TICK TOCK, TIKTOK: REGULATORY AND LEGAL APPROACHES TO MITIGATING A CHINESE THREAT

BY
MICHAEL G. MCLAUGHLIN

Michael McLaughlin is a cybersecurity attorney in the Washington D.C. office of Baker, Donelson, Bearman, Caldwell & Berkowitz. He is the former Senior Counterintelligence Advisor for U.S. Cyber Command and a veteran Naval Intelligence Officer. His forthcoming book, Battlefield Cyber: How China and Russia are Undermining Our Democracy and National Security, will be released this summer.

Visit www.competitionpolicyinternational.com for access to these articles and more!

TICK TOCK, TIKTOK: REGULATORY AND LEGAL APPROACHES TO MITIGATING A CHINESE THREAT

By Michael G. McLaughlin

The risks posed by TikTok have garnered significant attention due to concerns about potential threats to users and to national security. Recent reports suggest that cyberattacks, including those linked to China, are increasing, with hackers targeting personal data. A comprehensive approach is necessary to effectively address the multifaceted risks posed by TikTok and its parent company, ByteDance. A ban on TikTok may be necessary to adequately protect national security and cybersecurity, given the potential risks and the limitations of regulatory approaches. However, a nationwide ban will face significant legal challenges. Alternative solutions, such as Oracle auditing TikTok's data transfer mechanisms, have been proposed, but there are concerns that such solutions may not be effective due to the potential conflict of interest of the auditing party. To address these concerns and to avoid the legal challenges of a nationwide ban, states should consider imposing penalties and injunctions through their consumer protection laws as a potential option to hold TikTok accountable for misleading consumers about its data collection practices and content moderation policies.

On March 1st, the House of Representatives passed a bill introduced by House Foreign Affairs Committee Chair Rep. Michael McCaul (R-TX) that would allow the President to ban TikTok through a revision of the 1988 Berman Amendments. This bill is one of the latest moves by lawmakers worldwide to control the national security, data privacy, and consumer protection risks posed by TikTok.

TikTok has come under mounting scrutiny due to its mature content, relationship with the Chinese government, and potential for the Chinese intelligence and security services to access user data. In late 2022, the U.S. Federal Government banned TikTok on all government devices and systems and prohibited internet traffic from reaching TikTok servers – adding to similar actions by Canada, Taiwan, and the European Union. Over the past year, more than half of all U.S. states have instituted similar bans on state government devices, including the open WiFi networks at many public universities.

Moreover, TikTok has been accused of misleading users about age restrictions and lying to Congress about the accessibility of American user data by personnel in China, raising concerns about national security and cybersecurity risks associated with its data collection and storage practices. These issues, coupled with TikTok's links to the Chinese government, have increasingly drawn scrutiny over threats TikTok poses to its users and to national interests worldwide.

As U.S. lawmakers increasingly call for a nationwide ban, it is important to understand the risks and legal issues at play.

01
BACKGROUND

TikTok is a widely used social media platform and mobile application that allows users to create and share short videos. TikTok's popularity is due, in large part, to its wide suite of tools that allow users to create and edit personal videos using filters, effects, and an extensive library of licensed music. Since its founding in 2017, TikTok has grown significantly in both its number of users and its reach, particularly in the United States. At the end of 2022, TikTok boasted over 1 billion monthly active global users, with nearly 100 million monthly active users in the United States alone. Of those American users, 32.5 percent are between the ages of 10 and 19.

However, TikTok's Chinese ownership and links to the Chinese Communist Party have raised concerns regarding user data privacy and national security. Specifically, there is fear the Chinese government could access sensitive personal information, such as location, contacts, and browsing history, collected by the app. There are also concerns that the app could be used for propaganda purposes or to censor content critical of the Chinese government, potentially impacting freedom of speech.

TikTok's parent company, ByteDance, is a Chinese technology company valued at nearly $300 billion. In addition to TikTok, ByteDance also owns a domestic Chinese video-sharing application, called Douyin, in which the Chinese government has taken a 1 percent ownership stake and one of three board seats. Apart from its stake in TikTok's sister company, the Chinese Communist Party maintains the legal authority to both direct corporate action and compel ByteDance and its subsidiaries to share with Chinese intelligence and security services all data maintained anywhere in the world.

