TikTok and US national security

Dr. Milton L Mueller and Dr Karim Farhat, Georgia Institute of Technology, School of Public Policy, Internet Governance Project[1]

Is TikTok a threat to U.S. national security? If so, what is the nature of that threat? Surprisingly, evidence-based answers to those questions are largely absent from the policy discussion in Congress and the media. Those who argue that TikTok is a national security threat have not provided detailed explanations of how the ownership and control of a single app can threaten the entire nation's security. Technical assessments of the TikTok app have analyzed the security features of the app's code, but technical security is not national security.[2] *National* security hinges on political and military capabilities and impacts, not on bare code.

This paper conducts a comprehensive national security threat analysis of TikTok. The analysis is based on cybersecurity principles that pertain to international rivalries and power struggles between states. The guiding questions of this study are whether TikTok can be considered a tool of information warfare, a form of espionage, and/or a tool for offensive cyber operations by the Chinese government. In assessing the risk of allowing TikTok, it weighs those risks against the costs and risks of a TikTok ban.

Executive Summary

The study reaches the following conclusions:

- TikTok is a commercially-motivated enterprise, not a tool of the Chinese state. ByteDance's organizational structure reflects an attempt to segregate the Chinese market from global markets so that it can export its AI services globally. This split works to the advantage of both sides.
- Chinese government efforts to assert control over ByteDance's Chinese subsidiaries are targeting its domestic (Chinese) services, not its overseas operations.

---

[1] This report did not receive any funding from TikTok, ByteDance, or any interested party. IGP as an organization has not received funding from TikTok at any time in its history.

[2] P Lin, "TikTok vs Douyin A Security and Privacy Analysis." CitizenLab March 22, 2021; E.Alderson, "TikTok: Logs, logs, logs." Medium Aug 3, 2020; M Eberl, "Privacy Analysis of TikTok's app and website." Rufposten blog, December 2020.

TikTok and US national security

- TikTok is not exporting censorship, either directly by blocking material, or indirectly via its recommendation algorithm. Its content policies are governed by market forces.
- The data collected by TikTok can only be of espionage value if it comes from users who are intimately connected to national security functions and use the app in ways that expose sensitive information. These risks arise from the use of any social media app, not just TikTok, and cannot be mitigated by arbitrarily banning one app.
- Because social media apps publish and share so much data, China does not need to have special legal powers over ByteDance to use TikTok (or any other social media app) to monitor users. Open source intelligence tools (OSINT) can be used to gather extensive data about social media users regardless of whether the service provider cooperates. If this is a “threat,” it is one that applies to all social media, regardless of the provider’s national origin.
- The costs of a ban were considered. These include:
    - Banning TikTok would harm the 90 million + Americans who use the app. It would deprive them of free expression rights, and destroy their equity in their creations and followers.
    - Banning TikTok would expropriate the investors who have provided capital to the company, and eliminate thousands of US jobs.
    - Banning TikTok would weaken competition in the social media/advertising industry.
    - China could retaliate against American businesses in China
    - Banning TikTok would encourage other countries to enact techno-nationalist and data protectionist policies, which would have negative effects primarily on US-based social media firms.

Contents

Background

For nearly three years, TikTok, the popular short-video social media application, has been under attack from the U.S. federal government. This in itself is phenomenal. The United States of America, with the world's strongest constitutional protections for free speech and a longtime advocate of a globally open and free internet, is seriously considering banning a service that 94 million Americans use. In August of 2020, the Trump administration tried to ban TikTok by Executive Order, but it was ruled illegal by U.S. courts, citing freedom of expression protections that had been built into the law.[3] The Biden administration signed an executive order that revoked Trump's ban, but set in motion a governmental evaluation of the risk of apps connected to foreign adversaries.[4] By the end of 2022, the view of TikTok as a national security risk achieved bipartisan status.[5] In the final days of the 117th Congress, a bill banning TikTok on government devices passed the Senate unanimously.[6] A bill to ban TikTok completely was introduced by two Republicans and one Democrat December 13.[7]

TikTok is an odd target for this Red Scare. It is a private, commercial business, with multinational ownership. Its app has attracted a community of users outside of China who thrive on exchanges of videos, comments and live sessions. That community has grown to exceed 90 million in the United States. As American users have converged on it in record numbers, and advertisers have bought more time on it, a new competitor is succeeding in the market for social media services. In 2022, TikTok became the third most popular Internet service worldwide,[8] generating healthy competition against the dominant platforms, such as Meta (Facebook, Instagram) and Alphabet (Google, YouTube).

---

[3] Opinion, TIKTOK INC., et al., Plaintiffs, v. Donald J. TRUMP, President of the United States, et al., Defendants. Civil Action No. 1:20-cv-02658 (CJN) September 27, 2020. (United States District Court for the District of Columbia. Opinion, TIKTOK INC., et al., Plaintiffs, v. Donald J. TRUMP, President of the United States, et al., Defendants. Civil Action No. 1:20-cv-02658 (CJN) December 7, 2020.

[4] L Feiner, "Biden revokes and replaces Trump executive orders that banned TikTok," CNBC June 9 2021

[5] A Republican FCC Commissioner made banning TikTok his personal crusade. Ten GOP-led state legislatures have passed laws dictating which applications their employees can access in response to the alleged threat. B, Allen-Ebrahimian, "FCC commissioner says government should ban TikTok", Axios, November 1st, 2022.

[6] I Smith, "Efforts to ban TikTok for federal employees using 2023 NDAA Fail," FedSmith.com. December 15, 2022. S Woo, K O'Keefe, A Viswanatha, "TikTok Security Dilemma Revives Push for U.S. Control: Some Biden administration officials think TikTok will remain security risk as long as it is owned by Chinese company." Wall Street Journal, Dec 26, 2022.

[7] Rubio, Gallagher Introduce Bipartisan Legislation to Ban TikTok - Press Releases - U.S. Senator for Florida, Marco Rubio. Rubio website, December 13, 2022.

[8] Cloudflare Radar 2022 Year in Review, December 31, 2022.

Platform	Global monthly active US users (2022)	Rate of change from last year	MDAU (US)	*Source*
TikTok	94 million	+45%	~87 million	Kepios; TikTok; Backlinko; Statista
Instagram	123 million	+4%	~115 million	Statista; Statista
Facebook	239 million	+2%	~235 million	Statista
Twitter	77 million	-0.6%	41 million	Statista

Another commonly overlooked fact in the TikTok debate is that the content on TikTok is produced by its users, not by the company or the Chinese government. TikTok's users are outside China. The app provides access to thousands of homegrown comedy acts, cartoonists, political commentators, singers, hustlers, lip-syncers, meet-ups, facts, and news sources. Anti-communists and communists, woke progressives and religious conservatives are all present on TikTok. Different schools of thought contend with each other there. Shutting down TikTok would silence the speech of 94 million US users, none of whom are in China or Chinese citizens. In fact, TikTok itself is banned in China precisely because it does not follow Chinese censorship restrictions.

When one investigates the statements and motives of TikTok's critics, one finds that many think any exports from China, or any trades with that country, should be treated as if they were weapons. The fate of TikTok in the U.S. therefore poses policy questions that go beyond TikTok itself. The controversy is part of a larger debate over strategic competition between the U.S. and China. And that debate is about things much larger than national security. It has profound implications for freedom of expression in the U.S. It affects U.S. regulatory policy towards platforms and platform competition. It affects international trade in the digital economy, and Internet freedom. In these debates, "national security" cannot be a trump card that can be invoked by any government, at any time, to do anything. Any claim that something is a national security threat must be backed by a threat analysis, and an understanding of how security should be traded off against other values.

This paper tries to analyze those risks and trade-offs. It is the first real attempt to do so.

Threat Analysis Framework

The threat analysis is organized around the following questions:

1. What drives the organization?

First, we look at TikTok as an organization: who owns it, who has invested in it, and what drives the organization's behavior? Is TikTok a commercial enterprise or is it reasonable to conclude that it is an agent of the Chinese state, or that it could be made into one?

2. In which military domain(s) is TikTok a threat?

Second, in which domain does TikTok threaten U.S. security: the human domain, the cyberspace domain, or both? A threat in the human domain, also known as *influence operations* or *information operations*, implies that the app is part of an attempt by China to shape what Americans think, or to spread disinformation in ways that degrade our readiness and capacity in military and foreign policy.

