

Committee on Energy and Commerce
Hearing entitled “TikTok: How Congress Can Safeguard American Data
Privacy and Protect Children from Online Harms”
[March 23, 2023]

Documents for the record

At the conclusion of the meeting, the Chair asked and was given unanimous consent to include the following documents into the record:

1. A Washington Post article entitled, “A former TikTok employee tells Congress the app is lying about Chinese spying,” March 10, 2023, submitted by Rep. Obernolte.
2. A Heritage Foundation article entitled, “TikTok Generation: A CCP Official in Every Pocket,” March 22, 2023, submitted by Rep. Duncan.
3. A BuzzFeed News article entitled, “Leaked Audio From 80 Internal TikTok Meetings Shows That US User Data Has Been Repeatedly Accessed From China,” June 17, 2022, submitted by the Majority.
4. A Forbes article entitled, “A China-Based ByteDance Team Investigated TikTok’s Global Security Chief, Who Oversaw U.S. Data Concerns,” Oct 25, 2022, submitted by the Majority.
5. A Forbes article entitled, “TikTok Couldn’t Ensure Accurate Responses To Government Inquiries, A ByteDance Risk Assessment Said,” Nov 28, 2022, submitted by the Majority.
6. A Forbes article entitled “TikTok Parent ByteDance Planned To Use TikTok To Monitor The Physical Location Of Specific American Citizens,” Oct 20, 2022, submitted by Rep. Dunn.
7. A Forbes article entitled, “EXCLUSIVE: TikTok Spied On Forbes Journalists,” Dec 22, 2022, submitted by the Majority.
8. A Forbes article entitled, “India Banned TikTok In 2020. TikTok Still Has Access To Years Of Indians’ Data,” March 21, 2023, submitted by Rep. Lesko.
9. An article entitled, “TikTok Insider: Zhang Yiming's Journey of Giant Waves,” April 24, 2022, submitted by the Majority.
10. A report entitled, “Assessment of cybersecurity of mobile devices supporting 5G technology sold in Lithuania, ANALYSIS OF PRODUCTS MADE BY Huawei, Xiaomi and OnePlus,” August 23, 2021, submitted by the Majority.

11. An article by the Cornell Tech Policy Institute entitled, “Banning TikTok: What’s At Stake and Would a Ban Address the National Security Risk?” submitted by the Majority.
12. A submission to the Senate Select Committee on Foreign Interference through Social Media entitled, “TikTok, ByteDance, and their ties to the Chinese Communist Party,” March 14, 2023, submitted by Rep. Balderson.
13. A Wall Street Journal article entitled, “How TikTok Serves Up Sex and Drug Videos to Minors,” September 8, 2021, submitted by the Majority.
14. A Wall Street Journal article entitled, “China Says It Opposes Forced Sale of TikTok,” March 23, 2023, submitted by Rep. Burgess.
15. A tweet from Ron Deibert concerning TikTok and Citizen Lab, submitted by Rep. Johnson.
16. An article from the Center for Democracy and Digital Inclusion entitled, “Crunch Time for TikTok and Americans’ Freedom of Speech,” March 22, 2023, submitted by the Minority.
17. A letter from stakeholders concerning federal legislation and proposals that seek to impose a wholesale ban on TikTok in the United States, submitted by the Minority.
18. An article from the Electronic Frontier Foundation entitled, “The Government Hasn’t Justified a TikTok Ban,” March 16, 2023, submitted by the Minority.

EXCLUSIVE

A former TikTok employee tells Congress the app is lying about Chinese spying

His claims of data-security flaws, which the company disputes, underscore how seriously Congress has begun taking the wildly popular short-video app with more than 100 million users nationwide.



By [Drew Harwell](#)

Updated March 10, 2023 at 11:33 a.m. EST | Published March 10, 2023 at 6:30 a.m. EST

A former risk manager at TikTok has met with congressional investigators to share his concerns that the company's plan for protecting United States user data is deeply flawed, pointing to evidence that could inflame lawmakers' suspicion of the app at a moment when many are considering a nationwide ban.

In an exclusive interview with The Washington Post, the former employee, who worked for six months in the company's Trust and Safety division ending in early 2022, said the issues could leave data from TikTok's more than 100 million U.S. users exposed to China-based employees of its parent company ByteDance, even as the company races to implement new safety rules walling off domestic user information.

His allegations threaten to undermine this \$1.5 billion restructuring plan, known as Project Texas, which TikTok has promoted widely in Washington as a way to neutralize the risk of data theft or misuse by the Chinese government.

They could also fuel speculation that the wildly popular short-video app remains vulnerable to having its video-recommendation algorithm and user data distorted for propaganda or espionage. Authorities in the United States have not shared evidence that the Chinese government has accessed TikTok's data or code.

TikTok and ByteDance officials have since 2019 been negotiating with a group of federal officials, known as the Committee on Foreign Investment in the United States, about which privacy standards and technical safeguards they'd need to adopt to satisfy U.S. national-security concerns. The company finalized its proposal in August and presented it to CFIUS, but it has yet to be approved, and CFIUS officials have declined to explain why.

The former employee, who spoke on the condition of anonymity because of fear of retaliation, has told congressional investigators that Project Texas does not go far enough and that a truly leakproof arrangement for Americans' data would require a "complete re-engineering" of how TikTok is run.

As one piece of evidence, he shared with The Post a snippet of code he said showed that TikTok could connect with systems linked to Toutiao, a popular Chinese news app run by ByteDance. That connection, he said, could allow for surreptitious interference in the flow of U.S. data.

TikTok officials said the former employee has misconstrued the plan and that his termination, months before it was finalized, means he "would have no knowledge of the current status of Project Texas and the many significant milestones the initiative has reached over the last year."

His Toutiao allegation was "unfounded," they said, and the code snippet he shared did not indicate any correlation or connectivity between the two apps. The Toutiao code, they said, does not link back to China and is "nothing more than a naming convention and technical relic" harking back to ByteDance's first successful app.

Officials also said they have already adopted one key pledge of Project Texas by moving U.S. user data and other critical code to servers run by the American tech giant Oracle — a move, they said, that would further undermine the claim that Toutiao officials could have any influence on TikTok's U.S. content or operations.

The former employee's ability to secure meetings with key senators' staff reinforces the expansiveness of Washington's interest in a youth-beloved app best known for its viral dances and challenges. TikTok's chief executive Shou Zi Chew probably will be grilled on Project Texas and the possibility of Chinese influence during a congressional hearing later this month.

His visits in Washington are also timed to accelerating concern about TikTok, including two recent legislative pushes that could lead to an unprecedented nationwide app ban. The former employee said he had met with staff in the offices of Sens. Charles E. Grassley (R-Iowa) and Mark R. Warner (D-Va.). Representatives from both offices confirmed the meetings but declined further comment.

Sen. Warner and a bipartisan group of senators on Tuesday proposed a bill that would give the Commerce Department a direct path to banning TikTok and other apps with foreign owners following a "risk-based" assessment. Another bill advanced by the House Foreign Affairs Committee last week would let President Biden ban TikTok outright.

The White House said Wednesday it supported Warner's bill but was also waiting for the CFIUS negotiations to conclude. More than two dozen states have passed measures banning TikTok on government-owned devices, but a 2020 federal court ruling — and a growing group of civil-liberties activists and congressional Democrats — have argued that a nationwide ban would violate Americans' First Amendment protections against any government law limiting freedom of speech.

The former employee worked as head of a unit within TikTok's Safety Operations team, which oversaw technical risk management and compliance issues, including which employees had access to company tools and user data, according to documents he shared with The Post.

