Indo-Pacific Security Program
Memorandum

IDENTIFYING THE NEXT TIKTOK

Which Apps Could Washington Target Next?

By Joel Thayer

BOTTOM LINE

1. The digital age has shaped America's competition with China in ways that make this second cold war categorically different from the first.
2. A bipartisan Congress responded by passing the Protecting Americans from Foreign Adversary Controlled Appliations Act. The Act is targeted at TikTok, but it could be a useful tool to rid America's networks of insidious malware.
3. The president could apply the Act to WeChat and Temu, which present similar national security concerns as TikTok.

In the first Cold War, the United States and Soviet Union clashed repeatedly through satellite states and proxies. Today, America finds itself locked in great power competition with the People's Republic of China (PRC). The digital age has shaped this conflict in ways that make this second cold war categorically different from the first. The PRC has infiltrated numerous aspects of America's communications networks. With the promise of cheap labor, Beijing stole American intellectual property. With the promise of cheap equipment, it took control of multiple U.S. routers, backhauls, cell sites, and mobile devices. With the promise of cheap laughs, it captured Americans' attention and siphoned data.

Congress has responded in bipartisan fashion, passing most recently the Protecting Americans from Foreign Adversary Controlled Applications Act (the Act).[1] The Act specifically mentions ByteDance and TikTok, which means that they and their subsidiaries are required to divest. However, the law's scope is not limited to just TikTok and ByteDance. The Act broadly applies foreign ownership restrictions to apps operating within the United States. In so doing, it follows legal

Joel Thayer *is the President of the Digital Progress Institute. He has founded his own law firm, Thayer PLLC, and was previously an associate at Phillips Lytle. Before that, he served as Policy Counsel for ACT | The App Association, where he advised on legal and policy issues related to antitrust, telecommunications, privacy, cybersecurity, and intellectual property in Washington, DC. His experience also includes working as a legal clerk for FCC Chairman Ajit Pai and FTC Commissioner Maureen Ohlhausen and as a congressional staffer for the Hon. Lee Terry and the Hon. Mary Bono.*

frameworks that America has implemented in separate contexts like telecommunications services, broadcasters, banking, and energy, to name a few.[2]

Likewise, the TikTok bill is bigger than TikTok. It could prove to be a useful tool to rid America's networks of insidious malware. What follows is an outline of the Act's substantive provisions, and an analysis on how the Act's framework can apply to other Chinese-based applications posing similar national security issues as TikTok and ByteDance. Specific attention is given to WeChat and Temu.

How the Act Works

The Act prevents any company, such as app store providers or web-hosting services, from distributing, maintaining, or updating "a foreign adversary controlled application" within the U.S. The Act's use of the term "application" includes everything from large social media apps to texting apps and online marketplaces.[3] It defines "foreign adversary governments" as China, North Korea, Russia, and Iran. The Act further specifies that the entity must be under the direction or control of the foreign adversarial government. Direction or control is a common legal phrase, used in a variety of statutes.[4] The language would require the U.S. government to "establish" that the foreign adversarial government "direct[s] or control[s] [the company's] actions."[5] This is a high bar to clear legally.[6]

The Act also requires a separate finding that the foreign adversary controlled app poses a "significant threat to national security." Hence, it is not enough to show ownership and control, but also that the app poses an imminent threat to U.S. national security.

If the president determines that such an app poses a national security threat to the United States, then the foreign company must divest. The Act provides a 270-day window for the company to divest after the President has made his determination.[7] If it doesn't, then the Act imposes a hefty fine of up to $5,000 for every U.S. user it maintains, plus a $500-per-U.S.-user fine for hosting and collecting their data and information.[8]

For the determination to be valid, the Act mandates an interagency process.[9] After the interagency investigation, the President must send a report to Congress articulating his reasoning thirty days before his determination takes effect. The Act also requires the President to release a public notice of his determination.

After the President publicly announces his finding, affected entities have 270 days to divest. During that time, the affected app can seek recourse in the courts—and until that time frame expires, the attorney general cannot enforce the president's determination against the affected app. To address any concerns about civil liberties, Section 2(f) of the Act makes clear that the Attorney General cannot use the Act's provisions to target U.S. TikTok users with legal action.

