

PROTECTING AMERICANS FROM FOREIGN ADVERSARY
CONTROLLED APPLICATIONS ACT

MARCH 11, 2024.—Committed to the Committee of the Whole House on the State
of the Union and ordered to be printed

Mrs. RODGERS of Washington, from the Committee on Energy and
Commerce, submitted the following

R E P O R T

[To accompany H.R. 7521]

The Committee on Energy and Commerce, to whom was referred the bill (H.R. 7521) to protect the national security of the United States from the threat posed by foreign adversary controlled applications, such as TikTok and any successor application or service and any other application or service developed or provided by ByteDance Ltd. or an entity under the control of ByteDance Ltd., having considered the same, reports favorably thereon without amendment and recommends that the bill do pass.

CONTENTS

	Page
Purpose and Summary	2
Background and Need for Legislation	2
Committee Action	12
Committee Votes	12
Oversight Findings and Recommendations	14
New Budget Authority, Entitlement Authority, and Tax Expenditures	14
Congressional Budget Office Estimate	14
Federal Mandates Statement	14
Statement of General Performance Goals and Objectives	14
Duplication of Federal Programs	14
Related Committee and Subcommittee Hearings	14
Committee Cost Estimate	15
Earmark, Limited Tax Benefits, and Limited Tariff Benefits	15
Advisory Committee Statement	15
Applicability to Legislative Branch	15
Section-by-Section Analysis of the Legislation	15
Changes in Existing Law Made by the Bill, as Reported	18

PURPOSE AND SUMMARY

Communications applications that are owned and operated by companies controlled by foreign adversary countries present a clear threat to the national security of the United States. This is because such applications can be used by those countries to collect vast amounts of data on Americans, conduct espionage campaigns, and push misinformation, disinformation, and propaganda on the American public.

The United States has, for more than 100 years, restricted foreign governments and persons from owning media outlets and holding broadcast licenses. However, current law does not address the situation where a foreign adversary country has significant control over a company that operates a technology application, even where such application poses a significant threat to national security.

H.R. 7521, the “Protecting Americans from Foreign Adversary Controlled Applications Act” protects Americans from national security risks posed certain by applications controlled by a foreign adversary of the United States. If an application is determined to be a foreign adversary controlled application, such as TikTok’s parent company ByteDance, the application must be divested so that is no longer in the foreign adversary’s control. If the application is not divested within 180 days, entities in the United States would be prohibited from distributing the application through an application marketplace or store, and from providing web hosting services. The 180 days would begin upon enactment of the legislation for ByteDance, TikTok, and other subsidiaries; for other foreign adversary controlled applications, the 180 days begins after a Presidential determination that the application poses a significant threat to national security. The legislation includes a requirement that foreign adversary controlled applications provide users, upon request, information related to the user’s account, including photos, videos, and posts, in a machine-readable format. This Act addresses the immediate national security risks posed by TikTok and establishes a framework for the Executive Branch to protect Americans from future foreign adversary controlled applications.

BACKGROUND AND NEED FOR LEGISLATION

Communications technologies and networks underpin the daily lives of the American public and economy. Foreign adversaries have used access to Americans’ data, communications networks, devices, and applications as entry points to disrupt Americans’ daily lives, conduct espionage activities, and push disinformation and propaganda campaigns in an attempt to undermine our democracy and gain worldwide influence and control. This is all a detriment to our national security interests.

One such adversary that has aggressively pursued this strategy is the People’s Republic of China (PRC). It has backed hackers to disrupt our communications networks¹ and used “deceptive and coercive methods” to shape global information. As described by the U.S. Department of State, its goals are to promote “digital authoritarianism.”² They have accomplished some of these goals

¹ <https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a>.

² <https://www.state.gov/gec-special-report-how-the-peoples-republic-of-china-seeks-to-reshape-the-global-information-environment/>.

through coercion of companies headquartered in the PRC. One way it does so is through its National Intelligence Law of 2017, which requires PRC individuals and entities to support PRC intelligence services, including by providing data without regard to where that data was collected and without any mechanism of due process.³

Beijing ByteDance Technology is a Chinese internet technology company headquartered in Beijing and operating in the United States through a holding company (“ByteDance Ltd.”) incorporated in the Cayman Islands.⁴ ByteDance Ltd., founded and headquartered in Beijing, was formed in 2012 and launched a number of applications and products which became extremely popular, including TikTok.⁵

TikTok is now one of the most popular social media platforms in the world. It is available in over 150 countries and serves over 1 billion users.⁶ In the United States, TikTok has over 170 million users and is especially popular among teenagers and young adults who represent 35 percent of its American user base.⁷

Foreign adversary controlled applications present a clear threat to the national security of the United States. This includes TikTok due to ByteDance, Ltd.’s ownership of the application.⁸

Outside reporting has indicated the breadth of TikTok’s reach, suggesting that its data collection practices extend to age, phone number, precise location, internet address, device used, phone contacts, social network connections, the content of private messages sent through the application, and videos watched.⁹ The risk posed by TikTok though is exacerbated by the difficulty in assessing precisely which categories of data it collects. For example, outside researchers have found embedded vulnerabilities that allow the company to collect more data than the app’s privacy policy indicates.¹⁰

Additionally, public reporting has repeatedly confirmed statements made by the Executive Branch regarding the tight interlinkages between ByteDance Ltd., TikTok, and the Chinese Communist Party (CCP). For example, the Secretary of ByteDance Ltd.’s CCP committee, Zhang Fuping, also serves as ByteDance Ltd.’s Editor-in-Chief and Vice President and has vowed that the CCP committee would “take the lead” across “all product lines and business lines,” which includes TikTok.

³ U.S. DEPARTMENT OF HOMELAND SECURITY, OFFICE OF STRATEGY, POLICY & PLANS, DATA SECURITY BUSINESS ADVISORY: RISKS AND CONSIDERATIONS FOR BUSINESSES USING DATA SERVICES AND EQUIPMENT FROM FIRMS LINKED TO THE PEOPLE’S REPUBLIC OF CHINA at 6 (December 22, 2020), https://www.dhs.gov/sites/default/files/publications/20_1222_data-security-business-advisory.pdf.