A threat in the cyberspace domain, in contrast, refers to the confidentiality, integrity and availability of networks, machines and data. A threat in the cyber domain means that China's military could use the app to weaken U.S. security. There are two ways it could do this: through espionage (collecting valuable intelligence from the app's users), or by becoming the agent of a large-scale cyberattack that was consequential enough to destabilize the country politically or militarily.

Human-domain and machine-domain threats operate in very different ways, and therefore must be carefully differentiated in any threat analysis. A single actor, however, can operate in both domains, and TikTok could be a threat in both domains.

3. The data and access to the data

Third, we look carefully at the data the company gathers from users of the app and the national security risks associated with possession and analysis of that data. We examine the assertion that this data can be used by a foreign power to undermine our nation's security. Here we push beyond the question that has dominated the U.S. policy debate: "can the Chinese government access TikTok data?" to the more fundamental question: do users of TikTok generate data that is valuable to an adversarial nation-state? Does it provide the type of data that one government could use to topple another? If this data is dangerous, are similar dangers posed by all other large-scale social media applications? In this section we also consider the legal requirements to

which TikTok's parent company in China is subject, and its implications for U.S. national security.

4. The risks and costs of a ban

Finally, we ask a question avoided by partisans in the TikTok debate: what costs and risks are posed by banning TikTok? What stakeholders are harmed, which ones gain? What risks would "eliminating" the purported risk of TikTok create? What kind of bad side-effects might such a policy have?

1. TikTok as an organization

TikTok's Chinese origins are used by critics to present it as an agent of the Chinese Communist Party. This is the Trojan Horse theory of US-China interactions: it asserts that every form of interaction, including trade and immigration, is or should be weaponized. The facts about TikTok's history and corporate organization do not support the theory that TikTok is a Trojan Horse.

Commercial Origins and Western Investors

TikTok is a product of ByteDance, Ltd, a multinational firm incorporated in the Cayman Islands. ByteDance is the product of Chinese computer entrepreneurs, Western capital and a globalized internet. This fusion started in 2012, when the parent company ByteDance was founded in a Beijing apartment. At that time, China's government was not interfering with the emergence of innovative digital platforms, and allowed them to rely on investment capital from America and Japan.

ByteDance was incorporated in the Caymans Islands because this was the way Chinese tech entrepreneurs gained access to Western capital while remaining nominally compliant with central government restrictions on foreign investment. If a domestic company qualified for a license, but it was part of a holding company somewhere outside of Chinese jurisdiction, Westerners could pour capital into the holding company, and the holding company, being Chinese-owned, could relay it to the legally "domestic" company that could obtain an operating license in China.

A few months after its incorporation in the Caymans, a Philadelphia-based options-trading firm, Susquehanna International Group Limited (SIG), invested US$5 million for a 15% stake in the company. That investment is now worth an estimated $15

billion - a potent indicator of the benefits to Americans of US-China trade.[9] And the money from Western investors kept flowing. Today, ByteDance investors are global institutional funds and venture capital firms like KKR, Sequoia Capital, and Softbank, as well as other corporate entities like Morgan Stanley, Goldman Sachs Group, Weibo, and others.[10] (See Annex 1 for more details.)

TikTok ultimately was an exported service that managed to participate in global trade while being anchored in a closed national market. It found ways to expand into the North American and world markets where the rules are very different.

What service does ByteDance export? An AI application. AI applications are not generic, but very specific: ByteDance's was focused on content management in a social media app. Its original apps for the Chinese market were *Jinri Toutiao* (Today's Headlines), an AI-driven service recommending news articles, and (in 2016) *Douyin,* a short-form video-sharing platform in China. The key to the success of both apps was said to be its algorithm, its AI application for putting user-behavior feedback into the recommendations of a social medium. It generated a growth cycle attracting users' time and attention and pulling in additional users. Usually this was monetized by means of advertising. If this sounds familiar, it is because that is exactly how the big American platforms work.

Just as American platforms went global, so did ByteDance. It tried to enter the North American market through acquisitions. After failing to acquire Reddit in 2016,[11] ByteDance acquired the Shanghai-based video-lip synching app Musical.ly in November 2017. Musical.ly was popular with US preteens and allowed ByteDance to jump-start its operations in the US and other markets outside China. The TikTok app launched in the US in May 2017 and merged with Musical.ly in August 2018. The union of both platforms allowed TikTok to reach more than a billion users in less than five years. But the AI engine and its engineers were based in China. TikTok's complex organizational structure is an attempt by an entrepreneurial, commercial company to reach global markets while conforming to national and international restrictions on free trade. But it is abundantly clear that it is engaged in business operations for commercial gain, not in cyber-warfare or espionage.

The current organizational structure starts with the primary holding company, ByteDance Ltd, in the Caymans. Its subsidiary TikTok Ltd, also incorporated in the Caymans, is another holding entity for multiple companies offering TikTok service

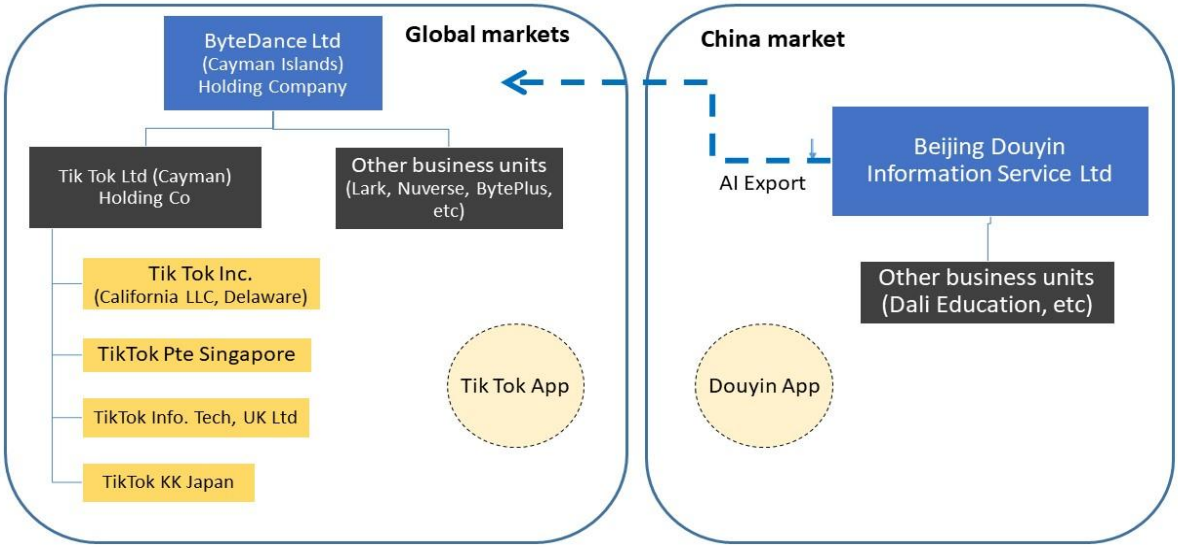
[9] Susquehanna was betting on ByteDance's original application, called *Jinri Toutiao* (Today's Headlines). It was valued at $20 billion in late 2017 and dubbed "the BuzzFeed of China." See K.F, Lee, "AI superpowers: China, Silicon Valley, and the new world order." Houghton Mifflin, 2018. Winkler, R, J. Yang, A. Osipovich, "Secretive High-Speed Trading Firm Hits Jackpot With TikTok." *The Wall Street Journal*, October 1st, 2020.