He argues that a nationwide ban would be unnecessary to resolve the technical concerns, which he said could be fixed with "doable and feasible" solutions that would go beyond Project Texas's protocols. He said he worked to address the data-privacy issues internally but was fired after raising his concerns.

In a December letter to TikTok's CEO, Chew, which he shared with The Post, the former employee wrote that senior managers were "responsible for the internal fraud pertaining to implementation of Project Texas," which he said involved them "intentionally lying" to U.S. government officials about how its controls had been tested and verified.

"Various TikTok executives were unduly pressuring me to sign off on Project Texas as if it was something accomplished [a] long time ago," he wrote. He demanded a "rapid internal investigation to ensure true risk management and my reinstatement."

ByteDance's head of global legal compliance acknowledged receiving his letter of concerns and said the company would "review them with expediency," according to a copy of the email reviewed by The Post. The company, he said, has not offered any updates since.

The former employee said he has not yet filed an official whistleblower complaint with the SEC, and his claims have not been corroborated by an official investigation.

He said he is also separate from an alleged whistleblower referenced in a Tuesday letter that Sen. Josh Hawley (R-Mo.) sent to the Treasury Department, first reported by Axios. That person said TikTok's data-access controls were "superficial" and that China-based engineers could use tools to access U.S. data with "the click of a button," wrote Hawley, one of TikTok's biggest critics in Congress. Those claims have also not been verified.

TikTok officials said in a statement Wednesday that the "analytic tools" did not grant direct access to data and that protected U.S. information is now stored on Oracle servers where it can be accessed only in "limited, monitored circumstances."

Project Texas would wall off TikTok's U.S. operations into a new subsidiary, TikTok U.S. Data Security, whose leaders would be vetted by the U.S. government and report to CFIUS, according to briefings the company has given to researchers, journalists and members of Congress.

All U.S. user data would be siloed in a system with monitored gateways for authorized use, according to the plan, and TikTok's code and recommendation algorithms would be reviewed by engineers from Oracle, who could alert U.S. regulators to possible concerns.

Some briefed on the plan have commended its rigor, including Samm Sacks, a senior fellow at Yale Law School's Paul Tsai China Center, who said it reflected a serious effort that would give the U.S. government an unprecedented level of supervision and control into how the company works.

"If it's not working, if there's data leakage or content that's problematic, TikTok would be subject to more oversight than any social media company operating in the U.S.," she said.

But skeptics have argued that no technical safeguard can protect from ByteDance's ownership, which they say could pressure TikTok managers to censor inconvenient topics, boost pro-government messages or introduce vulnerabilities through lines of code. TikTok employees told The Post last year that ByteDance teams in Beijing worked on design, engineering and software tools that they relied on for daily operations.

If Project Texas is rejected, some members of Congress have argued that the only solution would be to force ByteDance to sell TikTok to an American buyer — an idea, first floated by the Trump administration, that TikTok's supporters have compared to hostage-taking. Government authorities in Beijing used export laws to block the Trump proposal in 2020 and could do so again.

TikTok can collect a large range of user data, including video viewing histories, email addresses and contacts, though American tech giants such as Facebook and Google gather even more, including precise GPS locations, extensive biographical details and web-browsing histories, according to a Post review last month.

Chinese government authorities can, by law, compel tech companies to hand over user data to support "national intelligence" work. TikTok has argued that Americans' information would not be subject to that law because it is stored in servers in the U.S. and Singapore.

Critics of a ban have argued it would violate Americans' free-speech rights and fail to address the bigger need for a national law restricting how personal data is collected by all apps, not just TikTok. The digital rights group Fight for the Future said in a statement last month that the ban proposal amounted to "xenophobic showboating that does exactly nothing to protect anyone."

The former employee's claims match those from a source who shared hours of internal meeting recordings, first reported by BuzzFeed last year, in which company employees said they were working to close up ways in which U.S. data could be accessed by employees in China, in line with their CFIUS proposal.

Following that report, an internal ByteDance team used TikTok data such as users' IP addresses, which offer a general estimate of their location, in an attempt to identify how company information had been leaked. The attempt failed, according to ByteDance officials, who announced the attempt in December and said the four employees involved in the effort had been fired.

Chew, who met with The Post last month during a cross-Washington charm offensive, said the company was restructuring its internal-audit team and working to explain its safety controls to skeptical lawmakers and regulators. The scandal, he said, threatened to “erode all the work that we have done.”

TikTok Generation: A CCP Official in Every Pocket

Kara Frederick

KEY TAKEAWAYS

TikTok's data exploitation practices, privacy abuses, influence operations, and promotion of social contagions leave Americans vulnerable to the CCP.

Given the current threat environment, a wholesale ban of TikTok's operations in the U.S. is the only viable option to protect the United States and Americans.

A systemic, risk framework applied to foreign-owned platforms will prevent another TikTok from infiltrating America.

Three hundred billion dollars, three billion downloads, and at least 90 minutes of attention per user every day—TikTok and its China-based parent company have captured much of the world in more ways than one.¹ Yet today's most popular social media app poses a distinct threat to American citizens. From logging keystrokes to laundering pro-Chinese Communist Party (CCP) narratives to U.S. audiences, TikTok—via its Beijing-based parent company ByteDance—exposes Americans to a host of abuses by the Chinese government.

TikTok's data-collection and exploitation practices, abuses of privacy, propagation of influence operations, and promotion of social contagions that rend America's social fabric require immediate attention from policymakers. If America is to preserve her

This paper, in its entirety, can be found at <http://report.heritage.org/bg3757>

The Heritage Foundation | 214 Massachusetts Avenue, NE | Washington, DC 20002 | (202) 546-4400 | heritage.org

Nothing written here is to be construed as necessarily reflecting the views of The Heritage Foundation or as an attempt to aid or hinder the passage of any bill before Congress.

self-governing republic, especially in the psyches of the next generation, dealing with TikTok and successor platforms is both a strategic and moral imperative.

TikTok and the CCP

TikTok’s parent company, ByteDance, is subject to the People’s Republic of China’s (PRC) laws and policies that permit the CCP’s access to the data ByteDance collects. One such policy is China’s 2017 National Intelligence Law, which compels private entities and individuals to cooperate with “state intelligence work.”² Specifically, Article 7 of this law declares that “any organization or citizen shall support, assist, and cooperate with state intelligence work according to the law.”³

Beyond this, Chinese officials—former and current—are embedded in TikTok’s parent company and involved in the company’s inner workings.⁴ In April 2021, the Chinese government acquired a 1 percent stake in ByteDance’s main domestic subsidiary and the board seat that came along with it. This action makes at least one of the three board members, Wu Shugang, a card-carrying official of the Chinese government.⁵ Further, a U.S. Department of Justice filing against TikTok assessed in September 2020 that “ByteDance contains an internal corporate CCP committee through which the CCP exercises influence at the company.”⁶ At lower levels, an August 2022 *Forbes* review found more than 300 LinkedIn profiles of current TikTok and ByteDance employees with ties to the Chinese state media apparatus.⁷ Fifteen of these profiles indicate that these professionals are both employed by ByteDance and official Chinese propaganda arms at the same time.⁸

In fact, TikTok’s ties to the CCP via ByteDance are so deep that TikTok’s public relations strategy from leaked documents published by *Gizmodo* in July 2022 in a document titled, “TikTok Master Messaging,” include imperatives to “[d]ownplay the parent company ByteDance, downplay the China association,” as two of the first four exhortations on the list.⁹

TikTok’s Data Privacy and Collection Methods

While a number of private American platforms engage in controversial data-collection and tracking practices, TikTok’s CCP links intensify debates over privacy invasion. Given its influence over the app, the CCP would likely encourage more collection, not less. And while the commercial surveillance practices of many American

companies are exploitative, direct comparisons do not account for the differences in corporate governance between American and Chinese companies as well as the stark contrasts between U.S. and Chinese political systems. America—though under internal pressure—retains a relatively open society, free press, engaged citizenry, and independent judiciary to hold both the U.S. government and private companies accountable for their data-collection practices.¹⁰ China does not have a remotely comparable approach.