Several Chinese laws related to national security, cybersecurity, and national intelligence exacerbate these concerns. The National Security Law, enacted in 2015, broadly defines national security to include political, economic, military, and cultural factors. This law grants Chinese authorities the power to take measures to protect national security, including surveillance and censorship. The Cybersecurity Law, passed in 2017, establishes a regulatory framework for cybersecurity in China, requiring network operators to store user data within China and imposing cybersecurity obligations on network operators and other entities. The National Intelligence Law, also enacted in 2017, requires Chinese organizations and citizens to cooperate with state intelligence work and provides legal grounds for intelligence-gathering activities.

For Chinese companies that host massive amounts of data, especially data that originates from other parts of the world—including the United States, there is no option but to share all data requested by the Chinese government. Moreover, the legal control that the Chinese government exerts over TikTok and ByteDance is substantial, contrary to TikTok's representations. For example, in the weeks before the 2022 U.S. midterm elections, the Chinese Communist Party used TikTok to push divisive political videos targeting American consumers from accounts managed by Chinese registered foreign agents.

02

TIKTOK'S MISLEADING PRACTICES

In a lawsuit filed by the Indiana Attorney General in December 2022, TikTok has been accused of misleading users about appropriate age restrictions and engaging in deceptive age verification practices. In the Apple App Store, Google Play Store, and Microsoft Store, TikTok advertises that its content is suitable for children as young as age 12. TikTok knowingly subjects minors to mature, obscene, and harmful content that influences their behavior with detrimental effect. Indiana has alleged TikTok engages in unfair and deceptive practices by self-reporting false information to Apple to obtain a “12+” rating and to Microsoft and Google to receive a “T” for “Teen” rating for the TikTok application.

TikTok knows that the information it falsely self-reports has been and continues to be reported directly to consumers. TikTok has represented to consumers that “Alcohol, Tobacco, and Drug References,” “Sexual Content or Nudity,” “Mature/Suggestive Themes,” and “Profanity or Crude Humor” are “Infrequent/Mild” on the platform, when, in fact, these types of content are frequent and intense. TikTok has also been accused of intentionally misleading Apple, Google, and Microsoft by presenting a sanitized version of the app during the review process for age rating. This would have allowed TikTok to bypass restrictions and gain access to younger users who otherwise would not be permitted to use the app.

In doing so, Indiana alleges, TikTok knowingly takes advantage of and profits from the exposure of harmful content to minor consumers who are reasonably unable to protect their own interests. By targeting younger users with inappropriate content, TikTok may be contributing to the normalization of sexual behavior and activities among minors — the outcome of which is likened to sexual grooming by child predators.

Beyond the age rating of its app, TikTok has been accused of intentionally misleading Apple, Google, and Microsoft by violating their respective app store policies. Specifically, TikTok was found to be using an unusual tactic known as "device fingerprinting" to track users across multiple devices without their knowledge or consent. Device fingerprinting is a technique that collects device-specific information, such as the operating system version and the device's hardware specifications and combines it to create a unique identifier for each device.

Apple, Google, and Microsoft have strict policies against app developers using device fingerprinting to track users, and TikTok was found to have circumvented these policies by using an encrypted payload to conceal the data collection. This allowed TikTok to collect user data without being detected by app store security checks. By intentionally misleading these app store providers, TikTok was able to continue its data collection practices without being subject to the consequences of violating app store policies.

In 2019, TikTok representatives testified before Congress regarding concerns about the company's data security practices and its ties to the Chinese government. During the hearing, TikTok's representatives stated that the company's data was stored in the United States and Singapore, and that the company had strict data privacy policies in place to protect user data. However, subsequent reporting revealed these statements may have been misleading.

In November 2019, the Committee on Foreign Investment in the United States (CFIUS) launched an investigation into TikTok's parent company, ByteDance, over concerns about the company's data security practices and its ties to the Chinese government. CFIUS has the authority to review foreign investments in the United States for national security concerns, and in this case, the agency was concerned that TikTok's data practices could put American users' data at risk.

During the course of the CFIUS investigation, it was revealed that TikTok's data was not solely stored in the United States and Singapore, as the company had previously claimed. Instead, it was discovered that TikTok stored American user data on servers located in China, which raised concerns about the Chinese government's access to American user data. This discovery contradicted TikTok's previous statements to Congress and raised concerns about the company's credibility and its commitment to transparency. TikTok's parent company, ByteDance, has strong ties to the Chinese government, which has led to concerns about the company's compliance with Chinese laws that could require it to provide access to user data to the Chinese government.