⁴ Beijing ByteDance Technology and its Cayman Island holding company, ByteDance Ltd., will interchangeably be referred to as “ByteDance.”

⁵ Joe Tidy and Sophia Smith Galer, *TikTok: The story of a social media giant*, BBC News (5 August 2020), <https://www.bbc.com/news/technology-53640724>.

⁶ *TikTok Statistics For 2024: Users, Demographics, Trend*, What’s The Big Data (Nov. 29, 2023), <https://whatsthebigdata.com/tiktok-statistics/>.

⁷ Jamie Ding, *Why TikTok is dangerously good at making you spend money*, L.A. Times (Dec. 3, 2023), <https://www.latimes.com/business/story/2023-12-03/why-tiktok-is-dangerously-good-at-making-you-spend-money>.

⁸ Judy Woodruff, *CIA Director Bill Burns on War in Ukraine, Intelligence Challenges Posed by China*, PBS (Dec. 16, 2022, 6:50 P.M.), <https://www.pbs.org/newshour/show/cia-director-bill-burns-on-war-in-ukraine-intelligence-challenges-posed-by-china>.

⁹ Geoffrey A. Fowler, *Is it time to delete TikTok? A guide to the rumors and the real privacy risks*, WASH. POST (July 13, 2020), <https://www.washingtonpost.com/technology/2020/07/13/tiktok-privacy/>. See also Office of the Director of National Intelligence, *National Counterintelligence and Security Center, “Operations Security (OPSEC) Advisory, TikTok Concerns and Vulnerabilities”* (Mar. 2023), https://www.dni.gov/files/NCSC/documents/nittf/OPSEC_Advisory_TikTok_Concerns_and_Vulnerabilities.pdf.

¹⁰ Fowler, *supra* note 2.

Moreover, pursuant to the PRC's laws, the PRC can require a company headquartered in the PRC to surrender all its data to the PRC, making companies headquartered there an espionage tool of the CCP:

- The National Intelligence Law, passed in China in 2017, requires that “any organization” must assist or cooperate with CCP intelligence work.¹¹ Such assistance or cooperation must also remain secret at the PRC's request.¹²
- The PRC's 2014 Counter-Espionage Law requires that “relevant organizations . . . may not refuse” to collect evidence for an investigation.¹³
- The PRC's Data Security Law of 2021 establishes that the PRC has the power to access and control private data.¹⁴
- The PRC's Counter-Espionage Law grants PRC security agencies nearly unfettered discretion, if acting under an unrestricted understanding of national security, to access data from companies.¹⁵

As a result, the Department of Homeland Security has warned that “[t]he PRC's data collection actions result in numerous risks to U.S. businesses and customers, including: the theft of trade secrets, of intellectual property, and of other confidential business information; violations of U.S. export control laws; violations of U.S. privacy laws; breaches of contractual provisions and terms of service; security and privacy risks to customers and employees; risk of PRC surveillance and tracking of regime critics; and reputational harm to U.S. businesses.”¹⁶ These risks are imminent, but other, unforeseen risks may also exist.

Prior to 2022, several federal agencies, including the Departments of Defense, State, and Homeland Security, issued orders banning TikTok on devices for which those specific agencies are responsible.¹⁷ A majority of states in the United States have banned TikTok on state government devices due to the national security threat posed by the application under its current ownership.¹⁸

As has been widely reported, TikTok has proposed an alternative to a ban, a proposal referred to as “Project Texas,” which is an initiative to try and satisfy concerns relating to TikTok's handling of U.S. user data. This proposal was rolled out in July 2022. Under the proposal, U.S. user data would be stored in the United States, using the infrastructure of a trusted third party.¹⁹ How-

¹¹ Joe McDonald & Zen Soo, *Why Does US See Chinese-Owned TikTok as a Security Threat?*, AP NEWS (Mar. 24, 2023, 10:24 A.M.), <https://apnews.com/article/tiktok-bytedance-shou-zi-chew-8d8a6a9694357040d484670b7f4833be>.

¹² U.S. DEPARTMENT OF HOMELAND SECURITY, OFFICE OF STRATEGY, POLICY & PLANS, DATA SECURITY BUSINESS ADVISORY: RISKS AND CONSIDERATIONS FOR BUSINESSES USING DATA SERVICES AND EQUIPMENT FROM FIRMS LINKED TO THE PEOPLE'S REPUBLIC OF CHINA at 6 (December 22, 2020), https://www.dhs.gov/sites/default/files/publications/20_1222_data-security-business-advisory.pdf.

¹³ McDonald & Soo, *infra* note 5.

¹⁴ Code Civil, Data Security Law of the People's Republic of China, 2021, art (China).

¹⁵ Library of Congress, China: Counterespionage Law Revised, <https://www.loc.gov/item/global-legal-monitor/2023-09-21/china-counterespionage-law-revised/>.

¹⁶ DATA SECURITY BUSINESS ADVISORY, *supra* note 6.

¹⁷ See, e.g., Neil Vigdor, “U.S. Military Branches Block Access to TikTok App Amid Pentagon Warning,” N.Y. TIMES (Jan. 4, 2020), <https://www.nytimes.com/2020/01/04/us/tiktok-pentagon-military-ban.html>.

¹⁸ Sawdah Bhainmiya, *Here's a full list of the US states that have introduced full or partial TikTok bans on government devices over mounting security concerns*, Business Insider (Jan. 15, 2023, 5:00 AM), <https://www.businessinsider.com/tiktok-banned-us-government-state-devices-2023-1>.

¹⁹ TikTok Response to Sen Blackburn, June 30, 2022, <https://www.blackburn.senate.gov/services/files/A5027CD8-73DE-4571-95B0-AA7064F707C1>, p.2.

ever, under the initiative, the application algorithm, source code, and development activities would remain in China under ByteDance Ltd.'s control and subject to PRC laws, subject to proposed safeguards relating to cloud infrastructure and other data security concerns. Project Texas would also allow ByteDance Ltd. to continue to have a role in certain aspects of TikTok's U.S. operations.²⁰

Additionally, Project Texas would allow TikTok to continue to rely on the engineers and back-end support in China to update its algorithms and the source code needed to run the TikTok application in the U.S.²¹ But allowing code development in and access to U.S. user data from China potentially exposes U.S. users to malicious code, backdoor vulnerabilities, surreptitious surveillance, and other problematic activities tied to source code development. Furthermore, allowing back-end support, code development, and operational activities to remain in China would also require TikTok to continue to send U.S. user data to China to update the machine learning algorithms and source code for the application, and to conduct related back-end services, like managing users' accounts.²²

As of March 2024, Project Texas has not been completed. Until Project Texas is complete, Beijing-based employees of TikTok can access U.S. user data.²³

Finally, as TikTok's popularity continues to grow in the United States, so does the risk it poses. Attempted action by the Executive Branch to mitigate these risks has proven unsuccessful, and therefore Congress must act to provide congressional authority to protect U.S. national security.

