President and the Secretary made reasonable determinations that the specific prohibitions contained in the Identification "are necessary for the protection of U.S. national security." ER244. For example, prohibiting new U.S. users from downloading the WeChat app stymies PRC efforts to collect intelligence on more Americans. And economic restrictions on updating the app and businesses that facilitate the app's functioning similarly limit WeChat's capabilities while providing an incentive for current U.S. users to move to safer platforms. Those determinations suffice to demonstrate that the government's national-security interests "would be achieved less effectively absent the regulation," which is all that narrow tailoring requires. *Lone Star*, 827 F.3d at 1200 (quoting *Ward v. Rock Against Racism*, 491 U.S. 781, 799 (1989)); *see Humanitarian Law Project*, 561 U.S. at 34 (holding, even under First Amendment strict scrutiny, that "respect for the Government's conclusions" based on "national security and foreign policy concerns" is "appropriate"). And contrary to plaintiffs' suggestions in this litigation, *see* Stay Resp. 15, the fact that the Executive Branch could have imposed even more restrictions on WeChat-related transactions to further its national-security interests does not mean that the prohibitions it did impose somehow fail narrow tailoring. *See Williams-Yulee v. Florida Bar*, 575 U.S. 433, 449 (2015) (even under strict scrutiny, the government "need not address all aspects of a problem in one fell swoop").

The Executive in its informed judgment also declined to adopt two narrower options—Tencent's mitigation proposal and a prohibition limited to government

employees. The district court faulted the Secretary for not adopting those potential alternatives, based on a view that they would be less restrictive. *See* ER16-17. But the question is not, as the court apparently believed, whether other alternatives would have "*arguably* addresse[d] the government's national-security interests," ER16 (emphasis added), as the Executive Branch is under no obligation to jeopardize the Nation's security through half-measures. The decision memorandum indeed made clear that, on the facts of this case, neither of the two proposed alternatives would have been adequate to protect national security.

First, the Secretary considered Tencent's mitigation proposal but concluded that the proposal would not "be sufficient to address the aforementioned national security risk presented by WeChat" because the proposal "still allowed Tencent to retain ownership of WeChat"—and thus significant control of the app. ER244; *see* ER562 (Under Seal) (Tencent proposal). Mitigation proposals are, in essence, agreements that entrust companies with basic responsibilities in service of national security and in place of the government's direct imposition of national-security requirements. *See* John C. Demers, Ass't Att'y Gen., Nat'l Sec. Div., U.S. Dep't of Justice, *Remarks at ACI's Sixth National Conference on CFIUS: Compliance and Enforcement* (July 16, 2020), https://go.usa.gov/x7jYp ("I want to highlight that for mitigation to be a feasible option, we need to have confidence that the party with whom we are engaged can be trusted" and is not "under the jurisdiction of a government that … can compel that company to act in ways that violate its mitigation agreement."). The

Secretary was not required to entrust Tencent with those national-security responsibilities here. Given Tencent's deep ties to the CCP, the PRC legal framework compelling Tencent's confidential cooperation in the PRC's intelligence work, Tencent's continued efforts to support PRC goals, and the PRC intelligence services' continued attempts to collect Americans' sensitive personal information, the Secretary concluded that there is simply not "a baseline of trust" between the United States and Tencent "that would allow for effective mitigation." ER244.

Second, the Secretary's memorandum stated that it had accounted for the DHS CISA assessment. That assessment focused only on the harms to government employees and to the "critical infrastructure" community. ER251-54. Based on that focus, CISA recommended prohibiting WeChat on government devices and in other critical infrastructure operations to "reduce the national security risks," while recognizing that "[f]urther steps are available." ER254. That CISA recommendation was not intended to address, and would not have effectively addressed, any of the broader national-security concerns discussed in the Secretary's memorandum. As the Secretary made clear, the national-security risks posed by WeChat indeed extend far beyond current government employees or people operating critical infrastructure because China obtains substantial strategic value from its systemic collection of millions of Americans' personal data. *See* ER236, 242. Given the Executive's factual conclusions related to "national security and foreign policy concerns"—conclusions for which the courts' "respect" is "appropriate," *Humanitarian Law Project*, 561 U.S. at

34—the Executive properly determined that neither this alternative nor Tencent's own proposal sufficed, and that is all that narrow tailoring requires.

