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 and WILBER ROSS, in his official capacity as Secretary of Commerce,

DEFENDANTS- APPELLANTS

On Appeal from the United States District Court
District for Northern California, San Francisco
3:20-cv-05910-LB

Hon. Lauren D. Beeler, Magistrate Judge

BRIEF OF AMICI CURIAE THE ELECTRONIC FRONTIER FOUNDATION, THE CENTER FOR DEMOCRACY & TECHNOLOGY, AND THE INTERNET SOCIETY IN SUPPORT OF PLAINTIFFS-APPELLEES AND AFFIRMANCE

Avery Gardiner
CENTER FOR DEMOCRACY & TECHNOLOGY
1401 K St. NW, Suite 200
Washington, DC 20005

Andrew Crocker
Hannah Zhao
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Email: andrew@eff.org
Telephone: (415) 436-9333
Fax: (415) 436-9993

Counsel for Amici Curiae

CORPORATE DISCLOSURE STATEMENT

Pursuant to Rule 26.1 of the Federal Rules of Appellate Procedure, amici state that they do not have a parent corporation and that no publicly held corporation owns 10% or more of their stock.

Dated: December 4, 2020

By: /s/ *Andrew Crocker*
Andrew Crocker

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Executive Orders

Other Authorities

STATEMENT OF INTEREST OF AMICI[1]

The Electronic Frontier Foundation ("EFF") is a non-profit civil liberties organization with more than 30,000 dues-paying members that has worked for 30 years to ensure that technology supports freedom, justice, and innovation for all people of the world. EFF has campaigned both in the United States and worldwide against ill-considered efforts to block, filter, or degrade access to the public Internet. EFF also works to support digital security and fight censorship and overbroad surveillance, including assistance with training and publicizing human rights violations against digital activists and technologists.

The Center for Democracy & Technology ("CDT") is a nonprofit public interest group that seeks to put democracy and individual rights at the center of the digital revolution. CDT supports laws, corporate policies, and technical tools that protect the civil liberties of internet users and represents the public's interest in maintaining an open internet. In furtherance of this mission, CDT supports legal and policy decisions that preserve individual rights, are based on a thorough understanding of how technologies work, and promote the overall security of the internet and its users.

---

[1] Pursuant to Federal Rule of Appellate Procedure Rule 29(a)(4)(E), amici certify that no person or entity, other than amici curiae, their members, or their counsel, made a monetary contribution to the preparation or submission of this brief or authored this brief in whole or in part. The parties have consented to the filing of this brief.

The Internet Society ("ISOC") is a non-governmental global organization headquartered in Reston, Virginia and Geneva, Switzerland for the worldwide coordination of, and collaboration on, Internet issues, standards, and applications. With more than 75,000 members, 131 voluntary Chapters and Special Interest Groups, and 98 organizational members in over 150 countries of the world, ISOC serves to assure the beneficial, open evolution of the global Internet and its related internetworking technologies. It has issued statements on both the TikTok and WeChat bans[2] as well as on the more general "US Clean Network Program," which would similarly ban U.S. entities from engaging in similar activities with any Chinese entity.[3]

INTRODUCTION

Amici are organizations dedicated to ensuring that individuals around the world can use the Internet and other technology to communicate freely and securely. Amici agree with and support the arguments made by the Plaintiffs-Appellees, WeChat users in the United States, that the U.S. government's orders

---

[2] Internet Society, *U.S. Administration ban of TikTok and WeChat is a direct attack on the Internet* (Sep. 18, 2020), https://www.internetsociety.org/news/statements/2020/internet-society-u-s-administration-ban-of-tiktok-and-wechat-is-a-direct-attack-on-the-internet.

[3] Internet Society, Internet Society Statement on U.S. Clean Network Program (Aug. 7, 2020), https://www.internetsociety.org/news/statements/2020/internet-society-statement-on-u-s-clean-network-program/.

targeting WeChat violate the First Amendment. They write separately to explain how these orders are also dangerous and ill-conceived as a technical matter. If allowed to go into effect, the Commerce Department's Identification of Prohibited Transactions to Implement Executive Order 13943 ("Prohibited Transactions"), 2-ER-228–29, will make not just U.S. WeChat users but all users of the Internet less secure than they are today. The Prohibited Transactions also set a dangerous precedent that misunderstands the fundamental interconnectedness of the Internet, undermines longstanding U.S. Internet freedom foreign policy goals, and worsens global fragmentation of the Internet.

ARGUMENT

I. BANNING WECHAT FROM APP STORES PUTS USERS AT RISK AND MAKES THE INTERNET LESS SECURE.

Security experts and the government itself have long emphasized the critical role of software updates in the Internet's security infrastructure. But the Commerce Department's "Prohibited Transaction 1," which would prevent WeChat users from receiving application security updates, goes directly against that body of expertise. The result is that U.S. WeChat users will be left uniquely vulnerable to the very harm that the government claims that it is trying to prevent: the unauthorized access of WeChat users' personal information. In turn, Prohibited Transaction 1 undercuts the security community's longstanding efforts to impress upon users the critical importance of installing security updates from software

developers. Given the fundamentally interconnected nature of the Internet, the result of Prohibited Transaction 1 is that it would likely make the Internet as a whole less secure.

A. Preventing WeChat from issuing security updates leaves WeChat's 19 million U.S. users vulnerable to bad actors and weakens security across the Internet.

Internet security bears many similarities to public health.[4] Just as vaccines can prevent the spread of a virus, software updates can prevent bad actors from compromising vulnerable devices, and then using those devices to cause further harms, including to other devices they interact with. But Prohibited Transaction 1 takes the possibility of updates off the table for WeChat users in the United States and thus fails to consider the serious potential security risks to these users.

