

**UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA**

TIKTOK INC., BYTEDANCE LTD.,

Plaintiffs,

v.

DONALD J. TRUMP, in his official capacity as
President of the United States, WILBUR L.
ROSS, JR., in his official capacity as Secretary
of Commerce, UNITED STATES
DEPARTMENT OF COMMERCE,

Defendants.

Civil Case No. 20-cv-2658

BRIEF OF AMICUS CURIAE NETCHOICE IN SUPPORT OF PLAINTIFFS

TABLE OF CONTENTS

STATEMENT OF INTEREST 1

SUMMARY OF ARGUMENT 2

ARGUMENT..... 3

 1. The Government’s Regulations Violate the First Amendment Rights of Existing and Future TikTok Users in the United States..... 4

 2. The Government’s Regulations Violate the First Amendment Rights of U.S. Companies and Developers 7

 3. The Government’s Actions Risk Collateral Damage to First Amendment Interests, Including from Foreign Governments Well Beyond China 9

CONCLUSION 13

TABLE OF AUTHORITIES

Cases

Citizens United v. FEC, 558 U.S. 310 (2010)..... 5

Holder v. Humanitarian Law Project, 561 U.S. 1 (2010) 4

Junger v. Daley, 209 F.3d 481 (6th Cir. 2000)..... 8

McCullen v. Coakley, 573 U.S. 464 (2014) 6

Packingham v. North Carolina, 137 S. Ct. 1730 (2017) 4, 5

Reed v. Town of Gilbert, 576 U.S. 155 (2015)..... 8

Reno v. American Civil Liberties Union, 521 U.S. 844 (1997) 4, 5

Ward v. Rock Against Racism, 491 U.S. 781 (1989) 6

Orders and Regulations

U.S. Dep’t of Commerce, *Identification of Prohibited Transactions to Implement Executive Order 13942 and Address the Threat Posed by TikTok and the National Emergency with Respect to the Information and Communications Technology and Services Supply Chain* (Sept. 24, 2020), <https://www.federalregister.gov/documents/2020/09/24/2020-21193/identification-of-prohibited-transactions-to-implement-executive-order-13942-and-address-the-threat>..... 1, 7

White House, *Executive Order on Addressing the Threat Posed by TikTok* (Aug. 6, 2020), <https://www.whitehouse.gov/presidential-actions/executive-order-addressing-threat-posed-tiktok/> (“August 6 order”)..... 1

Other Authorities

Aditya Kalra, *Exclusive: U.S. Senators Urge India to Soften Data Localization Stance*, REUTERS (Oct. 13, 2018), <https://www.reuters.com/article/us-india-data-localisation-exclusive/exclusive-u-s-senators-urge-india-to-soften-data-localization-stance-idUSKCN1MN0CN> 11

Albright Stone Group, *Data Localization: A Challenge to Global Commerce* (Sept. 2015), <https://www.albrightstonebridge.com/files/ASG%20Data%20Localization%20Report%20-%20September%202015.pdf>..... 11

John Herrman, *TikTok Is Shaping Politics. But How?*, N.Y. TIMES (June, 28, 2020), <https://www.nytimes.com/2020/06/28/style/tiktok-teen-politics-gen-z.html>. 5

David E. Sanger & Julian E. Barnes, *Is TikTok More of a Parenting Problem Than a Security Threat?*, N.Y. TIMES (last updated Aug. 7, 2020), <https://www.nytimes.com/2020/08/07/us/politics/tiktok-security-threat.html>..... 2

Steve Kovach, *Trump to Block Downloads of TikTok, WeChat on Sunday*, CNBC (last updated Sept. 18, 2020 at 3:46PM), <https://www.cnn.com/2020/09/18/trump-to-block-us-downloads-of-tiktok-wechat-on-sunday-officials-tell-reuters.html>..... 9

Will Rinehart, *Don't Ban TikTok Before A Public Trial*, DAILY CALLER (Aug. 12, 2020), <https://dailycaller.com/2020/08/12/rinehart-dont-ban-tiktok-before-a-public-trial/>. 12

STATEMENT OF INTEREST

NetChoice¹ is a national trade association of leading e-commerce and online businesses that share the goal of promoting convenience, choice, and commerce on the internet. NetChoice zealously defends American free enterprise and free expression from threats both foreign and domestic. At the same time, NetChoice believes that any online technology that actually undermines the United States' national security or consumer privacy should not be allowed to operate in the United States. We wish to address the First Amendment rights of freedom of speech and assembly and the dangerous precedent being set by the executive order issued on August 6, 2020,² and the Commerce Department's regulations implementing it³.