As of today, TikTok’s invasive data-collection practices include gathering users’ Global Positioning System (GPS) locations, Internet protocol (IP) addresses, content, contacts, images, microphone access (for “voiceprints”), and other biometric, personally identifiable, or device information.¹¹ Its 2023 Privacy Policy also includes admissions that TikTok collects the mobile carriers, time zone settings, models, networks, device identifiers, screen resolution, operating systems, app and file names and types, along with keystroke patterns or rhythms of its users.¹²

In terms of comparative data-collection practices to other platforms, a February 2023 report by cybersecurity company Internet 2.0 alleges that TikTok’s data-collection behaviors are among the worst in the industry.¹³ For example, TikTok’s Malcore (malware analysis tool) score was 63.1 out of 100, the highest and worst score of the more than 20 digital applications it tested. The average application’s score was 28.8, with no other app ranking as poorly in terms of data privacy and security as TikTok. According to the report, TikTok’s performance was due, in part, to the security vulnerabilities in TikTok’s code and the abundance of data trackers riddling the platform.¹⁴

Particularly troubling is the extent to which TikTok conceals atypical elements of its collection practices. In August 2020, *The Wall Street Journal* revealed that TikTok exploited a loophole in Google’s Android operating system that allowed it to track the media access control (MAC) addresses (the unique device identifiers) of its users for at least 15 months. When TikTok was first installed on a new device over that time period, the company reportedly bundled these identifiers and other device data to send to parent company ByteDance.¹⁵ During the 15-month period, TikTok reportedly took steps to cover its tracks and conceal its exploitation of this loophole via a layer of encryption.¹⁶ TikTok also reportedly accessed user clipboards on Apple’s mobile operating system for a time, reading the clipboard in every instance the app was opened, potentially exposing sensitive information, such as passwords and banking information, to TikTok.¹⁷

Whose Data? Everyone's Data

Hard security concerns, such as vulnerability to intrusion and hacking through lax security measures, backdoors, and even bugdoors (security flaws hidden in a programming vulnerability—wittingly or unwittingly) are present whenever a device connects to the Internet. Yet TikTok appears to have deliberately engineered access to non-public datasets for certain individuals. Leaked audio of 80 internal TikTok meetings obtained by *Buzzfeed* captured an external auditor as he mused: “I feel like with these tools, there’s some backdoor to access user data in almost all of them.”¹⁸ If not backdoors, bugdoors can be introduced later via a software update that can provide access to certain systems. Additionally, TikTok could serve as a potential entry point to access the data of other people using the same Wi-Fi network.¹⁹

This matters because China-based engineers employed by ByteDance reportedly accessed U.S. user data multiple times over the course of at least four months from 2021 to 2022.²⁰ In June 2022, the same *Buzzfeed*-obtained leaked audio from TikTok’s internal company meetings confirmed that China-based engineers accessed U.S. user information that was not public, to include birthdays and phone numbers.²¹ Before that, TikTok’s former chief information security officer tacitly admitted that employees in China had access to U.S. user data in a blog post in 2020.²²

Separate whistleblower leaks point to access of U.S. user data by China-based employees as a pervasive practice among ByteDance employees. In a March 2023 letter to Committee on Foreign Investment in the United States (CFIUS) chair Janet Yellen, Senator Josh Hawley (R–MO) wrote that a former ByteDance employee with direct knowledge of TikTok’s operations admitted that his colleagues could “switch between Chinese and U.S. data with nothing more than the click of a button using a proprietary tool...just like a light switch.”²³ In this case, extensive safeguards to shield U.S. user data likely did not exist and it was not difficult for ByteDance employees to access the data of Americans at will. In 2022, ByteDance conceded that it built an entire initiative centered around using TikTok to monitor the locations of at least two U.S. journalists.²⁴ Known as Project Raven internally, this effort to track the physical locations of Americans was approved by ByteDance employees in China, likely as an attempt to ferret out the employees that leaked to *Buzzfeed* in the summer of 2022.²⁵

Beyond access to data, the CCP’s likely control over TikTok’s algorithm—originally designed using ByteDance’s algorithms and artificial intelligence (AI) models—raises questions about the app’s potential

to be actively manipulated by CCP-linked actors.²⁶ During divestment talks with Oracle in 2020, ByteDance representatives reportedly indicated that they would not surrender TikTok’s source code to the U.S. company and would instead retain it in China.²⁷ After all, the CCP would have much to lose if ByteDance transferred the algorithm to an American company. FBI Director Christopher Wray appeared to explain why in a public speech more than two years later, asserting that the Chinese government both controls ByteDance and has the “ability to control the recommendation algorithm.”²⁸ In a later hearing in front of the Senate Intelligence Committee in 2023, Director Wray testified that the Chinese government could control the software and data of millions of users who have TikTok on their devices, as well as spread propaganda within America.²⁹ Given the CCP’s authoritarian track record, it is naive to believe that it has not taken advantage of these capabilities.

Manipulating the Information Environment

Concerns over data security do not scratch the surface of TikTok’s ability to manipulate the information environment. ByteDance and TikTok have already pushed pro-CCP narratives to the U.S. public, censored content of which the party-state disapproves, and gathered the necessary information to conduct tailored influence campaigns. In two years, the percentage of adults who get their news from TikTok on a regular basis rose from only 3 percent in 2020 to 10 percent of American adults in 2022—roughly tripling this audience.³⁰ Now, nearly a quarter of adults in the United States under the age of 30 claim to regularly get their news from TikTok, according to the same survey.³¹ This creates yet another vector for the CCP through which to expand its influence over the cognitive landscape of the American body politic.

In one example of these soft influence operations against U.S. users, former ByteDance employees alleged in 2022 that TikTok’s parent company deliberately served pro-China content to a U.S. audience through its old news app, TopBuzz, in addition to censoring stories unfavorable to the Chinese government.³² In 2020, TikTok confirmed that the Chinese government asked its employees to set up an account, under the radar, that “[showcases] the best side of China (some sort of propaganda),” according to a TikTok employee.³³ Leaked documents revealed that TikTok censors content that exposes the CCP’s genocide against its Uyghur community in the Xinjiang region and videos about Tiananmen Square, Tibetan independence, and Hong Kong protests.³⁴ Concurrently, TikTok accounts linked to Chinese

state media pushed divisive content to users during the 2022 U.S. midterm elections focusing on cultural flashpoints, such as the abortion debate, and mostly criticizing Republican candidates while favoring Democrats.³⁵

TikTok’s algorithm and unique technical features, such as “heating,” or artificially picking stories to go viral, also facilitate its manipulation of the information environment.³⁶ Since the algorithm trains on data drawn from individual user preferences and engagement versus connections and “friend” networks, it amounts to a more bespoke vector for propaganda delivery. When information is tailored to individuals based on their unique digital profiles, it could supercharge, at scale, custom CCP influence operations against U.S. citizens.³⁷ It is not hard to envision how these techniques could be deployed for the next U.S. presidential election in 2024.

The Long Game: Integrating TikTok Data with Stolen Datasets to Map U.S. Networks and Life Patterns

Americans should be concerned about the integration of TikTok data with China’s growing trove of stolen datasets from hacks conducted at least as far back as 2014. Seemingly disparate datasets, once integrated, can help foreign adversaries to create profiles of American citizens that are ripe for blackmail, espionage, and more.

