Nos. 24-656 & 24-657

IN THE

Supreme Court of the United States

TIKTOK, INC., *et al.*,

Petitioners,

v.

MERRICK B. GARLAND, ATTORNEY GENERAL

Respondent.

BRIAN FIREBAUGH, *et al.*

Petitioners,

v.

MERRICK B. GARLAND, ATTORNEY GENERAL

Respondent.

On Writs of Certiorari to the United States
Court of Appeals for the District of Columbia Circuit

BRIEF OF NATIONAL SECURITY PROFESSORS AARONSON, EDGAR, AND KLEIN AS *AMICUS CURIAE* IN SUPPORT OF PETITIONERS

MARK S. DAVIES
Counsel of Record
KUFERE LAING
EDRED RICHARDSON
WHITE & CASE LLP
701 Thirteenth Street NW
Washington, D.C 20005
(202) 626-3600
mark.davies@whitecase.com

December 27, 2024

Counsel for Amicus Curiae

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

Edenfield v. Fane,
507 U.S. 761 (1993) 25

FEC v. Cruz,
596 U.S. 289 (2022) 16, 21

Holder v. Humanitarian Law Project,
561 U.S. 1 (2010) 26

Lamont v. Postmaster Gen.,
381 U.S. 301 (1965) 12

New York Times Co. v. Sullivan,
376 U.S. 254 (1964) 12

Reno v. ACLU,
521 U.S. 844 (1997) 16

TikTok, Inc. v. Garland,
24-1113, 2024 WL 4996719 (D.C. Cir.
Dec. 6, 2024) 2, 3, 25, 26, 27

United States v. Playboy Ent. Grp.,
529 U.S. 803 (2000) 25

United States v. Robel,
289 U.S. 258 (1967) 3, 26, 27

Federal Statutes

Protecting Americans from Foreign Adversary Controlled Applications Act of 2024 (PADFA) 3, 24

Other Authorities

About Project Texas, TikTok, (Dec. 23, 2024)........ 10

Brief for Petitioners, TikTok, Inc. and Bytedance Inc., *TikTok, Inc. v. Garland*, No. 24-1183 (D.C. Cir. June 20, 2024). 5

Community Guidelines, TikTok, (Dec. 23, 2024) 9

Contracts for Dec. 7, 2022, U.S. Dep't Def., (Dec. 23, 2024)... 8

EA China, Electronic Arts, (Jun. 12, 2024).......... 14

Ellen Nakashima, *Hacks of OPM databased compromised 22.1 million people, federal authorities say*, The Wash. Post (July 9, 2015) 24

FIFA 23, Active Player, (Jun. 12, 2024) 15

Garrett M. Graff, *China's Hacking Spree Will Have a Decades-Long Fallout*, Wired (Feb. 11, 2020)....................................... 24

Gary Smith, *Top Phishing Statistics for 2024: Latest Figures and Trends*, StationX, (Apr. 10, 2024) 25

H.R. Comm. on Energy & Com., Protecting Americans from Foreign Adversary Controlled Applications Act, H.R. Rep. No. 118-417 (2024) 4, 12

Lily Hay Newman, *The NSA Seems Pretty Stressed About the Threat of Chinese Hackers in U.S. Critical Infrastructure*, Wired (Nov. 18, 2023). 25

Matt Perault & Samm Sacks, Project Texas: *The Details of TikTok's Plan to Remain Operational in the United States*, Lawfare (Jan. 26, 2023) 6

National Security Agreement 6, 7, 8, 9, 10, 11, 13, 18, 19, 20, 21, 22

The Sims 4 Becomes the Most Widely Played Game, Electronic Arts, (Apr. 18, 2023) 15

Susan A. Aaronson, *Data is Dangerous: Comparing the Risks That the United States, Canada, and Germany See in Data Trovers*, Center Int'l Gov. Innovation, (Apr. 2020)............................... 24, 25

United States (U.S.) Army to Modernize its Integrated Personnel and Pay System (IPPS-A) on Oracle Cloud Infrastructure, Oracle, (Dec. 23, 2024).. 8

INTEREST OF THE *AMICUS CURIAE*

This brief is submitted on behalf of Professors Susan A. Aaronson, Timothy H. Edgar, and Hans Klein ("Amici").[1]

Amici are internationally prominent scholars who specialize in the intersections of national security, AI, cybersecurity, data, internet governance, and public affairs.

Professor Aaronson is a Research Professor at the Elliot School of International Affairs at George Washington University and a George Washington University Public Interest Technology Scholar. She is also co-principal investigator with the National Science Foundation and National Institute of Standard Technology Institute for Trustworthy AI in Law & Society, where she leads research on data and AI governance.