In 2022, TikTok executives again testified before Congress that, although the company has China-based employees, there are “very strict access controls around the type of data that they can access and where that data is stored, which is here in the United States.” Moreover, TikTok executives testified that “under no circumstances would [they] give that data to China.” However, in December 2022, in a rare admission, ByteDance confirmed its engineers in China used TikTok to monitor U.S. journalists’ physical location and contacts in an effort to identify an information leak. For users, this means that, under Chinese law, these same employees can be forced to track the location and activities of any TikTok user and turn that data over to the Chinese government.

03
NATIONAL SECURITY AND CYBERSECURITY RISKS

Given that TikTok is a Chinese-owned app, there is concern that the Chinese government may use it to collect intelligence and data on foreign citizens. This is a cause for alarm because the Chinese government has historically used its technology companies for such purposes. For example, in 2020, reports emerged indicating the Chinese government actors used technologies manufactured by Chinese companies – including tech giant Huawei – installed in more than 180 facilities across Africa to spy on members of the African Union.

Where the Chinese government subverts other technologies to commit espionage, TikTok is a tool tailor-made for spying on large swaths of the population.

TikTok collects vast amounts of user data, including personal information such as names, email addresses, phone numbers, and other identifiers from its users' accounts. It also collects browsing and search history, device information, and location data from the device, as well as biometric information from each video uploaded. TikTok has also been shown to use covert methods to collect data on its users, such as accessing the clipboard on iOS devices without user consent. This exposes sensitive data, including passwords and other confidential information, to potential attackers. As demonstrated by the ByteDance engineers in December 2022, this data is accessible to TikTok and ByteDance employees and stored on servers in China, where it is subject to Chinese government access under Chinese law.

The Chinese government's access to user data could potentially compromise national security by allowing them to monitor the activities of US citizens who use the app. This is especially concerning as it could result in the identification and tracking of US government officials, military personnel, or other individuals who could be targeted for espionage or other forms of foreign influence. From a foreign influence perspective, given TikTok's significant penetration of American society, it is a uniquely capable tool. TikTok's algorithms use machine learning to analyze user behavior and preferences to deliver personalized content and advertising. This data could be used to influence or manipulate users through racially or politically divisive content or other content that is detrimental to American interests.

And China's legal framework is not limited to data sharing. China's 2015 National Security Law stipulates: "Citizens and organizations shall provide . . . national security authorities, public security authorities, and military authorities with *needed support and assistance*." (emphasis added). This means the Chinese government could potentially influence what is shown to users on TikTok, censoring content that is critical of the Chinese government or promoting content that aligns with Chinese propaganda. Furthermore, the Chinese government could use TikTok as a tool for disinformation and manipulation by using bots or fake accounts to spread false information or influence public opinion on a global scale through TikTok's platform — all outside the jurisdiction and control of U.S. law enforcement.

In addition to the risks associated with the Chinese government's access to TikTok data and control over content, there is concern over how ByteDance, TikTok's parent company, uses TikTok user data to advance its artificial intelligence ("AI") capabilities. ByteDance has stated that it uses AI to analyze user behavior and preferences to improve its recommendation algorithms and better tailor content to users. However, there is the possibility that the company is also using this data for other purposes, such as developing AI technology for the Chinese government or other entities. This raises concerns about potential misuse of user data and the implications for national security and cybersecurity. Additionally, the lack of transparency surrounding how ByteDance uses TikTok data makes it difficult to assess the full extent of the risks associated with this practice.

04
REGULATING TIKTOK

There are several potential regulatory options available to the U.S. government to address the concerns related to TikTok. These options are generally classified into two categories: regulation and prohibition.

One potential regulatory option is for the U.S. government to impose strict regulations on TikTok's data collection and storage practices. This could involve requiring TikTok to store all user data on servers located within the United States and allowing independent audits of its algorithms, source code, and data security practices. However, there are shortcomings to this approach.

TikTok's recently proposed "Project Texas," which is TikTok's regulatory concession to stave off a nationwide ban, includes hosting U.S. data in Oracle Cloud, including the algorithm and content moderation functions, and having Oracle serve as the third-party reviewer of TikTok source code and data flows. There are three fatal flaws with Project Texas.