At all events, the First Amendment does not require the government's "elimination of all less restrictive alternatives" but only "that the regulation not burden substantially more speech than is necessary to further the government's legitimate interests." *Board of Trs. of State Univ. of N.Y. v. Fox*, 492 U.S. 469, 478 (1989) (quotation omitted). And in applying that test, the courts "have been loath to second-guess the Government's judgment to that effect," *id.*—a principle all the more applicable where, as here, the government is taking "preventive measure[s]," which "must often be based on informed judgment rather than concrete evidence" but which nevertheless are entitled to respect from the Judiciary, *Humanitarian Law Project*, 561 U.S. at 34-35.

3. The prohibitions leave open ample alternative channels of communication

The restrictions in the Identification also leave open multiple alternative channels for communication. The Identification involves economic restrictions on a single mobile app, leaving untouched numerous other prevalent avenues of communication, from physical mail to electronic mail, from telephone calls to video calls, and including many other mobile apps, web-based applications, or social-media platforms. Individuals in the United States—even in the Chinese-American community—have long had communication options that are available to them.

Even limiting the analysis to other mobile apps, plaintiffs still have ample alternatives—including Facebook, Facebook Messenger, FaceTime, Instagram, Twitter, Google groups and Google Hangouts, Line, Telegram, Signal, Snapchat, Zoom, Skype, iChat, and WhatsApp, among others. ER400 n.2. And even limiting it further to mobile apps readily available in the PRC (assuming that is relevant to the First Amendment analysis at all), plaintiffs may use Signal, iMessage, Line, Wickr, Xiaomi Mitalk, Zoom, and Skype. *Id.* Moreover, plaintiffs are all current users of WeChat, which means that they may continue to use the app for now, even if the app may degrade technologically over time.

The district court improperly elevated plaintiffs' mere *preference* for using WeChat (with peak functionality) because of its apparent prevalence in the Chinese-American community. But this Court has made clear that such a preference is not sufficient to invalidate a regulation under the First Amendment. *See Lone Star*, 827 F.3d at 1202 (holding that a regulation need not ensure the availability of a "preferred method of communication" to satisfy judicial review). This Court has instead warned that courts may "invalidat[e] government regulations for failing to leave open ample alternative channels" only where a "regulation forecloses an entire medium"—not merely a single platform—"of public expression across the landscape of a particular community or setting." *G.K. Ltd. Travel v. City of Lake Oswego*, 436 F.3d 1064, 1074 (9th Cir. 2006) (cleaned up). Similarly, although the PRC may have imposed some restrictions on the use of some of those alternative apps in China, plaintiffs have not

demonstrated that there is no alternative method of communicating with individuals in China beyond WeChat. And in any event, it would be a perverse result if the PRC's ability to stifle other avenues of communication to its populace in China could somehow result in special First Amendment protection for the PRC's hand-picked, state-monitored avenue for communication in the United States. In other words, the PRC's efforts to funnel communications through limited channels to facilitate surveillance does not endow special protections on those channels. Plaintiffs should not be able to leverage repressive censorship policies to demand First Amendment protection for their own continued unrestricted use of this particular app—use that prevents the government from addressing serious national-security risks.

II. THE REMAINING EQUITABLE FACTORS REQUIRE VACATUR OF THE OVERBROAD PRELIMINARY INJUNCTION

A preliminary injunction is an "extraordinary remedy that may only be awarded upon a clear showing that the plaintiff is entitled to such relief." *Winter*, 555 U.S. at 22. Indeed, a "plaintiff seeking a preliminary injunction must establish that he is likely to succeed on the merits," *id.* at 20, and this Court has recognized that likelihood of success is "the most important factor," *California ex rel. Becerra v. Azar*, 950 F.3d 1067, 1083 (9th Cir. 2020) (en banc) (quotation omitted). Plaintiffs are not entitled to injunctive relief here because, as explained above, their claims are meritless. But even if plaintiffs could demonstrate a likelihood of success on the merits, they are not entitled to injunctive relief "as a matter of course." *Winter*, 555 U.S. at 32 (quotation

omitted). In balancing the equities as to plaintiffs, the government, and the public in determining whether relief is warranted, courts "should pay particular regard for the public consequences." *Id.* at 24 (quotation omitted).