[10] For a complete list of investors, see Annex 1

[11] J Osawa, S Saitto, J Lessin, "China's Toutiao Tried to Buy Reddit," The Information, Nov. 7, 2017.

outside of China. This includes the U.S. company Tiktok Inc., which is incorporated in California and Delaware and employs thousands of Americans. Similar subsidiaries are incorporated in other parts of the world to facilitate compliance with national laws. (See Figure 1) ByteDance's five-person governing board consists of 3 Western investors, a Hong Kong investor, and ByteDance co-founder and current CEO Rubo Liang.[12]

Figure 1: ByteDance corporate structure



Chinese government involvement

ByteDance was conceived and developed to be a global company. Unlike Huawei, none of ByteDance's services received early investment funds or subsidies from Beijing. On the contrary, China's manufacturing-focused industrial policy starved digital platforms of capital, which is why so many of them engaged in "creative" organizational forms to raise capital from the West.[13] Further, in its early years Chinese censors repeatedly disciplined Douyin because its algorithms recommended content that was popular with users but deemed "immoral," or not supporting "socialist values."[14]

[12] ByteDance's governing board consists of Bill Ford of General Atlantic, Arthur Dantchik of SIG, Coatue Management's Philippe Laffont, Neil Shen from Sequoia China (HK), and ByteDance co-founder Liang Rubo. ByteDance Ltd. also claimed it will add four board seats in 2023. The names of the new board members have yet to be determined. See Z Xin, C Fend, "Exclusive: TikTok's owner ByteDance to add four directors to expand its board to nine amid growing US scrutiny over the app's Beijing link," South China Morning Post, September 28, 2022.

[13] Burke, Q. L., & Eaton, T. V. (2016). Alibaba group initial public offering: A case study of financial reporting issues. Issues in Accounting Education American Accounting Association, 31(4), 449–460.

[14] A. Palmer, "How TikTok Became a Diplomatic Crisis." The New York Times, December 20, 2022.

Eventually, Douyin reached the size and profitability for the Party-state to move in. On April 30, 2021, ByteDance's Chinese subsidiary Douyin sold a 1% "stake" to Wang Tou Zhong Wen Technology, which is owned by three state entities. One of them is linked to The China Internet Investment Fund (CIIF), which is backed by the Cyberspace Administration of China (CAC), the central internet regulator for the People's Republic of China.[15] In a letter to lawmakers in June 2022, the CEO of TikTok Inc (US) confirmed that the transaction with the CAC-linked state-owned enterprise was necessary to obtain licenses for several China-based content applications, such as Douyin and Toutiao.[16] China's domestic licensing regime is governed by these kinds of bargains. Licenses are not awarded to anyone, especially in media and communications.

This bargain has been misrepresented as a "golden share" that gives Chinese censors control over TikTok. In fact, the stake gave CIIF a board seat on *Douyin*, the subsidiary that operates mainland China services. It did not give the CIIF a board seat on ByteDance Ltd or TikTok Ltd, the global entities. TikTok is not under the management control of the Douyin subsidiary, and the Douyin subsidiary has no ownership, visibility or input into TikTok.[17]

This segregation of the Chinese and world markets allows a company like ByteDance to export its competitive service (AI applications) to world markets. A Chinese scholar has called it "One company, Two Systems."[18]

Like Alibaba, ByteDance was caught up in Beijing's April 2021 crackdown on Chinese tech platforms. Its plans for a Hong Kong Initial Public Offering were put on hold due to increased political and security scrutiny from the Party and the Government for dual-listing offshore companies.[19] Only a month later, in May 2021, founder Zhang Yiming announced he would be stepping down as CEO of ByteDance to be replaced by his co-founder Liang Rubo.[20]

As the Chinese government reigned in the "disorderly expansion of capital," we can see that it targeted the biggest and most internationalized Chinese platforms, and viewed

---

[15] The China Internet Investment Fund (CIIF), was established in 2016 by the CAC and run by the finance ministry. T. Arbel, Z. Soo, "China state firms invest in TikTok sibling, Weibo chat app." August 18, 2021 China's communist authorities are tightening their grip on the private sector. The Economist, November 18, 2021.

[16] New York Times, TikTok letter to Republican Senators, June 30, 2022.

[17] Reuters noted that Douyin typically engages the CAC directly, because the government board member, Wu Shugang, "rarely attend[s] meetings. Fretting about data security, China's government expands its use of 'golden shares.' Reuters, December 16, 2021.

[18] Liu, J. and Yang, L., 2022. "Dual-Track" platform governance on content: A comparative study between China and United States. *Policy & Internet*.

[19] ByteDance restructured itself into six business units and dissolved its strategic investment unit. I Deng, "TikTok owner ByteDance renames some subsidiaries, reviving speculation of Hong Kong IPO." South China Morning Post, May 8, 2022.

[20] Yiming retains strong influence on decision-making according to multiple sources. TikTok's CEO Navigates the Limits of His Power - The New York Times

their commercial, globalized nature as threats to its domestic control. It limited their access to foreign capital, resisted international audits and subjected them to "cybersecurity reviews" and charges of privacy violations. Some apps, such as ride-hailing service Didi, were offline for months. This thickening of the walls between the US and Chinese digital economies was a defensive measure, not an offensive one.[21]

Any analysis of the "threat" posed by an actor has to look at the incentives that drive its behavior, and the binding rules under which it operates. Considering TikTok's multi-national ownership and investors, its participation in global, competitive markets and its commercial success, its incentives are clearly economic. TikTok is a market-driven organization, not a political or military one. ByteDance wants to export AI to international markets. It can't succeed in doing that if it is seen as an agent of a foreign power. It is not a Trojan Horse.

The Chinese government, on the other hand, has every reason to favor continued segregation of the information services market in the way ByteDance/TikTok has structured it. China's one party state would have a difficult time handling exposure to unfiltered external media sources. A national perimeter is easier to defend than a global one. China knows that it has no capability to extend its control of information any further than it is already stretched. So its incentives are to stay in control of what it already controls - a huge domestic market with a restricted and subordinated digital economy.

[21] A. Chen, "Renaming of ByteDance subsidiaries revives speculation on TikTok's Hong Kong IPO", PingWest, May 9, 2022.

2. Is TikTok a Chinese Information Operation?

Many attacks on TikTok portray it as Chinese propaganda or "information warfare." Information operations are used in military parlance to describe the production of messages that "influence, disrupt, corrupt, or usurp the decision making of adversaries."[22] It includes propaganda, disinformation and the export of censorship.[23]

Is TikTok a tool of Chinese information warfare? Three assertions in support of this contention have been put forth by Congress and certain individuals and government agencies:

1. TikTok exports Chinese censorship;
2. TikTok's recommendation algorithm is manipulated by the CCP.
3. TikTok is or could become a powerful propaganda outlet for the Chinese state.

All three assertions can be empirically tested. All are false.

Censorship.

This charge is easily disposed of. TikTok is not censored by the Chinese government. A technical examination of TikTok's software and control processes by the University of Toronto's CitizenLab proved that the keyword blocks and censorship mechanisms included in ByteDance's Douyin app, which is used in China, have been eliminated from the two versions of the software released outside of China. The researchers concluded:

> "TikTok does not employ overt political censorship. Because none of the [5,420] politically sensitive search terms returned empty search results, we conclude that it is unlikely TikTok employs political censorship in the search feature."[24]

TikTok and Douyin's content is now segregated so users cannot access videos across platforms.[25] This supports our segregation of services argument from Section 1.

A simpler and more forceful proof of the absence of censorship can be had by simply finding content on TikTok known to be major Communist Party taboos. The following topics would be tightly controlled in any media outlet subject to Chinese government control:

- Falun Gong, an anti-communist religious movement that is persecuted in China

[22] Air Force Doctrine Publication (AFDP) 3-13, Information Operations, Curtis E. LeMay Center for Doctrine Development and Education, April 28, 2016.
[23] In wartime it can involve interference with an enemy's command and control systems, but since China and the US are not at war, this aspect is not relevant to the analysis.
[24] P Lin, "TikTok vs Douyin A Security and Privacy Analysis." CitizenLab, March 22, 2021.
[25] Two sides of the same code - Protocol

- Advocacy of the independence of Taiwan
- Claims that the Uyghurs in Xinjiang Province are being exploited or oppressed
- Ridicule of Chinese Premier Xi Jinping
- Demonstrations calling for the ouster of Xi Jinping or the CCP
- Support for Hong Kong independence and positive portrayals of Hong Kong democracy protesters.

Videos in all of these categories can easily be found on TikTok. Many are popular and widely shared.

At the top of our search for "Taiwan independence," for example, was this video expressing support for Republic of China (ROC) independence. There was also a Taiwanese nationalist video that was both anti-PRC and anti-ROC, a few videos supportive of China's claim to Taiwan, as well as neutral news reports discussing the issue. The mix of views is not unlike what might be found on Twitter, Google or Facebook.