By completely banning U.S. access to TikTok, the Government's actions directly infringe upon the First Amendment rights of over 90 million U.S. users of one of the most popular social media platforms in America. The question before the Court is whether that infringement is a necessary cost of meeting overriding

¹ Amicus is a 501(C)(6) trade association based in Washington, D.C. As publicly disclosed on its website, NetChoice.org, amicus counts among its members nearly all of the leading tech companies in the United States, including TikTok Inc., a party in this case. NetChoice states that it has no parent company and that no publicly held company has 10% or greater ownership in NetChoice. No party or counsel for a party in this pending case authored the proposed amicus curiae brief in whole or in part or made a monetary contribution intended to fund the preparation or submission of the proposed brief. No person or entity other than the amicus, its members, or its counsel made a monetary contribution intended to fund the preparation or submission of the proposed brief.

² White House, *Executive Order on Addressing the Threat Posed by TikTok* (Aug. 6, 2020), <https://www.whitehouse.gov/presidential-actions/executive-order-addressing-threat-posed-tiktok/> ("August 6 order").

³ U.S. Dep't of Commerce, *Identification of Prohibited Transactions to Implement Executive Order 13942 and Address the Threat Posed by TikTok and the National Emergency with Respect to the Information and Communications Technology and Services Supply Chain* (Sept. 24, 2020), <https://www.federalregister.gov/documents/2020/09/24/2020-21193/identification-of-prohibited-transactions-to-implement-executive-order-13942-and-address-the-threat>.

requirements of U.S. national security.

Based on its background and experience with free speech and commerce online, amicus is able to provide information that is important to the Court in answering that question.⁴

SUMMARY OF ARGUMENT

The actions taken by the White House and the Department of Commerce (together, the “Government’s actions”) in this case are so unnecessarily broad that they fail the First Amendment requirement to employ the least-restrictive means of achieving the competing government aims of national security. Today, according to media reports of Central Intelligence Agency findings⁵, no data on American users of TikTok is stored in or been shared with China. The Administration has thus far provided no evidence to the contrary, nor has it provided evidence that China’s Communist Party or military have acquired data on TikTok’s users in the United States.

To the extent that the Administration may provide the court with classified information bearing on these questions that it cannot share with the public, that information must be of sufficient probity, weight, and certitude to warrant sweeping aside the significant First Amendment interests. Otherwise, the lack of evidence—and the breadth of the proposed ban on a social media platform that would curtail access for nearly a quarter of the U.S. population—leads to the conclusion that the

⁴ The brief complies with this Court’s standing order and does not exceed the page limit.

⁵ See, e.g., David E. Sanger & Julian E. Barnes, *Is TikTok More of a Parenting Problem Than a Security Threat?*, N.Y. TIMES (last updated Aug. 7, 2020), <https://www.nytimes.com/2020/08/07/us/politics/tiktok-security-threat.html>.

Government's actions fail to meet the requirement of narrow tailoring as set forth in applicable Supreme Court precedents.

The Government's actions are unprecedented in scope. There is no previous example in U.S. history of a complete ban of a media platform that directly deprives a quarter of the U.S. population access to information on that platform. Neither is there any precedent for depriving so many Americans of their opportunity to express themselves on that medium. As outlined below, the needless breadth of the Government's actions leaves open the opportunity to employ far less restrictive means to achieve its objectives. Because less-restrictive means are available to vindicate the Administration's national security concerns, the Government's actions should not be implemented as proposed.

ARGUMENT

The Government's actions deprive all U.S. citizens of access they currently enjoy to one of the leading social media platforms in America, and as such these actions necessarily infringe upon the First Amendment rights of all U.S. citizens. That infringement rises to the level of a First Amendment violation because the Government's actions are not narrowly tailored to accommodate First Amendment interests.

Beyond directly impacting the ability of U.S. citizens to access TikTok, and to express themselves on this social media platform, the Government's actions also cut off the ability of U.S. companies to host, and of U.S. developers to use, TikTok's coding and related infrastructure. Furthermore, by inviting not only retaliation from China but also emulation from other nations, the Government's actions pave

the way for more widespread restrictions on U.S.-based social media platforms that currently address a global audience.