TikTok data, if fused with other information, could paint comprehensive intelligence pictures of American users. This type of data integration involves bringing together distinct data sources and synthesizing them into something new and more useful than the constituent sources. Such integration can also be as simple as cross-referencing data to make inferences and assessments.

Relatedly, China’s strides in AI development indicate that the Chinese party-state can and will apply emerging technologies to such datasets to expeditiously exploit its collection. Leveraging applications of AI, such as machine learning, and analytics can transform data into insights. These technologies can parse through raw data at machine speed and make it useful, such as by identifying patterns and anomalies or predicting and mapping trends. Big data analytics can help to process and analyze large volumes of data and extract meaning or flag items of interest. With the advent of these technologies, data that was previously discarded or ignored now has value. What TikTok collects is thus even more useful to the PRC.

China is no stranger to employing these techniques. In fact, CCP officials are already using analytics and data integration to enforce internal control in places like the Xinjiang Uyghur Autonomous Region using an “Integrated

Joint Operations Platform.”³⁸ Through this and other systems, Chinese authorities aggregate behavioral and biometric data, such as whether its inhabitants use an abnormal amount of electricity, display religious enthusiasm, or fail to show up to the local CCP activity of the day.³⁹ Authorities collect iris scans, cheek swabs, eyelash and voice samples, and even 360 degree captures of an individual’s gait, all with the intent of integrating these pieces of data to create a multimodal profile of individuals and identify potential threats to the regime.⁴⁰ TikTok—given the depth and scope of data it collects—could be used by the Chinese government to build digital profiles, determine patterns of life, and even map out the social networks of Americans.

The CCP can easily construct digital profiles of Americans using the surveillance footholds it has already gained in the United States and other parts of the West. China reportedly created dossiers on prominent Americans and those hailing from allied countries like Australia, Canada, and Great Britain as recently as 2020 with both stolen and publicly available datasets.⁴¹ This is just the tip of the iceberg. The CCP could add TikTok and other “open-source” data to cross-reference data from the Chinese hack of the Office of Personnel Management detected in 2014, which exposed the Social Security numbers, addresses, and family contacts of thousands of U.S. government employees, among other sensitive information.⁴² This data can be added to that from other hacks linked to the Chinese state, such as the hack of the Marriott hotel system in 2018, the Anthem health care system hack from 2015 and the Equifax financial services hack in 2017 to enable the CCP to track where U.S. citizens stay, who they travel with, and any vulnerabilities in their health, medical, or financial lives.⁴³ Patterns of life from digital platforms like TikTok, with real-time GPS and biometric data-collection capabilities, can fill in many gaps. As former Google CEO Eric Schmidt warns in a 2023 *Foreign Affairs* essay:

[T]he warfare of the future will target individuals in completely new ways: authoritarian states such as China and Russia may be able to collect individual data on Americans’ shopping habits, location, and even DNA profiles, allowing for tailor-made disinformation campaigns and even targeted biological attacks and assassinations.⁴⁴

The Chinese party-state has already unleashed an advanced surveillance state on its own people. All efforts by the CCP to apply its surveillance apparatus to Americans must be actively repudiated.

Recommendations for the United States

Given the current threat environment, The Heritage Foundation recommends a wholesale ban of TikTok's operations in the United States (and, eventually, all U.S. allied countries). After implementing a U.S. ban, the federal government should craft, publicize, and enforce a risk framework for foreign-owned platforms and applications seeking entry into the U.S. market.⁴⁵ A systemic approach is required to prevent another TikTok from infiltrating America in the future.⁴⁶

To achieve this outcome, Congress, along with the executive branch and relevant agencies, should:

Ban TikTok from Operating in the U.S. Market. Congress should eliminate the loophole that prevents the President from enforcing sanctions against TikTok. To do so, U.S. legislators should update the International Emergency Economic Powers Act's (IEEPA's) Berman Amendment. IEEPA generally grants the President broad authority to contend with unusual or extraordinary foreign threats through measures like economic sanctions or embargoes.⁴⁷ A 2020 executive order by President Trump attempted to use IEEPA authorities to ban TikTok as a national security threat.⁴⁸ TikTok sued the Trump Administration that same year and a federal judge sided with TikTok by relying in part on a loophole for "informational materials" in the Berman Amendment, which is a set of amendments to IEEPA originally meant to protect the free flow of legitimate communication, such as films and photographs, to the United States from hostile nations like Cuba.⁴⁹

Congress should update the statute to account for today's information environment and data exploitation practices by foreign-owned digital platforms and their proxies.⁵⁰ Specifically, the informational materials exemption could be qualified with language to indicate that these materials should be reasonably free from malign state actor links and influence. TikTok, by virtue of its parent company ByteDance, would not meet this criterion for exemption.⁵¹

- Congress can make clear, for example, that under such an update to the Berman Amendment, the President can deem these foreign-owned digital platforms (1) a national security threat, and (2) under the influence of a malign state actor. Alternatively, Congress can find that TikTok already qualifies as a national security threat under malign state actor influence.

- Legislators can also engineer a ban through other avenues that eliminate the Berman Amendment loophole or otherwise allow the use of IEEPA authorities to ban TikTok. Such efforts include Senator Marco Rubio's (R-FL) draft bill Averting the National Threat of Internet Surveillance, Oppressive Censorship and Influence, and Algorithmic Learning by the Chinese Communist Party (ANTI-SOCIAL CCP) Act, a bipartisan companion bill in the House sponsored by Representatives Mike Gallagher (R-WI) and Raja Krishnamoorthi (D-IL), and Representative Mike McCaul's (R-TX) Deterring America's Technological Adversaries (DATA) Act.⁵²

Institute a Risk-Based Framework that Triggers Specific Policies for Foreign-Owned Digital Platforms that Want to Operate in the United States. A solution to the next TikTok exists in a country-neutral risk framework applied to foreign-owned platforms.⁵³ When met, these criteria would trigger an if-then ruleset for more focused policy prescriptions. *If* a particular criterion or set of criteria is met, *then* a particular policy action should be enacted.⁵⁴ The Treasury Department, Commerce Department, State Department, and the National Institute of Standards and Technology can contribute to the development of this framework. Essential elements of risk-based criteria that, when met, should trigger specific policy action include:⁵⁵

- **The digital platform's target audience and monthly active users** (such as the size of the digital platform's American userbase and scale of growth). Meeting high-risk criteria under this description would not trigger a specific policy action but would help to inform the next three criteria.
- **The platform's overall security** (such as vulnerability to hard security problems like hacking and intrusion). Meeting high-risk criteria under this description would likely trigger a CFIUS review.
- **The platform's collection and information-control practices** (such as features of its algorithms, content moderation, and censorship policies). Meeting high-risk criteria under this description would likely trigger the use of IEEPA sanctions.
- **The platform's home jurisdiction.** This last element should encompass a foreign government's data practices (that is, asking: Does the

foreign government use AI-driven systems for surveillance that data collection from a U.S. market will help to improve?), the foreign government's human rights record, and the foreign government's governance atmosphere.⁵⁶ Platforms emanating from adversary nations like Iran, North Korea, or Russia would effectively trigger specific policy action.⁵⁷ Meeting specific high-risk criteria in this description would likely trigger a combination of CFIUS review and Leahy Law restrictions.

Pass a National Data-Protection Framework to Address Third-Party Data Collection and Sharing Mechanisms for U.S. Users.

Congress should prohibit digital applications from sending U.S. user data to TikTok/ByteDance and similar foreign-owned digital platforms that represent legitimate national security threats to the United States.