Professor Edgar is a Professor of the Practice of Computer Science at Brown University, Senior Fellow at the Watson Institute of International and Public Affairs, and Lecturer on Law at Harvard Law School. He helped launch Brown University's professional Cybersecurity degree program. Prior to his academic career, Professor Edgar served as the first-ever privacy and civil liberties official in the White House National Security Staff under President Barack Obama, and as a privacy official in the Office of the

[1] Pursuant to Supreme Court Rule 37.6, Amicus states that this brief was prepared in its entirety by *amicus curiae* and its counsel. No monetary contribution toward the preparation or submission of this brief was made by any person other than *amicus curiae* and its counsel.

Director of National Intelligence under President George W. Bush.

Professor Klein is an Associate Professor in the School of Public Policy at the Georgia Institute of Technology. His research focuses on globalization, democracy, and internet governance. Professor Klein has served as the Chair of Computer Professionals for Social Responsibility and led their activities on global internet governance.

The National Security Agreement (NSA) reflects "significant" and "extensive" negotiations between TikTok and Executive Branch officials to address the Executive's national security concerns. *TikTok, Inc. v. Garland*, 24-1113, 2024 WL 4996719, at *13 (D.C. Cir. Dec. 6, 2024). Mr. Christopher Simpkins is a former Senior Counsel at the Justice Department who was responsible for its participation in the Committee on Foreign Investment in the United States (CFIUS). Mr. Simpkins explains that "the NSA would effectively mitigate [] U.S. national security risks," "if implemented as written."[2]

Amici agree. The NSA offers unprecedented oversight, monitoring, and enforcement mechanisms that rely on strategic partners such as Oracle and CFIUS. The NSA is a robust cybersecurity risk mitigation plan that follows best practices for securing sensitive user information. Many scholars—including Amici—have concluded that the NSA would mitigate the national security risks that the

[2] Simkins ¶8.

Government alleges supports the TikTok Ban.[3] Indeed, under the NSA, TikTok would offer far more robust privacy and security protections than any American-based social media platform.

Amici also submit this brief to explain that the Ban is unconstitutional in light of the NSA. The D.C. Circuit was correct to assume that banning TikTok—a U.S. platform with First Amendment protections—must satisfy strict scrutiny, the Constitution's most demanding test. *TikTok, Inc.*, 2024 WL 4996719, at *9. As this brief demonstrates, the Ban does not pass strict scrutiny because the NSA is a less-restrictive alternative that accomplishes the Government's national security interests. True, Congress has "the power to safeguard its vital interests," some of which concern "the danger of sabotage and espionage." *United States v. Robel*, 289 U.S. 258, 266 (1967). But "the concept of national defense cannot be deemed an end in itself, justifying any exercise of legislative power designed to promote such a goal." *Id.* at 265 (internal quotations omitted).

SUMMARY OF THE ARGUMENT

I. The National Security Agreement mitigates the Government's national security concerns. For example, it creates a new entity, TikTok U.S. Data Security Inc. (TTUSDS), that controls TikTok's algorithm along with Oracle, a Government and Military partner. The NSA allows the Government to

[3] The Ban refers to the Protecting Americans from Foreign Adversary Controlled Applications Act.

continually inspect the algorithm, source code, promotion and filtering decisions, and watch for covert manipulation. All told, the NSA gives the Government more visibility into TikTok's operations than any other social media network operating in the U.S.

II. The Ban cannot survive strict scrutiny. The Government does not provide any evidence that the NSA does not mitigate its national security concerns. Instead, it restates that its general interest in national security makes the Ban the only viable option. As this Court has often instructed, the First Amendment's force does not lessen just because the Government asserts that it needs to protect against foreign adversaries. Although courts will generally defer to Congress's judgments about our Nation's security, a reasonable exercise of judgment does not ignore constitutional protections. The NSA is a less restrictive, indeed superior, alternative to the Ban.

ARGUMENT

I. The National Security Agreement mitigates the national security risks by providing unprecedented safeguards.

The Government has given three justifications for the Ban: *First*, that TikTok "collect[s] vast amounts of data on Americans" and that this data could be used to "conduct espionage campaigns," such as by tracking specific individuals.[4] *Second*, TikTok could be an influence operation or "propaganda threat." *Third*, that under several of the People's Republic of China's (PRC) laws, the PRC can require TikTok to surrender all its data to the PRC. The NSA accounts for, and eliminates, each concern.

A. The NSA provides unprecedented oversight.

The NSA is a comprehensive cybersecurity mitigation strategy that has robust operational and technological safeguards.[5] Proposed and refined over 18 months of negotiations between TikTok and CFIUS, the NSA allows TikTok to address the Government's legal, data security, and content manipulation concerns. It also includes auditing measures that ensure TikTok's compliance. In sum, TikTok invested "more than $2 billion" and began to "voluntarily implement" many the NSA's measures before the Government "ceased substantive

[4] H.R. Comm. on Energy & Com., Protecting Americans from Foreign Adversary Controlled Applications Act, H.R. Rep. No. 118-417 (2024) [hereinafter House Report].