The TikTok bill is bigger than TikTok. *It could prove to be useful to rid America's networks of insidious malware.*

Factors to Determine a National Security Threat

Understanding the relationship between TikTok and the PRC government will establish a barometer to predict how administrations could leverage the Act against other entities in the future.

FBI Director Christopher Wray's description of TikTok as "a tool that is ultimately within the control of the Chinese government—and it…screams out with national security concerns."[10] President Biden's Director of National Intelligence Avril Haines also stated that China uses apps (like TikTok) and communication networks to "develop[] frameworks for collecting foreign data and pulling it in . . . to target audiences for information campaigns or for other things."[11]

TikTok of course protests these characterizations, but recent reporting suggests that the company's promises of protecting the privacy and security of American data ring hollow. Leaked audio from internal TikTok meetings shows that, at least through January 2022, engineers in China had access to U.S. data.[12] "Everything is seen in China," said one member of TikTok's Trust and Safety team.[13] And eight different U.S. employees explained having to repeatedly turn to Chinese colleagues because U.S. staff "did not have permission or knowledge of how to access the data on their own."[14] Meanwhile, TikTok's parent ByteDance has admitted to tracking at least two U.S.-based journalists,[15] and reports show that ByteDance had in fact intended to use TikTok to monitor specific American citizens.[16] The U.S. Department of Justice is investigating this spying.[17]

The relationship between the foreign adversary country and the app is a critical component to the determination. For instance, ByteDance has had an internal party committee as part of its governance structure since 2017 to ensure alignment with Beijing's policies.[18] And TikTok CEO Shou Zi Chew, who promised to localize all U.S. user data, served as ByteDance's CFO for most of 2021 and before that was president of international operations for Xiaomi Technology, a software developer the Pentagon considers a "Communist Chinese military company."[19] On November 1, 2023, TikTok's internal platform, "which houses its most sensitive information, was inspected in person by CCP cybersecurity agents in the lead-up to the CCP's 20th National Congress."[20] Moreover, the PRC has multiple laws that require companies operating within China to share information, including data and proprietary information, with the Chinese government on national security grounds. As TikTok's parent company, ByteDance falls under these laws.

*The next administration should evaluate Tencent's ownership of **WeChat** and PPD's ownership of **Temu**.*

Thus, the national security concerns surrounding TikTok are inextricably linked to the app's data collection practices and the adversary government's ability to direct, audit, and manipulate them.

Likely Targets Outside of TikTok and ByteDance

To understand other entities that could fall under the Act, it is helpful to first identify companies that are clearly outside the Act's scope. X and Telegram are two notable examples.

X falls outside the scope of the Act because it is owned and controlled by Elon Musk. It has nothing to do with the foreign adversaries listed in the Act—China, North Korea, Russia, or Iran. Telegram may appear to be a closer call because it was founded in Russia. But ownership by a corporation with ties back into a foreign adversary like Russia is not a triggering condition under the Act. The president would need to demonstrate that the app is controlled in the same way the PRC controls TikTok. Given that Telegram is encrypted and the Russian government once banned Telegram for 2 years for not decrypting it, there appears to be little case for targeting Telegram under the Act.

What companies, then, would fall under the Act's parameters? One obvious target would be WeChat, a social media app that is owned and operated by the Chinese multimedia conglomerate Tencent. Both WeChat and Tencent have come under a significant amount of scrutiny with respect to their relationship with the PRC. There are also parallels between their relationship and the one between ByteDance and TikTok. Like TikTok, WeChat is a social media app that allows Chinese citizens to text with Americans, facilitate financial transactions, share videos and photos, and play video games. Some users describe WeChat as the "everything app" because Chinese citizens find it "nearly impossible to navigate without WeChat…." Also like TikTok, researchers have found that WeChat provides very few privacy protections to its consumers. A group of researchers at Citizens Lab reversed engineered WeChat's network management practices and found (1) that it collects far more data than

what it publicly discloses, and (2) user's communications are not private. Moreover, unlike apps like Telegram and Signal, WeChat's encryption is not end-to-end. Citizens Lab found that WeChat censors chat images via a hodgepodge of text and visual recognition software built into the app.