- A TikTok ban is not sufficient to protect U.S. data because myriad apps and trackers can send U.S. data to TikTok even if a user has not downloaded the TikTok app.⁵⁸ In the future, *if* a company like TikTok/ByteDance meets specific high-risk criteria under the risk-based framework proposed in this *Backgrounder*, *then* these apps should be prevented from sending U.S. data to these designated companies.
- Congress can take steps to prevent applications from providing TikTok, and therefore ByteDance, with U.S. data via a data-protection framework with appropriate standards and oversight for how commercial entities collect, store, and share U.S. user data.⁵⁹

Private companies should:

Remove TikTok from Their App Stores While Congress Negotiates a Solution to the TikTok Problem. Pending congressional action on TikTok, U.S. tech companies, including Google and Apple, should remove TikTok from their app stores due to its relationship to the CCP and legitimate threat to national security.⁶⁰

Conclusion

Every day that TikTok is allowed to operate in the United States is another day that China can collect information about U.S. citizens and sharpen its ability to exploit Americans—especially the young. The more that TikTok becomes embedded in the United States, the harder it will be to uproot.

Even so, there will be another TikTok. Without implementing a systemic, risk-based framework to proactively address the next TikTok now, the U.S. will have ceded yet another critical digital battlespace to its adversaries. More so, U.S. policymakers have a duty to safeguard America's social fabric and protect young citizens from the whims of an adversary nation. Failing to deliver means that the next generation of Americans will pay the price for Washington's lassitude.

Kara Frederick is Director of the Technology Policy Center at The Heritage Foundation.

Endnotes

1. "TikTok Owner ByteDance Increases Price of Stock Option Buyback," Reuters, October 12, 2022, <https://www.reuters.com/technology/TikTok-owner-ByteDance-increases-price-share-buyback-staff-sources-2022-10-12/> (accessed March 11, 2023); "TikTok Hits 3 Billion Downloads," CNET, July 14, 2021, <https://www.cnet.com/tech/services-and-software/TikTok-hits-3-billion-downloads/> (accessed March 11, 2023); Sarah Perez, "Kids and Teens Now Spend More Time Watching TikTok than YouTube, New Data Shows," TechCrunch, July 13, 2022, <https://techcrunch.com/2022/07/13/kids-and-teens-watch-more-TikTok-than-youtube-TikTok-91-minutes-in-2021-youtube-56/> (accessed March 11, 2023); "BTN Newsbreak," Australian Broadcast Corporation, March 2, 2023, <https://www.abc.net.au/btn/newsbreak/btn-newsbreak-20230302/102045772> (accessed March 14, 2023); Drew Harwell, "How TikTok Ate the Internet," *The Washington Post*, October 14, 2022, <https://www.washingtonpost.com/technology/interactive/2022/TikTok-popularity/> (accessed March 10, 2023); and "Watch Live: Sen. Warner Holds Press Briefing on TikTok," *The Hill*, March 7, 2023, video, <https://thehill.com/homenews/3888161-watch-live-sen-warner-holds-press-briefing-on-TikTok/> (accessed March 10, 2023).
2. Murray Scot Tanner, "National Intelligence Law: From Defense to Offense," Lawfare, July 20, 2017, <https://www.lawfareblog.com/beijings-new-national-intelligence-law-defense-offense> (accessed March 10, 2023). See also the following excerpt from the author's 2019 white paper for the U.S. Cybersecurity Solarium Commission, with language from the author's 2019 testimony in front of the U.S. Senate Judiciary Subcommittee on Crime and Terrorism: Another similar policy is China's 2017 Cybersecurity Law, which is broadly written and provides a low threshold for access to data by the state. "[T]he CAC [Cyberspace Administration of China] updated the law in May 2019 to include a 'Data Security Management Measures' document, complete with 'personal information protection' and provisions for AI-driven content. Previous versions of the law invoke 'critical information infrastructure' and define 'network operators' in broad terms that extend beyond internet service providers to any entity using information and communication technologies (ICTs). As public policy researchers teased out for American media, these laws '[entail] strict provisions requiring data to be housed inside China, as well as spot inspections and even black-box security audits.' Finally, China's full 'internet security plan,' encompassing a soon-to-be-implemented 2020 Foreign Investment Law, will no longer render foreign-owned companies in China exempt from the Cybersecurity Law. Effectively, any data on communications networks in China will soon be subject to the Chinese Cybersecurity Bureau's scrutiny, without requiring an official request. This ability to access more data from more sources lays the groundwork for its exploitation." Kara Frederick, "How Corporations and Big Tech Leave Our Data Exposed to Criminals, China, and Other Bad Actors," testimony before the Subcommittee on Crime and Terrorism, Judiciary Committee, U.S. Senate, November 5, 2019, <https://www.judiciary.senate.gov/imo/media/doc/Frederick%20Testimony1.pdf> (accessed March 20, 2023).
3. Tanner, "National Intelligence Law: From Defense to Offense."
4. Ryan McMorow, Qianer Liu, and Cheng Leng, "China Mes to Take 'Golden Shares' in Alibaba and Tencent Units," *Financial Times*, January 12, 2023, <https://www.ft.com/content/65e60815-c5a0-4c4a-bcec-4af0f76462de> (accessed March 20, 2023).
5. Coco Feng, "Chinese Government Takes Minority Stake, Board Seat in TikTok Owner ByteDance's Main Domestic Subsidiary," *South China Morning Post*, August 17, 2021, <https://www.scmp.com/tech/big-tech/article/3145362/chinese-government-takes-minority-stake-board-seat-tiktok-owner> (accessed March 14, 2023), and "Exclusive: Fretting About Data Security, China's Government Expands Its Use of 'Golden Shares,'" Reuters, December 16, 2021, <https://www.reuters.com/markets/deals/exclusive-fretting-about-data-security-chinas-government-expands-its-use-golden-2021-12-15/> (accessed March 14, 2023).
6. U.S. Department of Justice, "Defendants' Memorandum in Opposition to Plaintiffs' Motion for a Preliminary Injunction," September 25, 2020, <https://www.documentcloud.org/documents/7218230-DOJ-s-MEMORANDUM-in-OPPOSITION-to-TIKTOK.html> (accessed March 10, 2023).
7. Emily Baker-White, "LinkedIn Profiles Indicate 300 Current TikTok and ByteDance Employees Used to Work for Chinese State Media—and Some Still Do," *Forbes*, August 11, 2022, <https://www.forbes.com/sites/emilybaker-white/2022/08/10/ByteDance-TikTok-china-state-media-propaganda/?sh=68359903322f> (accessed March 10, 2023).
8. Ibid.
9. Chris Stokel-Walker, "Inside TikTok's Attempts to 'Downplay the China Association,'" *Gizmodo*, July 27, 2022, <https://gizmodo.com/TikTok-master-messaging-pr-playbook-china-music-1849334736> (accessed March 10, 2023).
10. Kara Frederick, "The Razor's Edge: Liberalizing the Digital Surveillance Ecosystem," Center for a New American Security, September 3, 2020, <https://www.cnas.org/publications/reports/the-razors-edge-liberalizing-the-digital-surveillance-ecosystem> (accessed March 12, 2023).
11. TikTok, "Privacy Policy," January 1, 2023, <https://www.tiktok.com/legal/page/us/privacy-policy/en> (accessed March 20, 2023).
12. TikTok, "Privacy Policy," and Paul Mozur, Ryan Mac, and Chang Che, "TikTok Browser Can Track Users' Keystrokes, According to New Research," *The New York Times*, August 29, 2022, <https://www.nytimes.com/2022/08/19/technology/TikTok-browser-tracking.html> (accessed March 10, 2023).
13. David Robinson, "TikTok Scores 63.1—Designed to Collect Data with Highest Malcore Score in Industry," Malcore, February 13, 2023, <https://blog.malcore.io/p/TikTok-scores-631-designed-to-collect> (accessed March 10, 2023).
14. Ibid.
15. Kevin Poulsen and Robert McMillan, "TikTok Tracked User Data Using Tactic Banned by Google," *The Wall Street Journal*, August 11, 2020, <https://www.wsj.com/articles/TikTok-tracked-user-data-using-tactic-banned-by-google-11597176738> (accessed March 10, 2023).