A search for 'Xinjiang' reveals a list of related search terms that by themselves are likely illegal on Chinese social media, including 'xinjiang fire,' 'xinjiang concentration camps,' 'xinjiang internment camps'. The top result was a video showing how a locked door enforcing the Covid lockdown led to deaths by fire. Next in the list were videos of crackdowns on civilian protests against covid lockdowns in Xinjiang in November; a video showing the faces of Muslims in China's detention camps; a video exposing several hundred quickly-constructed square cabins to house Xinjiang detainees. There are also a few pro-China videos on this topic. A young girl explains how China has invested in modernized cotton production in the Province. This was the only overtly political pro-China message on that topic we found, however. We also see an individual male doing a "Xinjiang dance," and a happy "Uyghur girl in China" dancing. Again the diversity of views matches what one could find on any Western social medium.

Searching for Communist Party of China, XiJinping and other things related to the CCP produces a mix that would never be allowed inside China: western news coverage of the October Party Congress by CBS, NPR, and Sky News; several videos of Hu Jintao being escorted out of the CCP meeting (a scene that has been banned on Chinese social media); satirical criticism of the CCP; a video about China "exploding" in protest in November 2022; a discussion of why China bans Winnie the Pooh; a discussion of the Tiananmen massacre in 1989.

Whoever or whatever controls these search results, it is not the Communist Party of China.[26]

[26] Some Chinese expats on TikTok who are critical of the CCP have expressed concern that the CCP will retaliate against their family. This could have and probably has had a chilling effect on some users. However, this threat exists regardless of what social media application is used. Chinese expats who post

A Manipulated Algorithm?

The second prong of the Chinese information warfare argument focuses on TikTok's recommendation algorithm, known as "For You." The For You feed is widely seen as TikTok's secret sauce. As we have seen, the design and engineering of this AI does come from ByteDance in Beijing, although TikTok and Douyin are separate, non-interoperable apps.

Recommendation algorithms are AI applications that regulate the posts to which an individual user is exposed. They are an automated, social media equivalent of a newspaper's editorial policy - they select and prioritize certain posts, and render others less visible, only at a scale and speed that no newspaper could ever match and in a way that draws on immediate, ongoing feedback from the user. In social media platforms, feeds of recommended videos are based on a user's demonstrated likes and prior engagement patterns.

TikTok's parent company, ByteDance, is famous for algorithms that promote engagement. It was one of the early AI innovators in China's digital economy.[27] When exported to the U.S., its short-video format and recommendation algorithm successfully predicted users' interests, and thus encouraged continued engagement and growth.[28] This accounts for TikTok's rapid commercial success, including its ability to enter and succeed in a market dominated by incumbents.

FBI Director Chris Wray purports to see a national security threat, not good old-fashioned free enterprise. China's government, he asserts, could "control the recommendation algorithm, which could be used for influence operations."[29] Note that Wray does not assert that China's government *currently* controls the recommendation algorithm - it doesn't. No TikTok critics have provided any examples of this happening, no TikTok users complain about it. Note also that Wray has no scientific basis for believing that a recommendation algorithm on one app can alter the political environment of an entire country.[30]

---

critical comments on Twitter, Facebook, cable TV or any other public media would face the same problem. Banning, blocking, or changing the ownership of TikTok would have no impact on this threat.

[27] Lee, K.F., 2018. *AI superpowers: China, Silicon Valley, and the new world order*. Houghton Mifflin.

[28] The New York Times obtained an internal document explaining the workings of TikTok's algorithm. B Smith, How TikTok Reads Your Mind, The New York Times, Dec 5, 2021. The company provides an explanation of the factors that go into #ForYou recommendations on this web page.

[29] D. Shepardson, U.S. FBI director says TikTok poses national security concerns. Reuters, November 15, 2022. Wray issued this opinion despite the fact that his agency has no expertise in information operations and no legal authorization to participate in such activity,

[30] There is very little basis for the belief that controlling recommendation algorithms allow an adversary to influence a population strongly enough to generate a true national security threat. Machine learning algorithms are good at predicting what users might like based on their past activities on the platform - but they do not know how to control or change what the users' like, or to shape what their interests are. They can only reinforce or amplify tendencies that already exist. Perhaps FBI Director Wray thinks that the majority of Americans adore the Chinese system, have a latent love for Communist Party and will

Wray only says that China “could” control it. But could it, and if so, how and to what effect? We have already established that TikTok’s services and markets are external to China. Its management had the autonomy and commercial incentives to eliminate Chinese censorship in the app outside China. If TikTok can avoid direct Chinese censorship to make its service more marketable outside China, why would it suddenly succumb to indirect censorship by algorithmic manipulation?

Wray’s scenario is self-defeating. Retooling the algorithm to recommend the messages of the Chinese Communist Party in defiance of user preferences would undermine the very thing that makes TikTok popular. The app would gradually lose its audience, and with it, its effectiveness as a vehicle for influence operations. CCP propaganda is not what the vast majority of TikTok’s user base wants to see.

TikTok’s success - both as a commercial enterprise and as a point of convergence for the exchange of cultural products at scale - is based on identifying what people want, and giving it to them. Even if one considers TikTok (like other social media) to be the digital equivalent of an addictive drug,[31] the chemistry of this drug requires letting users freely choose to engage with the content that interests them. Only then do platforms acquire data that trains effective AI recommendations. Without this feedback, the ‘drug’ doesn’t work. Not many Americans get their endorphins from videos of Xi Jinping, the 17th 5-year plan, or militant images of Chinese nationalism.

TikTok does engage in content moderation, which is often mistakenly equated with censorship.[32] Like all other platforms, it restricts content considered harmful or unwanted by its users, and its recommendation algorithm can be tuned to limit the reach of certain kinds of content. In its early years (2017-2019), TikTok was not as transparent as US platforms about its standards for moderation. Its policies reflected standards more appropriate to the suppressed Chinese environment. Now, however, its categories of restricted posts are very similar to the standards enforced by Facebook, YouTube or Twitter.[33] Like the American social media firms, TikTok also detects and prohibits “coordinated inauthentic behavior,” which it defines as “the use of multiple accounts to exert influence and sway public opinion while misleading individuals, our community, or our systems about the account's identity, location, relationships, popularity, or purpose.” The report for 2022 shows that the company eliminated five “covert influence operation”

---

suddenly be persuaded to join it and overthrow their own government if CCP-approved videos are recommended to them. We don’t.

[31] K McSweeney, This is Your Brain on Instagram: Effects of Social Media on the Brain, NOW, March 17, 2019.

[32] Censorship refers to state action to block or punish content and involves the use of coercive force. The decisions by a private social media platform to block, suppress or promote certain kinds of content do not qualify as censorship but are the equivalent of editorial decisions. Under American law a private publisher or platform’s right to exercise editorial discretion is itself considered part of their right of free expression.

[33] TikTok’s community guidelines and categories of restricted material are listed here. It includes things like self-harm, violent extremism, hateful speech, etc.

networks, including two networks operated from Russia that amplified “a pro-Russia viewpoint targeting discourse about the war in Ukraine.” Like its American counterparts, TikTok now produces regular transparency reports.[34]

TikTok’s content moderation standards have evolved. In 2019 the *Washington Post*, the *Guardian* and the German blog *Netpolitik*.org published stories that TikTok was “censoring” news of protests.[35] All three stories implied that this policy was a product of Chinese state censorship, but the facts reported show that TikTok’s policy was to stifle ALL political criticism, regardless of ideology, in order to maintain a “happier,” less divisive atmosphere on the platform. In fact, TikTok abandoned that policy several months before these news reports were published, because the restrictions were unpopular with users. Its new policy explicitly recognized users “right to express their experience and/or opinions of political situations.”[36] In 2021 the company updated its automated takedown system and allowed users to appeal removals.[37]

An objective appraisal of TikTok’s content moderation does not reveal a Chinese government-controlled influence operation, but a young, profit-motivated private company based in China internationalizing its operations and gradually adjusting its policies to non-Chinese markets, and progressively deviating from standards and practices enforced in China. This learning process occurred in response to commercial and normative pressures from outside China. There is no evidence that the Chinese government interfered with it.