First, the proposal only protects U.S. person data and information that is within the U.S. However, TikTok is a global platform that connects users worldwide. As soon American users' videos are accessed by foreign users, all data from the video would transfer out of Oracle's cloud to TikTok's global servers – subjecting that data to the same risks it faces now.

Second, the proposal that Oracle — which hosts TikTok's data and derives a significant amount of revenue from the platform — conducts the audit of TikTok's data transfer mechanisms to address national security and cybersecurity concerns raises potential conflicts of interest. Oracle may be incentivized to overlook or downplay any potential issues in order to protect its business relationship with TikTok. This could undermine the effectiveness and impartiality of any audit conducted by Oracle, and ultimately fail to adequately address the national security and cybersecurity risks posed by TikTok.

Third, TikTok's proposal does nothing to address misleading age ratings, harmful content targeted towards children, or the Chinese government's ability to leverage the platform for malign influence.

While some of these issues can be mitigated — such as mandating TikTok implement stronger age verification measures by requiring government-issued identification from users to verify their age — many are unable to be resolved so long as TikTok is subject to Chinese laws.

As a result, a ban on TikTok seems necessary to protect users, national security, and cybersecurity interests. This would involve removing the app from the Apple App Store and Google Play Store and blocking access to the app's servers from within the United States.

05
COUNTERARGUMENTS AND RESPONSES

There are several counterarguments related to the First Amendment, economic principles, and industry practice that are frequently raised in opposition to a nationwide ban of TikTok.

First, TikTok supporters argue that a ban on TikTok would violate the First Amendment, which protects freedom of speech and expression. TikTok is a social media platform that allows users a unique venue and method of expressing themselves creatively through videos. Proponents of TikTok argue that any attempt to ban or regulate the app would infringe upon users' rights enshrined in the First Amendment.

While the Federal Government is generally prohibited from banning speech, this is not absolute, and a ban would not necessarily violate the First Amendment. A nationwide ban likely would come under the International Economic Emergency Powers Act ("IEEPA"), which gives the President broad authority to act in the national interest with respect to foreign entities. While IEEPA does not give the President the authority to suspend the Constitution, it does give him the authority to ban Apple, Google, and Microsoft from carrying TikTok in their app stores and to block all internet traffic routing from TikTok servers.

However, as soon a ban goes into effect, an American TikTok user very likely would file suit against the government alleging the ban violates the Constitution — as happened following the Trump administration's ban in 2020. This likely would lead to an injunction, which would allow TikTok to continue operating until either the ban is revoked, or courts analyze the constitutionality of such a ban — which could take several years.

Under the First Amendment, government restrictions on speech must be content neutral – that is, applicable to all expression without regard for substance, narrowly tailored to serve a significant government interest, and must leave open ample alternative channels for communicating. A ban on TikTok would be without regard for the content of speech. It would serve not only a significant government interest, but a compelling one — that of national security — and in the context of national security, courts have generally given deference to the government's assessment of the threat and have upheld government actions that were reasonably designed to address that threat. Finally, it would not foreclose other channels of speech. Where alternative means of communication exist, such as Instagram Reels and YouTube, a TikTok ban may withstand First Amendment scrutiny. The question is how long that process would take.

Second, opponents of a TikTok ban argue that it sets a dangerous precedent for government interference in private enterprise. The U.S. has traditionally been a champion of free markets, and any attempt to ban or regulate a popular app like TikTok could be seen as an overreach of government power.

The Constitution grants the government broad powers to safeguard U.S. national interests. Where international trade is concerned, the Commerce Clause gives Congress exclusive power of trade with foreign countries. When emergency powers are granted by Congress, IEEPA provides the President broad authority to regulate foreign trade with specific nations or specific companies. However, there are limitations to such authorities. IEEPA includes a non-exhaustive

exemplary list of information materials that are not subject to IEEPA regulation, including films, art, photographs, and newsfeeds. These limitations are put in place precisely to limit government overreach. Barring an amendment to IEEPA, these counterarguments likely would prevail — at least to preliminarily enjoin government action — were the government to institute a ban.

Third, many TikTok supporters also point to collection practices by other social media platforms and the largely unregulated sale of personal information by data aggregators as a reason why a ban on TikTok would not achieve the desired outcome of limiting the Chinese government's access to Americans' data.