16. Ibid.
17. Fergus Ryan, Audrey Fritz, and Daria Impiombato, "TikTok and WeChat: Curtailing and Controlling Global Information Flows," Australian Strategic Policy Institute, 2020, p. 40, https://s3-ap-southeast-2.amazonaws.com/ad-aspi/2020-09/TikTok%20and%20WeChat.pdf?7BNJWaoHImPVE_6KKcBP1JRD5fRnAVTZ= (accessed March 10, 2023).
18. Emily Baker-White, "Leaked Audio from 80 Internal TikTok Meetings Shows That US User Data Has Been Repeatedly Accessed from China," *BuzzFeed News*, June 17, 2022, <https://www.buzzfeednews.com/article/emilybakerwhite/TikTok-tapes-us-user-data-china-ByteDance-access> (accessed March 10, 2023).
19. Kurt Zindulka, "Former MI6 Chief: TikTok Gives CCP a Backdoor into Politicians' Data," *Breitbart*, August 12, 2020, <https://www.breitbart.com/europe/2020/08/11/former-mi6-chief-tiktok-gives-ccp-a-backdoor-into-politicians-data-through-their-kids-smartphone/> (accessed March 10, 2023).
20. Baker-White, "Leaked Audio from 80 Internal TikTok Meetings Shows That US User Data Has Been Repeatedly Accessed from China."
21. Ibid.
22. Roland Cloutier, "Our Approach to Security," TikTok, April 28, 2020, <https://newsroom.TikTok.com/en-us/our-approach-to-security> (accessed March 10, 2023).
23. Josh Hawley, letter to Janet Yellen, March 7, 2023, <https://www.documentcloud.org/documents/23698254-2023-03-07-hawley-letter-to-yellen-TikTok> (accessed March 10, 2023).
24. Emily Baker-White, "Exclusive: TikTok Spied on Forbes Journalists," *Forbes*, December 2, 2022, <https://www.forbes.com/sites/emilybaker-white/2022/12/22/TikTok-tracks-forbes-journalists-ByteDance/?sh=55bb707e7da5> (accessed March 10, 2023).
25. Ibid.
26. Liza Lin and Raffaele Huang, "TikTok's Talks with U.S. Have an Unofficial Player: China," *The Wall Street Journal*, February 14, 2023, <https://www.wsj.com/articles/TikToks-talks-with-u-s-have-an-unofficial-player-china-f5fec4ec> (accessed March 10, 2023).
27. Aaron Tilley, "TikTok Says All Data for U.S. Users Now Routed to Oracle Cloud," *The Wall Street Journal*, June 17, 2022, <https://www.wsj.com/articles/TikTok-says-all-data-for-u-s-users-now-routed-to-oracle-cloud-11655503707> (accessed March 12, 2023); Jonathan Cheng, "Chinese State Television: 'ByteDance Will Not Sell TikTok's U.S. Operations to Microsoft or Oracle, nor Will the Company Give the Source Code to Any U.S. Buyers, Sources Said,'" Twitter, September 14, 2020, <https://twitter.com/jchengwsj/status/1305381978422812673> (accessed March 10, 2023), and Georgia Wells and Aaron Tilley, "Oracle Wins Bid for TikTok in U.S., Beating Microsoft," *The Wall Street Journal*, September 14, 2020, <https://www.wsj.com/articles/microsoft-drops-out-of-bidding-for-TikToks-u-s-operations-11600039821> (accessed March 10, 2023).
28. Christopher Wray, "2022 Josh Rosenthal Memorial Talk," The Ford School at the University of Michigan, December 2, 2022, <https://fordschool.umich.edu/video/2022/christopher-wray-2022-josh-rosenthal-memorial-talk> (accessed March 10, 2023).
29. Ivana Saric, "China Could Use TikTok to Control Users' Devices, FBI Director Says," *Axios*, March 8, 2023, <https://www.axios.com/2023/03/08/china-TikTok-fbi-director-congress> (accessed March 10, 2023).
30. Katerina Eva Matsa, "More Americans Are Getting News on TikTok, Bucking the Trend on Other Social Media Sites," Pew Research Center, October 21, 2022, <https://www.pewresearch.org/fact-tank/2022/10/21/more-americans-are-getting-news-on-TikTok-bucking-the-trend-on-other-social-media-sites/> (accessed March 10, 2023).
31. Ibid.
32. Emily Baker-White, "TikTok Owner ByteDance Used a News App on Millions of Phones to Push Pro-China Messages, Ex-Employees Say," *Buzzfeed News*, July 26, 2022, <https://www.buzzfeednews.com/article/emilybakerwhite/TikTok-ByteDance-topbuzz-pro-china-content> (accessed March 10, 2023).
33. Olivia Solon, "Chinese Government Asked TikTok for Stealth Propaganda Account," *Bloomberg*, July 29, 2022, <https://www.bloomberg.com/news/articles/2022-07-29/chinese-government-asked-tiktok-for-stealth-propaganda-account?leadSource=uverify%20wall> (accessed March 12, 2023), and Drew Harwell and Tony Room, "TikTok's Beijing Roots Fuel Censorship Suspicion as it Builds a Huge U.S. Audience," *The Washington Post*, September 15, 2019, <https://www.washingtonpost.com/technology/2019/09/15/TikToks-beijing-roots-fuel-censorship-suspicion-it-builds-huge-us-audience/> (accessed March 10, 2023).
34. Fergus Ryan, Audrey Fritz, and Daria Impiombato, "TikTok and WeChat: Curtailing and Controlling Global Information Flows," Australian Strategic Policy Institute, 2020, p. 15, https://s3-ap-southeast-2.amazonaws.com/ad-aspi/2020-09/TikTok%20and%20WeChat.pdf?7BNJWaoHImPVE_6KKcBP1JRD5fRnAVTZ= (accessed March 10, 2023), and Alex Hern, "Revealed: How TikTok Censors Videos that Do Not Please Beijing," *The Guardian*, September 25, 2019, <https://www.theguardian.com/technology/2019/sep/25/revealed-how-tiktok-censors-videos-that-do-not-please-beijing> (accessed March 10, 2023).
35. Emily Baker-White and Iain Martin, "On TikTok, Chinese State Media Pushes Divisive Videos about U.S. Politicians," *Forbes*, December 1, 2022, <https://www.forbes.com/sites/emilybaker-white/2022/11/30/TikTok-chinese-state-media-divisive-politics> (accessed March 10, 2023).
36. Emily Baker-White, "TikTok's Secret 'Heating' Button Can Make Anyone Go Viral," *Forbes*, January 20, 2023, <https://www.forbes.com/sites/emilybaker-white/2023/01/20/TikToks-secret-heating-button-can-make-anyone-go-viral> (accessed March 10, 2023).