[5] As an example of an operational failure, in 2013, the U.S. Info Search database was breached when a man named Hieu Minh Ngo posing as a private investigator from Singapore "obtained access to U.S. Info Search data" through a subsidiary of Experian (Court Ventures).

engagement regarding the Agreement in September 2022."[6]

The final 103-page NSA proposal, Mr. Simkin avers, is "the most sophisticated and thorough mitigation agreement I have reviewed in my 20 years of working on national security agreements, including my time as a member of CFIUS."[7] As Mr. Simkin explains "[t]he primary thrust of the NSA is that it sets up key technical and operational security provisions that govern use of the App and the Platform."[8] The NSA has several key provisions.[9]

First, the NSA creates a new, U.S.-based subsidiary, called TTUSDS that is independent of TikTok's global operations, and has primary responsibility for securing TikTok and protected user data in the U.S.[10] TTUSDS houses TikTok teams that access protected U.S. user data and TikTok's software code and back-end systems.[11] TTUSDS employees would be vetted with robust background and security

[6] Brief for Petitioners, TikTok, Inc. and Bytedance, Inc. at 17, *TikTok, Inc. v. Garland*, No. 24-1183 (D.C. Cir. June 20, 2024).

[7] Simkins, ¶37.

[8] Simkin, ¶53.

[9] Matt Perault & Samm Sacks, Project Texas: *The Details of TikTok's Plan to Remain Operational in the United States*, Lawfare (Jan. 26, 2023), https://perma.cc/WXR5-AZ2H.

[10] Simkin, ¶40; NSA, §1.22, art. II; NSA, §2.4.

[11] Simkin, ¶¶39-40, 46-50; NSA, §2.4.

checks.[12] Upon full implementation, TTUSDS will be overseen by an independent board of directors.[13]

TTUSDS is an example of both an operational and technical mitigation strategy. On the operations side, access to protected U.S. user data along with TikTok's software code and back-end systems would be monitored and tightly controlled by TTUSDS. Thus, TTUSDS mitigates the risk that the PRC could target and influence individuals with access to protected U.S. user data. At the same time, TTUSDS (alongside Oracle) controls the physical hardware used to run TikTok in the U.S. These operational and technical controls help mitigate the ability of the PRC to leverage their laws, citizens, and companies to influence TikTok.

Second, Oracle, a U.S.-based software company, strictly monitors TikTok to ensure compliance with the NSA.[14] Oracle Cloud will host the TikTok platform and app in the United States.[15] Within this secure environment, Oracle and TTUSDS will control

[12] NSA, §5.3.

[13] NSA, art. III.

[14] NSA, §8.4 ("The TTP implements processes and controls to monitor these environments to ensure compliance with this Agreement.")

[15] NSA, art. VIII (USDC "in coordination with the TTP, take all steps necessary to facilitate TTUSDS's initial deployment of the TikTok U.S. Platform in the TTP's secure cloud.")

and monitor data leaving the secure environment under established protocol.

The hosting, monitoring and control provision of the NSA are additional examples of operational and technical mitigation strategies. Oracle Could is used to build many of the Government's most sensitive databases including the U.S. Army's Integrated Personnel and Pay System (IPPS-A) and the Department of Defense's enterprise servers.[16] Therefore, as part of the NSA, TikTok's software and data would be hosted using the same provider that our military and national security apparatus use.

Oracle will also use automated processes and human review to monitor data flows for security breaches or improprieties. Attempts to move, copy, transfer, or otherwise exfiltrate large amounts of data from TikTok would be detected and stopped by Oracle. Therefore, by default, U.S. user data is stored within a U.S. environment that strictly controls and monitors that data and includes stringent access control measures.

Third, to prevent manipulation of TikTok's content, Oracle Cloud will host TikTok's content

[16] United States (U.S.) Army to Modernize its Integrated Personnel and Pay System (IPPS-A) on Oracle Cloud Infrastructure*,* Oracle*,* www.oracle.com/news/announcement/us-army-to-modernize-its-personnel-and-pay-system-on-oracle-cloud-infrastructure-2024-10-16/ (last visited Dec. 23, 2024); Contracts for Dec. 7, 2022, U.S. Dep't Def., https://www.defense.gov/News/Contracts/Contract/Article/3239197/ (last visited Dec. 23, 2024).

recommendation system[17] and content promotion system.[18] As to the content recommendation system, Oracle will inspect, test and train the Recommendation Engine[19] in the secure cloud environment to ensure it is not recommending content that isn't suggested by a user's in-app behavior. TikTok's content moderation functions[20] will also be subject to outside review, to confirm that moderation is taking place only in accordance with TikTok's published Community Guidelines. Regarding content promotion, TTUSDS will implement promotions and filters using applicable rules, algorithms, logic, or guidelines, and Oracle will have oversight authority. Promotional decisions will be transparent and auditable to third-party auditors.[21]

This is another example of a robust operational and technical mitigation strategy. The systems/operations that determine what content is suggested to users (or removed from the platform) will be continuously reviewed, tested, and monitored by

[17] The content recommendation system suggests new content and videos for users.