For a number of reasons, mobile devices have become a prime target for bad actors. As a recent assessment of the mobile security landscape explains:

> mobile devices [. . .] often do not have access to the same level of security monitoring as desktop computers and servers. In fact, the successful compromise of mobile devices provides more extensive access to large amounts of personal data, as they often aggregate multiple data sources (such as email accounts) along with mechanisms for authenticating with other services as part of two-factor authentication capability. Furthermore, many devices can also provide the geographic location of their owners through access to global positioning service hardware and cell tower information. This density

[4] Christopher Soghoian, *The technology at the heart of the Apple-FBI debate, explained*, Wash. Post (Feb. 29, 2016), https://www.washingtonpost.com/news/the-switch/wp/2016/02/29/the-technology-at-the-heart-of-the-apple-fbi-debate-explained.

> of personal information offers an attractive target to a range of adversaries, leading to an uptick in both targeted and commercial mobile malware families.[5]

In this environment, U.S. WeChat users would be especially vulnerable targets under the Commerce Department's order.[6] First, because it would be widely known that U.S. WeChat users are running software that will not be patched, bad actors will have extra incentives to uncover and exploit vulnerabilities in the WeChat application. Second, as WeChat will continue to provide security patches to its non-U.S. users, experts will likely be able to reverse engineer those patches and derive information about vulnerabilities that the patches remedy.[7] To be sure,

---

[5] Crowdstrike, *2019 Mobile Threat Landscape Report: A Comprehensive Review Of Mobile Malware Trends* 3 (2019), https://www.crowdstrike.com/resources/reports/mobile-threat-report-2019/.

[6] Amici agree with the WeChat Users that the purpose of the Prohibited Transactions is to completely "shut down" WeChat as soon as possible. WeChat Users' Br. at 22. Despite its stated intent, though, the government claims that individual users are likely to attempt to use as the application for up to two years even as its functionality quickly degrades. 1-ER-12. In fact, the possible delayed effects of the Prohibited Transactions merely underscore their constitutional infirmity. WeChat Users' Br. at 34; *see also N.Y. Times Co. v. United States (Pentagon Papers),* 403 U.S. 713, 733 (1971) (Stewart, J., concurring) (noting that efficacy of prior restraint was "doubtful at best"). In any case, it is difficult to predict how long an individual may continue to use the app without receiving updates, and even as the WeChat application is deprived of U.S.-based hosting, content delivery, and other network services. *See* Section II, *infra.* Amici's concerns about the security vulnerabilities apply regardless of whether the government's prediction is accurate.

[7] *See, e.g.,* David Brumley, et al*, Automatic Patch-Based Exploit Generation Is Possible: Techniques and Implications*, IEEE Symposium on Security and Privacy (May 2008), http://bitblaze.cs.berkeley.edu/papers/apeg.pdf.

the complexity of modern computing and human fallibility make bugs inevitable. But it is simply irresponsible to subject U.S.-based WeChat users to such increased risk as the app degrades.

Countless high-profile security incidents in recent years have demonstrated the importance of allowing users to install official updates (like those available from the Apple or Google stores). For example, a 2015 security vulnerability in Android phones called Stagefright affected at least 950 million devices, a discovery the FTC described as "a seminal moment for the industry."[8] In response, the companies that produce devices that use Android software initiated a massive effort to patch vulnerable devices.[9] But even as companies like Apple and Google have taken steps to better secure mobile operating systems against serious vulnerabilities, attackers have increasingly sought to exploit vulnerabilities in apps, particularly messaging apps like WhatsApp and Signal—and WeChat as well.[10]

---

[8] FTC, *Mobile Security Updates: Understanding the Issues* 8 (Feb. 2018), https://www.ftc.gov/system/files/documents/reports/mobile-security-updates-understanding-issues/mobile_security_updates_understanding_the_issues_publication_final.pdf.

[9] Russell Brandom, *How the Stagefright bug changed Android security*, The Verge (Aug. 5, 2015), https://www.theverge.com/2015/8/5/9099627/google-stagefright-android-vulnerability-protect-patch.

[10] Dan Goodin, *Zeroday exploit prices are higher than ever, especially for iOS and messaging apps*, Ars Technica (Jan. 8, 2019),https://arstechnica.com/information-technology/2019/01/zeroday-exploit-prices-continue-to-soar-especially-for-ios-and-messaging-apps.

Earlier this year, the media reported that Amazon CEO Jeff Bezos's iPhone had been breached in 2018 through a vulnerability in the popular messaging application WhatsApp.[11] In recent years, WhatsApp has disclosed and patched a number of security flaws, issuing 15 security advisories in 2020,[12] 8 in 2019, and 5 in 2018.[13] Similarly, the revelation that a series of flaws in iPhone software were exploited to surveil members of China's Uyghur population in 2019 reportedly drove Apple to release updates fixing those weaknesses.[14]

Prohibited Transaction 1 also harms security by incentivizing users—new and existing—to seek to download the WeChat app from unofficial sources, a practice known as sideloading. In addition to offering updates from developers, official app stores implement guardrails to protect users from counterfeit or modified apps that deliver malware, secretly siphon user data, or otherwise harm

---

[11] Stephanie Kirchgaessner, *Jeff Bezos hack: Amazon boss's phone 'hacked by Saudi crown prince,'* The Guardian (Jan. 22, 2020), https://www.theguardian.com/technology/2020/jan/21/amazon-boss-jeff-bezoss-phone-hacked-by-saudi-crown-prince.