37. Michael Horowitz et al., “Artificial Intelligence and International Security,” Center for a New American Security, July 10, 2018, <https://www.cnas.org/publications/reports/artificial-intelligence-and-international-security> (accessed March 10, 2023); Jordan Schneider, “What to Do About TikTok and WeChat,” *ChinaTalk*, July 20, 2020, <https://chinatalk.substack.com/p/what-to-do-about-TikTok> (accessed March 12, 2023); and Brit McCandless Farmer, “How TikTok Could Be Used for Disinformation and Espionage,” CBS News, November 15, 2020, <https://www.cbsnews.com/news/TikTok-disinformation-espionage-60-minutes-2020-11-15/> (accessed March 10, 2023).
38. Australian Strategic Policy Institute, “How Mass Surveillance Works in Xinjiang: Reverse Engineering the Police Mass Surveillance App,” April 2019, <https://xjdp.aspi.org.au/explainers/how-mass-surveillance-works-in-xinjiang/> (accessed March 16, 2023), and Human Rights Watch, “China’s Algorithms of Repression,” May 1, 2019, <https://www.hrw.org/report/2019/05/01/chinas-algorithms-repression/reverse-engineering-xinjiang-police-mass> (accessed March 12, 2023).
39. Human Rights Watch, “China’s Algorithms of Repression,” and Yael Grauer, “Revealed: Massive Chinese Police Database,” *The Intercept*, January 29, 2021, <https://theintercept.com/2021/01/29/china-uyghur-muslim-surveillance-police/> (accessed March 16, 2023).
40. Megan Rajagopalan, “They Thought They’d Left the Surveillance State Behind. They Were Wrong,” BuzzFeed, July 9, 2018, <https://www.buzzfeednews.com/article/meghara/china-uyghur-spies-surveillance> (accessed March 12, 2023).
41. Andrew Probyn and Matthew Doran, “China’s ‘Hybrid War’: Beijing’s Mass Surveillance of Australia and the World for Secrets and Scandal,” Australian Broadcasting Corporation, September 13, 2020, <https://www.abc.net.au/news/2020-09-14/chinese-data-leak-linked-to-military-names-australians/12656668> (accessed March 10, 2023).
42. Evan Perez, “FBI Arrests Chinese National Connected to Malware Used in OPM Data Breach,” CNN, <https://www.cnn.com/2017/08/24/politics/fbi-arrests-chinese-national-in-opm-data-breach/index.html> (accessed March 10, 2023).
43. David E. Sanger et al., “Marriott Data Breach Is Traced to Chinese Hackers as U.S. Readies Crackdown on Beijing,” *The New York Times*, December 10, 2018, <https://www.nytimes.com/2018/12/11/us/politics/trump-china-trade.html> (accessed March 10, 2023); Eric Geller, “Chinese Nationals Charged for Anthem Hack, ‘One of the Worst Data Breaches in History,’” *Politico*, May 9, 2019, <https://www.politico.com/story/2019/05/09/chinese-hackers-anthem-data-breach-1421341> (accessed March 10, 2023); and Federal Bureau of Investigation, “Chinese Military Hackers Charged in Equifax Breach,” February 10, 2020, <https://www.fbi.gov/news/stories/chinese-hackers-charged-in-equifax-breach-021020> (accessed March 10, 2023).
44. Eric Schmidt, “Innovation Power: Why Technology Will Define the Future of Geopolitics,” *Foreign Affairs*, February 28, 2023, <https://www.foreignaffairs.com/united-states/eric-schmidt-innovation-power-technology-geopolitics> (accessed March 10, 2023).
45. Kara Frederick, Chris Estep, and Megan Lamberth, “Beyond TikTok: Preparing for Future Digital Threats,” *War on the Rocks*, August 20, 2020, <https://warontherocks.com/2020/08/beyond-TikTok-preparing-for-future-digital-threats/> (accessed March 3, 2023).
46. Kara Frederick, “Democracy by Design,” Center for a New American Security, December 15, 2020, <https://www.cnas.org/publications/reports/democracy-by-design> (accessed March 3, 2023).
47. 50 U.S. Code § 1701-1702, International Emergency Economic Powers Act.
48. The White House, “Executive Order on Addressing the Threat Posed by TikTok,” August 6, 2020, <https://trumpwhitehouse.archives.gov/presidential-actions/executive-order-addressing-threat-posed-TikTok/> (accessed March 10, 2023).
49. John D. McKinnon, “TikTok Ban Faces Obscure Hurdle: The Berman Amendments,” *The Wall Street Journal*, January 29, 2023, <https://www.wsj.com/articles/tiktok-ban-faces-obscure-hurdle-the-berman-amendments-11674964611> (accessed March 14, 2023); *TikTok, Inc., et al., v. Donald J Trump*, Civil Action No. 1:20-cv-02658 [federal court], https://ecf.dcd.uscourts.gov/cgi-bin/show_public_doc?2020cv2658-30 (accessed March 20, 2023); 50 U.S. Code § 1701-1702, International Emergency Economic Powers Act; and Christopher A. Casey et al., “The International Emergency Economic Powers Act: Origins, Evolution, and Use,” Congressional Research Service R45618, July 14, 2020, <https://fas.org/sgp/crs/natsec/R45618.pdf> (accessed March 17, 2023). As researchers at the Center for a New American Security highlighted in a 2021 report, any presidential Administration’s “hands are effectively tied...when it comes to using IEEPA to address the national security concerns associated with social media applications and websites” due to the Berman Amendment’s exemption for “informational materials.”
50. John Costello, Martijn Rasser, and Megan Lamberth, “From Plan to Action: Operationalizing a U.S. National Technology Strategy,” Center for a New American Security, July 29, 2021, <https://www.cnas.org/publications/reports/from-plan-to-action> (accessed March 10, 2023).
51. Other proposals, such as the Data and Algorithm Transparency Agreement (DATA) Act, suggest exempting “sensitive personal data” from Berman Amendment protections.
52. Marco Rubio and Mike Gallagher, “TikTok, Time’s Up. The App Should Be Banned in America,” *The Washington Post*, November 10, 2022, <https://www.washingtonpost.com/opinions/2022/11/10/marco-rubio-ban-TikTok-america-china-mike-gallagher/> (accessed March 10, 2023); The White House “Executive Order on Addressing the Threat Posed by TikTok”; David Feith, “Opportunities and Challenges for Trade Policy in the Digital Economy,” Center for a New American Security, November 30, 2022, <https://www.cnas.org/publications/congressional-testimony/opportunities-and-challenges-for-trade-policy-in-the-digital-economy> (accessed March 10, 2023); and Brendan Bordelon, “GOP Rams Through TikTok Ban Bill Over Dem Objections,” *Politico*, March 1, 2023, <https://www.politico.com/news/2023/03/01/house-republicans-TikTok-ban-00084951> (accessed March 2023).
53. This concept of systemic risk and a risk-based framework with a ruleset to contend with future challenges is derived from the author’s previous publications and communications with Administration officials and journalists starting in 2019, including but not limited to: Frederick, “The Razor’s Edge: Liberalizing the Digital Surveillance Ecosystem”; Frederick, “Democracy by Design”; Frederick, Estep, and Lamberth, “Beyond TikTok: Preparing

for Future Digital Threats”; Kara Frederick, “How Corporations and Big Tech Leave Our Data Exposed to Criminals, China, and Other Bad Actors,” testimony before the Subcommittee on Crime and Terrorism, Judiciary Committee, U.S. Senate, November 5, 2019, <https://www.judiciary.senate.gov/imo/media/doc/Frederick%20Testimony1.pdf> (accessed March 20, 2023); and David Wertime, “America’s Problem Is Much Bigger than TikTok,” *Politico*, September 3, 2020, <https://www.politico.com/newsletters/politico-china-watcher/2020/09/03/beijing-washington-next-TikTok-data-rules-standards-490242> (accessed March 10, 2023).