[18] The content promotion system promote particular content.

[19] NSA, §1.24 (defining Recommendation Engine).

[20] The content moderation functions include both machine and human review of posts to ensure they comply with TikTok's community guidelines. *See* Community Guidelines, TikTok, https://www.tiktok.com/communityguidelines/en?lang=en (last visited Dec. 23, 2024).

[21] NSA §9.13; Simkin, ¶71.

third parties (including Oracle) to ensure that they are free from any foreign or outside influence. Hosting the code and data responsible for TikTok's content-moderation, promotion, and recommendation systems in Oracle Cloud mitigates the likelihood that these systems can be used to support certain viewpoints.

Fourth, TikTok has stated that under the NSA "every single line of source code that goes into the secure environment, whether it comes from TikTok, Bytedance, open source, or third-party, will be inspected and tested."[22] In short, the code will be transparently reviewable by Oracle and a third-party security inspector. The code, or any updates to the code, "can't run," if they fail inspection.[23]

Moreover, Oracle, and not TikTok, will review the app source code, compile the app, and deliver it directly to the app stores (such as Apple and Google) to maintain the chain of custody.[24] So there is no opportunity for TikTok to inject new code into the TikTok app before it is deployed in the U.S.

The source code for TikTok's platform will also be inspected "in accordance with the Software Assurance Protocols."[25] The code for the platform will be

[22] *See About Project Texas*, TikTok, https://usds.tiktok.com/usds-about/ (last visited Dec. 23, 2024).

[23] NSA art. IX; §9.5; Simkins, ¶¶57-64.

[24] NSA §8.4; Simkins, ¶¶67-68.

[25] NSA §9.10(1).

"compiled exclusively within the TTP[(Oracle)]'s secure cloud infrastructure."[26]

The code review, control, and validation provisions of the NSA are another example of both an operational and technical mitigation strategy. The code is technically validated to mitigate the risk of backdoors or data leakage. Operationally, Oracle maintains chain of custody over the code. The NSA, therefore, includes multiple layers of third-party and independent review of source code and puts mechanisms in place to validate the code.

Fifth, CFIUS will play an ongoing role in monitoring TikTok's compliance with the NSA.[27] CFIUS also has a "shut-down option" or "kill switch.'[28] Aside from the Kill Switch, CFIUS can impose "a civil penalty" if it determines TikTok has breached the NSA.[29]

Thus, the NSA uses a series of interlocking operational and technical safeguards to protect user data. And TTUSDS and Oracle would also have a legal reporting obligation directly to the Government.[30] If an "identified security problem is not fixed"[31] to the satisfaction of TTUSDS, Oracle, and

[26] *Id.*

[27] Simkins, ¶74; NSA §17.1.

[28] NSA §§9.14-9.15; §§21.3-21.5; Simkins, ¶74-74.

[29] NSA §21.1.

[30] NSA §9.18.

the U.S. Government, the NSA gives authority to suspend using the App and the Platform in the U.S.[32]

B. The NSA provides unprecedented risk management.

1. The NSA mitigates the national security concerns identified by the Government. No other social media platform in the world protects user data to the extent the NSA requires.[33] Each provision of the NSA creates operational and technical hurdles that make subversion very difficult.

Since all protected U.S. user data is housed in Oracle Cloud the NSA would mitigate the risk that the user data TikTok collects could be used to "conduct espionage campaigns," such as tracking specific individuals.[34] Also, since the source code is inspected and tested by outside reviewers, any code enabling tracking or "espionage campaigns" could be identified and isolated.

The NSA mitigates the risk that TikTok could be used in an influence operation (IO) or pose a "propaganda threat."[35] In particular, the content recommendation system and content promotion systems are monitored and controlled by Oracle and each line of source code is reviewed by outside code

[32] Simkins, ¶65.

[33] Weber, ¶22.

[34] House Report at 2, 4.

[35] House Report at 8.

reviewers.[36] Outside reviewers also monitor TikTok's content moderation to confirm that the moderation complies with TikTok's published Community Guidelines.

Additionally, since TTUSDS would be an independent U.S.-based company, with significant control over TikTok in the United States, the NSA mitigates the threat that the PRC can require TikTok to surrender all its data or that an insider could gain access to protected U.S. user data. As explained above, any data exfiltration programs by the PRC (or an insider) would be detected by TTUSDS and Oracle. Moreover, access to protected U.S. user data is restricted under the NSA.[37]

Last, if TikTok launched an "espionage campaign," engaged in propaganda, or was ordered to turn over all data, CFIUS, or Oracle could activate the Kill Switch and turn off TikTok at any time.