Worse, there is evidence that the Chinese government controls certain aspects of the app. An article in MIT Technology Review reported that WeChat censors content that may offend the CCP. Notably, when protestors hung up banners on a bridge in Beijing before the 20th Communist Party Congress criticizing the CCP's handling of the COVID-19 pandemic, the app censored texts and content that referenced "Beijing," "bridge," and "brave" were removed.

Even worse, as Arthur Herman reported in Forbes, "WeChat may pose an even greater danger from the angle that alarmed government officials from the very start, as an app that gives the Chinese government direct access to user data in the US."

The Temu app owned by PDD Holdings may also be a likely candidate for the Act's review. Temu is an increasingly popular online marketplace in the United States, and Americans are spending twice as much time on it than on Amazon. Like ByteDance, PDD is based in Beijing and has connections to CCP officials. For instance, PDD's top leaders are Xu Mintao, who was previously a senior official in the State Administration for Market Regulation, and Zhou Qingtian, who was deputy director of the Regulation Department of the Shanghai Administration for Market Regulation. The connections do not stop there. PPD's director of public affairs served as the deputy director of China's Trademark Office of the State Intellectual Property Office, and its vice president is a former official at the Shanghai Administration for Industry and Commerce, and its legal department is headed by two former judges of the People's Court of Shanghai.

PDD's links to the PRC government is especially problematic, given the recent charge of data mismanagement levied against Temu by Arkansas's attorney general's office. Arkansas alleges that Temu violated its consumer protection and privacy laws by unlawfully "access[ing] . . . use[r's] phone operating system, including . . . [their] camera, specific location, contacts, text messages, documents, and other applications." As the Texas Public Policy Foundation rightly notes, Temu's access could permit "the CCP [to] theoretically install applications and spyware files on an individual's smart device to use for complete surveillance of all user activity on a phone." These are precisely the same concerns raised with respect to TikTok and ByteDance.

In sum, the Act lays out a specific and narrow path for the executive branch to designate apps and their owners' national security threats. Users of apps that pose no threat, like X or Telegram, have no cause for concern. Given the time needed to build a new case under the Act, the next presidential administration should begin evaluating Tencent's ownership of WeChat and PDD's ownership of Temu in early 2025.

ENDNOTES

1. P.L. 118-50, Division H. Hereafter referred to as "The Act." https://www.congress.gov/118/bills/hr815/BILLS-118hr815enr.pdf.
2. Ganesh Sitaraman, The Regulation of Foreign Platforms, 74 Stan. L. Rev. (2022). For an example, consider the Secure and Trusted Communications Network Act of 2019. See P.L. 116-124, March 12, 2020, https://www.govinfo.gov/content/pkg/PLAW-116publ124/pdf/PLAW-116publ124.pdf. It targeted Huawei and ZTE, but also allowed for the designation of other national security threats to our communications networks. It required the Federal Communications Commission (FCC) "to create a list of 'covered' telecommunications equipment posing such a [national security] threat." Beyond Huawei and ZTE, the FCC also placed other companies to the list, including Hangzhou Hikvision Digital Technology Company, Dahua Technology Company, AO Kaspersky Lab, and China Mobile. See "List of Equipment and Services Covered By Section 2 of The Secure Networks Act," Federal Communications Commission, https://www.fcc.gov/supplychain/coveredlist.
3. The Act § 2(g)(2)(A).
4. See, *e.g.*, 18 U.S.C. § 2339(B)(h); 15 U.S.C. § 4651(6)(B)(iii); 18 U.S.C. § 951(d); 22 U.S.C. § 611(c)(1); 18 U.S.C. § 175(b)(d)(G)(ii), (I); 15 C.F.R. § 7.2.