Congress has previously taken such action with respect to media companies in passing the Communications Act of 1934, which limits foreign investment in television and radio broadcast licenses.²⁴ These foreign ownership restrictions were originally adopted to protect national security interests during wartime by preventing the airing of foreign propaganda on broadcast stations.²⁵ Today, applications like TikTok operate in similar manner as other media companies in the United States, and therefore they should be subject to foreign ownership scrutiny too.

Below is a list of public statements that have been made regarding the national security risks posed by ByteDance Ltd., TikTok, and the CCP as well as past and ongoing actions being taken to mitigate the national security risks associated with these entities and similarly situated companies:

- In May 2019, in connection with a review by the Committee on Foreign Investment in the United States (CFIUS), a company based in the PRC agreed to divest its interest in a popular software application reportedly due to concerns relat-

²⁰ See, e.g., *TikTok v. Trump*, 490 F.Supp.3d 73 (D.D.C. Sept. 27, 2020); *Marland v. Trump*, 20-cv-04597 (E.D. Pa. Sept. 18, 2020).

²¹ *Id.*, p.3-5.

²² See, e.g., Emily Baker White, EXCLUSIVE: TikTok Spied On Forbes Journalists, *Forbes* (December 22, 2022), <https://www.forbes.com/sites/emilybaker-white/2022/12/22/tiktok-tracks-forbes-journalists-bytedance/?sh=68c05b5d7da5>.

²³ Christianna Silva, What is Project Texas, TikTok's Best Chance to Avoid a Deal, *Mashable* (March 28, 2023), <https://mashable.com/article/project-texas-tiktok>.

²⁴ 47 U.S.C. 310(b).

²⁵ *In re Commission Policies and Procedures Under Section 310(b)(4) of the Communications Act, Foreign Investment in Broadcast Licenses*, 28 FCC Rcd 16244 (2013), <https://www.fcc.gov/document/fcc-clarifies-policy-foreign-investment-broadcast-licensees-0>.

ing to potential access by the PRC to American user data from the application.²⁶

- On May 15, 2019, the President of the United States (President) issued an Executive Order on Securing the Information and Communications Technology and Services Supply Chain, which stated that “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 . . . constitutes an unusual and extraordinary threat to the national security, foreign policy, and economy of the United States.”²⁷

- On August 2, 2020, then-Secretary of State Mike Pompeo stated that PRC-based companies “are feeding data directly to the Chinese Communist Party, their national security apparatus.”²⁸

- On August 6, 2020, the President concluded that TikTok “automatically captures vast swaths of information from its users” and that TikTok’s ownership by ByteDance Ltd. enables the PRC and CCP to gain access to “Americans’ personal and proprietary information,” potentially allowing the CCP “to track the locations of Federal employees and contractors, build dossiers of personal information for blackmail, and conduct corporate espionage.”²⁹

- On August 6, 2020, the President issued an Executive Order (E.O. 13942) that directed the Secretary of Commerce to take actions that would have prohibited certain transactions related to TikTok in 45 days if ByteDance failed to divest its ownership of TikTok.³⁰ The companies and content creators using the TikTok mobile application filed lawsuits challenging those prohibitions, as a result of which two district courts issued preliminary injunctions enjoining the prohibitions.³¹

- On August 14, 2020, the President found “there is credible evidence . . . that ByteDance Ltd. . . . might take action that threatens to impair the national security of the United States.”³²

- On August 14, 2020, the President issued an Executive Order directing ByteDance Ltd. to divest any assets or property used to enable or support ByteDance Ltd.’s operation of the TikTok application in the United States and any data ob-

²⁶Zack Whittaker, *Grindr sold by Chinese owner after US raised national security concerns*, *Tech Crunch*. (March 6, 2020, 1:06 PM), <https://techcrunch.com/2020/03/06/grindr-sold-china-national-security/>.

²⁷Exec. Order No. 13,873, 84 FR 22689 (May 15, 2019), <https://www.federalregister.gov/documents/2019/05/17/2019-10538/securing-the-information-and-communications-technology-and-services-supply-chain>.

²⁸Ronn Blitzer, *Pompeo Warns TikTok Users’ Personal Info Could Be Going Directly to the Chinese Communist Party*, *FOX NEWS* (Aug. 2, 2020, 12:39 P.M.), <https://www.foxnews.com/politics/pompeo-warns-tiktok-users-data-including-facial-pattern-residence-phone-number-could-be-going-directly-to-the-chinese-communist-party>.

²⁹Exec. Order No. 13,942, 85 Fed. Reg. 48,637 (Aug. 6, 2020), <https://www.federalregister.gov/documents/2020/08/11/2020-17699/addressing-the-threat-posed-by-tiktok-and-taking-additional-steps-to-address-the-national-emergency> (revoked by Exec. Order No. 14,034 (June 9, 2021), <https://www.federalregister.gov/documents/2021/06/11/2021-12506/protecting-americans-sensitive-data-from-foreign-adversaries>).

³⁰Exec. Order No. 13942, 85 Fed. Reg. 51297 (Aug. 6, 2020).

³¹*See, e.g., TikTok v. Trump*, 490 F.Supp.3d 73 (D.D.C. Sept. 27, 2020); *Marland v. Trump*, 20-cv-04597 (E.D. Pa. Sept. 18, 2020).

³²Order of August 14, 2020, 85 Fed. Reg. 51,297 (Aug. 19, 2020), <https://www.govinfo.gov/content/pkg/FR-2020-08-19/pdf/2020-18360.pdf>.

tained or derived from TikTok application or musical.ly application users in the United States.³³ The Order, however, remains the subject of litigation.