2. The House Report[38] raises three arguments against the NSA: (1) Bytedance would continue to have a role in certain aspects of TikTok's U.S. operations and would be subject to PRC law; (2) the NSA would allow TikTok to continue to rely on the

[36] The First Amendment creates "breathing space" protecting the false statements, propaganda, and hyperbole that are "inevitable in free debate." *New York Times Co. v. Sullivan*, 376 U.S. 254, 272 (1964). The Government generally cannot prevent "political propaganda." *See, e.g.*, *Lamont v. Postmaster Gen.*, 381 U.S. 301 (1965).

[37] NSA arts. 8 & 9.

[38] The House Report is based on a different version of the Ban using different language.

engineers and back-end support in China; and (3) that the NSA has not been completed. None of the Government's reasoning is compelling, nor does it align with generally accepted principles of cybersecurity.

(1) While Bytedance's Chinese subsidiaries are subject to Chinese law, the record does not explain why Bytedance's role in TikTok raises a national security concern. Many U.S. technology companies—including Cisco, Dell, Electronic Arts, Hewlett-Packard, IBM, LiveRamp, and Palo Alto Networks—have Chinese-headquartered subsidiaries and, therefore, face the same theoretical risk that Chinese government officials may seek to compel disclosure of customer or user data from those companies.[39]

Under the NSA, however, Oracle Cloud will host TikTok in the United States. So even if Bytedance were ordered by the PRC to turn over some or all data, it is unclear how Bytedance could comply. That is because Oracle hosts the protected data, and it would be alerted to any data exfiltration program. In response, Oracle could activate the Kill Switch. Thus, the NSA ensures that TikTok, unlike the other U.S. technology companies with Chinese headquartered subsidiaries, accounts for the risk of PRC coercion.

(2) American-based social media companies have offices in China that employ engineers and back-end support staff. Electronic Arts, for example, maintains a major development studio in China that, as of June

[39] Weber, ¶18.

2024, has over 400 employees.[40] These employees work on developing popular video games such as FIFA and The Sims, both have millions of U.S. and international users.[41]

Congress never explains why a national security concern arises from the mere possibility that an engineer in China might have an engineering role. But in any event, Congress does not explain why the NSA does not mitigate this risk. Under the NSA, TikTok's software code and back-end systems would be maintained in the U.S., not China, and Oracle would verify and inspect the code. Oracle would thus detect any effort to introduce vulnerabilities or manipulate its algorithm.

(3) Congress's criticism that TikTok has not unilaterally implemented the NSA is in bad faith. TikTok "has begun the process of voluntarily implementing" the NSA and has spent more than "$2 billion on Project Texas."[42] "After August 2022, however, CFIUS, without explanation, stopped engaging with Petitioners in meaningful discussions." The NSA requires assistance from CFIUS as some of the provisions require CFIUS to play an ongoing role

[40] EA China, Electronic Arts (last accessed Jun. 12, 2024), https://perma.cc/Y43K-GKKV.

[41] *The Sims 4 Becomes the Most Widely Played Game*, Electronic Arts (Apr. 18, 2023), https://perma.cc/57E4-K2JD; *FIFA 23*, Active Player (last accessed Jun. 12, 2024), https://perma.cc/8937-UEZ5.

[42] "Project Texas" refers to the voluntary implementation by Petitioners of some of the NSA's provisions.

in monitoring TikTok's compliance. Thus, TikTok has not implemented the NSA because the Government has refused to cooperate.

II. The NSA is a less restrictive alternative to the Ban.

When seeking to enforce a law that broadly restricts speech, the Government must "explain why a less restrictive provision would not be as effective." *Reno v. ACLU*, 521 U.S. 844, 879 (1997). And when the Government rejects a potential alternative "to prevent an anticipated harm, it must do more than simply posit the existence of the disease sought to be cured." *FEC v. Cruz*, 596 U.S. 289, 307 (2022) (internal quotations omitted). Instead, the Government must "point to record evidence or legislative findings demonstrating the need to address a special problem." *Id.* (internal quotations omitted). Mere "conjecture" has never been accepted as an "adequate" justification to "carry a First Amendment burden." *Id.* (internal quotations omitted). But conjecture is the most that the Government has provided here.

A. The Government fails to provide any evidence that the NSA is an ineffective alternative.

The Ban cannot survive strict scrutiny unless the Government can explain why the NSA is an insufficient alternative. The Government cannot carry this burden. For starters, the Government's legal arguments defending the Ban differ from the grounds Congress invoked when enacting the Ban.

Thus, the post-hoc justifications that appear in legal briefs, but not the congressional record, must be treated with suspicion. There is no sign that Congress considered any of the justifications that the Government raises. But even if the Government's legal arguments reflected Congress's deliberations, the record shows that the NSA accounts for each argument the Government raises.