The district court held that plaintiffs were entitled to a preliminary injunction because, in its view, they raised "serious questions" on the merits and the equities favored plaintiffs. ER17, 81-83 (quotation omitted). That equitable balancing was incorrect, where the government and the public have the utmost interest in preventing espionage from the PRC and where plaintiffs claim only an interest in a more functional mobile app. And the court's balancing was even more inappropriate because, under this Court's "serious questions" test, a party seeking a preliminary injunction show both "serious questions going to the merits" and that "the balance of hardships tips sharply in [her] favor." *Alliance for the Wild Rockies v. Cottrell*, 632 F.3d 1127, 1131 (9th Cir. 2011) (quotation omitted).[5] The district court found only that the "balance of the equities favors the plaintiffs," ER86, and though the court later stated

[5] The government acknowledges that this Court has concluded that "the 'serious questions' version of the sliding scale test for preliminary injunctions remains viable after the Supreme Court's decision in *Winter*." *Alliance for the Wild Rockies*, 632 F.3d at 1134. The government respectfully disagrees with that conclusion, which binds this panel. But even under the "serious questions" sliding-scale test, plaintiffs are not entitled to an injunction because they fail to satisfy the most important requirement of success on the merits, *see California*, 950 F.3d at 1083, and because the equities tilt in the government's favor—not in plaintiffs' favor (much less "sharply" in their favor, as required under that test).

that the equities "sharply" favored plaintiffs, ER17, it did not explain that bare statement.

Under any metric, however, the district court abused its discretion in concluding that a preliminary injunction was warranted, both because it misapprehended the limited effect that the prohibitions will have on the plaintiffs and because it failed to adequately grasp the government's, and the public's, substantial interest in combatting the national-security threats posed by WeChat. A proper assessment demonstrates that the plaintiffs will suffer no irreparable harm from the restrictions and that, even assuming their alleged harms would occur, the balance of the equities in fact favors the government's and the public's interests. And the court's abuse of discretion is especially pronounced with regard to its decision to enjoin the first prohibited transaction under the Identification, because enjoining that prohibition is not at all necessary to redress plaintiffs' claimed First Amendment harms.

1. The district court erroneously viewed the alleged harm to plaintiffs as if the regulations imposed an "effective ban of WeChat for all U.S. users." ER84. But as the Secretary made clear, the restrictions do not prohibit "use of the WeChat app" and do "not require the removal of the app from user devices" where "the app has been downloaded prior to the order." ER244-45. Instead, as relevant here, they restrict only future downloading of the app, as well as various commercial transactions related to optimizing or updating the app's functionality. As the Secretary recognized, those

"prohibitions may ultimately make the application less effective," ER245, but they do not block current users' access to the app.

Because plaintiffs are all current users of the WeChat app, they will suffer no immediate harm from the prohibitions. They may continue to use the app in its current form, even if the app degrades technologically over time. And because plaintiffs may continue to use the app for expressive activities, the only asserted harm relied on by the district court does not exist. *See* AER86 (only identifying as irreparable harm the "immediate threat" of "the elimination of [plaintiffs'] platform for communication"). That alone requires reversal of the order granting a preliminary injunction. *See Winter*, 555 U.S. at 22 (holding that "plaintiffs seeking preliminary relief" are "require[d]" to "demonstrate that irreparable injury is likely in the absence of an injunction.").

2. The inadequacy of plaintiffs' claims of irreparable harm is thrown into even starker relief when contrasted with the clear and documented harms to the government—and to the public interest, which "merge[s]" with the government's interest, *Nken v. Holder*, 556 U.S. 418, 435 (2009). The Executive Branch has used its collective experience and judgment to conclude that WeChat's extraordinarily vast collection and retention of Americans' personal information poses an unacceptable risk to national security by putting that sensitive data at the fingertips of the CCP and the PRC. Under the injunction, WeChat will continue to gather extensive data on U.S. users—and will be able to augment its data collection every day as new American

users download the app—and will, in turn, aid the PRC's efforts to "conduct espionage" and "build dossiers on millions of U.S. persons" for intelligence purposes. ER243. That harm is clear and irreparable, and is exacerbated by the fact that there is no present mechanism for the government to require new users to remove WeChat, or to recover user data acquired by the PRC, even if the government ultimately prevails in this litigation.