- On September 17, 2020, the Department of Commerce concluded that the PRC, to advance “its intelligence-gathering and to understand more about who to target for espionage, whether electronically or via human recruitment,” is constructing “massive databases of Americans’ personal information” and that ByteDance Ltd. has close ties to the CCP, including a cooperation agreement with a security agency and over 130 CCP members in management positions.³⁴

- Following the multiple judicial rulings that enjoined the Executive Branch from enforcing the regulations contemplated in E.O. 13942, on June 9, 2021, the President issued a new Executive Order that rescinded E.O. 13942 and directed the Secretary of Commerce to assess and take action, where possible, against connected software applications that pose a threat to national security more broadly.³⁵

- On June 9, 2021, the President issued an Executive Order on Protecting Americans’ Sensitive Data from Foreign Adversaries, which stated that “[f]oreign adversary access to large repositories of United States persons’ data also presents a significant risk.”³⁶ The EO stated that “the United States must act to protect against the risks associated with connected software applications that are designed, developed, manufactured, or supplied by persons owned or controlled by, or subject to the jurisdiction or direction of, a foreign adversary.”³⁷

- On October 26, 2021, lawmakers expressed concerns that TikTok’s audio and user location data could be used by the CCP during the testimony of Michael Beckerman, TikTok head of public policy for the Americas and registered lobbyist for ByteDance Ltd., before a Senate Commerce Subcommittee on Consumer Protection hearing.³⁸

- On June 17, 2022, public reporting revealed that leaked audio from more than 80 internal TikTok meetings, China-based employees of ByteDance Ltd. repeatedly accessed non-public data about U.S. TikTok users, including the physical locations of specific U.S. citizens.³⁹

- On September 14, 2022, lawmakers expressed concerns over TikTok’s algorithm and content recommendations posing a national security threat during a hearing before the Senate

³³ Order of Aug. 14, 2020, “Regarding the Acquisition of Musical.ly By Bytedance Ltd.” 85 Fed. Reg. 51297 (Aug. 19, 2020).

³⁴ *TikTok Inc. v. Trump*, 490 F. Supp. 3d 73, 78 (D.D.C. 2020) (mem.). [BETTER CITATION: U.S. Dep’t of Commerce, Mem. for the Sec’y, *Proposed Prohibited Transactions Related to TikTok Pursuant to Executive Order 13942* (Sept. 17, 2020), ECF No. 22–1]

³⁵ Exec. Order No. 14034, 86 Fed. Reg. 31423 (June 9, 2021).

³⁶ Exec. Order No. 14,034, 86 FR 31423 (Jun 9, 2021), <https://www.federalregister.gov/documents/2021/06/11/2021-12506/protecting-americans-sensitive-data-from-foreign-adversaries>.

³⁷ *Id.*

³⁸ Diane Bartz & Sheila Dang, *TikTok Tells U.S. Lawmakers It Does Not Give Information to China’s Government*, REUTERS (Oct. 26, 2021, 4:53 P.M.), <https://www.reuters.com/technology/tiktok-tells-us-lawmakers-it-does-not-give-information-chinas-government-2021-10-26/>.

³⁹ Emily Baket-White, *Leaked Audio From 80 Internal TikTok Meetings Shows That US User Data Has Been Repeatedly Accessed From China*, BUZZFEED. (June, 17, 2022), [HTTPS://WWW.BUZZFEEDNEWS.COM/ARTICLE/EMILYBAKERWHITE/TIKTOK-TAPES-US-USER-DATA-CHINA-BYTEDANCE-ACCESS](https://www.buzzfeednews.com/article/emilybakerwhite/tiktok-tapes-us-user-data-china-bytedance-access).

Committee on Homeland Security and Governmental Affairs with Vanessa Pappas, Chief Operating Officer of TikTok.⁴⁰

- On November 15, 2022, Federal Bureau of Investigation (FBI) Director Christopher Wray testified before the House Committee on Homeland Security that TikTok’s national security concerns “include the possibility that the [CCP] could use it to control data collection on millions of users or control the recommendation algorithm, which could be used for influence operations if they so choose, or to control software on millions of devices, which gives it an opportunity to potentially technically compromise personal devices.”⁴¹

- On December 2, 2022, FBI Director Wray stated that TikTok’s data repositories on Americans “are in the hands of a government that doesn’t share our values and that has a mission that’s very much at odds with what’s in the best interests of the United States. . . . The [CCP] has shown a willingness to steal Americans data on a scale that dwarfs any other.”⁴²

- On December 5, 2022, Director of National Intelligence Avril Haines stated, when asked about TikTok and PRC ownership, “It is extraordinary the degree to which [the PRC] . . . [is] developing [] frameworks for collecting foreign data and pulling it in, and their capacity to then turn that around and use it to target audiences for information campaigns and other things, but also to have it for the future so that they can use it for a variety of means.”⁴³

- On December 16, 2022, Central Intelligence Agency Director William Burns explained that “because the parent company of TikTok is a [PRC] company, the [CCP] is able to insist upon extracting the private data of a lot of TikTok users in this country, and also to shape the content of what goes on to TikTok as well to suit the interests of the Chinese leadership.”⁴⁴

- On December 22, 2022, public reporting revealed that ByteDance Ltd. employees accessed TikTok user data and IP addresses to monitor the physical locations of specific U.S. citizens.⁴⁵

- On December 29, 2022, following its adoption by Congress, the President signed into law a bill banning the use of TikTok

⁴⁰ Vanessa Pappas, Testimony Before the U.S. Senate Committee on Homeland Security and Governmental Affairs, <https://www.hsgac.senate.gov/wp-content/uploads/imo/media/doc/Testimony-Pappas-2022-09-14-REVISED.pdf>.

⁴¹ Ariana Figueroa, *Members of Congress Sign Up for TikTok, Despite Security Concerns*, IDAHO CAP. SUN (Jan. 19, 2023, 12:26 P.M.), <https://idahocapitalsun.com/2023/01/19/members-of-congress-sign-up-for-tiktok-despite-security-concerns/>.

⁴² Anisha Kohli, *Why the FBI Is Concerned About TikTok*, TIME MAG. (Dec. 3, 2022, 3:42 P.M.), <https://time.com/6238540/tiktok-fbi-security-concerns/>.