The Government must be granted a certain amount of leeway “when seeking to prevent imminent harms in the context of international affairs and national security.” *Holder v. Humanitarian Law Project*, 561 U.S. 1, 35 (2010). But no imminent harm has been identified by the Government; instead, it has identified only potential harm not established by evidence before the Court.

1. The Government’s Regulations Violate the First Amendment Rights of Existing and Future TikTok Users in the United States.

The Government’s unprecedented step of blocking all access to TikTok in the United States starting November 12, and the restrictions currently in place, directly impinge upon the First Amendment rights of the platform’s over 90 million U.S. users. “A fundamental principle of the First Amendment is that all persons have access to places where they can speak and listen.” *Packingham v. North Carolina*, 137 S. Ct. 1730, 1735 (2017). Today the most important place for most Americans to speak and listen “is cyberspace—the ‘vast democratic forums of the Internet’ in general, and social media in particular.” *Id.* (quoting *Reno v. American Civil Liberties Union*, 521 U.S. 844, 868 (1997)). For more than 90 million Americans—over a quarter of the total population of the United States—that forum is TikTok. But the Government seeks to evict these 90 million Americans from TikTok and shut down their forum entirely.

When it comes to digital platforms, courts “must exercise extreme caution before suggesting that the First Amendment provides insufficient protection for

access to vast [digital] networks.” *Id.* Moreover, TikTok’s reach, and the breadth of its use by Americans, extends far beyond the traditional “quintessential forum” for free speech—a geographically limited place used by “the individual on a soapbox and the lonely pamphleteer.” *Citizens United v. FEC*, 558 U.S. 310, 373 (2010) (Roberts, C.J., concurring). TikTok is a nationwide place for over 90 million Americans “to engage in a wide array of protected First Amendment activity.” *Packingham*, 137 S. Ct. at 1736 (citing *Reno*, 521 U.S. at 870). Its users can reach millions in an instant. This has made TikTok a platform for “millions of young Americans,” for whom it is a venue not only for entertainment but for “ideological formation” and “political activism.”⁶

TikTok’s short, simple videos have become a widely used format for “youth political expression.”⁷ Its users range from a “liberal activist community” to “plenty of conservative[,] pro-Trump voices.”⁸ Many videos pack a powerful punch, touching on everything from gun rights to police brutality.

Wholesale blocking of all U.S. citizens’ access to this public forum is an extreme remedy, one that must be justified against the countervailing First Amendment interests it implicates. The Supreme Court’s guidance on such matters is clear. There is modest allowance for restrictions on public forums, so long as those restrictions are “narrowly tailored to serve a significant governmental interest.”

⁶ John Herrman, *TikTok Is Shaping Politics. But How?*, N.Y. TIMES (June, 28, 2020), <https://www.nytimes.com/2020/06/28/style/tiktok-teen-politics-gen-z.html>.

⁷ *Id.*

⁸ *Id.*

McCullen v. Coakley, 573 U.S. 464, 477 (2014). Inasmuch as national security is a significant governmental interest, meeting this test requires only that the Government's actions are narrowly tailored. But here they are not.

Far short of banning an entire forum used by nearly a quarter of the U.S. population, the Government can use other tools in its toolkit to address the specific national security concerns it has identified. These include the power of the Committee on Foreign Investment in the United States to appoint a special master to monitor compliance with data privacy protections; the power to force extensive revisions of TikTok policies and processes; and the power to force divestiture of foreign ownership. Because the Government has prematurely chosen to require a divestiture—a process that has not been allowed to finish—the imposition of a wholesale ban on U.S. citizen access to TikTok appears especially overbroad in this context.

The unprecedented step of banning a public forum used by over 90 million Americans will cut off access to a significant amount of user-created political content. It will deprive millions of Americans of a favored vehicle for targeting a younger audience with political speech and advocacy campaigns. Measured against alternative and less-restrictive means at the Government's disposal, such a broad speech ban “burden[s] substantially more speech than is necessary to further the government's legitimate interests.” *Id.* at 486 (quoting *Ward v. Rock Against Racism*, 491 U.S. 781, 799 (1989) (internal quotation marks omitted)).

In sum, the Government’s actions are overbroad, insufficiently sensitive to the constitutional rights of U.S. citizens, and for these reasons—barring the emergence of new evidence in the form of classified information the Court finds negates the evidence currently before it—violative of the First Amendment. The national security concerns the Government has expressed may be addressed through less-restrictive means that would simultaneously protect the First Amendment rights of U.S. users of TikTok.