[12] WhatsApp, *Security Advisories 2020 Updates*, https://www.whatsapp.com/security/advisories/2020/.

[13] WhatsApp, *Security Advisories Archive*, https://www.whatsapp.com/security/advisories/archive/.

[14] Zack Whittaker, *Sources say China used iPhone hacks to target Uyghur Muslims*, Tech Crunch (Sept. 1, 2019),https://techcrunch.com/2019/08/31/china-google-iphone-uyghur.

devices.[15] While sideloading is not inherently dangerous, users in the U.S. seeking to update or newly install WeChat will likely download the application from third-party software repositories outside of the United States. This further raises the prospect of users downloading malicious updates or counterfeit versions of the application. Indeed, researchers have specifically identified the prevalence of sideloading from third-party app stores in China as a significant source of malware infections.[16]

As the WeChat mobile application degrades over time without receiving further updates, it will become a source of insecurity not just for the mobile device on which it resides, but other users as well. These insecurities can be leveraged by malicious attackers using malicious software—malware—to mount a variety of attacks that can destabilize the Internet and services that use it. This includes compromised devices participating in a botnet—a group of devices that a malicious attacker uses in concert to attack other computers on the Internet—to launch

[15] David Nielo, *How to Install Apps From Outside Your Phone's App Store*, Wired (Aug. 9, 2020), https://www.wired.com/story/install-apps-outside-app-store-sideload/.

[16] Noah Gamer, *Stay away from third party app stores*, Trend Micro (Mar. 8, 2016), https://blog.trendmicro.com/stay-away-from-third-party-app-stores; *see also* Alfred Ng, *Your smartphones are getting more valuable for hackers*, CNET (Mar. 8, 2018), https://www.cnet.com/news/your-smartphones-are-getting-more-valuable-for-hackers.

distributed denial of service ("DDOS") attacks, steal credentials, and perform ransomware attacks.[17]

The security imperative for allowing users to download apps and updates from official app stores is clear. As a blue-ribbon task force appointed by President Obama put it, "Eliminating the vulnerabilities—'patching' them—strengthens the security of US Government, critical infrastructure, and other computer systems."[18]

B. Preventing WeChat from issuing security updates to its U.S. users contravenes longstanding U.S. government policy.

The U.S. government is well aware that mobile applications are a source of insecurity in mobile devices. In 2015, Congress directed the Department of Homeland Security to issue a study of the security threats to government mobile devices.[19] That study laid out "several examples of vulnerabilities in software that expose the user to excessive risk."[20]

---

[17] *See, e.g.,* Danny Palmer, *This huge Android trojan malware campaign was discovered after the gang behind it made basic security mistakes*, ZDNet (Oct. 3, 2019), https://www.zdnet.com/article/a-huge-android-trojan-malware-campaign-was-discovered-after-the-gang-behind-it-made-basic-security-mistakes.

[18] President's Review Group on Intelligence and Communications Technologies, *Liberty and Security in a Changing World* 220 (Dec. 12, 2013), https://obamawhitehouse.archives.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf.

[19] DHS, *Study on Mobile Device Security* 1 (Apr. 2017) (citing § 401, Pub. L. 114-113, 129 Stat. 2244, 2977-78 (2015)), https://www.dhs.gov/sites/default/files/publications/DHS%20Study%20on%20Mobile%20Device%20Security%20-%20April%202017-FINAL.pdf.

[20] *Id.* at 28.

Recognizing the risk of insecure mobile applications, the government has consistently urged companies to provide security updates to consumers,[21] going back as far as two decades.[22] In a 2015 report, the Federal Trade Commission stated that "[o]utdated software undermines security" and that "[t]he solution is to update it regularly and implement third-party patches."[23] In 2018, the FTC devoted an entire study to the importance of mobile security updates, concluding unequivocally that "[p]atching is essential to maintaining the security of software-based products."[24] And it is unsurprising that the U.S. Cybersecurity & Infrastructure Security Agency advises users and administrators that it is a best practice to stop using software when a company ceases to service its software product through updates.[25] But according to the government's own estimation,

---

[21] FTC, *Mobile Security Updates: Understanding the Issues*, *supra* note 8, at 11–14.

[22] *See, e.g.*, U.S. Gen. Accounting Office, *Information Security-Effective Patch Management Is Critical to Mitigating Software Vulnerabilities* (Sep. 10, 2003), https://www.gao.gov/products/GAO-03-1138T.

[23] FTC, *Start with Security: A Guide for Business* 12 (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.

[24] FTC, *Mobile Security Updates: Understanding the Issues*, *supra* n.8 at 20.

[25] U.S. Cybersecurity and Infrastructure Agency, *Security Tip (ST04-006): Understanding Patches and Software Updates* (Nov. 19, 2019), https://us-cert.cisa.gov/ncas/tips/ST04-006.

WeChat users in the United States will not immediately abandon the app, placing them at heightened risk.

The government has also recognized the importance of software security updates in encouraging companies to adopt programs that allow for the disclosure of vulnerabilities. For example, the National Institute of Standards and Technology endorsed the development of such a program in the 2018 revision to its cybersecurity guidance for critical infrastructure owners and operators.[26] Likewise, the FTC recommends that "companies should communicate and coordinate with the security research community as part of a continuous process of detecting and remediating software vulnerabilities."[27] These programs are of critical importance because they can provide companies the ability to issue a patch before a vulnerability can be exploited by bad actors.

