QUINCY INSTITUTE FOR RESPONSIBLE STATECRAFT

LEGISLATIVE & POLICY NOTES

The Lessons of Tik Tok

Marcus Stanley, Director of Studies

OVERVIEW

The application of the law to ban TikTok access in the U.S. has been only briefly delayed by President Trump's actions. Further, the ban could be only the first step in a broader future effort to firewall the American internet from Chinese and foreign influence.

As the date of actual implementation drew near, the TikTok ban drew significant political opposition from ordinary Americans due to the economic harm it would do and the burden it would place on the constitutional right to free speech. Important lessons can come from the TikTok ban concerning the ways in which policies advanced as opposing China can instead rebound to harm Americans domestically, without tangibly improving the American strategic position with respect to China.

Policies sold as opposing Chinese influence often call for significant social changes in the U.S. based on hypothetical or potential Chinese threats, without documenting a real likelihood of harm. There is also a tendency to leverage domestic policy concerns into policies that target China but do not address the broader problem — such as, in the case of TikTok, the general failure to establish privacy regulations for big tech. When the actual costs to the American public become clear, policymakers can be blindsided. We can see these lessons in the TikTok case.

BACKGROUND

On April 24, 2024, President Biden signed H.R. 815 into law. This legislation took the first steps toward creating what, by analogy, might be called an American "Great Firewall" around the internet. It did so by banning "foreign adversary controlled applications," meaning social media applications with any significant ownership by individuals or entities from "adversary nations" (defined under 10 USC 4872 as China, Russia, North Korea, and Iran).

Although the authority granted in H.R. 815 permits the president to ban any social media application controlled by a foreign adversary, the only application specifically identified in the bill was TikTok. The legislation required TikTok's Chinese parent company, ByteDance, to sell the company to an American owner by Jan. 19, 2025. If it did not, web hosting services operating in the U.S. could no longer maintain the app and app stores could no longer offer it.

When President Trump took office, he issued an executive order instructing the attorney general not to take any action enforcing the ban on TikTok for the next 75 days (until April 5, 2025). H.R. 815 itself also permits the president to provide a single, 90-day extension to TikTok's availability in the U.S., subject to assurances about its eventual sale.

Rumors abound concerning potential buyers, including Microsoft and other tech giants, but ByteDance itself appears reluctant to engage in a forced sale. As long as the statutory ban remains in place, TikTok's future remains highly uncertain. The application has 170 million American users; a third of U.S. adults — including over half of adults under 30 — report being regular users. Many report using it for news or political information.

The TikTok ban points toward a future where the national security state takes a more active role in determining what Americans can access on the internet. The authority already granted by H.R. 815 could permit the president to ban American access to some dimensions of Chinese software like the recently released artificial intelligence, or AI, application DeepSeek, depending on whether aspects of AI apps meet the definition of social media under the bill. Over the last six years, both the Trump and Biden administrations also issued executive orders claiming unilateral presidential authority to restrict and ban internet applications based on access or control by foreign adversaries, without congressional action. In 2019, President Trump issued Executive Order 13873, which declared a national emergency under the International Emergency Economic Powers Act, IEEPA, related to foreign adversary control of U.S. information and communication technology and services, or ICTS. The Biden administration then issued Executive Order 14034, which used the powers authorized under the Trump emergency declaration to instruct regulatory and national security agencies to protect against security threats created by any ICTS owned by foreign adversaries.

DISCUSSION AND RECOMMENDATIONS

In light of what are likely to be continuing efforts to ban or restrict foreign-owned internet services, it is useful to take a deeper look at the experience so far of the legislative ban on TikTok, and what it tells us about the potential firewalling of the American internet space.

Real economic value is lost by a ban on the app — and this drives political opposition. A report from Oxford Economics found that TikTok created $24 billion in economic value in 2023 and supported over 200,000 jobs. Given the uncertainties in economic modeling and the fact that the Oxford Economics report was commissioned by TikTok, one could certainly contest these exact figures. But there can be no doubt that small- and medium-size businesses and individual creators invested significant resources in their TikTok presences.

As the deadline for the TikTok ban approached, small business opposition surged. Broader public opinion also seemed to move against a ban, with only 32 percent of Americans supporting a ban and 39 percent opposing it by late 2024, a sharp decline from previous years. President Trump reflected these views when he stated that "I have a warm spot in my heart for TikTok. … It's a very popular site, and the kids are loving it, and some of the parents are loving it. And if we can save it, I think that would be a very good thing. And I think it would be economically good for America." In the end, there was enough opposition that President Trump's decision to postpone the ban was viewed as highly politically beneficial.

The national security justifications for the ban rest more on potential rather than actually documented harm. The House Energy and Commerce Committee produced a supporting 18-page committee report on TikTok legislation. The report documented that TikTok (like many big tech apps) collected extensive data on its users, and that TikTok's parent company was subject to the jurisdiction of the Chinese Communist Party, or CCP, which created the potential for that information to be abused. However, it did not document any proven cases of TikTok being used to harm Americans or its use by the CCP to manipulate the American information environment. Nor did it fully assess the effectiveness of potential technical and governance firewalls between TikTok's U.S. business and its ByteDance parent, which had not been fully implemented at that time.