We conclude that TikTok’s algorithm and content moderation policies are not tools of CCP influence operations, and that the company has strong incentives to avoid doing that. Its very success as a business depends on not doing that. And it has these incentives precisely because we allow it to operate in the US market.

State Propaganda Organ

If TikTok is not subject to Chinese censorship and its recommendation algorithm is not controlled by the Chinese state, then is TikTok a vehicle for the distribution of Chinese

---

[34] TikTok, Transparency Report for 2022-23.
According to Kai Fu Lee, author of AI superpowers, ByteDance was ahead of the curve on fake news detection. In 2017 Jinri Toutiao was taking in user-generated reports of fake medical treatments to train an algorithm that could identify fake news. They also trained a separate algorithm to write fake news and then pitted both against each other to reinforce their detection capabilities. So ByteDance has a history of being keenly aware of the nefarious potential of AI and how to use it properly.
[35] A Hern, “Revealed: How TikTok censors videos that do not please Beijing.” The Guardian, Sept 25, 2019.
M Reuter, “Cheerfulness and Censorship,” Netzpolitik.org Nov 23, 2019.
D Harwell, T Romm “TikTok’s Beijing roots fuel censorship suspicion as it builds a huge U.S. audience,” Washington Post, Sept 15, 2019
[36] This did not stop the papers from exploiting the clickbait value of the ‘China censorship’ charge, contributing to the company’s bad reputation.
[37] C M Rodrigo, “TikTok updates automated takedown system,” The Hill, July 9, 2021.

propaganda? A *Forbes Magazine* article tried to make this case, arguing that some ByteDance employees had a background in state media and that “China could use TikTok’s broad cultural influence in the US for its own ends.”[38]

This argument also fails to establish a serious national security threat. News and opinion distributed by Chinese propaganda organs are already available in the U.S. Google’s search engine happily points anyone to the English language website of the People’s Daily, the official newspaper of the Central Committee of the Chinese Communist Party, which also has a Twitter and Facebook account. The Global Times newspaper, which is even more propagandistic than People’s Daily, is available on the web and has 1.8 million followers on Twitter. If this material is a threat on TikTok, why is it not also a threat on Twitter, Google, YouTube, and the open Web? Conversely, if the presence of Chinese propaganda on TikTok is so dangerous as to justify banning it, shouldn't advocates of a ban also push to ban Google searches for CCP materials, ban Twitter, and block all forms of Internet access to state-affiliated media from China?

US values and access to Chinese information

Ironically, calls to ban TikTok as a form of propaganda or IO lead inexorably to an American version of the Great Firewall of China: an Internet in which the government censors foreign information sources. If nationalistic fears about Chinese influence operations lead to a departure from American constitutional principles supporting free and open political discourse, we will have succeeded in undermining our system of government more effectively than any Chinese propaganda could do.

The U.S. has a highly diverse media environment, with thousands of information sources competing for our attention. Although its user base is large, TikTok is not the biggest platform and does not have anything close to a monopoly on culture, entertainment or news outlets in the U.S. Unless the U.S. population welcomes it, an app entirely controlled by the Chinese government could only have a marginal impact on public opinion, no different than the presence of *People’s Daily* on the web. TikTok itself, of course, has strong reasons to resist becoming a tool of the CCP. If it becomes boring or propagandistic, users and advertisers will abandon it.

Americans can cope with freedom online. There is no need for a “national security” intervention here.

[38] E Baker-White, “TikTok’s China Problem,” Forbes, Aug 11, 2022.

3. Is TikTok a Cybersecurity Threat?

Cybersecurity is defined as protecting the confidentiality, integrity and availability of data, networks and information systems. Security in this domain refers not to the ability to influence human psychology, but to the ability to compromise control of the machines, networks and data that comprise cyberspace. Although its critics often fail to differentiate between influence operations and cybersecurity, the strongest concerns about TikTok have been based on the claim that it can provide the Chinese government with data that poses a cybersecurity threat.[39]

The threat scenario rests on two key assumptions: 1) the data generated by the TikTok app provides China's state with unique and valuable insights into systemic U.S. vulnerabilities; 2) China's government can only get access to that data because TikTok's parent company, ByteDance, is Chinese.

In line with this alleged threat scenario, our analysis proceeds in three steps: First, what **data** does TikTok collect? Second, what is the **value** of that data for undermining U.S. national security? Third, if that data does have value, does the TikTok enterprise provide the Chinese state with the only way, or the best way, to **access** that data?

Data collection

Like all social media, TikTok collects a lot of data about its users and uses. There are basically three types of data:

- **Information about the device**: this includes device identifiers such as IMSI and IMEI numbers, the device type, the device brand, the Operating System and API version.
- **Information about the app**: app type, language, version code, version name, build number.
- **Info about the user**: various account IDs, phone number or email address, current region, location if permission was given. This also includes data about user activity on the app, such as:
    - The videos uploaded
    - The number of likes a video obtains
    - How many times a video is shared

[39] The Trump Executive Order seeking to ban TikTok concluded that TikTok's foreign ownership and data collection pose a risk that the Chinese Communist Party can access "Americans' personal and proprietary information—potentially allowing China to track the locations of Federal employees and contractors, build dossiers of personal information for blackmail, and conduct corporate espionage."

- Who commented, the date of the comment, and what they said;
- Followers: how many and who
- Following: how many and who

TikTok includes two types of trackers: first-party trackers that send information to app developers, and third-party trackers that send information to other companies. Usually, these trackers collect device information for advertisement targeting, telemetry, debugging, and anti-abuse purposes. This information serves operational purposes but also allows precise identification of individual users and profiling of them.

Security researchers have criticized some of TikTok's data collection practices, but these critiques pertain to individual privacy of users, not to national security threats.[40] The key fact here is that most other social media and mobile apps do the same things. Baptiste Robert, a French security researcher who studied the app, concluded that "TikTok's behavior is not suspicious and it is not exfiltrating unusual data. Getting data about the user device is quite common in the mobile world and we would obtain similar results with Facebook, Snapchat, Instagram and others."[41] Citizen Lab's software analysis concurred, concluding that the app does not collect contact lists, record or send photos, audio, videos or geolocation coordinates without user permission. "While TikTok collected many data items, overall they still fall within general industry norms for user data collection."

Data Value

The US has been burned in the past 8 years by Chinese cyber-espionage operations that have successfully acquired access to large collections of valuable, sensitive information. The Marriott Hotel data breach of 2014 yielded 500 million guest records that included name, mailing address, phone number, email address, passport number, account information, date of birth, gender, arrival and departure information, reservation dates, and payment card data. Experts attributed the attack to a Chinese state-sponsored intelligence-gathering effort. In June 2015, the federal Office of Personnel Management (OPM) discovered that the background investigation records of current, former, and prospective Federal employees and contractors had been stolen. The lost data included the names and Social Security Numbers (SSNs) of 21.5 million individuals, information from background investigations, some fingerprints, and the usernames and passwords that applicants used to fill out their background investigation forms. This breach, too, has been attributed to Chinese cyber-operatives. Another major data breach in 2017 involved Equifax, which allowed the credit records, names,

[40] For example, the Eberl blog (2019) asserts that TikTok is not compliant with Europe's GDPR. Of course, neither were Facebook or YouTube
[41] B Roberts, "TikTok: Logs, Logs, Logs." Medium, Aug 3, 2020.

addresses, SSNs, and drivers license numbers of 143 million people to be exfiltrated. About 200,000 of the records also included credit card numbers. This breach, too, was eventually attributed to China. So the U.S. has every reason to be concerned about Chinese cyber-espionage.

But it is difficult to see how these concerns can be rationally translated into treating TikTok as a national security threat. The Hotel data could be used to track the movements of American diplomats, corporate executives and spies, especially given the presence of passport numbers. The OPM breach was a national security catastrophe, allowing the adversary to know some of the most intimate details of anyone who applied for a federal security clearance. The Equifax data was almost as sensitive, involving financial information, SSNs, and drivers' licenses. No one has made a case that records of TikTok activity have similar national security implications.