The government's guidance in this area is the product of decades-old efforts to keep U.S. Internet infrastructure secure. The Commerce Department's Prohibited

---

[26] NIST, *Cybersecurity Framework Version 1.1, RS.AN-5*, (Apr. 16, 2018), https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

[27] FTC, *Public Comment on NTIA Safety Working Group's "Coordinated Vulnerability Disclosure 'Early Stage' Template,"* (Feb. 15, 2017), https://www.ftc.gov/system/files/documents/advocacy_documents/ftc-staff-comment-national-telecommunications-information-administration-regarding-safety-working/170215ntiacomment.pdf.

Transactions are an about-face from ordinary security policies, putting Internet users at considerable risk.

C. Preventing U.S. WeChat users from updating their apps undermines the U.S. government's longstanding efforts to educate the public about the importance of online security hygiene.

Security updates are only effective if users download them. But users frequently do not understand the importance of updates and avoid installing them. At a hearing, the late Senator John McCain noted a widely shared frustration with app updates when he asked Apple CEO Tim Cook: "Why the hell do I have to keep updating my apps on my iPhone all the time and why you don't fix that?"[28] Indeed, one study found that fully 59% of Android users had chosen not to update an application despite the availability of an update, while another found that ten percent of users *never* update.[29] In order to overcome users' reluctance to install updates, researchers studying the issue have found that educating users about the

[28] Alexis Kleinman, *John McCain Asks Apple CEO Tim Cook: 'Why The Hell Do I Have To Keep Updating My Apps'?*, Huffington Post (May 21, 2013), https://www.huffpost.com/entry/john-mccain-apple_n_3314325.

[29] Yuan Tian, et al., *Supporting Privacy-Conscious App Update Decisions with User Reviews* 55, Procs. of the 5th Annual ACM CCS Workshop on Security and Privacy in Smartphones and Mobile Devices (Oct. 2015), https://dl.acm.org/doi/pdf/10.1145/2808117.2808124; Aaron Smith, *Password management and mobile security*, Pew Research Center, (Jan. 26, 2017), https://www.pewresearch.org/internet/2017/01/26/2-password-management-and-mobile-security.

ways in which they will benefit from an update is an important factor in persuading them to download security updates.[30]

In recent years, the U.S. government has made considerable effort to educate the public on the importance of basic online security hygiene practices like updating apps—as have organizations dedicated to protecting user security and privacy.[31] As part of a recent consumer protection campaign, the FTC instructed mobile device users to update their applications since they are "access points for criminals to enter your devices."[32] Similarly, the second top priority on the Department of Homeland Security's "Mobile Security Tip Card" instructs:

> **Keep software up to date.** Install updates for apps and your device's operating system as soon as they are available. Keeping the software on your mobile device up to date will prevent attackers from being able to take advantage of known vulnerabilities.[33]

---

[30] Kami Vaniea & Yasmeen Rashidi, *Tales of Software Updates: The Process of Updating Software*, 2016 Procs. of the 34th Ann. ACM Conference On Human Factors In Computing Systems (2016), https://vaniea.com/papers/chi2016.pdf.

[31] *See, e.g.,* EFF, *How Do I Protect Myself Against Malware?*, https://ssd.eff.org/en/module/how-do-i-protect-myself-against-malware (last updated Aug. 29, 2018).

[32] Ari Lazarus, *Update Your Software Now*, FTC Consumer Info. Blog (June 13, 2019), https://www.consumer.ftc.gov/blog/2019/06/update-your-software-now.

[33] DHS, *Mobile Security Tip Card*, https://www.cisa.gov/sites/default/files/publications/Mobile%20Security%20Tip%20Card_7.pdf.

Another Homeland Security advisory instructs:

> Enable automatic app updates in your device settings or when they pop up, because having the most up-to-date software doesn't just make things run smoother—it helps keep you patched and protected against ever-evolving cyber threats![34]

But Prohibited Transaction 1 goes against this guidance. Rather than encouraging users to obtain updates, the government is prohibiting updates altogether, despite its statements that many people may carry on using the WeChat app. This conditions users to ignore the importance of software updates and sends the message that application security can be sacrificed in favor of blunt efforts to ban WeChat as a medium of communication. At a moment when app updates are a necessary part of the Internet security infrastructure, the government is pushing users in the wrong direction.

D. Potential alternatives to WeChat also create security and privacy risks.

It will not be easy for U.S. WeChat users to find a replacement application to communicate with people in China and the Chinese-speaking diaspora. Over 99% of Chinese Internet communicate through instant messaging, compared to a much lower level of email usage.[35] The instant messaging apps best suited to

---

[34] DHS, *Cyber Lessons: Arm Yourself with Knowledge to Stay Ahead of the Game*, https://www.dhs.gov/be-cyber-smart/cyber-lessons.

[35] China Internet Network Information Center, *Statistical Report on Internet Development in China* 25 (Apr. 2020), https://cnnic.com.cn/IDR/ReportDownloads/202008/P020200827549953874912.p

replacing WeChat that can be lawfully used within China also tend to be those created by Chinese companies, as they have robust language support for Chinese speakers. However, these apps—such as QQ, which is also owned by Tencent—would arguably entail the same security risks referenced in Prohibited Transactions and the underlying executive order. Apps from non-Chinese developers that are accessible within China may have limited Chinese language implementation, including a lack of or low-quality Chinese language user interface, notifications, and customer service. These complications increase the difficulty for former WeChat users in configuring the settings of the substitute apps or comprehending the implications of their app interactions on their security and privacy.

Finally, accessing WeChat alternatives risks furthering human rights violations against users within China**.** In the wake of the WeChat Executive Order, popular websites suggested that WeChat users shift their communications to alternative messaging applications that are banned in China, including WhatsApp, Facebook Messenger, Telegram, Line, and Snapchat.[36] To access banned apps,

---

df; Lu-Hai Liang, *Why email loses out to popular apps in China*, BBC (July 10, 2020), https://www.bbc.com/worklife/article/20200707-why-email-loses-out-to-popular-apps-in-china.

