DOI:10.1145/3473606

Anupam Chander

▸ **James Grimmelmann,** Column Editor

Law and Technology

Protecting the Global Internet from Technology Cold Wars

Considering the perceived dangers of the global information flow.

In the summer of 2020, the global Internet suffered two setbacks in quick succession. First, the Court of Justice of the European Union struck down the principal mechanism for personal-data transfers from Europe to the U.S.[a] Two weeks later, President Donald Trump announced the U.S. was banning TikTok, an app owned by a company headquartered in Beijing, China. Perhaps surprisingly, both of these actions shared a common justification: data flowing to a company with foreign ties might subject that data to foreign surveillance. Thus, not only is it unsafe to send data across the Atlantic, it is unsafe to send data across the Pacific. Call this the "dangerous waters" theory of the Internet.

Invocations of the dangerous waters theory are piling up. In March 2021, the Bavarian data protection authority banned the use of U.S.-based MailChimp because of the possibility of U.S. surveillance. The next month, Portugal's data protection authority similarly barred national census data from being sent to U.S.-based Cloudflare. In May 2021, the European Data Protection Supervisor opened an inquiry into the public use of Amazon Web Services and Microsoft Office 365. Word, apparently, may be a weapon.

The dangerous waters theory threatens the foundations of the global Internet. Focusing on the TikTok ban, I argue in this column that app bans should be carefully scrutinized, lest they be used as cover for other political ends. I begin by describing how President Trump's TikTok ban represented a major departure from a quarter-century of U.S. support for a global Internet, and then argue that the national security claims against TikTok proved overblown, and describe lessons from this experience.

President Trump's About Face on the Global Internet

China started it. At the dawn of the Internet age, it adopted a "Golden Shield"—what we came to call the Great Firewall of China—the modern version of an ancient effort to keep barbarians at bay. As James Fallows describes, "In China, the Internet came with choke points built in." American sites such as Facebook, Google's search, Twitter, and Wikipedia would be banned, accessible only via virtual private networks that dodged the address blocks.

For decades, the U.S. deplored the Chinese efforts to erect barriers to cross-border information flows. In 2000, President Bill Clinton famously scoffed that these Chinese efforts were "like trying to nail Jell-O to the wall." A decade later, Secretary of State Hillary Clinton added "the freedom to connect" to the four freedoms enunciated by President Franklin Delano Roosevelt—the freedom of expression, freedom of worship, freedom from want, and freedom from

a Court of Justice of the European Union. *Data Protection Commissioner v. Facebook Ireland and Maximillian Schrems*, Case C-311/18 (2020).

fear. Secretary Clinton put the U.S. firmly on the side of the global Internet: "We stand for a single Internet where all of humanity has equal access to knowledge and ideas." For decades, then, the U.S. advocated for an Internet where information could flow across borders relatively unencumbered, subject to a few limitations such as local hate-speech laws.

But in 2020, the U.S. retreated sharply from that vision. On July 31, 2020, President Trump surprised the country by declaring, "as far as TikTok is concerned, we're banning them from the U.S." An app designed to share short video clips with the world, TikTok now found itself in the middle of a geopolitical storm.

Is the TikTok ban merely turnabout as fair play? Or does it herald a dangerous turn—when the champion of a global Internet declares it too dangerous to tolerate?

IMAGE BY ANDRIJ BORYS ASSOCIATES. USING SHUTTERSTOCK

TikTok as National Security Threat

On August 6, 2020, President Trump followed through on his threat and issued twin executive orders targeting TikTok, as well as another popular app originally from China, WeChat. The orders were based on the President's powers under the International Emergency Economic Powers Act (IEEPA).[b,c] The TikTok executive order provided that within 45 days, "any person..., subject to the jurisdiction of the United States" would be prohibited from transacting with ByteDance Ltd., the China-headquartered owner of TikTok, or any of its subsidiaries. The Department of Commerce implemented this order by making it illegal to provide hosting, peering, or mobile app store services to TikTok—services it would need to keep running in the U.S.

On August 14, 2020, President Trump followed up with a second order requiring ByteDance to sell or transfer TikTok within 90 days, based on a review by the Committee on Foreign Investment in the United States (CFIUS).[d]

The executive orders made two central claims as to TikTok's national-security threat, one about the collection of information and the other about its dissemination. First, the U.S. claimed the Chinese government would use TikTok to gather compromising data about Americans, which it could then use for "blackmail." The Trump Administration seemed to be relying on a frighteningly broad provision of the Chinese National Intelligence Law, Article 7, which states "any organization or citizen shall support, assist, and cooperate with state intelligence work according to law."

Second, the U.S. argued the Chinese government would use the app to censor American speech or to disseminate propaganda. For example, TikTok had indeed been caught suspending an American teenager who cleverly used an eyelash tutorial to criticize the Chinese government's treatment of Uyghur Muslims. When this act drew public attention, TikTok quickly apologized for what it described as an error and restored her account. Since that time, posts with the hashtag #uyghur have garnered 82.5 million views on the app.

