TOPIC: TIKTOK

"Banning TikTok": Legislative Proposals and Their Implications

Overview

Current legislative proposals to "ban TikTok" have implications that go far beyond the Chinese-owned social media platform. The leading bills active in Congress today, such as the DATA Act (H.R. 1153) and the RESTRICT Act (S. 686) are sweeping new national security mandates on the Federal government. Within the United States, they could unacceptably restrict the First Amendment rights of U.S. citizens. Overseas, they could alienate potential allies, cut off opportunities for beneficial economic interaction, and lead to reprisals that could divide the world into competing technology zones.

Congress should consider whether a more nuanced approach would yield better results in addressing the risks created by foreign ownership of U.S. communications infrastructure. TikTok in particular merges a number of concerns, including negative effects of addictive social media that are common to domestic and foreign owned platforms, software market access issues more associated with trade than national security, and security issues related to foreign ownership. Responding to these issues with sweeping new federal national security mandates may risk unnecessary and possibly harmful overreach.

Background

TikTok, a video sharing app, is among the most popular social media platforms in the United States, with some 150 million U.S. users. It is owned by ByteDance, a company founded in China by a Chinese software engineer and headquartered in Beijing. The corporate structure of ByteDance is complex, but it is known that the Chinese Communist Party (CCP) holds a board seat and partial ownership in at least the ByteDance subsidiary that owns and manages the Chinese version of TikTok, known as Douyin.

The fact that TikTok was created and is still owned by a Chinese company has led to accusations that the CCP essentially controls the technology, and could use the app for surveillance of American citizens and manipulation of information. Speaking at a March 2023 hearing, House Commerce Committee Chair Cathy McMorris Roberts stated:

"TikTok collects nearly every data point imaginable from people's location to what they type and who they talk to, biometric data and more, even if they've never been on TikTok. Your trackers are embedded in sites across the web. TikTok surveils us all, and the Chinese Communist Party is able to use this as a tool to manipulate America as a whole….

TOPIC: TIKTOK

Today, the CCP's laws require Chinese companies like ByteDance to spy on their behalf. That means any Chinese company must grant the CCP access and manipulation capabilities as a design feature. Right now, ByteDance is under investigation by the DOJ for surveilling American journalists, both digital activity and physical movements through TikTok."

TikTok itself denies that it is controlled by the CCP. It points out that ByteDance is majority controlled by non-Chinese investors, claims that CCP involvement is limited to the subsidiary operating the Douyin software in China, that U.S. data is protected and firewalled from any Chinese government access, and[2] that it takes no requests from any foreign governments related to content moderation. Some have also pointed out that **extensive surveillance and collection of private information from internet users by software companies is endemic across all companies, including U.S.-owned companies, and these harms could be better addressed by general privacy legislation.**

Beginning under the Trump administration, the federal government began taking steps to ban the use of TikTok in the United States, at least as long as it remains owned by a Chinese company. In 2019 the Trump administration declared a national emergency with respect to the security[3] of the U.S. information and communications technology systems (ICTS) infrastructure. Such an emergency declaration can be used to invoke the International Emergency Economic Powers Act (IEEPA), which grants the federal government a wide variety of powers to restrict and control economic activity.

Using IEEPA authority, the Trump administration[4] issued what was essentially a blanket ban on the use of TikTok on U.S. computer systems. The Trump administration also attempted to use its review authority under the Committee on Foreign Investment in the United States (CFIUS), which permits review and restriction of various business transactions involving[5] foreign control of U.S. companies, to force ByteDance to sell TikTok and its data.

The IEEPA-based ban on TikTok use was challenged and overturned in court. For First Amendment/freedom of speech reasons, IEEPA contains exemptions that do not allow the government to use emergency economic authority to restrict personal communications between citizens or transactions that involve purely informational transfers. Two courts found that those exemptions prevented the government from using IEEPA to ban[6] TikTok. Another court also cited First Amendment grounds directly in overturning the Trump administration's attempted use of IEEPA to shut down the Chinese app WeChat in the U.S.

The CFIUS-based effort to force divestment of TikTok by ByteDance led to negotiations between TikTok and the federal government regarding firewalls and protection of U.S. data from ByteDance and any Chinese government influence.