[36] Alison D. Rayome, *WeChat ban on hold for now, but you can still try these messaging app alternatives*, CNET (Sept. 21, 2020), https://www.cnet.com/news/wechat-ban-blocked-for-now-but-you-still-may-want-to-try-these-messaging-app-alternatives; Camila Barbeito, *WeChat Has Been*

users within China must employ circumvention tools to bypass the Great Firewall. For the millions of Chinese citizens who used to effortlessly connect to the U.S. Chinese-speaking community via WeChat, the Prohibited Transactions may lead them to take steps that increase their risk of repressive state action in China.

Since rising to power in 2012, Xi Jinping has moved swiftly and severely against dissenting voices in the online world just as he has in the physical world, with unprecedented monitoring and censorship, even for China. A year later, he issued a call to arms for a cyberarmy to advance a pro-PRC propaganda war on the Internet.[37] In 2015, the Chinese government launched the Great Cannon, which can replace and redirect content transmitted on the Internet, and used it to levy a DDOS attack against GitHub, in an effort to prevent those in China from accessing blocked websites.[38] That same year, popular virtual private networks ("VPNs") used to access banned content, which had been nominally prohibited but tolerated in practice for over a decade, were shut down, despite their widespread usage by

Officially Banned in the US — Here Are the Best Alternative Apps, Popsugar (Sept. 20, 2020), https://www.popsugar.com/tech/wechat-alternatives-47805419.

[37] Cary Huang and Keith Zhai, *Xi Jinping rallies party for propaganda war on internet*, South China Morning Post (Sept. 4, 2013), https://www.scmp.com/news/china/article/1302857/xi-jinping-rallies-party-propaganda-war-internet.

[38] Bill Marczak, et. al, *China's Great Cannon*, Citizen Lab (Apr. 10, 2015), https://citizenlab.ca/2015/04/chinas-great-cannon.

expats and international businesses located within China.[39] This draconian policing of Internet access has extended to the individual level, with private citizens suffering punishment even when the banned content they accessed was apolitical.[40]

The implementation of the Prohibited Transactions thus puts WeChat users in China in the difficult position of choosing between not communicating with their loved ones in the U.S. and taking actions that put them at risk of human rights violations by the Chinese government.

II. PREVENTING WECHAT FROM RELYING ON HOSTING, CONTENT-DELIVERY, PEERING, AND TRANSIT SERVICES WITHIN THE U.S. WOULD CREATE ADDITIONAL SECURITY RISKS AND LEAD TO INTERNET FRAGMENTATION.

In addition to the prohibitions on hosting, updating, and using constituent components of the WeChat application itself, the Commerce Department's Prohibited Transactions take aim at a wide array of Internet infrastructure services that support a vast number of applications and services available in the U.S., including WeChat. Like the app store prohibitions, these rules are severely misguided. They raise additional Internet security concerns and risk collateral

---

[39] Andrew Jacobs, *China Further Tightens Grip on the Internet*, N.Y. Times (Jan. 29, 2015), https://www.nytimes.com/2015/01/30/world/asia/china-clamps-down-still-harder-on-internet-access.html.

[40] Masha Borak, *Man punished for using a VPN to scale China's Great Firewall and watch porn*, Abacus (July 30, 2020), https://www.scmp.com/abacus/tech/article/3095201/man-punished-using-vpn-scale-chinas-great-firewall-and-watch-porn.

degradation of other Internet services and applications, further harming American economic and security interests. And fundamentally, they mimic repressive tactics used by authoritarian regimes such as China itself to fragment the Internet and reduce freedom of expression.

A. The Prohibitions on hosting and content create new security risks for users of WeChat.

The Commerce Department's second and third "Prohibited Transactions"—respectively prohibiting U.S. Internet hosting and content delivery services that support WeChat, *see* 2-ER-228—might accomplish their goal of degrading the functionality of WeChat, but they would do so at considerable cost to Americans' Internet security by creating new surveillance opportunities for malicious actors outside the U.S. As the WeChat users' expert Adam Roach explains, the result of these prohibitions will be to deprive U.S. authorities of insight and oversight into whether and how collection of users' information is occurring via these hosting and content delivery services. 2-ER-409–10 (Roach decl. ¶ 8). Correspondingly, WeChat will be forced to rely more heavily on the next most efficient content and hosting services in other jurisdictions, thereby newly exposing user data stored in those jurisdictions to surveillance and other threats. Similarly, the ban on peering (Prohibited Transaction 4) will cause WeChat traffic bound for existing U.S. users to take more complex routing paths, exposing these data flows to surveillance and

other threats as it passes through new jurisdictions.[41] And while manipulation of traffic for government or corporate surveillance is by no means unheard of within the United States, it is commonplace in countries like Turkey and China itself.[42] Notably, these risks apply even to users accessing content from outside these countries' borders.[43] The new surveillance opportunities for malicious actors to attack Americans is a risk to national security outside the U.S.

B. The Prohibited Transactions risk degrading other services and may lead to overbroad content blocking.

Even though the list of prohibited transactions is specifically directed at WeChat, its full implementation would require significant reconfiguration of affected Internet infrastructure, with collateral effects on services beyond WeChat itself.

---

[41] The NSA reportedly uses analogous techniques known as "traffic shaping" to deliberately reroute Internet traffic to create opportunities for surveillance outside the borders of the United States. *See* Sharon Goldberg, *Surveillance without Borders: The "Traffic Shaping" Loophole and Why It Matters*, The Century Found. (June 22, 2017), https://tcf.org/content/report/surveillance-without-borders-the-traffic-shaping-loophole-and-why-it-matters.