2. The Government’s Regulations Violate the First Amendment Rights of U.S. Companies and Developers.

The Government’s actions infringe upon First Amendment interests beyond those of TikTok’s users. The Government’s actions extend to prohibiting all U.S. persons from hosting or using TikTok’s code in *any* manner. Under Department of Commerce regulations, U.S. companies are prohibited from offering “[a]ny provision of service to distribute or maintain the WeChat or TikTok mobile applications, constituent code, or application updates through an online mobile application store in the U.S.”⁹ And U.S. developers are prohibited from “[a]ny utilization of the mobile application’s constituent code, functions, or services in the functioning of software or services developed and/or accessible within the U.S.”¹⁰

⁹ U.S. Dep’t of Commerce, *Identification of Prohibited Transactions to Implement Executive Order 13942 and Address the Threat Posed by TikTok and the National Emergency with Respect to the Information and Communications Technology and Services Supply Chain* (Sept. 24, 2020), <https://www.federalregister.gov/documents/2020/09/24/2020-21193/identification-of-prohibited-transactions-to-implement-executive-order-13942-and-address-the-threat>.

¹⁰ *Id.*

These regulations are content based on their face, “[b]ecause computer source code is an expressive means for the exchange of information and ideas about computer programming [that] is protected by the First Amendment.” *Junger v. Daley*, 209 F.3d 481, 485 (6th Cir. 2000). And because coding is protected speech and because the regulations specifically target coding, the regulations are “presumptively unconstitutional and may be justified only if the government proves that they are narrowly tailored to serve compelling state interests.” *See Reed v. Town of Gilbert*, 576 U.S. 155, 163 (2015).

The Government’s actions are not narrowly tailored. *All* U.S. companies and developers are prohibited from using TikTok’s “constituent code, functions, or services” for any purpose—even when doing so *supports* the Government’s goal of protecting the data of U.S. users. Indeed, the Government’s actions would prevent existing U.S. users of TikTok from obtaining security updates for their apps from trusted U.S. sources because third-party businesses in the U.S. would be prohibited from hosting or offering *any* TikTok software updates. And because security updates from trusted U.S. sources would make the app more secure, the overbreadth of the Government’s actions undermines the Government’s own goal. More narrowly tailored regulations would not so interfere with the ability of U.S. third parties to make security improvements that are in U.S. consumers’ best interests.

Likewise, the Government’s actions violate the rights of developers, whose coding is, as noted above, protected under the First Amendment. The Commerce

regulations prohibit *any* use of TikTok’s code by U.S. developers. This means that U.S. developers who are not in any manner connected to China or the PRC government would not be able to create software that incorporates even a small amount of such code, even if the purpose and effect of their development work was to ensure that all U.S. security concerns are met.¹¹ By making TikTok’s code entirely off-limits, and by foreclosing even cybersecurity efforts aimed at ensuring the code is free of harmful elements, the regulations are far more restrictive than called for; indeed they are counterproductive.

The Government’s actions also create a dangerous precedent. The prohibition on any use of TikTok code by U.S. developers for any purpose is effectively a ban on the building blocks of digital free expression. From the standpoint of the First Amendment rights of Americans, it is tantamount to banning the use of certain letters of the alphabet: while the Government is not banning language outright, it is most definitely curtailing communication. Beyond violating the First Amendment rights of developers, the Government’s actions threaten to put all social media users at risk.

3. The Government’s Actions Risk Collateral Damage to First Amendment Interests, Including from Foreign Governments Well Beyond China.

The Government’s actions invite not only retaliation from China, but also

¹¹ According to media reports, Secretary of Commerce Wilbur Ross described the prohibitions set to take effect September 27 this way: “As to TikTok, it’s just upgrades, maintenance[,] things like that, that would be shut down at this stage. The real shutdown would come after Nov. 12.” See Steve Kovach, *Trump to Block Downloads of TikTok, WeChat on Sunday*, CNBC (last updated Sept. 18, 2020 at 3:46PM), <https://www.cnbc.com/2020/09/18/trump-to-block-us-downloads-of-tiktok-wechat-on-sunday-officials-tell-reuters.html>.

emulation by other nations. Although the Government may not intend these consequences, and although it cannot eliminate all risk, its actions here entail far more risk of unintended consequences than would result if its actions were narrowly tailored to accommodate the First Amendment rights of U.S. citizens. Chief among these unintended consequences is the likelihood that foreign governments will point to the Government's actions here as justification for banning or restricting the activities of U.S. internet businesses, including U.S.-based social media platforms on which most of the U.S. citizenry relies.