TOPIC: TIKTOK

As mentioned above, TikTok has taken measures over the past several years that it claims have achieved this goal. The negotiation process has continued under the Biden administration, but the U.S. government has not yet attempted to enforce the CFIUS divestment requirement in court.

In addition to these measures to outright ban or force the sale of TikTok, the Trump administration Commerce Department released a proposed rule that would set up a national security review process to restrict transactions that could give entities influenced by "foreign adversaries" control over ICTS infrastructure. If this process determined that such transactions posed a risk to national security, it would allow the federal government to ban or reverse such transactions or take steps to mitigate such risks.

The Biden administration has essentially continued the Trump administration's attempts to restrict TikTok. The Biden Commerce Department has also expanded Trump's efforts to create a national security review process for ICTS infrastructure, including by defining connected software applications such as TikTok as ICTS infrastructure subject to national security review.

But this national security review process rests on uncertain legal grounds. The statutory authority that the Trump and Biden Commerce Departments have relied upon to establish national security review of ICTS infrastructure is the same IEEPA authority that was rejected by the courts as a grounds for banning TikTok, due to the information and communications exemptions in the legislation. It therefore may not survive a court challenge.

Congress is now stepping in with multiple legislative proposals designed to increase the federal government's powers to control communications and information technologies, or to directly mandate such actions be taken.

Current Legislation

Two major bills that would impose sweeping restrictions on Chinese-owned software are currently working their way through the House (H.R. 1153) and Senate (S. 686).

H.R. 1153, the DATA Act, recently passed the House Foreign Affairs Committee on a partisan vote. This legislation would mandate the full force of U.S. sanctions authority be used to penalize any companies or entities that transferred the personal information of U.S. citizens to Chinese-influenced companies, or in some cases dealt in Chinese-influenced software. The sweep of the bill and the penalties it imposes are extraordinarily broad and could lead to unintended consequences. Section 102 of H.R. 1153, oriented toward penalties on U.S. citizens, would require the secretary of the

treasury to ban any U.S. financial transactions by any American who had knowingly transferred sensitive personal information of an American citizen to any entity subject to Chinese jurisdiction, "directly or indirectly operating on behalf of China," "directly or indirectly controlled by," or even "subject to the influence of" China.

The bill defines "sensitive personal information" by reference to Section 7.2 of Title 15 in the Code of Federal Regulations, which is extraordinarily broad. For example, it encompasses any financial information included in consumer reporting, any health insurance information, any email communications, and any information on a government ID such as address information. Given the breadth of this definition, any company or individual who had, for example, forwarded emails or shared health insurance or personal address information with a company that had even partial Chinese ownership could find themselves banned from all financial transactions.

A blanket ban on financial transactions is a very harsh penalty, implying that all assets of the target entity would be effectively frozen. For example, an individual or company subject to the penalty would be unable to use their credit cards, access cash in their bank accounts, or pay their mortgage.
While protection of genuinely sensitive personal information is a worthy goal, the combination of the sweep of this legislation and the harshness of its penalties could exercise a profound chilling effect. The threat of an asset freeze could make it prohibitively risky for Americans to interact with any entity that was even minority owned or "influenced" by Chinese citizens or companies.

Title II of the H.R. 1153 focuses on foreign jurisdictions. It would require the U.S. government to freeze all U.S. assets of a foreign person anywhere in the world who "operates, directs, or otherwise deals in" a connected software application that is Chinese-owned or "subject to the influence of" China, if such software either facilitates Chinese military, surveillance, or censorship activities, or if it involves Chinese access to recommendation algorithms that could manipulate content.

Again, this is an extraordinarily broad prohibition, connected to extreme penalties. If implemented, it would direct the U.S. government to exploit the global predominance of the U.S. financial system to in effect ban the use of a wide range of Chinese software anywhere in the world, including in nations that are allies or partners. One may question whether this is a reasonable use of scarce governmental resources. It could also backfire by causing significant ill will against the U.S. government around the world, including among friendly nations. It would also certainly greatly increase pressures to avoid the U.S. financial system and the use of the U.S. dollar, since dollar assets transmitted through U.S. banks could at any time be frozen due to even innocent use of Chinese-linked software.
Many of the issues with H.R. 1153 were pointed out by Rep. Gregory Meeks (D-N.Y.) and other Democratic members of the House Foreign Affairs Committee during the committee debate on the

bill, and the bill passed on a partisan vote.[10] This makes it less likely that it will become law.