[42] Bill Marczak, et al., *Bad Traffic: Sandvine's PacketLogic Devices Used to Deploy Government Spyware in Turkey and Redirect Egyptian Users to Affiliate Ads?*, Citizen Lab (Mar. 9, 2018), https://citizenlab.ca/2018/03/bad-traffic-sandvines-packetlogic-devices-deploy-government-spyware-turkey-syria; Gabi Nakibly, et al., *Website-Targeted False Content Injection by Network Operators* (Feb. 23, 2016), https://arxiv.org/pdf/1602.07128v1.pdf.

[43] *Id.* at 6 ("We note that the networks we monitored are not located in China or the Far East, but in a Western country.").

For example, Prohibited Transaction 3 fails to grasp the particular architecture of content delivery networks or content distribution networks ("CDNs"). A CDN is a geographically distributed network of caching servers and their data centers. The goal of a CDN is to provide high availability and performance by distributing the service geographically relative to end users, thus reducing the amount of time for content to load. When a device requests content via a CDN, the content is sent back through optimized routing from the closest server, instead of where the content was originally hosted. A properly configured CDN may also act as a proxy to help protect websites against some common malicious attacks, such as DDOS attacks.[44]

Although there are ways to differentiate content requests, such as by geographic location, [45] CDNs may not be configured to distinguish between requests made by different apps, and reconfiguring them to do so may not be possible, technically or financially. A CDN may be configured to host a copy of a specific image file—such as a product logo—on thousands of computers across the

[44] *See, e.g.*, Akamai, *CDN DDoS*, https://www.akamai.com/us/en/resources/cdn-ddos.jsp.

[45] Even geographic filtering raises privacy and technical challenges for CDNs and other service providers (such as mesh networks) at the borders of the United States. CDNs that serve Mexico and the United States, or Canada and the United States, for example, will have to filter traffic differently depending on its destination. That is likely to degrade the quality of service for the users who rely on such infrastructure.

planet so that when someone requests a web page that contains that logo, the file is served by the computer that can most quickly reply. However, for technical reasons, in many cases the operator of a CDN will know only that it is serving a certain image file, not that it is sending it to be rendered in the WeChat app on a mobile device.[46] Moreover, the network operators facilitating this transaction have even less information, and have no insight into the particular CDN service contracted by an app like WeChat that one of their users happens to use.

Hence, giving full effect to this prohibition likely requires disabling content delivery services to other applications not targeted by the Commerce Department Prohibitions and lead to over-blocking of CDNs. At minimum, the result would be a slower Internet for all U.S. users.

Similarly, the Prohibited Transaction 4—barring the "provision of directly contracted or arranged internet transit or peering services enabling the functioning or optimization" of WeChat in the United States, 2-ER-229—poses significant risk of overbroad degradation of traffic.

---

[46] Most modern apps use cloud hosting such as Amazon Web Services (AWS) or Microsoft Azure rather than self-hosting their applications. Hence a file served by a CDN to a WeChat user may appear to be sent to a cloud hosting service operated by third party, rather than to TenCent itself. Moreover, due to the prevalence of encryption of content "in transit" on the Internet, the CDN operator may not even have access to the full domain to which it is transmitting its content. S*ee* EFF, *What Should I Know About Encryption?* (Nov. 24, 2018) (discussing encryption in transit), https://ssd.eff.org/en/module/what-should-i-know-about-encryption#1.

As an initial matter, peering and transit relationships are vital to the fabric of the modern Internet. The Internet is a "network of networks" that provides connectivity between end points connected via Internet service providers ("ISPs"). ISPs themselves connect via "backbone" networks, "long-haul fiber-optic links and high-speed routers capable of transmitting vast amounts of data." *United States Telecom Ass'n v. FCC*, 825 F.3d 674, 690 (D.C. Cir. 2016). Connections between users, websites and applications such as WeChat, and their respective ISPs depend on agreements to exchange Internet traffic with each other over the backbone, known as "peering" links.[47] Operators of backbone and web services make peering agreements with ISPs about how to exchange Internet traffic so that data can be carried efficiently from one part of the Internet to another. Although private parties are responsible for almost all peering arrangements, these arrangements have "ensured the provision of a stable, integrated global public Internet."[48]

[47] "Peering" and "transit" typically both refer to forms of interconnection agreements between backbone networks, which are usually differentiated by whether they entail bilateral sharing of data and whether money changes hands. *See* Michael Kende, *The Digital Handshake: Connecting Internet Backbones* 4-8, FCC Office of Plans & Policy (Sept. 2000), https://transition.fcc.gov/Bureaus/OPP/working_papers/oppwp32.pdf.

[48] William J. Drake, Vinton G. Cerf & Wolfgang Kleinwächter, *Internet Fragmentation: An Overview* 49, World Econ. Forum (Jan. 2016), http://www3.weforum.org/docs/WEF_FII_Internet_Fragmentation_An_Overview_2016.pdf.