Full access to all TikTok data would provide aggregate data about the user population's video uploading and consumption behavior. This would provide commercially valuable data about what devices and apps are being used, the distribution of different operating systems, the location of users, uploaded videos, likes, comments, etc., which could reveal a lot about the market and the individuals in it, but it has value primarily to TikTok (to drive its recommendation engine), to developers, and to advertisers trying to match users to ads.

It is logically impossible to prove that such data cannot pose any risk, ever, but we are not aware of any plausible scenario in which aggregate data from TikTok provides special insight into the control of critical infrastructure, military secrets, opportunities for corporate espionage, or knowledge of weapons systems. Not unless one thinks that CIA agents are posting videos of their offices and colleagues on TikTok, or that defense contractors are posting videos of employees dancing around prototypes of the latest weapons system.

Insofar as a foreign power's access to this data poses a national security risk, it depends entirely on **who the user is**. There is a plausible risk, in other words, ONLY IF:

- The TikTok user is an individual whose actions or locations can have an impact on US national security, AND
- That user participates in TikTok in a way that allows the person to be identified and tracked, or exposes valuable, confidential information about the US government or its military and intelligence agencies.

We refer to this as a **person of interest**. If a person of interest posts videos of a confidential military installation, or views or posts videos that would facilitate blackmailing that individual, there is a national security issue. Those conditions do not

apply to the overwhelming majority of TikTok users nor do they apply to most of the data. Given the small number of individuals subject to this risk, it can be mitigated well short of a ban. Individuals in sensitive positions should be careful about what they upload, or should not use TikTok at all. Importantly, the same risks apply to ALL social media. As explained below in the section on access, persons of interest should restrict their use of ANY social media, not just TikTok. TikTok, and the fact that its parent company is in China, does not pose a unique threat.

Data Access

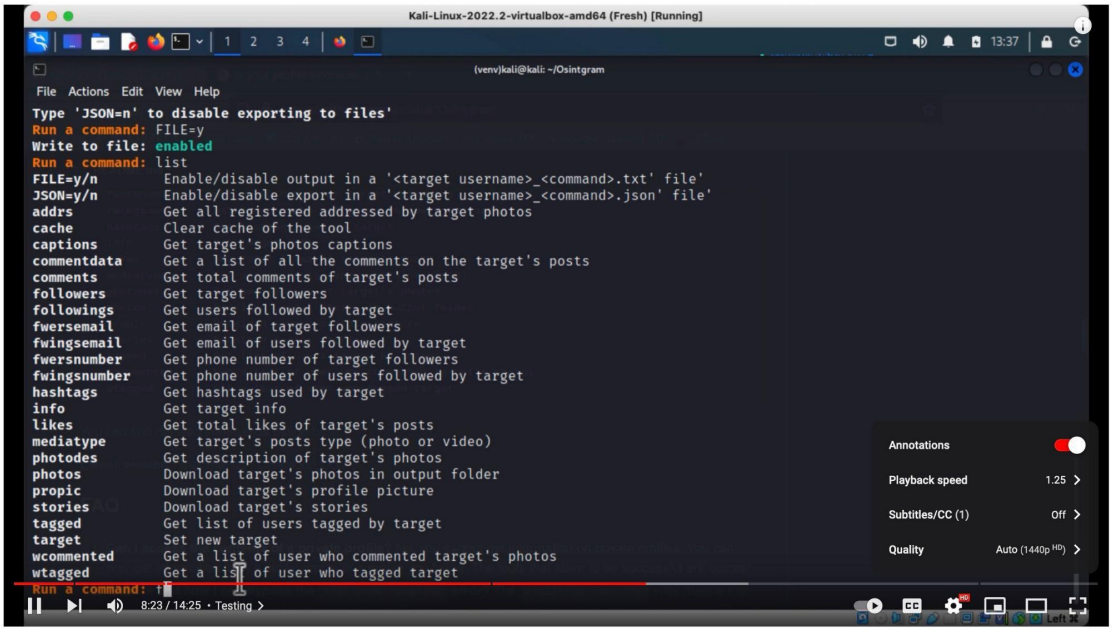
Critical to the hypothetical threat scenario advocated by TikTok's opponents is the question of ***access*** to the aggregate data. TikTok's critics allege that its status as a Chinese-owned subsidiary poses a unique risk because China's government can simply demand that data and get all of it. Some of these allegations are based on highly selective and distorted readings of China's National Intelligence Law (see Annex 2: Laws Governing Access to Data for a more detailed refutation of this claim).

TikTok has segregated its U.S. operations from the Chinese-based app and claims it would not turn over the data. TikTok's incentives as a commercial enterprise are fully in line with this claim, as it would threaten its profitable business. Relying on TikTok's private incentives would not be advisable, however, if the aggregate data it gathers is truly unique, sensitive and valuable. But there is no evidence that it is.

The whole debate about Chinese government access to TikTok data is in many ways a distraction, a red herring. The discussion of access to TikTok data has lost sight of a basic fact: *all social media are fundamentally about sharing and publishing information*. *Any social media user is revealing a lot about themselves to anyone who wants to find it*. This is true whether or not the aggregated raw data is given to a government by the service provider. To put it bluntly, if China wants to spy on a social media user, it doesn't need TikTok to do so.

If the DATA VALUE conditions described above are met (i.e. the user is a **person of interest** and their behavior and posts on TikTok **expose confidential, valuable information related to national security**) Chinese state intelligence could obtain that data simply by monitoring what is posted on TikTok (and LinkedIn, Facebook, Twitter, etc.). It could supplement this monitoring with an increasingly powerful array of Open Source Intelligence (OSINT) tools to correlate user activities and identities across multiple social media. Detailed analytics can be accessed without the cooperation of the app's operator through proxy setups that allow third parties to observe the traffic

between the app and the service provider.[42] An open source tool known as “Sherlock” allows anyone to “Hunt down social media accounts by username across social networks”[43] Some OSINT tools can be used to analyze images and geolocate or identify elements on them.[44] A tool known as OSINTGRAM (Figure 2 below) allows its user to get a list of an Instagram user’s followers, the phone number and email addresses of followers, the users tagged, etc. Tools such as these can be used to monitor any social media application: LinkedIn, Facebook, Twitter, Reddit. Insofar as there is a threat of foreign intel agencies gaining access to social media data, it is not unique to TikTok and banning the app would not solve it.



In short, to monitor persons of interest on TikTok (and other social media), the Chinese government need not have any special legal or political authority over TikTok. In assessing the intelligence value of TikTok, we conclude that whatever intel value a record of TikTok usage has, most of it can be harvested without any cooperation from the company, and that the same risks apply to all social media.

---

[42] BTF_117, “TikTok OSINT: Targeted user investigation“ (3 parts), April 19 - May 5th, 2020. Using JSON (JavaScript Object Notation), the investigator was able to discover account names, region (country code), various URLs of posts, IDs of followers, how many videos the user has posted, the URLs of the videos, the sound track, the raw videos, the creation date and time of the videos, when it was uploaded (last modified), The statistics array contains information on the interactions with the video: comment_count, digg (likes) count, download_count, play_count, share_count, forward_count

[43] GitHub, Sherlock Project. https://github.com/sherlock-project/sherlock

[44] OSINT at Home #4 - Identify a location from a photo or video. YouTube video, See also the Sector035 newsletter, “Week in OSINT.”

4. Costs and Risks of a TikTok Ban

We have established that many of the national security risks of TikTok are non-existent or exaggerated. Now it is time to consider the costs and risks of banning TikTok.

Loss of equity by established users

The most direct harm caused by a TikTok ban occurs to its American users. It is quite astounding how advocates of a ban ignore these costs. Many TikTok account holders have invested tremendous amounts of time and creativity into their video productions. They have built up followings of thousands, sometimes millions of other users, users who also have rights to view and enjoy the content of their choosing. Advertisers and event promoters would also suffer direct economic harm, as their plans or contracts to promote events or products using the app would be disrupted. A ban on an established app is both an interference with users' free expression rights and a costly economic intervention that would affect nearly 100 million Americans.