Threats Posed by China: The Government's primary justification for imposing the Ban rather than agreeing to the NSA is that the PRC is an adversary that can directly, or indirectly, require Chinese-owned companies, and their U.S. subsidiaries, to support strategic Chinese initiatives.[43] But there is an important distinction between the risks created by the PRC and the NSA's ability to adequately mitigate those risks. As explained further below, the NSA effectively cuts off the avenues by which the PRC could exploit TikTok for its own goals.

Independence of TTUSDS: The Government also "doubt[ed] the true independence TTUSDS would possess under the Final Proposed NSA."[44] As Mr. Simkin explained: "The governance provisions in the NSA for TTUSDS (i.e., the reliance on independent Outside Directors) are modeled on governance

[43] Blackburn, ¶9, ¶23; Vorndran, ¶10.

[44] Newman, ¶99.

provisions that have been used by the U.S. Government in hundreds of mitigation agreements."[45]

The Government's "doubts," therefore, are undercut by the fact that these provisions are common in CFIUS agreements. The Government also ignores that the NSA does not rely on TTUSDS in isolation. Oracle, CFIUS, and an approved third-party inspector each have ongoing monitoring and inspection roles.

The Kill Switch: The Government offers to two reasons to support its claim that the "Kill Switch" is not a "realistic option to deter noncompliance with the Final Proposed NSA."[46] Neither justification is persuasive.

First, the Government claims that the Kill Switch "does not permit a temporary stop based on concerns related to the algorithm or whether U.S. persons' data is accessible by the PRC government."[47] That is incorrect. Under the NSA, the Kill Switch is available for concerns related to the algorithm and access to U.S. users' data.[48] The Government's rebuttal also ignores that the NSA allows Oracle to suspend user access to the TikTok U.S. Platform specifically where Oracle identifies issues related to the Source Code.[49]

[45] Simkin Re., ¶41.

[46] Newman, ¶111.

[47] Newman, ¶114.b.

[48] NSA §21.3(7), (10).

[49] NSA §9.15(2).

Second, the Government asserts that the Kill Switch would "would have required the government to know, in sufficient time to act, of an imminent threat."[50] This abstract justification is pretextual. Again, the NSA provides unprecedented levels of Government oversight into a social media platform's data collection and content moderation operations. The NSA's other provisions are designed to allow the Government to monitor and identify any imminent threat. It cannot be that a threat has materialized past a point of mitigation simply because the threat is identifiable.

Influence Operations (IO): One of the Government's principal concerns is that the PRC will manipulate TikTok's algorithm "in ways that benefit the PRC and harm the United States."[51] But the NSA mitigates this risk. The content recommendation system, content moderation algorithm, and content promotion systems are all monitored and/or controlled by Oracle and outside reviewers. Further, TTUSDS and Oracle—not Bytedance—will control the Recommendation Engine, and the engine's training will take place in the United States within the Secure Oracle Cloud.[52] In short, the fear of IO is effectively mitigated by the NSA because the PRC lacks sufficient technical access to control how TikTok distributes content.

[50] Newman, ¶111.

[51] Blackburn, ¶9, ¶76; Vorndran, ¶32.

[52] NSA §9.13(2)(i).

Data Flows and Access: The Government claims that "the proposed agreement contemplated extensive data flows of U.S. users back to Bytedance and thus to China."[53] This is wrong: The NSA explicitly prohibits the flow of Protected Data to China, including even "anonymized" data.[54] While there are categories of data that can be sent to Bytedance, those exceptions are narrow, and subject to the Government's explicit consent.[55] These provisions apply to sensitive data too.[56] So if the Government never consents to the flow of extensive data, no such transmission can occur.

The Government's concern that Protected Data flowing from U.S. users to international location "would not be subject to direct U.S. government monitoring"[57] and could be intercepted by the PRC is also misplaced. Under the NSA, the Government can monitor all interactions and data elements, including all user data, between TikTok and any internet host.[58] Even more, Oracle monitors all data transmissions, and the NSA specifically notes that TTUSDS must

[53] Vorndran, ¶18.

[54] NSA §§1.22, 9.8, 11.7-11.9, 11.12.

[55] NSA §§1.11, 1.23, 9.8, 11.1-2, 11.7-11.9, 11.12.

[56] The Government also questions the Limited Access Protocols in the NSA, claiming it allows Bytedance to access data in many scenarios. The NSA, however, requires all access protocols to be approved by CFIUS. NSA §11.9(2).

[57] Newman, ¶78.a.