By the government's own admission, Prohibited Transaction 4 is intended to severely disrupt this efficient exchange of information. As the WeChat users' expert Adam Roach explains, peering agreements are usually "made on behalf of all of the customers of the backbone providers, including their customers' customers." 2-ER-410 (Roach decl. ¶9). Thus, the prohibition on peering would have a massive collateral effect, not just on WeChat or its parent company Tencent, but potentially on all US businesses that use ISPs to carry their traffic to China. This is because, as Roach points out, there are a very limited number of ISPs in China. *Id.* (¶10). Prohibiting U.S. businesses from peering with or offering transit to Tencent means these businesses must not connect to these Chinese ISPs, as that is how Tencent's traffic is served to the larger Internet. Tencent has a very rich set of network peering relationships—232 at the time of writing[49]—each of which would have to be investigated by providers in the U.S. to avoid facilitating the WeChat application. In order to truly eliminate peering that enables efficient routing of WeChat, the government would need to prohibit all peering agreements

[49] Tencent's network is assigned Autonomous System Number (ASN) AS132203, which has 232 Border Gateway Protocol (BGP) "neighbours." *See* RIPE Network Coordination Centre, *Routing Status* (AS132203), https://stat.ripe.net/AS132203#tabId=routing (for Autonomous System Number (ASN) AS132203) (last visited Dec. 3, 2020); *See also Border Gateway Protocol*, Wikipedia, https://en.wikipedia.org/wiki/Border_Gateway_Protocol (discussing BGP neighbors and peering).

with Chinese backbone providers used by WeChat's parent company Tencent, "effectively ending all direct Internet traffic" between the two countries. *Id.*

Within the United States, Prohibited Transaction 4 could also diminish user privacy. The text of Prohibited Transaction 4 bars a company from carrying traffic for another firm if that peering relationship "enable[s] the functioning" of WeChat. 2-ER-229. U.S. providers may read this to require them to inspect every packet they put on their network, where possible, to be certain that they are not inadvertently carrying WeChat content. They cannot, technologically, inspect only WeChat packets; instead, they would have to inspect every packet, thus revealing to the company every website visited, every video downloaded, and more. This data can reveal sensitive personal information, such as a user's religious beliefs, political preferences, and health status. Thus, the order may have a severe privacy impact. And, of course, if companies have any concerns about whether traffic might help the functioning of WeChat, they may choose to block that traffic rather than risk violating the order. The result would be that American users may be unable to access legal content due to such over-blocking.

The government argues its order would prohibit only peering contracts with U.S. providers to which Tencent is a party, not all U.S.-Chinese peering arrangements that benefit WeChat's efficient operation. 2-ER-402–03 (Second Costello decl. ¶14). Of course, this is not what the text says; it prohibits all

"directly contracted or arranged" services that have the effect of enabling the WeChat application. 2-ER-229. But regardless of whether the government's narrower interpretation is consistent with the applicable language of Prohibited Transaction 4, it would set a new and dangerous precedent for intentionally prohibiting interconnection.

C. The Prohibited Transactions fuel Internet fragmentation and undermine Internet freedom.

By severing links between a major Chinese application provider and the United States, the Commerce Department's order contributes to so-called Internet fragmentation—the erosion of an "open global public Internet."[50] Internet fragmentation has a variety of causes—technical, governmental, and commercial—and although not all Internet fragmentation is equally serious or even intentional, its proliferation can undermine and even destroy the prospect of an open Internet.[51] Notably, both the U.S. State Department and the United Nations Human Rights Council have expressed support for protecting the open Internet in order to promote human rights Internet online.[52] Fragmentation also goes against the set of "critical properties" that "makes the Internet 'the Internet,'" as described by the

---

[50] Drake, et al., *supra* note 48, at 10.

[51] *Id.* at 4, 15-16.

[52] U.S. Dep't of State, *Internet Freedom* (Nov. 27, 2017), https://www.state.gov/internet-freedom; United Nations Human Rights Council Res. 38/7, U.N. Doc. A/HRC/RES/38/7 (July 17, 2018).

Internet Society in a recent publication.[53] In particular, the Prohibited Transactions violate Critical Property Three, which focuses on the importance of decentralized management of the Internet in delivering key benefits such as global connectivity, resilience, and optimized connectivity.[54]

An example of how the Prohibited Transactions establish a fragmentary precedent that could undermine the interconnectivity and innovation concerns the Internet of Things ("IoT"), billions of Internet-connected physical devices around the world, such as thermostats, security cameras, smart devices, and multitudes of other devices and sensors. IoT devices depend on the availability of Application Programming Interfaces ("APIs"), software intermediaries that allow applications to communicate (interoperate) with one another, across the cloud. APIs provide routines, protocols, and tools for developers building software applications, while enabling the extraction and sharing of data in an accessible and regular manner. IoT applications and devices use APIs to gather data, or even control other devices. If access to an API is limited, then this seamless integration falters. The

[53] Internet Society, *Internet Impact Assessment Toolkit: Introduction* (Sep. 9, 2020), https://www.internetsociety.org/resources/doc/2020/internet-impact-assessment-toolkit/introduction.

[54] Internet Society, *The Internet Way of Networking: Defining the critical properties of the Internet* (Sep. 2020), https://www.internetsociety.org/wp-content/uploads/2020/09/IWN-IIAT-Defining-the-critical-properties-of-the-Internet.pdf.

government apparently asserts the ability to block specific APIs with Prohibited Transaction 6, which it says is intended to "prevent interoperability of third-party apps that utilize WeChat functions and services," 2-ER-404 (Second Costello decl. ¶18).

While it is relatively common for some governments to contribute to Internet fragmentation by restricting access to content deemed illegal or offensive within their own jurisdictions, efforts to prohibit network interconnection have previously been the domain of authoritarian governments like China and Russia. Building on its robust Great Firewall censorship network, China has long advocated for the concept of "cyber sovereignty" or "Internet sovereignty," which entails national oversight of all connections in and out of the country.[55] As discussed in Section I.D, *supra*, China's online surveillance, censorship, and policing extend to nearly every facet of its domestic networks. Russia passed its own "sovereign Internet" legislation in 2019, giving the government unilateral power to censor websites and applications or even cut Russia off from the global Internet.[56] Human rights organizations condemning these developments have traced the trend toward digital

[55] Michael Bristow, *China defends Internet censorship*, BBC (June 8, 2010), http://news.bbc.co.uk/2/hi/8727647.stm.