Internet fragmentation

The national security case against TikTok is a bit like the NotPetya malware; it has the capability to spread indiscriminately against unintended as well as intended targets. We say this because if TikTok is a national security threat, nearly all forms of global digital connectivity could also be construed as national security threats. TikTok is one app in the digital ecosystem. It is a lot like Instagram, Twitter and YouTube in that regard, only the country of origin is different. If that kind of a business is a national security risk, then so are all social media applications, so are all websites (cookies, logs of IP addresses, etc), so are all proprietary operating systems and business software applications. The exchange of traffic signals among Internet service providers, known as BGP routing announcements, provides a gold mine of operational knowledge about how the Internet infrastructure works.

All Internet services generate storable, open source data that can be processed by AI engineers. Consequently, all of these activities provide some “intelligence” about users and systems that “could be” exploited by an adversary.

The most rational response to this is improved cybersecurity and privacy standards and practices at the organizational level. These safeguards should apply to all protocols, all organizations and all service providers, regardless of their national origin. They should be based on technical standards and regulations that are global, not national, in scope. If, instead, the national origin of a software application or network becomes the basis for

claiming a national security threat, then the entire global internet could begin to unravel. Few nation-states trust each other and all have incentives to pursue "digital sovereignty," i.e., policies that exclude service providers and technologies produced in foreign countries. One country's decision to pursue digital sovereignty only reinforces the tendency for other governments to do it.

The U.S. economy would be the main loser if that happens. If foreign apps are considered inherently threatening, this is bad news for Apple, Google, Microsoft, Amazon, Facebook and virtually all American software companies, which are the world leaders in the sector and do substantial business in foreign countries.

Core American values are at stake here. A ban on TikTok represents a major divergence from US principles and values of a free and open Internet and globally competitive markets.

The Threat of Retaliation

A U.S. ban on TikTok encourages retaliation against, or reciprocal treatment of U.S. companies that try to participate in the Chinese market. Apple seems to be the most exposed. This is an American-owned company that sells a large number of smartphones in the Chinese market. Apple's software ecosystem gives it tremendous visibility into the activities and uses of iPhone users. It can control the behavior of the devices, and is engaged in constant updating and modification of the software. If TikTok, which is merely an app and does not control the hardware or the operating system, can be targeted as a national security threat to the U.S., then surely anti-American elements in China could portray Apple iPhones as a serious national security threat to China. Microsoft is also exposed. Whether the Chinese would retaliate in this way is unknown, of course, but it is unrealistic for Americans to think that they can act unilaterally against a Chinese company without China's government returning the favor in some way.

The US Commerce Department has characterized data localization as a "barrier to digital trade" and a threat to Internet freedom.[45] Yet the US assault on TikTok is in many ways based on a policy of data localization. It asserts that any data not stored in facilities owned in the U.S. is a national security threat. In fact, the territorial location of data has little to do with its technical security, as the Chinese exploits and data breaches of the past decade show. But if we insist on localizing data of foreign service providers, then other countries are encouraged to do it to U.S. companies. A study by the CSIS noted that "National security justifications for [data localization] mandates are

[45] Office of the U.S. Trade Representative, "2018 Fact Sheet: Key Barriers to Digital Trade." March 2018. A Declaration for the Future of the Internet, April 2022.
The U.S.-led Declaration, signed by 60 countries, says "Digital technologies reliant on the Internet, will yield the greatest dividends when they operate as an open, free, global, interoperable, reliable, and secure systems."

often thinly veiled attempts at asserting greater control of the domestic digital domain; meanwhile, data localization has had negative impacts on human rights, privacy, and [U.S.] economic interests."[46]

Loss of competition in the social media market

Many politicians and regulators, as well as some consumers, have complained that social media platforms are too concentrated and monopolistic. Why, then, would the U.S. purge a company that has proven its ability to compete with them, offering consumers and advertisers a choice? Entry into markets by foreign companies has been an important source of new competition in the U.S. since the 1870s and 1880s. Foreign capital has funded start-up competitors and new technologies. In some cases foreign firms entered concentrated or oligopolistic US markets, such as automobiles, to enliven competition and innovation. TikTok's success in the American market has had an impact on Snapchat, Facebook and others. The competition from TikTok was so strong that Facebook hired a lobbying firm to orchestrate a nationwide campaign against it.[47] One can only speculate about how much of the national security case against TikTok is really motivated by companies seeking protection from competition.

Conclusion

Our conclusions can be summarized as follows:

- All evidence indicates that TikTok is a commercially-motivated enterprise and not a tool of the Chinese state. Its organizational structure reflects an attempt to segregate the Chinese regime from its global service offerings, with different corporations and software versions for each. Recent Chinese government efforts to assert more control over ByteDance (the Chinese side) are targeting its domestic (Chinese) services, and have not affected its overseas operations.
- TikTok is not exporting censorship, either directly by blocking material, or indirectly via its recommendation algorithm. Over the past 3 years the company has progressively moved its content moderation policies in a direction that converges with Western norms. We have high confidence in this conclusion not only because of empirical observations but also because any attempt to use TikTok for CCP influence operations would destroy its success as a commercial enterprise.

[46] E. Yayboke, "The Real National Security Concerns over Data Localization" CSIS Briefs, July 23, 2021.
[47] T Lorenz and D Harwell, "Facebook paid GOP firm to malign TikTok," Washington Post, March 30, 2022.

- The data collected by the TikTok app is very similar to the data collected by its peer competitors. This data can only be of espionage value if it comes from users who are intimately connected to national security functions and use the app in ways that expose sensitive information. These risks arise from the use of any social media app, not just TikTok. They can easily be mitigated without banning the app.
- Because social media apps publish and share so much data, China's government does not need special legal powers over ByteDance to gain access to most user data. Open source intelligence tools (OSINT) can be used to gather much of this data regardless of whether the service provider cooperates.
- Banning TikTok would impose unfair harms on millions of innocent American users of the app, who have established equity in their creations and followers. It would expropriate investors and eliminate hundreds of US jobs. Competition in the industry would be weakened. It would also risk retaliation against American businesses by China, and provide fuel for hitting US firms with tech-nationalist and data protectionist policies in other countries.

As noted earlier, American policy toward TikTok raises important economic and trade policy questions. At the root of the controversy is the relationship between the world's two largest economies and political powers. The unstated policy question behind the controversy is whether global markets can be integrated and function cooperatively even if their political systems are adversarial.

Our answer is yes, they can be, and should be. It is highly unlikely that China will ever be a liberal democracy or dominated by the U.S., and it is equally unlikely that the U.S. will become communist or dominated by China. Co-existence and trade is the only way forward. TikTok in its current form is an example of beneficial economic co-existence between the U.S. and China. It shows Chinese talent and capital escaping China's CCP by expanding to foreign markets and playing by international rules. It is a case of Americans profiting from investments in the China market, and of Chinese companies offering innovative products and creating thousands of U.S. jobs.

The attack on TikTok is really a kind of proxy war waged by a specific political faction in the US. This faction wants to fully decouple the US and Chinese economies because it sees US-China relations entirely as a zero-sum struggle for world dominance, and rejects peaceful co-existence. This faction can further its agenda by presenting any form of economic interaction with the Chinese economy as a national security threat. The attack on TikTok takes this logic to an absurd extent. Our analysis of the national security risks of TikTok exposes how indiscriminate and weak their case is, and how destructive it can be.

Annex 1: ByteDance earnings and investors

As a privately held company ByteDance keeps most data about its revenues and employment private. Reports from business data aggregators are inconsistent, and therefore all numbers on ByteDance and TikTok financials should be regarded as estimates.[48] Despite operating losses and unrealized market losses on convertible securities, there is no denying the exponential growth of ByteDance Ltd and TikTok over the last five years.[49] The company remains cash-heavy and seeks to diversify its revenue stream. It has acquired game developers, invested in Robotics and healthcare.

The major source of its revenue is targeted advertisements. In Q3 2022, TikTok was the highest revenue-generating non-game app on the iOS App Store, and second on the Google Play Store.[50] TikTok is also able to leverage tools such as live streaming influencers or hashtag challenges where brands create custom videos with their products that are used to drive engagement and lead to sales revenue by advertisers.

ByteDance Ltd. (parent company)

Year	2022	2021	2020	2019	2018	2017
Revenue $BN	?	58	34.3	17.5	8	2.5
Employees	110,000	100,000 -130,000*	60,000	60,000	4,000	1,000

*Source: Privco data * WSJ claimed 130k*

TikTok - a separate subsidiary of ByteDance - achieved revenue that ranges anywhere from $3.88 to 4.6 billion in 2021 and closer to $10 billion in 2022 (*Source: Bloomberg, eMarketer, Business of Apps, Satista)*. TikTok's users ranged from 655 million to 1.2 billion depending on the source.