5. See *United States v. Chung*, 659 F.3d 815, 823 (9th Cir. 2011).
6. See *United States v. Alshahhi*, 2022 WL 2239624, at *4 (E.D.N.Y. 2022).
7. Id. § 2(a)(2)(B).
8. Id. at (d)(1).
9. The interagency process remains unclear, but a July 2024 memo from President Biden delegated certain authorities under the Act. Therein, the president delegated "to the Attorney General, in consultation with the Secretary of the Treasury, the Secretary of Commerce, and the Secretary of Homeland Security." It also established a "Committee for the Review of Foreign Adversary Controlled Applications (Committee), composed of the Secretary of State, the Secretary of the Treasury, the Secretary of Defense, the Attorney General, the Secretary of Commerce, the Secretary of Homeland Security, and the Director of National Intelligence." The memo requires the "Director of National Intelligence and the heads of other relevant agencies, as the Attorney General…or…the Committee," to provide assessments "of the threat to national security posed by foreign adversary controlled applications…" See "Memorandum on the Delegation of Authority Under the Protecting Americans from Foreign Adversary Controlled Applications Act," The White House, July 24, 2024, https://www.whitehouse.gov/briefing-room/presidential-actions/2024/07/24/memorandum-on-the-delegation-of-authority-under-the-protecting-americans-from-foreign-adversary-controlled-applications-act/.
10. Michael Martina & Patricia Zengerle, "FBI chief says TikTok 'screams' of US national security concerns," Reuters, March 9, 2023, https://www.reuters.com/technology/fbi-chief-says-tiktok-screams-us-national-security-concerns-2023-03-08/.
11. Andrea Mitchell Report, "DNI Avril Haines: Parents 'should be' concerned about kids' privacy and data on Tik-Tok," *MSNBC*, December 5, 2022, https://on.msnbc.com/3OWZn97.
12. Emily Baker-White, "Leaked Audio from 80 Internal TikTok Meetings Shows that US User Data Has Been Repeatedly Accessed From China," BuzzFeed News, June 17, 2022, https://www.buzzfeednews.com/article/emilybakerwhite/tiktok-tapes-us-user-data-china-bytedance-access.
13. Ibid.
14. Ibid.
15. Clare Duffy, "TikTok confirms that journalists data was accessed by employees of its parent company," *CNN*, December 22, 2022, https://www.cnn.com/2022/12/22/tech/tiktok-bytedance-journalist-data/index.html.
16. Emily Baker-White, "TikTok Parent ByteDance Planned To Use TikTok To Monitor The Physical Location Of Specific American Citizens," *Forbes*, October 20, 2022, https://www.forbes.com/sites/emilybaker-white/2022/10/20/tiktok-bytedance-surveillance-american-user-data/?sh=3a9689556c2d.
17. Alexander Mallin & Luke Barr, "DOJ investigating TikTok owners for possible surveillance of US journalists: Sources," *ABC News*, March 17, 2023, https://abcn.ws/47Pr2Bm.
18. Yaqiu Wang, "Targeting TikTok's privacy alone misses a larger issue: Chinese state control," Human Rights Watch, January 24, 2020, https://www.hrw.org/news/2020/01/24/targeting-tiktoks-privacy-alone-misses-larger-issue-chinese-state-control.
19. Jerry Dunleavy, "TikTok CEO's Chinese government ties in spotlight ahead of Capitol Hill testimony," *Washington Examiner*, March 23, 2023, https://www.washingtonexaminer.com/news/2580100/tiktok-ceos-chinese-government-ties-in-spotlight-ahead-of-capitol-hill-testimony/.
20. Letter from Congressional Members to FBI Christopher Wray, December 7, 2023, https://www.politico.com/f/?id=0000018c-4eb1-d99d-a9cf-7ffdbb6a0000.
21. The Act § 2(g)(3)(B)(ii).
22. "Russia Lifts Ban on Telegram Messaging App After Failing to Block It," Reuters, June 18, 2020, https://www.reuters.com/article/idUSKBN23P2DY/.
23. Harshawn Ratanpal, "After U.S. Scrutiny of WeChat, Chines Conglomerate Tencent Holdings Spent Millions on Federal Lobbying," Open Secrets, February 7, 2023, https://www.opensecrets.org/news/2023/02/after-us-scrutiny-of-wechat-chinese-conglomerate-tencent-holdings-spent-millions-on-federal-lobbying/.
24. Betsy Reed, "'The Everything App': Why Elon Musk Wants X to be a WeChat for the West," *The Guardian*, July 29, 2023, https://www.theguardian.com/media/2023/jul/29/elon-musk-wechat-twitter-rebranding-everything-app-for-west.
25. Mona Wang, Pellaeon Lin, & Jeffery Knockel, "Should We Chat? Privacy in the WeChat Ecosystem," The Citizen Lab, June 28, 2023, https://citizenlab.ca/2023/06/privacy-in-the-wechat-ecosystem-full-report/.
26. Ibid.
27. David Strom, "The WeChat App Is Anything But Private. If You Must Use It, Here's How to Protect Yourself," *Silicon Angle*, July 3, 2023, https://siliconangle.com/2023/07/03/wechat-app-anything-private-must-use-heres-protect/.
28. Ibid.
29. Zeyi Yang, "The Dark Side of a Super App Like WeChat," MIT, October 18, 2022, https://www.technologyreview.com/2022/10/18/1061899/dark-side-super-app-wechat/.
30. Ibid.
31. Arthur Herman, "WeChat: China's Other Trojan Horse," *Forbes*, February 3, 2023, https://www.forbes.com/sites/arthurherman/2023/02/03/wechat-chinas-other-trojan-horse/.
32. Jinshan Hong, "Shoppers Spend Almost Twice as Long on Temu App Than Key Rivals," Bloomberg, December 11, 2023, https://www.bnnbloomberg.ca/shoppers-spend-almost-twice-as-long-on-temu-app-than-key-rivals-1.2010364.
33. Jon Levine, "Temu Parent Company Led by Top Former