S. 686, the "Restrict Act," is the leading Senate bill to restrict TikTok and appears to have a much greater chance of becoming law than HR 1153 does.[11] This legislation has 21 bipartisan co-sponsors and has been endorsed by the Biden administration. It essentially creates through statute the sweeping new ICTS national security review process that the Trump and Biden administrations have tried to establish through regulation.

The bill would grant the executive branch extensive new national security powers over commerce in information and communication technologies, and by extension over speech. The core mandate in Section 3 of the bill requires the executive branch to prohibit or otherwise "mitigate" any transaction or activity in information and communications technologies by companies controlled by a "foreign adversary" if the commerce secretary determines that such a transaction poses any risk to U.S. national security.

Section 3(a)(1) of the bill defines national security risks broadly, mandating action in the case of any "undue or unacceptable risk." Specific listed areas of concern include "sabotage or subversion" of communications technologies, "election interference," or "coercive or criminal activities" that "steer policy and regulatory decisions" in favor of the interests of a foreign adversary. Section 5 of the bill contains a long list of priority areas of concern in communications infrastructure, ranging from physical infrastructure to software content delivery applications.

The initial list of "foreign adversaries" in the bill includes China, Cuba, Russia, Iran, Venezuela, and North Korea. The executive branch could add additional foreign adversary nations at will. This choice could only be overridden by a majority vote of both houses of Congress.

Section 11 of the bill grants the president a wide range of civil and criminal options to enforce the mitigation of national security risks. These include forced divestment of assets and seizure of assets. Criminal penalties for those who seek to evade the enforcement of this law include fines up to $1 million or prison terms of up to 20 years. Under Section 12 of the bill, legal avenues to contest such actions are limited. They are restricted to challenges filed in the U.S. Court of Appeals for the District of Columbia within 60 days, and must meet the high standard of a constitutional violation or "patent violation of a clear and mandatory statutory command.

The powers granted by the RESTRICT Act would be discretionary, and could theoretically be used in a restrained and measured way. At minimum, they would set up a review standard similar to CFIUS review, but applied to all investment in U.S. communications channels by "foreign adversaries."

However, it is notable that the legislation does not include any limiting principles, such as a requirement to use the least restrictive form of mitigation that protects national security goals. The extremely broad scope of the national security mandates in the bill also lend themselves toward maximal use of the powers granted to the federal government.

Without limiting principles, and with restricted opportunities for legal challenge, S. 686 would press the federal government to ban or censor any significant information and communications technologies within the U.S. market that are economically influenced by foreign nations viewed as adversaries of the United States. Such technologies could be subject to censorship or restriction at will, with heavy penalties potentially levied on any U.S. citizens who attempted to access them.

Such actions could have significant ramifications internationally and domestically. We may see retaliatory bans on the use of U.S. software and communications technologies in foreign countries targeted as "adversary nations." This could accelerate the division of the world into rival information technology spheres protected by "great firewalls" like that imposed by China, which itself sharply restricts or bans U.S. information technology companies.

Domestically, Section 11 of the bill establishes draconian penalties for American citizens who violate it by attempting to evade or help others to evade new restrictions on foreign-owned information and communications technologies. While it is somewhat ambiguous how far this could go, it could lead to American citizens being prosecuted for accessing information on a wide range of foreign-owned technology platforms.

This kind of censorship, based on foreign ownership rather than content, has not been tested under First Amendment law, but it could have profound implications.[12] The ACLU has already stated its opposition to the bill on freedom of expression grounds. The court decision overruling a ban on WeChat use by American citizens on First Amendment grounds is further demonstration that such concerns have validity.[13]

Some Policy Conclusions and Recommendations

Of the two major TikTok bills moving through Congress, H.R. 1153 most clearly overreaches in its extreme penalties on U.S. citizens for interaction with Chinese-influenced companies, and its use of U.S. sanctions to try to force worldwide divestment from Chinese software. S. 686, the RESTRICT Act seems more likely to pass into law in some form. While it too goes well beyond TikTok, it clearly reflects recent policy momentum in Washington for a new CFIUS-like oversight procedure for foreign investment in U.S. communications.