[56] Human Rights Watch, *Russia: New Law Expands Government Control Online* (Oct. 31, 2019), https://www.hrw.org/news/2019/10/31/russia-new-law-expands-government-control-online.

authoritarianism, as more countries are "embracing the Chinese model of extensive censorship and automated surveillance systems."[57] Meanwhile, as part of its "Internet Freedom strategy" under both the Obama and Trump administrations, the State Department has denounced these developments and funded the development of projects intended to combat authoritarian control of the Internet.[58] Yet the Prohibited Transactions are a step in the opposite direction of Internet freedom and toward the normalization of the restrictive virtual world imagined by China.

Finally, the U.S. government's normalization of authoritarian tactics to carve up the Internet invites further retaliation from China. China's centralized control of its domestic network infrastructure gives it the power to even more severely degrade and interfere with traffic to the United States and intermediate destinations.[59] For example, a researcher uncovered a significant misdirection of

---

[57] Adrian Shahbaz, *The Rise of Digital Authoritarianism*, Freedom House (2018), https://freedomhouse.org/report/freedom-net/2018/rise-digital-authoritarianism; *see also* Ana Swanson, et al., *Trump's Attacks on TikTok and WeChat Could Further Fracture the Internet*, N.Y. Times (Aug. 17, 2020), https://www.nytimes.com/2020/08/17/technology/trump-tiktok-wechat-ban.html.

[58] U.S. Dep't of State, *Internet Freedom* (deprecated), *available at* https://web.archive.org/web/20170609001151/https:/www.state.gov/j/drl/internetfreedom/index.htm; U.S. Dep't of State, *Internet Freedom: Advancing and Promoting Peer-to-Peer Communications Technologies* (Feb. 13, 2020), https://www.state.gov/internet-freedom-advancing-and-promoting-peer-to-peer-communications-technologies/ (citing Freedom House report on Internet censorship).

[59] See Danny O'Brien, *China's Global Reach: Surveillance and Censorship Beyond the Great Firewall*, EFF (Oct. 10, 2019),

traffic in 2017 that led communications between users within the U.S. to be routed through an ISP in China.[60] While it is unclear whether this misdirection was intentional, the Commerce Department's Prohibitions could encourage Chinese actors to deliberately create similar misdirection by taking advantage of the Internet's interconnectedness, particularly at the peering layer,[61] to cause larger disruption and fragmentation.

Thus, even the more limited interpretations of Prohibited Transactions advanced by the government below would constitute an unprecedented, intentional fragmentation of the Internet by the U.S. government and an endorsement of the authoritarian tactics the government has sought to combat through its foreign policy. It would also lead to escalating retribution.

---

https://www.eff.org/deeplinks/2019/10/chinas-global-reach-surveillance-and-censorship-beyond-great-firewall.

[60] Dan Goodin, *Strange snafu misroutes domestic US Internet traffic through China Telecom*, Ars Technica (Nov. 6, 2018), https://arstechnica.com/information-technology/2018/11/strange-snafu-misroutes-domestic-us-internet-traffic-through-china-telecom.

[61] The researcher pointed to risks in peering infrastructure that may have led to the 2017 misdirection of traffic through China. Doug Madory, *China Telecom's Internet Traffic Misdirection*, Oracle (Nov. 5, 2018), https://internetintel.oracle.com/blog-single.html?id=China+Telecom%27s+Internet+Traffic+Misdirection; *see also* Doug Madory, *Use Protection if Peering Promiscuously*, Oracle (Nov. 12, 2014), https://blogs.oracle.com/internetintelligence/use-protection-if-peering-promiscuously-v3.

CONCLUSION

For the reasons stated above, this Court should affirm the preliminary injunction.

Dated: December 4, 2020

By: /s/ *Andrew Crocker*
Andrew Crocker

Hannah Zhao
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Telephone: (415) 436-9333
andrew@eff.org

Avery Gardiner
CENTER FOR DEMOCRACY & TECHNOLOGY
1401 K St. NW, Suite 200
Washington, DC 20005

Counsel for Amici Curiae

CERTIFICATE OF COMPLIANCE

Pursuant to Fed. R. App. P. 32(g), I certify as follows:

1. This Brief of Amici Curiae the Electronic Frontier Foundation, The Center for Democracy & Technology, and the Internet Society in Support of Plaintiffs-Appellees and Affirmance complies with the type-volume limitation of Fed. R. App. P. 32(a)(7)(B) because this brief contains 6,364 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(f); and

2. This brief complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type style requirements of Fed. R. App. P. 32(a)(6) because this brief has been prepared in a proportionally spaced typeface using Microsoft Word 2016, the word processing system used to prepare the brief, in 14 point font in Times New Roman font.

Dated: December 4, 2020

By: /s/ *Andrew Crocker*
Andrew Crocker

Counsel for Amici Curiae

CERTIFICATE OF SERVICE

I hereby certify that I electronically filed the foregoing with the Clerk of the Court for the United States Court of Appeals for the Ninth Circuit by using the appellate CM/ECF system on December 4, 2020.

I certify that all participants in the case are registered CM/ECF users and that service will be accomplished by the appellate CM/ECF system.

Dated: December 4, 2020

By: /s/ *Andrew Crocker*
Andrew Crocker

Counsel for Amici Curiae