Funding

ByteDance has raised a total of $15.5B in funding over multiple rounds, most of it from foreign or multinational sources.

[48] Leaked financial disclosures reported by the Wall Street Journal shed some light on ByteDance's financials including losses, cash assets and ….
[49] TikTok Parent ByteDance Sees Losses Swell in Push for Growth - WSJ
[50] Global App Revenue Declined 5% Year-Over-Year to $31.6 Billion in Q3 2022 (sensortower.com)

Date	Funding type	Investor name/type	Valuation and round total in USD
Sep 2021	Venture Capital	Tiger Global Management LLC	$460 billion valuation and $1.1 billion round total
Feb 2021	Venture Capital	China Internet Investment Fund	$360 billion valuation and $5 billion round total
Dec 2020	Private Equity Private Equity Venture Capital Family Office Venture Capital Private Equity Venture Capital	Fidelity China Special Situations Kohlberg Kravis Roberts & Co. L.P. (KKR) Rencent Capital Rhea Fund Sequoia Capital China Carlyle Group Xiang He Capital	$180 billion valuation and $2 billion round total
Jul 2019	Venture Capital Private Equity Venture Capital Private Equity Venture Capital	Aglae Venture Tiger Global Management LLC All Blue Capital Mind Fund EDB Investments Pte Ltd.	?
April 2019	Private Equity Corporate Corporate	Morgan Stanley Goldman Sachs Group, Inc. Bank of China, Wing Lung Bank	$1.3 billion round total (find valuation)
Oct 2018	Venture Capital Private Equity Private Equity	SOFTBANK Capital Kohlberg Kravis Roberts & Co. L.P. (KKR) General Atlantic LLC	$75-$78 billion valuation and $3 billion round total
Aug 2017	Private Equity	General Atlantic LLC	$20 billion valuation and $2 billion round total
April 2017	Venture Capital Venture Capital Venture Capital Venture Capital Venture Capital	Sequoia Capital China CCB International Asset Management Ltd Qiming Venture Partners K3 Ventures Altimeter Capital	$11 billion valuation and $1billion round total
June 2014	Venture Capital Corporate Venture Capital	Sequoia Capital China Weibo Corporation Source Code Capital	$500 million valuation and $100 million round total
Sept 2013	Venture Capital	DST Global	$10 million round total
July 2012	Investment management firm	Susquehanna International Group Limited	$5 million round total

TikTok and US national security

Bytedance Ltd corporate acquisitions and investments (incomplete list)

Date	Target	Price / type
August 2022	Amcare Healthcare	1.5 BN acquisition
April 2022	VisionNav Robotics	$76.0 MM investment
August 2021	Pico Interactive, Inc.	--- acquisition
April 2021	C4 Games	--- acquisition
March 2021	Moonton	4 BN
November 2020	Zhangyue Technology	$170 MM investment
May 2020	Baikemy.com	--- acquisition
April 2020	Verse Innovation Pvt. Ltd.	$35 MM investment
August 2019	Li Auto, Inc	$530 MM investment
July 2019	Minerva Project	
June 2019	Hupu	$188.1 MM investment
July 2016	Verse Innovation Pvt. Ltd.	$25 investment

Annex 2: Laws Governing Access to Data

China's National Intelligence Law

At many points in the TikTok controversy, advocates of a ban have cited China's National Intelligence Law. American government officials, especially during the Trump administration, made a big deal out of Article 7, which reads,

> **Article 7: All organizations and citizens shall support, assist, and cooperate with national intelligence efforts in accordance with law, and shall protect national intelligence work secrets they are aware of.**[51]

This was interpreted to mean that all Chinese companies and individuals are spies for the CCP, and must share any data with Beijing.[52] This interpretation of the law is distorted and taken out of context.

Like many Chinese laws, the NIL is a collection of broad prescriptions. How they are translated into practice is anyone's guess, but the representation of Article 7 as a sweeping transformation of all Chinese companies, even subsidiaries incorporated and operating in foreign countries, into extensions of China's military and intelligence agencies, is distorted and propagandistic. It is based on a selective, out-of-context reading of the law's provisions.

The repeated citations of Article 7 by anti-TikTok partisans ignore Article 8, which immediately follows it:

> **Article 8: National intelligence efforts shall be conducted in accordance with law, shall respect and protect human rights, and shall preserve the lawful rights and interests of individuals and organizations.**

Article 19 also (nominally) affords individuals and companies protection:

> **Article 19: National intelligence work institutions and their staffs shall handle matters strictly in accordance with law, and must not exceed or abuse their authority, must not violate the lawful rights and interests of citizens and organizations, must not use their position to facilitate seeking benefits for themselves or others, and must not leak state secrets, commercial secrets, and personal information.**

---

[51] All our translations rely on the website Chinalawtranslate.com
https://www.chinalawtranslate.com/en/national-intelligence-law-of-the-p-r-c-2017/

[52] P Sucio, "Is TikTok Really A National Security Threat?" Forbes, November 18, 2022.

And Article 27 (nominally) provides citizens with recourse against intelligence abuses:

> **Article 27: Any individual or organization has the right to make a report or accusation about national intelligence work institutions or their staffs exceeding the scope of their authority. abusing their authority, or other conduct in violation of laws or discipline. Relevant organs receiving reports or accusations shall promptly investigate and inform the informant or accuser of the results of the inspection. Individuals and organizations lawfully making reports or accusations about national intelligence work institutions and their staffs must not be suppressed or retaliated against by any individual or organization. …**

Do we think Articles 8, 19 and 27 guarantee that the Chinese government abides by the rule of law and respects human rights? No. China is a one-party state without democratic accountability and an independent judiciary. But it does mean that Article 7 cannot be put forward as a blanket authorization to collect anything and everything. One cannot cite one section of the law to "prove" that TikTok is a national security threat, any more than one can cite Articles 8, 18 and 27 to prove that China is bound by the rule of law and a rights-respecting government.

A careful reading of the law in total, and related laws pertaining to data and national security, such as the 2021 Data Security Law, show that the Chinese state's main concern is protecting data about China and its citizens from foreigners, and maintaining extensive surveillance powers over its own territory.[53] Since the data generated by TikTok is about foreigners, most Chinese laws regarding data security and protection are not clearly applicable to it.

While there are many examples of the PRC military and intelligence agencies gathering data by hacking foreign companies and government agencies, there is nothing in the NIL that authorizes the PRC to demand data about foreigners from a Chinese company's foreign subsidiary operating overseas. We are unaware of any concrete examples of the PRC government doing that. On the contrary, there are several examples of the Chinese state resisting opening up the records of Chinese companies listed on U.S. stock exchanges to scrutiny by foreign auditors.

US National Security Letters and Cloud Act

There is also an element of hypocrisy in the U.S. indignation about Chinese government access to information. The Cloud Act requires U.S. social media or information service companies to provide data in their possession, custody, or control regardless of whether

[53] See T Funk et al, "China Data Privacy Laws, WeChat Muddy Cross-Border Inquiries," Bloomberg Law, Oct. 27, 2022

the data was located in the United States.[54] National Security Letters are more sweeping U.S. investigative tools, used to obtain information from companies as part of national security-related investigations.[55] The USA PATRIOT Act of 2001 “radically expanded the FBI's authority to demand personal customer records from Internet Service Providers” according to the ACLU. They allow the FBI, and in limited circumstances other federal agencies, to demand that companies turn over data about their customers’ use of services such as banking, telephone, and Internet usage records. Although there are procedures for review after they are issued, NSLs can be issued by the FBI without any judicial oversight. The provision also allows the FBI to forbid or "gag" anyone who receives an NSL from telling anyone about the record demand. Here again we have a situation in which the Chinese government could make the same arguments against American online service providers that our government is making against TikTok.

[54] U.S. Justice Department, Frequently Asked Questions: Purpose and Impact of the Cloud Act, April 2019.
[55] Electronic Frontier Foundation, National Security Letters FAQ. Undated.