[58] NSA §9.17.

inform CFIUS if any provisions of the NSA do not comply with European Union's General Data Protection Regulation ("GDPR"). The NSA, therefore, envisions that Oracle's role as data monitor includes monitoring data flows going anywhere, even though allied third-party nations.[59]

The Government also asserts that the NSA's data collection provisions are ineffective because Oracle would be unable to identify "whether information was routed for legitimate commercial reasons or nefarious reasons at the request of PRC actors." This is an odd concern. Oracle is a sophisticated and highly capable U.S. technology company with decades of experience managing complex datasets and a long-standing customer relationship with the U.S. Government and military. There is no indication in the record that this concern is anything but "conjecture." *Cruz*, 596 U.S. at 307.

Source Code Review: The Government also argues that source code review is ineffective. First, the Government asserts that under Chinese law, TikTok cannot export the Source Code.[60] But this is not a legitimate justification, if TikTok cannot export the Source Code, then it cannot comply with the NSA.[61] And if TikTok cannot comply with the NSA, then the Kill Switch turns TikTok off. Second, the Government contends that Bytedance will still

[59] NSA §9.17.

[60] Blackburn, ¶¶76-78.

[61] NSA §§21.2, 21.3(6), 21.4.

develop TikTok's source code; but again, Oracle and an outside code reviewer will validate every source code file. So even if an exploit were added to the code in China, there are multiple safeguards in place before that exploit could be deployed in the U.S. Third, the Government claims that Source Code review would be ineffective because of "heating," a feature that allows TikTok employees to boost certain content. But the NSA specifically regulates the "Content Promotion and Filtering function" of TikTok. Any video campaign selected for "heating" would need to be approved and deployed by TTUSDS in the U.S. Oracle and the Third-Party Monitor would review the Content Promotion and Filtering software and data for compliance with relevant policies.

The Government alternatively argues that the source code review provisions are insufficient because they amount to a "monumental undertaking."[62] This rebuttal, if anything, proves that the NSA is a viable alternative. The Government cannot fault TikTok for offering an alternative that requires lots of effort.

And there is no evidence to suggest that this monumental undertaking is unfeasible. Oracle has never asserted that its engineers will be unable finish the initial Source Code review within 180 days of the NSA's execution (the timeline set out in the NSA).[63] Moreover, the Source Code review includes further assistance from TTUSDS and a Source Code

[62] Newman, ¶80.

[63] NSA §9.9(1).

Inspector. CFIUS can also request additional security testing at any time. The Government's protests here just confirm Mr. Simkin's assessment that "it is difficult to imagine a more robust Source Code review process than that which is included in the NSA."[64]

Enforcement: The Government claims that "it lack[s] the resources and capabilities to fully monitor and verify Bytedance's compliance with the Final Proposed NSA."[65] But TTUSDS and Oracle bear the primary burden of monitoring compliance—not the Government. As already explained, the NSA provides unprecedented levels access to the Government, so it does not have to expend resources searching for problems; noncompliance will either jump out, or it will be reported by TTUSDS or Oracle, if not both.

B. The Ban does not address the Government's national security concerns.

The Ban is both more restrictive of speech and less effective in addressing the government's national security concerns than the NSA. If TikTok is forced to cease its U.S. operations, many Americans—and their data—will move to other platforms. "[T]he type and amount of data that TikTok collects from U.S. users ... is comparable to the type and amount of data that other social media platforms and applications

[64] Simkin Re., ¶32.

[65] Newman, ¶75.

collect from U.S. users."[66] Yet no other social media company has a data protection model that comes close to offering the same levels of cybersecurity as the NSA. So, once the data migrates, the threats that underlie the Ban only worsen.

Consider the Government's concerns about data flow, for example. Data brokers openly sell large amounts of location data.[67] Likewise, troves of digital data are open source, so foreign and domestic companies alike take this data too.[68] The Ban does nothing to stem this persistent issue.

The Ban also does not mitigate the Government's concerns about threats from the PRC. Indeed, China is a sophisticated cyber-actor that can gain access to many existing social media datasets through these avenues.[69] For example, in 2015, China hacked into the Federal Government's Office of Personnel Management's systems, and accessed 22 million records.[70] Among other sensitive items, the PRC exfiltrated security clearance applications (including

[66] Weber, ¶8.

[67] Congress recently passed the Protecting Americans' Data from Foreign Adversaries Act of 2024 (PADFA) which restricts foreign data sales by U.S. companies.

[68] Susan A. Aaronson, *Data is Dangerous: Comparing the Risks That the United States, Canada, and Germany See in Data Trovers*, Center Int'l Gov. Innovation (Apr. 2020), https://perma.cc/F4H2-CVGW.

[69] Weber ¶¶14-16.

[70] Ellen Nakashima, *Hacks of OPM databased compromised 22.1 million people, federal authorities say*, The Wash. Post (July 9, 2015, 8:33 PM), https://perma.cc/7MGP-3VRP.