TOPIC: TIKTOK

Yet the RESTRICT Act also has clear potential for overreach in the tremendous and largely unaccountable regulatory powers it grants the government to control communications potentially influenced by an "adversary nation." The idea of a national security review process holds useful potential because of its flexibility and the ability to pursue mitigation strategies appropriately tailored to the issue at hand, but only if it is limited and targeted in practice.

It is also striking that while these bills are very broad in the national security application, they are underinclusive in responding to concerns expressed about TikTok. For example, neither piece of legislation addresses concerns about TikTok that are not based on its Chinese ownership but are common to a wide range of social media apps, such as loss of privacy, gathering of personal data, targeting of young people, and the addictive quality of social media. Addressing these concerns requires broader internet privacy legislation that would apply to U.S. and foreign-owned apps alike.

Mandating sweeping national security restrictions on communications technology also loses the opportunity for a principled effort to liberalize Chinese software markets by seeking reciprocity in access to the U.S. and Chinese markets. U.S. social media companies are by and large banned in China; this alone creates an argument that Chinese software companies can be reciprocally banned in the U.S. unless China liberalizes access to its information space. By instead setting up procedures for blanket national security bans on foreign software, the U.S. effectively begins to follow China in placing sharp national security restrictions on the openness of our internet media. As Yale law professor Robert Williams stated, "the appropriate response to China's arbitrary application of 'national security' is not to imitate the Chinese approach."

With regard to the genuine national security concerns in play, it is striking that TikTok is already attempting to firewall its U.S. operations from Chinese influence and manipulation in response to U.S. government pressure. There are concerns regarding oversight of these efforts. But in many areas — such as content censorship or politically biased recommendation algorithms — the results of TikTok's efforts should be readily visible and open to monitoring. The implementation of broader legislation to protect user privacy across all software companies would also open up avenues to more closely monitor privacy firewalls that TikTok has promised to put in place.

In sum, legislation such as H.R. 1153 and S. 686, while framed as an effort to "ban TikTok," represent a major expansion of the national security state that may not be necessary to respond to issues raised by TikTok, and risks overreach with grave implications for the rights and liberties of U.S. citizens.

TOPIC: TIKTOK

1. Beijing takes stake, board seat in ByteDance's key China entity - The Information | Reuters
2. Myths vs Facts | TikTok
3. 2019-10538.pdf (govinfo.gov)
4. https://www.govinfo.gov/content/pkg/FR-2020-08-11/pdf/2020-17699.pdf
5. 2020-18360.pdf (govinfo.gov)
6. Marland v. Trump, 498 F. Supp. 3d 624 - Dist. Court, ED Pennsylvania 2020 - Google Scholar; US WeChat Users Alliance v. Trump, 488 F. Supp. 3d 912 - Dist. Court, ND California 2020 - Google Scholar
7. The Information and Communications Technology and Services (ICTS) Rule and Review Process (congress.gov)
8. 2021-25329.pdf (govinfo.gov)
9. Text - H.R.1153 - 118th Congress (2023-2024): DATA Act | Congress.gov | Library of Congress
10. February 28, 2023 House Foreign Affairs Committee markup, available at https://foreignaffairs.house.gov/markup/h-r-1093-h-r-1159-h-r-1189-h-r-1157-h-r-1107-h-r-1154-h-res-90-h-r-1151-h-r-406-h-r-1149-h-r-1153/
11. https://www.congress.gov/bill/118th-congress/senate-bill/686
12. ACLU Raises Concerns About Senate Bill Aimed at Banning TikTok | American Civil Liberties Union
13. https://scholar.google.com/scholar_case?case=4070455322955590 42#p926
14. The TikTok Debate Should Start With Reciprocity; Everything Else Is Secondary | ITIF
15. Beyond Huawei and TikTok: Untangling US concerns over Chinese tech companies and digital security (brookings.edu)