Those harms were, as is discussed above, *see supra* pp.36-39, improperly discounted by the district court, which repeatedly and inappropriately refused to give appropriate respect to the "evaluation of the facts by the Executive" regarding "sensitive and weighty interests of national security and foreign affairs." *Humanitarian Law Project*, 561 U.S. at 33-34. When the Executive Branch's national-security conclusions are given appropriate deference, the harms to the government and the public from the continued operation of WeChat would outweigh any harm that plaintiffs would suffer even if the government had banned the app entirely. As it is, the government's and public's harms outweigh any limited harms that plaintiffs might experience from the technological degradation that would be the only short-term effect of the prohibitions on current users such as plaintiffs.

3. At a minimum, the district court abused its discretion in enjoining the first prohibited transaction under the Identification, which involves the hosting of WeChat on mobile app stores for downloads and updates, because enjoining the first prohibition is not necessary to redress plaintiffs' claimed First Amendment harms,

and the government's interest in having that prohibition take effect is especially weighty.

Article III demands that a court's remedy must "be limited to the inadequacy that produced the injury in fact that the plaintiff has established." *Lewis v. Casey*, 518 U.S. 343, 357 (1996). And equitable principles likewise require that an injunction "be no more burdensome to the defendant than necessary to provide complete relief to the plaintiffs." *Madsen v. Women's Health Ctr., Inc.*, 512 U.S. 753, 765 (1994) (quotation omitted). That limit applies with special force to injunctions that impede the Executive Branch's ability to act in the national-security context. *See U.S. Dep't of Def. v. Meinhold*, 510 U.S. 939, 939 (1993) (partially staying injunction against military policy to limit any relief to the plaintiff).

The first prohibition inhibits only *new* U.S. users from downloading WeChat. But plaintiffs, who are all *current* users of WeChat, are not substantially injured by that prohibition. Although the first prohibition also limits the availability of future updates to the app, the First Amendment does not entitle the plaintiffs to an injunction that prohibits the government from addressing serious national-security threats merely to allow WeChat to continue evolving through such updates—and equitable principles forcefully caution against such an injunction that "will alter, rather than maintain, the status quo." *Tom Doherty Assocs. v. Saban Entm't, Inc.*, 60 F.3d 27, 33 (2d Cir. 1995); *contra* ER86 (maintaining that the injunction preserves "the status quo").

By contrast, while the plaintiffs' interests are at their nadir with respect to the first prohibition, the interests of the government and the public are at their acme. Although current users have already exposed some of their data to WeChat, the first prohibition—which requires app stores to remove the app and thereby prevent new downloads—is critical to ensure that additional American users do not suffer the same fate. Therefore, given the government's clear national-security interest in limiting WeChat's ongoing ability to increase the pool of sensitive data it collects from American users, any minimal injury sustained by plaintiffs from the first prohibition is insufficient to support the full breadth of injunctive relief, and the injunction should at least be vacated as to that prohibition.

CONCLUSION

For the foregoing reasons, the preliminary injunction should be vacated.

Respectfully submitted,

Of Counsel:

MICHAEL J. WALSH, JR.
Performing the Delegated Duties of the General Counsel

U.S. Department of Commerce

JEFFREY BOSSERT CLARK
Acting Assistant Attorney General

DAVID L. ANDERSON
United States Attorney

H. THOMAS BYRON III
DENNIS FAN

/s/ Sean Janda
SEAN JANDA
Attorneys, Appellate Staff
Civil Division, Room 7260
U.S. Department of Justice
950 Pennsylvania Avenue NW
Washington, DC 20530
(202) 514-3388
sean.r.janda@usdoj.gov

OCTOBER 2020

STATEMENT OF RELATED CASES

Pursuant to Ninth Circuit Rule 28-2.6, appellants state that they know of no related case pending in this Court.

/s/ Sean Janda
SEAN JANDA

CERTIFICATE OF COMPLIANCE

This brief complies with the type-volume limit of Federal Rule of Appellate Procedure 32(a)(7)(B) and Circuit Rule 32-1(a) because it contains 12,326 words. This brief also complies with the typeface and type-style requirements of Federal Rule of Appellate Procedure 32(a)(5) and (6) because it was prepared using Microsoft Word 2016 in Garamond 14-point font, a proportionally spaced typeface.

/s/ Sean Janda
SEAN JANDA