⁴³ Transcript, Avril Haines, Dir. of Nat’l Intel., Fireside Chat with DNI Haines at the Reagan National Defense Forum (Dec. 3, 2022), <https://www.dni.gov/index.php/newsroom/news-articles/news-articles-2022/3660-fireside-chat-with-dni-haines-at-the-reagan-national-defense-forum>.

⁴⁴ Judy Woodruff, *CIA Director Bill Burns on War in Ukraine, Intelligence Challenges Posed by China*, PBS (Dec. 16, 2022, 6:50 P.M.), <https://www.pbs.org/newshour/show/cia-director-bill-burns-on-war-in-ukraine-intelligence-challenges-posed-by-china>.

⁴⁵ Emily Baker White, *EXCLUSIVE: TikTok Spied On Forbes Journalists*, *Forbes* (December 22, 2022), <https://www.forbes.com/sites/emilybaker-white/2022/12/22/tiktok-tracks-forbes-journalists-bytedance/?sh=68c05b5d7da5>.

on government devices due to the national security threat posed by the application under its current ownership.⁴⁶

- On January 20, 2023, public reporting revealed that TikTok and ByteDance Ltd. employees regularly engage in practice called “heating,” which is a manual push to ensure specific videos “achieve a certain number of video views.”⁴⁷

- In a court filing in June 2023, a former employee of ByteDance Ltd. alleged that the CCP spied on pro-democracy protestors in Hong Kong in 2018 by using backdoor access to TikTok to identify and monitor activists’ locations and communications.⁴⁸

- On November 1, 2023, public reporting revealed that 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.⁴⁹

- In February 2023, Deputy Attorney General Lisa Monaco stated, “Our intelligence community has been very clear about [the CCP’s] efforts and intention to mold the use of [TikTok] using data in a worldview that is completely inconsistent with our own.”⁵⁰ Deputy AG Monaco also stated, “I don’t use TikTok and I would not advise anybody to do so because of [national security] concerns.”⁵¹

- On February 28, 2023, former Deputy National Security Advisor Matthew Pottinger emphasized that it has already been confirmed that TikTok’s parent company ByteDance has used the app to surveil U.S. journalist as a means to identify and retaliate against potential sources. The PRC has also shown a willingness to harass individuals abroad who take stances that contradict the Communist Party lines.⁵² The app can further be employed to help manipulate social discourse and amplify false information to tens of millions of Americans.⁵³

⁴⁶ David Ingram, *Biden Signs TikTok Ban for Government Devices, Setting Up a Chaotic 2023 for the App*, NBC NEWS (Dec. 30, 2022, 4:24 P.M.), <https://www.nbcnews.com/tech/tech-news/tiktok-ban-biden-government-college-state-federal-security-privacy-rcna63724>.

⁴⁷ Emily Baker-White, *TikTok’s Secret ‘Heating’ Button Can Make Anyone Go Viral*, FORBES (Jan. 20, 2023), <https://www.forbes.com/sites/emilybaker-white/2023/01/20/tiktoks-secret-heating-button-can-make-anyone-go-viral/?sh=62d61d006bfd>.

⁴⁸ Brian Fung, *Analysis: There is now some public evidence that China viewed TikTok data*, CNN (June 8, 2023, 10:28 A.M.), <https://www.cnn.com/2023/06/08/tech/tiktok-data-china/index.html>.

⁴⁹ Emily Baker-White, *A Platform Storing TikTok Corporate Secrets Was Inspected By The Chinese Government*, FORBES (Nov. 1, 2023, 6:30 A.M.), <https://www.forbes.com/sites/emilybaker-white/2023/11/01/a-platform-storing-tiktok-corporate-secrets-was-inspected-by-the-chinese-government/?sh=193ba64e23b2>.

⁵⁰ John D. McKinnon, *U.S. Threatens Ban if TikTok’s Chinese Owners Don’t Sell Stakes*, WALL ST. J. (Mar. 15, 2023, 6:45 P.M.), <https://www.wsj.com/articles/u-s-threatens-to-ban-tiktok-if-chinese-founder-doesnt-sell-ownership-stake-36d7295c>.

⁵¹ Lauren Feiner, *High-Ranking DOJ Official Says She ‘Would Not Advise’ Consumers to Use TikTok, Citing Security Concerns*, CNBC (Feb. 16, 2023, 4:55 P.M.), <https://www.cnbc.com/2023/02/16/doj-lisa-monaco-warns-against-tiktok-use-citing-security-concerns.html>.

⁵² On Hong Kong Authorities’ Transnational Repression, Press Statement, Anthony J. Blinken, Secretary of State (Dec. 15, 2023), <https://www.state.gov/on-hong-kong-authorities-transnational-repression/>; *Transnational Repression*, Freedom House, <https://freedomhouse.org/report/transnational-repression>; The PRC has also shown itself willing to harass Americans on U.S. soil. See, e.g., Josh Rogin, *Chinese police stations in NYC are part of a vast influence operation*, THE WASHINGTON POST (Apr. 19, 2023), <https://www.washingtonpost.com/opinions/2023/04/19/chinese-police-new-york-city-foreign-influence/>.

⁵³ Matthew Pottinger, Testimony Before the U.S. House Select Committee on the Chinese Communist Party, <https://selectcommitteeontheccp.house.gov/sites/evo-subsites/selectcommitteeontheccp.house.gov/files/evo-media-document/2.28.2023-hearing-transcript.pdf>.