This is a particularly worrisome aspect of the Government's actions, given that the world's leading social media companies are U.S. firms, with many more millions of users than TikTok. These U.S. firms operate domestically and abroad. The opportunities for First Amendment-protected expressive activity they offer include connecting millions of Americans with their family, friends, and peers across the nation and around the world.

The European Union, and also individual member states, could follow the precedent of the Government's actions in this matter to use allegations and suspicions over data privacy or national security as justification for restricting U.S. social media platforms in Europe. This could include banning or restricting the use of U.S. social media platforms by individuals and restricting advertising on American social media platforms. Similarly, the precedent of using allegations and suspicions over data privacy or national security could be used as justification for

forcing divestitures to European owners, following the pattern of the Government's actions in this case.

These are very real concerns. Several nations have already sought to impose limits on data flows to American technology businesses. The justification has often been the potential for security and privacy threats, rather than evidence-based concerns. In many cases, addressing the imagined "concerns" empowered foreign governments to receive financial benefits, as well as better surveillance of their citizens' online expressive activities.

An example of the kinds of anti-free speech activity the Government's actions risk encouraging are the so-called "data localization laws" that the United States opposes.¹² These data localization laws prohibit the transfer of citizen data outside of the nation. Some years ago, several nations including Russia and Indonesia enacted data localization laws.¹³ Couched as responses to "security" and "privacy" threats, these data localization laws in fact facilitated rent-seeking and governmental control. The power to ban data transfers because of "security and privacy concerns" provided a financial windfall in the form of new data center construction; it also provided the power to better surveil communications of the citizenry, as platforms willing to share user data with the government were permitted.

¹² See, e.g., Aditya Kalra, *Exclusive: U.S. Senators Urge India to Soften Data Localization Stance*, REUTERS (Oct. 13, 2018), <https://www.reuters.com/article/us-india-data-localisation-exclusive/exclusive-u-s-senators-urge-india-to-soften-data-localization-stance-idUSKCN1MN0CN>.

¹³ See Albright Stone Group, *Data Localization: A Challenge to Global Commerce* (Sept. 2015), <https://www.albrightstonebridge.com/files/ASG%20Data%20Localization%20Report%20-%20September%202015.pdf>.

Such data localization efforts are now extending to the European Union. Recently, European countries began blocking U.S. tech businesses from transferring European citizens' data to the United States. The stated concern is privacy, but the precedent established by the Government's actions here can serve as justification for blocking American technology businesses' access—and hence U.S. citizens' free speech—in European markets.

The end result of the Government's actions is to inadvertently provide foreign nations with new justifications for preventing American technology businesses from accessing foreign markets. It would be a sad irony if the United States, which traditionally has relied upon open debate and due process, were to become more like China as a result of its effort to protect our nation's citizens from the PRC.¹⁴

The United States' historical encouragement of the global free flow of data has been a beacon of justice and individual freedom, and a bulwark for individual resistance to repressive government activities around the world. It has provided the free world with uniquely valuable information from inside nations that do not respect free speech or other human rights. Consistent with the U.S. commitment to the global free flow of information, threats to citizen privacy or national security because of data transfers have been dealt with on an evidentiary basis. The Government's actions, in contrast, appear to be based not on evidence but on suspicion and theory. In this respect, as well, the Government's actions are overbroad and thus violative of the First Amendment.

¹⁴ See Will Rinehart, *Don't Ban TikTok Before A Public Trial*, DAILY CALLER (Aug. 12, 2020), <https://dailycaller.com/2020/08/12/rinehart-dont-ban-tiktok-before-a-public-trial/>.

CONCLUSION

For these reasons, NetChoice supports the Plaintiffs' request for Injunctive Relief.

September 26, 2020

By: /s/Jacob A. Sommer
Jacob A. Sommer
Marc J. Zwillinger
ZWILLGEN PLLC
1900 M St. NW, Suite 250
Washington, DC 20036
Phone: (202) 296-3585
Facsimile: (202) 706-5298
marc@zwillgen.com
jake@zwillgen.com

Attorneys for Amicus NetChoice