A 2023 CNN article summed up the views of experts by stating: "Security experts say the government's fears, while serious, currently appear to reflect only the potential for TikTok to be used for foreign intelligence, not that it has been. There is still no public evidence the Chinese government has actually spied on people through TikTok." Robert Joyce, the director of cybersecurity for the National Security Agency, was quoted in the article as stating: "People are always looking for the smoking gun in these technologies. I characterize it much more as a loaded gun," implying that the threat was potential. A 2023 analysis by the Center for Strategic and International Studies, CSIS, stated that "there is no direct evidence to show that the CCP has yet conducted influence operations through TikTok," and also pointed out that influence operations could easily be conducted through U.S.–owned platforms as well.

Broader societal concerns over tech will not be addressed by actions targeting adversary nations. The TikTok ban is an example of a frequent pattern in which a broad societal concern is ascribed to Chinese influence — in this case, the implications of social media platforms for user privacy and the manipulation of public discourse. Clearly, big tech platforms in general collect massive information on users and have recommendation algorithms capable of manipulating the public discourse. Third parties like data brokers have, at best, very limited restrictions on their ability to collect, buy, and sell information on web browsing by U.S. users — information that can be extremely private, especially when aggregated.

The debate over TikTok takes these broad and highly legitimate concerns and applies them only to the case of a single platform connected to a Chinese parent company. As the CSIS analysis states, "the strongest approach would be for Congress to establish comprehensive rules across the entire data ecosystem that would limit how all companies — including TikTok — use personal information," rather than focusing on the single case of TikTok.

The Supreme Court's TikTok decision shows that the courts will be highly deferential to actions justified by national security claims, even if they infringe on fundamental rights. The Supreme Court recently upheld the TikTok ban in a unanimous per curiam decision that accepted the government's national security justifications for banning the communications platform. Further, the court determined that, despite the sweeping nature of the action in banning a speech platform used by 170 million Americans, its uncontested impact on speech

rights, and the fact that the government acted essentially due to potential rather than documented harm, the TikTok ban did not require "strict scrutiny" under the First Amendment. That is, the question of whether the ban violated the constitutional rights of Americans, in this case the right to free speech, did not require the highest level of legal scrutiny because broad actions were justifiable given national security concerns. The finding was strongly opposed by nonpartisan free speech advocates.

Congress therefore bears an even more significant responsibility in when and how it invokes national security justifications, as the courts are likely to defer even if Congress uses such justifications in ways that potentially infringe upon fundamental rights.

The creation of a firewall around the U.S. internet will drive the fragmentation of the global internet in ways that could harm U.S. interests and its citizens. As discussed above, the TikTok ban could be just the first major step in an effort to firewall the American internet. We should ask whether such a firewall would really benefit the public, or whether following the approach of authoritarian countries like China by restricting internet access would really align with America's best approach to increasing its global influence. When TikTok was temporarily banned, over 700,000 Americans downloaded the Chinese app RedNote in protest. Positive interactions on RedNote between Chinese and American users led the Chinese government to tighten its censorship rules to prevent Chinese citizens from learning more about American life. This not only exposed Chinese users to the difference between Chinese and American values, but such censorship can also be a warning to Americans about the dangers of authoritarianism. The example of American principles of constitutional freedom and liberty is likely to be a more powerful way to support our national strengths than efforts at censorship.

About the Author

Marcus Stanley is director of studies at the Quincy Institute for Responsible Statecraft. Prior to joining the Quincy Institute, he spent a decade at Americans for Financial Reform, where he played a leadership role in policy formulation and advocacy to reform regulation of the U.S. financial system. He helped direct the efforts of a coalition of 200 organizations on a range of legislative and regulatory initiatives to challenge the power of Wall Street. His proudest accomplishment was the role he played in beating back numerous legislative efforts to weaken post-financial crisis regulatory reforms, as well as helping to change the inside the beltway dialogue on the significance of strong regulation of financial markets. Before that, he was an economic and policy advisor to Senator Barbara Boxer as a senior economist at the U.S. Joint Economic Committee. While there, he produced "War at Any Price?" — a seminal study on the full costs of the Iraq invasion, used to build political support to end the U.S. role in the war. He also taught Economics at Case Western Reserve University in Cleveland for six years. He has a PhD in public policy from Harvard, with a focus on economics.

About the Quincy Institute

The Quincy Institute for Responsible Statecraft believes that efforts to maintain unilateral U.S. dominance around the world through coercive force are neither possible nor desirable.

A transpartisan, action-oriented research institution, QI promotes ideas that move U.S. foreign policy away from endless war and towards vigorous diplomacy in pursuit of international peace. We connect and mobilize a network of policy experts and academics who are dedicated to a vision of American foreign policy based on military restraint rather than domination. We help increase and amplify their output, and give them a voice in Washington and in the media.

Since its establishment in 2019, QI has been committed to improving standards for think tank transparency and producing unbiased research. QI's conflict-of-interest policy can be viewed at www.quincyinst.org/coi/ and its list of donors at www.quincyinst.org/about.

2000 Pennsylvania Avenue NW
7th floor
Washington, DC 20006

+1 202-800-4662
info@quincyinst.org
www.quincyinst.org