- On March 8, 2023, FBI Director Christopher Wray testified before the Senate Permanent Select Committee on Intelligence that the CCP, through its ownership of ByteDance, could use TikTok to collect and control users' data and drive divisive narratives internationally.⁵⁴
- On March 22, 2023, elements of the intelligence community provided a classified briefing on the threat to members of the U.S. House of Representatives Permanent Select Committee on Intelligence and leadership of the Committee on Energy and Commerce.
- On March 23, 2023, Secretary of State Antony Blinken testified before the House Committee on Foreign Affairs that TikTok is a threat to national security that should be "ended one way or another."⁵⁵
- On March 23, 2023, during the testimony of TikTok CEO Shou Chew before the House Committee on Energy and Commerce, lawmakers expressed concerns about the safety and security of the app, including TikTok's relationship with the CCP.⁵⁶
- On March 23, 2023, Nury Turkel, the Chair of the United States Commission on International Religious Freedom, raised the alarm that TikTok's parent company, ByteDance Ltd., has a strategic partnership with China's Ministry of Public Security, and China's domestic version of the app, Douyin, has been used to collect sensitive information from Uyghurs and other oppressed ethnic minority groups.⁵⁷
- On April 26, 2023, the Executive Branch provided a classified briefing to members of the United States Senate Committee on Commerce, Science, and Transportation and the Senate Select Committee on Intelligence on the threat.
- On May 30, 2023, public reporting revealed that TikTok has stored sensitive financial information, including the Social Security numbers and tax identifications of TikTok influencers and United States small businesses, on servers in China accessible by ByteDance Ltd. employees.⁵⁸
- On June 5, 2023, the Executive Branch provided a classified briefing to staff of the United States Senate Committee on Banking and the U.S. House of Representatives Committee on Energy and Commerce on the threat.
- In June 2023, at the request of the House Permanent Select Committee on Intelligence, the intelligence community provided a classified threat briefing open to all members in the U.S. House of Representatives.

⁵⁴ *FBI Chief Says TikTok 'Screams' of US National Security Concerns*, REUTERS (Mar. 9, 2023, 4:43 P.M.), <https://www.reuters.com/technology/fbi-chief-says-tiktok-screams-us-national-security-concerns-2023-03-08/>.

⁵⁵ Houston Keene, *Blinken Suggests TikTok 'Should Be Ended One Way or Another'*, FOX NEWS (Mar. 23, 2023, 6:11 P.M.), <https://www.foxnews.com/politics/blinken-tiktok-should-be-ended>.

⁵⁶ Dara Kerr, *Lawmakers Grilled TikTok CEO Chew for 5 Hours in a High-Stakes Hearing About the App*, NPR (Mar. 23, 2023, 5:34 P.M.), <https://www.npr.org/2023/03/23/1165579717/tiktok-congress-hearing-shou-zi-chew-project-texas>.

⁵⁷ Nury Turkel, *Testimony Before the U.S. House Select Committee on the Chinese Communist Party*, <https://selectcommitteeontheccp.house.gov/sites/evo-subsites/selectcommitteeontheccp.house.gov/files/evo-media-document/3.23.23-hearing-transcript.pdf>.

⁵⁸ Alexandra S. Levine, *TikTok Creators' Financial Info, Social Security Numbers Have Been Stored In China*, FORBES (May 30, 2023, 6:30 A.M.), <https://www.forbes.com/sites/alexandralevine/2023/05/30/tiktok-creators-data-security-china/?sh=1af8f2657048>.

- On July 26, 2023, William Evanina, the former director of the National Counterintelligence and Security Center, pointed to TikTok as just one of many areas of concern regarding the CCP’s capabilities and intent as an adversarial, malign competitor.⁵⁹
- On September 28, 2023, the U.S. Department of State’s Global Engagement Center issued a report that found that “TikTok [c]reates [o]pportunities for PRC [g]lobal [c]ensorship. The report stated that U.S. Government information as of late 2020 showed that “ByteDance maintained a regularly updated internal list identifying people who were likely blocked or restricted from all ByteDance platforms, including TikTok, for reasons such as advocating for Uyghur independence.”
- On November 15, 2023, elements of the intelligence community provided a classified briefing to the United States Senate Select Committee on Intelligence and the Committee on Commerce, Science, and Transportation on the PRC’s conduct of global foreign malign influence operations, including through platforms such as TikTok.⁶⁰
- On November 30, 2023, John Garnaut of the Australian Strategic Policy Institute remarked that TikTok has sophisticated capabilities that create the risk that TikTok can clandestinely shape narratives and elevate favorable opinions while suppressing statements and news that the PRC deems negative.⁶¹
- On January 18, 2024, the U.S. House of Representatives Select Committee on Strategic Competition between the United States and the Chinese Communist Party was briefed by a set of senior interagency officials to discuss these matters.
- On January 31, 2024, FBI Director Wray testified before the Select Committee on Strategic Competition between the United States and the Chinese Communist Party that TikTok gives the PRC “the ability to control data collection on millions of users, which can be used for all sorts of intelligence operations or influence operations,” and “the ability, should they so choose, to control the software on millions of devices, which means the opportunity to technically compromise millions of devices.”⁶²
- On February 29, 2024, the U.S. House of Representatives Committee on Energy and Commerce was briefed by a set of senior interagency officials to discuss these matters.

⁵⁹William Evanina, Testimony Before the U.S. House Select Committee on Strategic Competition between the United States and the Chinese Communist Party, <https://selectcommitteeontheccp.house.gov/sites/evo-subsites/selectcommitteeontheccp.house.gov/files/evo-media-document/7.26.23-hearing-transcript.pdf>.

⁶⁰Reuters, U.S. to Brief Senators on Foreign Online Influence Focused on Israel, Ukraine (November 15, 2023), <https://www.reuters.com/world/us/us-senators-get-classified-briefing-foreign-online-influence-2023-11-15/>.

⁶¹John Garnaut, Testimony Before the U.S. House Select Committee on the Chinese Communist Party, <https://selectcommitteeontheccp.house.gov/sites/evo-subsites/selectcommitteeontheccp.house.gov/files/evo-media-document/11.30.23-hearing-transcript.pdf>.

⁶²The CCP Cyber Threat to the American Homeland and National Security, Hearing, The Select Committee on the CCP (March 1, 2024), <https://selectcommitteeontheccp.house.gov/committee-activity/hearings/hearing-notice-ccp-cyber-threat-american-homeland-and-national-security>.

COMMITTEE ACTION

On March 23, 2023, the Committee on Energy and Commerce held a full committee hearing. The title of the hearing was “TikTok: How Congress Can Safeguard American Data Privacy and Protect Children from Online Harms.” The Committee received testimony from:

- Shou Chew, CEO, TikTok Inc.