Professor Edgar's and Aaronson's security clearance records), one of the most sensitive data sets imaginable.[71] China has also hacked the databases of American-owned hotel chains, giving them access to travel patterns useful for locating government officials.[72] Many of these attacks rely on phishing, which can be executed by and can target anyone using email.[73] All these operations target systems such as Industrial Control Systems and other software applications and devices that are not owned, developed, or operated by Chinese-based companies.[74]

These examples highlight that the Government's focus on TikTok is misplaced. *See TikTok*, 2024 WL 4996719, at *11. The bottom line is that U.S. ownership does not guarantee data security. Thus, there is no indication that the Ban secures the user data that the Government claims poses a national security risk or otherwise "serve[s] a substantial state interest in a direct and material way." *Edenfield v. Fane*, 507 U.S. 761, 767 (1993).

[71] *Id.*

[72] Garrett M. Graff, *China's Hacking Spree Will Have a Decades-Long Fallout*, Wired (Feb. 11, 2020).

[73] Gary Smith, *Top Phishing Statistics for 2024: Latest Figures and Trends*, StationX (Apr. 10, 2024), https://perma.cc/K7W7-6SBW.

[74] Aaronson, *supra* note 69; Lily Hay Newman, *The NSA Seems Pretty Stressed About the Threat of Chinese Hackers in U.S. Critical Infrastructure*, Wired (Nov. 18, 2023, 4:42 PM).

C. The D.C. Circuit applied strict scrutiny in name only.

Though the D.C. Circuit assumed, but did not decide, that the Ban triggered strict scrutiny, it's application did not resemble the Constitution's most rigorous test. *See TikTok, Inc.*, 2024 WL 4996719 at *9. Under strict scrutiny, the Government must justify its decision to reject a less-restrictive alternative with "hard evidence." *United States v. Playboy Ent. Grp.*, 529 U.S. 803, 819 (2000). The D.C. Circuit ignored this standard. Instead, it deferred to the "Government's risk assessment" and "ultimate judgment" on matters of national security. *Id.* at *21. This unfettered deference was an error.

True enough, Congress has "the power to safeguard its vital interests," some of which concern "the danger of sabotage and espionage," but "the concept of national defense cannot be deemed an end in itself, justifying any exercise of legislative power designed to promote such a goal." *Robel*, 289 U.S. at 265-66. National defense includes "defending those values and ideals which set this Nation apart … the most cherished of those ideals have found expression in the First Amendment." *Id.* And this Court's "precedents, new and old make clear that concerns of national security do not warrant abdication of the judicial role.*" Holder v. Humanitarian Law Project*, 561 U.S. 1, 34 (2010).

So here, the D.C. Circuit was free to defer to the Government's judgment that the PRC presents a threat to the nation's security. *See TikTok, Inc.*, 2024

WL 4996719 at *16. But the initial judgment that the PRC presents a national security risk says nothing about the NSA's ability to mitigate that risk. Thus, under strict scrutiny, the Government has the burden to provide evidence that shows the NSA fails to mitigate specific national security risks; the Government cannot simply restate the underlying reasons that inspired the Ban: that it "lacks confidence that it has sufficient visibility and resources to monitor TikTok's promised measures, nor does it have the 'requisite trust' that Bytedance and TTUSDS would comply in good faith.'" *Id.*

Tellingly, in the few paragraphs where the D.C. Circuit addressed the NSA, its findings show that the NSA is a less restrictive alternative. Indeed, the D.C. Circuit acknowledged that the NSA's "broad contours … are undisputed," and that "the Government has never denied that TikTok's proposed NSA would mitigate the Government's concerns to some extent." *TikTok*, 2024 WL 4996719, at *5, *16. Thus, a simple question arises: Why is the Ban the only way the Government can assuage its national security concerns?

The D.C. Circuit did not substantively engage that question. And its failure to do so ignores a basic First Amendment principle: National security "cannot be invoked as a talismanic incantation to support any exercise of congressional power which can be brought within its ambit." *Robel*, 389 U.S. at 263. Where, as here, the Government invokes national security as a justification to restrict the exercise of free speech, the

First Amendment requires "narrowly drawn legislation." *Id.* at 266.

The Ban is everything but narrowly drawn. TikTok is a United States forum that hosts 170 million users who exercise every form of protected speech. Of course, TikTok manages data commensurate with its daily users and the content that those users create. But the Government's national security concerns arise from only a small portion of this data. The Ban, however, removes TikTok from the American marketplace, it violates the First Amendment.

CONCLUSION

For the foregoing reasons, the judgment of the D.C. Circuit should be reversed.

December 27, 2024 Respectfully submitted,

MARK S. DAVIES
Counsel of Record
KUFERE LAING
EDRED RICHARDSON
WHITE & CASE LLP
701 Thirteenth Street NW
Washington, D.C 20005
(202) 626-3600
mark.davies@whitecase.com

Counsel for Amicus Curiae