Chinese Communist Officials," *New York Post*, June 15, 2024, https://nypost.com/2024/06/15/tech/temu-parent-company-led-by-top-former-chinese-communist-officials/.

34. Ibid.
35. *Arkansas v. PDD Holding Inc.*, Case No. 12CV-24-149, Plaintiff's Complaint.
36. David Dunmoyer, "Why Communist China-Connected Temu Is Worse Than TikTok," Texas Public Policy Foundation, July 1, 2024, https://www.texaspolicy.com/why-communist-china-connected-temu-is-worse-than-tiktok.

Indo-Pacific Security Program

Memorandum

Issue 6 | September 2024

ABOUT THE PROGRAM

For the United States, the Indo-Pacific represents a region of significant security challenges and enormous political and economic opportunity. AFPC's Indo-Pacific Security Program seeks to provide policymakers and the general public with the analysis, insights and recommendations necessary to properly understand and navigate this vital region.

For more information about the program, please contact Michael Sobolik, Fellow in Indo-Pacific Studies, at sobolik@afpc.org.

ABOUT AFPC

For four decades, AFPC has played an essential role in the U.S. foreign policy debate. Founded in 1982, AFPC is a 501(c)(3) non-profit organization dedicated to bringing information to those who make or influence the foreign policy of the United States and to assisting world leaders with building democracies and market economies.

AFPC is widely recognized as a source of timely, insightful analysis on issues of foreign policy, and works closely with members of Congress, the Executive Branch and the policymaking community. It is staffed by noted specialists in foreign and defense policy, and serves as a valuable resource to officials in the highest levels of government.

AFPC MISSION STATEMENT

The American Foreign Policy Council seeks to advance the security and prosperity of the United States by:

- providing primary source information, as well as policy options, to persons and organizations who make or influence the national security and foreign policies of the United States;
- arranging meetings and facilitating dialogue between American Statesmen and their counterparts in other countries; and
- fostering the acceptance and development of representative institutions and free market economies throughout the world in a manner consistent with the Constitution, the national interest, and the values of the United States.

AMERICAN FOREIGN POLICY COUNCIL
509 C Street NE, Washington, D.C. 20002 | Telephone: 202.543.1006 | Fax: 202.543.1007 | www.afpc.org