On March 7, 2024, the Committee on Energy and Commerce held a full committee hearing to review H.R. 7521. The title of the hearing was “Legislation to Protect Americans from the National Security Threats Posed by Foreign Adversary Controlled Applications.” The Committee met in executive session pursuant to a motion by Chair Rodgers, which was adopted by a record vote of 43 yeas and 0 nays.

On March 7, 2024, the full Committee on Energy and Commerce met in open markup session and ordered H.R. 7521 favorably reported, without amendment, to the House by a record vote of 50 yeas and 0 nays.

COMMITTEE VOTES

Clause 3(b) of rule XIII requires the Committee to list the record votes on the motion to report legislation and amendments thereto. The following reflects the record votes taken during the Committee consideration:

**COMMITTEE ON ENERGY AND COMMERCE
118TH CONGRESS
ROLL CALL VOTE # 1**

BILL: H.R. 7521, Prohibition of Foreign Adversary Controlled Applications Act

AMENDMENT: A motion by Chair Rodgers to order H.R. 7521, Prohibition of Foreign Adversary Controlled Applications Act favorably reported to the House, without amendment. (Final Passage)

DISPOSITION: AGREED TO, by a roll call vote of 50 yeas to 0 nays.

REPRESENTATIVE	YEAS	NAYS	PRESENT	REPRESENTATIVE	YEAS	NAYS	PRESENT
Rep. Rodgers	X			Rep. Pallone	X		
Rep. Burgess	X			Rep. Eshoo	X		
Rep. Latta	X			Rep. DeGette	X		
Rep. Guthrie	X			Rep. Schakowsky	X		
Rep. Griffith	X			Rep. Matsui	X		
Rep. Bilirakis	X			Rep. Castor	X		
Rep. Bucshon	X			Rep. Sarbanes	X		
Rep. Hudson	X			Rep. Tonko	X		
Rep. Walberg	X			Rep. Clarke	X		
Rep. Carter	X			Rep. Cárdenas	X		
Rep. Duncan	X			Rep. Ruiz	X		
Rep. Palmer	X			Rep. Peters	X		
Rep. Dunn	X			Rep. Dingell	X		
Rep. Curtis	X			Rep. Veasey	X		
Rep. Lesko	X			Rep. Kuster	X		
Rep. Pence	X			Rep. Kelly	X		
Rep. Crenshaw	X			Rep. Barragán	X		
Rep. Joyce	X			Rep. Blunt Rochester			
Rep. Armstrong	X			Rep. Soto	X		
Rep. Weber	X			Rep. Craig	X		
Rep. Allen	X			Rep. Schrier	X		
Rep. Balderson	X			Rep. Trahan	X		
Rep. Fulcher	X			Rep. Fletcher	X		
Rep. Pfluger	X						
Rep. Harshbarger	X						
Rep. Miller-Meeks	X						
Rep. Cammack	X						
Rep. Obernolte	X						

OVERSIGHT FINDINGS AND RECOMMENDATIONS

Pursuant to clause 2(b)(1) of rule X and clause 3(c)(1) of rule XIII, the Committee held hearings and made findings that are reflected in this report.

NEW BUDGET AUTHORITY, ENTITLEMENT AUTHORITY, AND TAX EXPENDITURES

Pursuant to clause 3(c)(2) of rule XIII, the Committee finds that H.R. 7521 would result in no new or increased budget authority, entitlement authority, or tax expenditures or revenues.

CONGRESSIONAL BUDGET OFFICE ESTIMATE

Pursuant to clause 3(c)(3) of rule XIII, at the time this report was filed, the cost estimate prepared by the Director of the Congressional Budget Office pursuant to section 402 of the Congressional Budget Act of 1974 was not available.

FEDERAL MANDATES STATEMENT

The Committee adopts as its own the estimate of Federal mandates prepared by the Director of the Congressional Budget Office pursuant to section 423 of the Unfunded Mandates Reform Act.

STATEMENT OF GENERAL PERFORMANCE GOALS AND OBJECTIVES

Pursuant to clause 3(c)(4) of rule XIII, the general performance goal or objective of this legislation is to force a divestiture or prohibit the distribution, maintenance, or updating of foreign adversary controlled applications.

DUPLICATION OF FEDERAL PROGRAMS

Pursuant to clause 3(c)(5) of rule XIII, no provision of H.R. 7521 is known to be duplicative of another Federal program, including any program that was included in a report to Congress pursuant to section 21 of Public Law 111–139 or the most recent Catalog of Federal Domestic Assistance.

RELATED COMMITTEE AND SUBCOMMITTEE HEARINGS

Pursuant to clause 3(c)(6) of rule XIII, the following hearings were used to develop or consider H.R. 7521:

- On March 23, 2023, the Committee on Energy and Commerce held a full committee hearing. The title of the hearing was “TikTok: How Congress Can Safeguard American Data Privacy and Protect Children from Online Harms.” The Committee received testimony from:
 - Shou Chew, CEO, TikTok Inc.
- On March 7, 2024, the Committee on Energy and Commerce held a full committee hearing to review H.R. 7521. The title of the hearing was “Legislation to Protect Americans from the National Security Threats Posed by Foreign Adversary Controlled Applications.” The Committee met in executive session pursuant to a motion by Chair Rodgers, which was adopted by a record vote of 43 yeas and 0 nays.

COMMITTEE COST ESTIMATE

Pursuant to clause 3(d)(1) of rule XIII, the Committee adopts as its own the cost estimate prepared by the Director of the Congressional Budget Office pursuant to section 402 of the Congressional Budget Act of 1974. At the time this report was filed, the estimate was not available.

EARMARK, LIMITED TAX BENEFITS, AND LIMITED TARIFF BENEFITS

Pursuant to clause 9(e), 9(f), and 9(g) of rule XXI, the Committee finds that H.R. 7521 contains no earmarks, limited tax benefits, or limited tariff benefits.

ADVISORY COMMITTEE STATEMENT

No advisory committees within the meaning of section 5(b) of the Federal Advisory Committee Act were created by this legislation.

APPLICABILITY TO LEGISLATIVE BRANCH

The Committee finds that the legislation does not relate to the terms and conditions of employment or access to public services or accommodations within the meaning of section 102(b)(3) of the Congressional Accountability Act.