Overblown Fears

The TikTok ban was an improbable mechanism to improve national security for a number of reasons. Indeed, it is not clear whether the national emergency posed by TikTok was the threat of China exfiltrating data or Sarah Cooper's TikToks mercilessly mimicking

b Exec. Order No. 13,942, 85 Fed. Reg. 48,637 (Aug. 6, 2020).

c Exec. Order No. 13,943, 85 Fed. Reg. 48,641 (Aug. 6, 2020).

d Regarding the Acquisition of Musical.ly by ByteDance Ltd., Exec. Order, 85 Fed. Reg. 51297 (Aug. 14, 2020); https://bit.ly/3wvglQp

the president's own words or TikTok teens reserving tickets for his Tulsa rally they had no intention of using. TikTok, after all, was the largest social network the president or his supporters had failed to master. One could not have imagined the president targeting Twitter and jeopardizing his free platform to reach his millions of followers there.

First, the dangerous waters theory proves too much. China is hardly alone in having laws that compel the disclosure of data held overseas, though the standards to compel production will differ widely across the world. The CLOUD Act explicitly grants this authority to the U.S. government, subject to extensive procedural safeguards. Other countries with similar laws range from Australia to Serbia.[e]

Second, the dangerous waters theory would forbid even apps from domestic enterprises if they had operations in foreign jurisdictions that could compel them to produce data wherever it is held. Under this reasoning, even Apple might pose a national security risk to Americans because it is subject to Chinese jurisdiction.

Third, the TikTok ban undermines U.S. efforts against data localization. The U.S. has long made the free flow of data across borders a linchpin of its trade policy.

Fourth, TikTok could not have transferred all its data to the Chinese authorities without violating U.S. law. The Stored Communications Act bars companies from transferring the contents of communications to foreign authorities except under very narrow circumstances.

Fifth, there are many other ways to gather data about U.S. residents. Even weather apps can collect location data and sell it to data brokers who resell it to governments. Intelligence services certainly operate overseas. Supply-chain attacks like the SolarWinds hack, which was likely Russian in origin, suggest a particularly clever technique to exfiltrate data or compromise systems in bulk.

Sixth, TikTok was an odd target. It is not principally a private messaging platform, but rather an app that allows you to follow your interests or to share them with the world. Users posting videos typically expect those videos to be shared publicly. Where Grindr focuses on private dating, TikTok is better known for public dancing. As the comedian Jimmy Fallon joked, "Apparently this is a very real national security threat—China's government knowing which Americans can and can't dance."

Is the TikTok ban merely turnabout or fair play? Or does it herald a dangerous turn—when the champion of a global Internet declares it is too dangerous to tolerate?

Finally, subsequent history suggests the Trump Administration exaggerated the threat. Even when federal courts saw the government's secret evidence against TikTok, they still sided with TikTok. Judge Carl Nichols, a Trump appointee, halted the TikTok ban.[f] A second judge declared the government's concerns "hypothetical."[g] And thus far, the Biden Administration has declined to pursue the Trump ban or divestiture orders further, implicitly suggesting the security threat is not as severe as presented by the prior administration. In fact, Secretary of Transportation Pete Buttigieg appeared on TikTok in April 2021. In June 2021, the Biden Administration withdrew the Trump IEEPA executive orders against TikTok and WeChat, instituting instead a broad review of applications subject to the jurisdiction of a foreign adversary. It said such a review would be based on "rigorous, evidence-based analysis and should address any unacceptable or undue risks consistent with overall national security, foreign policy, and economic objectives, including the preservation and demonstration of America's core values and fundamental freedoms."[h] Coupling the rescission of the prior order with this statement suggests the earlier executive orders failed to meet those standards.

Standing Up for the Global Internet

The national security rationales were overblown from the start, used to justify actions that just happened to target platforms that had proved a thorn in the side of political leaders. Trump borrowed even more of the Chinese Internet strategy than might be obvious—like the Chinese government, he sought to silence his critics.

Thankfully, independent courts proved a bulwark against such digital authoritarianism. Technologists, too, should press governments to demonstrate the actual risks, and not be content with vague hints of sinister activity too dark to reveal. After all, foreign companies can be targeted because they might carry political reports that are too controversial for domestic news media,[i] or because they compete with favored local corporations.

When major Internet platforms suspended Trump in the wake of the January 6, 2021 insurrection, Trump Administration Secretary of State Mike Pompeo tweeted, "Silencing speech is dangerous. It's un-American." He continued, "We cannot let [the Left] silence 75 [Million] Americans. This isn't the CCP." But Secretary Pompeo had it backward. One cannot imagine any Chinese tech platform suspending the Chinese president. Only democratic nations provide the freedom to refuse to promote or carry the views of those in power.

The U.S. should not cede its advocacy for the global Internet, one that connects people across the world.[j] C

e U.S. Department of Justice. *Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act*, n.3 (Apr. 2019).

f United States District Court, District of Columbia. *TikTok Inc. v. Trump. Federal Supplement, Third Series*, 490, (2020), 77.

g United States District Court, Eastern District of Pennsylvania. *Marland v. Trump. Federal Supplement, Third Series*, 498, (2020), 642.

h See https://bit.ly/3yLCmfx

i Anupam Chander, Googling Freedom, 99 Calif. L. Rev. 1 (2011).

j For a vision of national regulation that protects consumers while embracing a global Internet, see Anupam Chander, *The Electronic Silk Road*. Yale University Press, New Haven, CT, 2013.

Anupam Chander (ac1931@georgetown.edu) is a professor of Law at Georgetown University, Washington, D.C., USA.

The author thanks *Communications* column editor James Grimmelmann as well as Kaitlyn Tsai and Lois Zhang for their research assistance.