This argument is not without merit, but it speaks a larger problem with U.S. data privacy regulations that needs to be addressed separately — namely, there is no federal data privacy law. But the fact that there are other data privacy regulatory issues Congress also needs to address does not negate the threat TikTok poses. TikTok's data collection and storage practices raise significant concerns about the Chinese government's potential access to sensitive information. Given the Chinese government's history of cyber espionage and intellectual property theft, it is not unreasonable to assume that TikTok data would also be exploited for nefarious purposes. For instance, the app's algorithms could be intentionally targeting vulnerable individuals with sensitive personal information, which could be used to compromise their security or blackmail them.

While a ban on TikTok may be a necessary step to protect national security and cybersecurity, it is likely to face significant legal challenges and be enjoined while the courts deliberate. In the meantime, TikTok will continue to operate and pose a threat to American users.

There is, perhaps, another option.

06
STATE ACTION

As previously discussed, the Indiana Attorney General filed two suits against TikTok and ByteDance in December 2022. This litigation could serve as a roadmap for individual states to bring actions against TikTok for violations of their respective consumer protection laws.

Indiana's first suit is based on a claim of data security misrepresentations surrounding its false, deceptive and misleading statements that U.S. user data is not subject to Chinese Laws requiring TikTok's cooperation with Chinese national intelligence, security, cybersecurity agencies. Indiana alleges TikTok misleads consumers about the risk of the Chinese government accessing and exploiting consumer data.

The second suit is based on claims of misleading and deceptive trade practices surrounding TikTok's age ratings. The crux of Indiana's claim is that TikTok knowingly subjects minors to mature, obscene, and harmful content that detrimentally influences their behavior. Indiana argues that TikTok has engaged in "unfair, abusive, or deceptive act[s] or practice[s] in connection with a consumer transaction," by self-reporting false information to the Apple to obtain a younger age rating. Indiana alleges TikTok knows that the information it falsely self-reports has been and continues to be reported directly to consumers.

For each of these suits, Indiana is seeking the following. First, declaration that TikTok's actions are unfair, abusive, and deceptive to Indiana consumers, which would open the door to civil and class action lawsuits against TikTok and ByteDance. Second, preliminary and permanent injunction against such actions by TikTok, which would prohibit TikTok from operating in Indiana until TikTok modifies its age rating or content and completely divests itself of Chinese ownership and control. Third, the maximum civil penalty permitted under Indiana's consumer protection laws — $5,000 per violation. A violation can be defined as each individual download of the app, resulting in the potential for billions of dollars in penalties.

Where the Federal Government may be restrained from impinging upon First Amendment freedoms through the institution of a ban, individual states bringing actions against TikTok for deceptive trade practices likely would face no such challenges.

07
CONCLUSION

Given the significant risks to individuals and to national security, a ban on TikTok may be necessary to adequately protect national security and cybersecurity. While alternative solutions, such as Oracle auditing TikTok's data transfer mechanisms, have been proposed, there are concerns that such solutions may not be effective due to the potential conflict of interest of the auditing party. However, a nationwide ban may not be the most effective tool.

Based on the risks to national security and cybersecurity posed by TikTok, it is a clear imperative that the govern-

ment take swift and decisive action to address these concerns. However, a complete ban on TikTok, which would effectively sever the connection between the Chinese government and TikTok's American user data, may face legal challenges. Alternatively, the U.S. government could pursue regulatory measures aimed at addressing specific concerns, such as data collection and storage practices, content moderation, and transparency. However, regulatory measures may be more challenging to enforce and could potentially be circumvented by TikTok and its parent company, ByteDance.

As a result, the solution that most effectively addresses the national security and cybersecurity risks associated with TikTok may not lie with the Federal Government. Instead, individual states should explore imposing penalties and injunctions through state consumer protection laws, which would hold TikTok accountable for misleading consumers about its data collection practices and content moderation policies.

> *Given the significant risks to individuals and to national security, a ban on TikTok may be necessary to adequately protect national security and cybersecurity*

CPI SUBSCRIPTIONS

CPI reaches more than **35,000 readers** in over **150 countries** every day. Our online library houses over **23,000 papers**, articles and interviews.

Visit **competitionpolicyinternational.com** today to see our available plans and join CPI's global community of antitrust experts.

CPI COMPETITION POLICY® INTERNATIONAL