SECTION-BY-SECTION ANALYSIS OF THE LEGISLATION

Section 1. Short title

This Section provides that the Act may be cited as the “Protecting Americans from Foreign Adversary Controlled Applications Act”.

Section 2. Prohibition of Foreign-Adversary Controlled Applications

Subsection (a)(1) makes it unlawful for an entity to distribute, maintain, update, or enable the distribution, maintenance, or updating of a foreign adversary controlled application in the United States.

Subsection (a)(2) provides the applicable dates of prohibitions in subsection (a)(1), which is 180 days after enactment for the foreign adversary controlled applications in (g)(3)(A), and beginning 180 days after the relevant determination in (g)(3)(B) that such application poses an unacceptable risk to national security.

Subsection (b) requires a foreign adversary controlled application to provide any U.S. user with all available data related to their account provided by that application, upon request by the user, in a machine readable format, including any data maintained by the application regarding the user’s account, such as the user’s content and all other account information.

Subsection (c) provides the exemptions for the prohibition in subsection (a). It provides that the prohibition in subsection (a) does not apply to a foreign adversary controlled application regarding which a qualified divestiture is executed and shall cease to apply if a qualified divestment is executed after the effective date. This subsection also states that subsection (a) also does not apply to services provided with respect to a foreign adversary controlled application that are necessary for an entity to attain compliance with this Act.

Subsection (d) outlines the civil penalties for an entity found violating subsection (a) or subsection (b). An entity found violating subsection (a) shall be subject an amount not to exceed the amount that results from multiplying \$5,000 by the number of U.S. users determined to have accessed, maintained, or updated an application. An entity found violating subsection (b) shall be subject to a civil penalty in an amount not to exceed \$500 per U.S. user with an account provided by that application. This subsection also directs the Attorney General to conduct investigations related to potential violations of this Act and pursue enforcement if a violation has occurred.

Subsection (e) is a severability provision. If any provision of this section or the application of this section to any person or circumstance is held invalid, the invalidity shall not affect the other provisions or applications of this section that can be given effect without the invalid provision or application. This subsection also clarifies that any invalidity of subsection (g)(3)(A) shall not affect or preclude the application from a determination as a foreign adversary controlled application under subsection (g)(3)(B).

Subsection (f) is a rule of construction stating that nothing in this Act may be construed to authorize the Attorney General to pursue enforcement other than what is specifically stated in this Act. It does not authorize the Attorney General to pursue enforcement against any individual user of the foreign adversary controlled application, nor does it alter or affect any other authority provided by or established under another provision of Federal law.

Subsection (g) defines key terms used throughout Section 2, including:

(1) The term “Controlled by a Foreign Adversary” means (A) a foreign person that is domiciled in, headquartered in, has its principal place of business in, or is organized under the laws of a foreign adversary country; (B) an entity in which an entity or combination of entities identified in subparagraph (A), directly or indirectly owns a twenty percent stake or greater; or (C) an entity subject to the direction, or control, or of an entity identified in subparagraph (A) or (B).

(2) The term “Covered Company” means an entity that operates, directly or indirectly, including through its parent company, subsidiaries, or affiliates, a website, desktop application, mobile application, or augmented or immersive technology application that permits a user to create an account or profile to generate, share, and view text, images, videos, real-time communications, or similar content; has more than 1,000,000 monthly active users for a majority of months during the preceding 3 months the Presidential determination; enables one or more users to generate or distribute content that can be viewed by other users of the website, desktop application, mobile application, or augmented or immersive technology; and enables one or more users to view content generated by other users of the website, desktop application, mobile application, or augmented or immersive technology.

(3) The term does not include any website, desktop application, or mobile application in the United States whose primary purpose is to allow users to post product reviews, business reviews, or travel information and reviews.

(4) The term “Foreign Adversary Controlled Application” means a website, desktop application, mobile application, or augmented or immersive technology application is that is operated, directly or indirectly, including through its parent company, subsidiaries, or affiliates by:

(A) any of (i) ByteDance, Ltd.; (ii) TikTok; (iii) a subsidiary of or a successor to ByteDance, Ltd. or TikTok that is controlled by a foreign adversary; or (iv) a company owned or controlled directly or indirectly by such an entity; or

(B) a covered company that is controlled by a foreign adversary; and that is determined by the President to present a significant threat to the national security of the United States following the issuance of a public notice of the proposed presidential determination, a public report to Congress, to be submitted not less than 30 days prior to the presidential determination, describing the specific national security concern, which shall contain a classified annex, and describing what assets would need to be divested to be a qualified divestiture.

(5) The term “Foreign Adversary Country” means the countries identified pursuant to section 4872(d)(2) of title 10, United States Code (North Korea, People Republic of China, Russia, Iran).

(6) The term “Internet Hosting Service” means a service through which storage and computing resources are provided to an individual or organization for the accommodation and maintenance of one or more websites or online services, and which may include file hosting, domain name server hosting, cloud hosting, and virtual private server hosting.

(7) The term “Qualified Divestiture” means a divestiture or similar transaction that the President, through an interagency process, determines results in the foreign adversary controlled application no longer being controlled by a foreign adversary; and the President determines, through an interagency process, precludes the establishment or maintenance of any operational relationship between the foreign adversary controlled application’s United States operations after the date of the transaction and any formerly affiliated entities that are controlled by a foreign adversary, including, but not limited to, any cooperation with respect to the operation of a content recommendation algorithm or agreement with respect to data sharing.

(8) The term “Source Code” means the combination of text and other characters comprising the content, both viewable and nonviewable, of a software application, including any publishing language, programming language, protocol, or functional content, as well as any successor languages or protocols.

(9) The term “United States” means the “United States” including the territories of the United States.

Section 3. Judicial review

This section requires any review challenging this Act to be filed only in the United States Court of Appeals for the District of Columbia Circuit. Subsection (b) provides that the United States Court of Appeals for the District of Columbia Circuit shall have exclusive jurisdiction over any challenge to this Act, or any action, finding, or determination under this Act. Subsection (c) places, upon enactment, a 165-day statute of limitation on any challenge

to this Act. This subsection also places a 90-day statute of limitations on any challenges to an action, finding, or determination under this Act.

CHANGES IN EXISTING LAW MADE BY THE BILL, AS REPORTED

This legislation does not amend any existing Federal statute.