54. These policy actions can be a combination of tools already in the U.S. government policy toolkit, such as IEEPA sanctions, Leahy Law restrictions, or CFIUS reviews.
55. Derived from the author’s e-mailed responses to David Wertime in the fall of 2020 for *Politico* China Watcher. Wertime, “America’s Problem Is Much Bigger than TikTok.”
56. From the author’s e-mailed responses to David Wertime in the fall of 2020 for *Politico* China Watcher: “A governance atmosphere encompasses the systemic risk a nation brings to the table through its political institutions and legal environment (e.g. China’s national intelligence law, Hong Kong’s national security law, etc). This would control for the lack of recourse against government demands for private data, information, and/or access, like an independent judiciary and free press.” And from Frederick, “The Razor’s Edge”: “For instance, China lacks sufficient rule-of-law protections, specific corporate governance practices, and democratic features that would allow companies to resist arbitrary requests for information from the Chinese government.” Also see Frederick, “Democracy by Design.”
57. This concept is not unlike the U.S. State Department’s annual International Religious Freedom report’s “Countries of Particular Concern” designations that lead to specific policy action.
58. Thomas Germain, “How TikTok Tracks You Across the Web, Even If You Don’t Use the App,” *Consumer Reports*, September 29, 2022, <https://www.consumerreports.org/electronics-computers/privacy/TikTok-tracks-you-across-the-web-even-if-you-dont-use-app-a4383537813/> (accessed March 10, 2023).
59. Kara Frederick, “Combating Big Tech’s Totalitarianism: A Road Map,” Heritage Foundation *Backgrounders* No. 3678, February 7, 2022, <https://www.heritage.org/technology/report/combating-big-techs-totalitarianism-road-map>.
60. Brendan Carr, Commissioner of the Federal Communications Commission, letter to Apple and Google, June 24, 2023, <https://www.fcc.gov/sites/default/files/carr-letter-apple-and-google.pdf> (accessed March 10, 2023).

TECH • CORPORATE ACCOUNTABILITY

Leaked Audio From 80 Internal TikTok Meetings Shows That US User Data Has Been Repeatedly Accessed From China

"I feel like with these tools, there's some backdoor to access user data in almost all of them," said an external auditor hired to help TikTok close off Chinese access to sensitive information, like Americans' birthdays and phone numbers.



Emily Baker-White
BuzzFeed News Reporter

Posted on June 17, 2022 at 12:31 pm

   [View 26 comments](#)



Erik Carter for BuzzFeed News

For years, TikTok has responded to data privacy concerns by promising that information gathered about users in the United States is stored in the United States, rather than China, where ByteDance, the video platform's parent company, is located. But according to leaked audio from more than 80 internal TikTok meetings, China-based employees of ByteDance have repeatedly accessed nonpublic data about US TikTok users — exactly the type of behavior that inspired former president Donald Trump to threaten to ban the app in the United States.

The recordings, which were reviewed by BuzzFeed News, contain 14 statements from nine different TikTok employees indicating that engineers in China had access to US data between September 2021 and January 2022, at the very least. Despite a TikTok executive's sworn testimony in an October 2021 Senate hearing that a “world-renowned, US-based security team” decides who gets access to this data, nine statements by eight different employees describe situations where US employees had to turn to their colleagues in China to determine how US user data was flowing. US staff did not have permission or knowledge of how to access the data on their own, according to the tapes.

ADVERTISEMENT

“Everything is seen in China,” said a member of TikTok’s Trust and Safety department in a September 2021 meeting. In another September meeting, a director referred to one Beijing-based engineer as a “Master Admin” who “has access to everything.” (While many employees introduced themselves by name and title in the recordings, BuzzFeed News is not naming anyone to protect their privacy.)

The recordings range from small-group meetings with company leaders and consultants to policy all-hands presentations and are corroborated by screenshots and other documents, providing a vast amount of evidence to corroborate prior reports of China-based employees accessing US user data. Their contents show that data was accessed far more frequently and recently than previously reported, painting a rich picture of the challenges the world’s most popular social media app has faced in attempting to disentangle its US operations from those of its parent company in Beijing. Ultimately, the tapes suggest that the company may have misled lawmakers, its users, and the public by downplaying that data stored in the US could still be accessed by employees in China.

In response to an exhaustive list of examples and questions about data access, TikTok spokesperson Maureen Shanahan responded with a short statement: "We know we're among the most scrutinized platforms from a security standpoint, and we aim to remove any doubt about the security of US user data. That's why we hire experts in their fields, continually work to validate our security standards, and bring in reputable, independent third parties to test our defenses." ByteDance did not provide additional comment.

"Everything is seen in China."

In 2019, the Committee on Foreign Investment in the United States began investigating the national security implications of TikTok’s collection of American data. And in 2020, then-president Donald Trump threatened to ban the app entirely over concerns that the Chinese government could use ByteDance to amass dossiers of personal information about US TikTok users. TikTok’s “data collection threatens to allow the Chinese Communist Party access to Americans’ personal and proprietary information,” Trump wrote in his executive order. TikTok has said it has never shared user data with the Chinese government and would not do so if asked.

Most of the recorded meetings focus on TikTok’s response to these concerns. The company is currently attempting to redirect its pipes so that certain, “protected” data can no longer flow out of the United States and into China, an effort known internally as Project Texas. In the recordings, the vast majority of situations where China-based staff accessed US user data were in service of Project Texas's aim to halt this data access.

Project Texas is key to a contract that TikTok is currently negotiating with cloud services provider Oracle and CFIUS. Under the CFIUS agreement, TikTok would hold US users’ protected private information, like phone numbers and birthdays, exclusively at a data center managed by Oracle in Texas (hence the project name). This data would only be accessible by specific US-based TikTok employees. What data counts as “protected” is still being negotiated, but the recordings indicate that all public data, including users’ public profiles and everything they post, will not be

included. (Disclosure: In a previous life, I held policy positions at Facebook and Spotify.) Oracle did not respond to a request for comment. CFIUS declined to comment.

Shortly before publication of this story, TikTok published a blog post announcing that it has changed the “default storage location of US user data” and that today, “100% of US user traffic is being routed to Oracle Cloud Infrastructure. We still use our US and Singapore data centers for backup, but as we continue our work we expect to delete US users' private data from our own data centers and fully pivot to Oracle cloud servers located in the US.”

Lawmakers' fear that the Chinese government will be able to get its hands on American data through ByteDance is rooted in the reality that Chinese companies are subject to the whims of the authoritarian Chinese Communist Party, which has been cracking down on its homegrown tech giants over the last year. The risk is that the government could force ByteDance to collect and turn over information as a form of “data espionage.”

There is, however, another concern: that the soft power of the Chinese government could impact how ByteDance executives direct their American counterparts to adjust the levers of TikTok's powerful “For You” algorithm, which recommends videos to its more than 1 billion users. Sen. Ted Cruz, for instance, has called TikTok “a Trojan horse the Chinese Communist Party can use to influence what Americans see, hear, and ultimately think.”

Project Texas's narrow focus on the security of a specific slice of US user data, much of which the Chinese government could simply buy from data brokers if it so chose, does not address fears that China, through ByteDance, could use TikTok to influence Americans' commercial, cultural, or political behavior.

The headquarters of ByteDance, the parent company of video-sharing app TikTok, in Beijing.
Greg Baker / AFP via Getty Images

ADVERTISEMENT

TikTok has said in [blog posts](#) and [public statements](#) that it physically stores all data about its US users in the US, with backups in Singapore. This does mitigate some risks — the company says this data is not subject to Chinese law — but it does not address the fact that China-based employees can access the data, experts say.

“Physical location does not matter if the data can still be accessed from China,” Adam Segal, director of the Digital and Cyberspace Policy Program at the Council on Foreign Relations, told BuzzFeed News in an email. He said the “concern would be that data would still end up in the hands of Chinese intelligence if people in China were still accessing.”

TikTok itself acknowledged its access issue in a [2020 blog post](#). “Our goal is to minimize data access across regions so that, for example, employees in the APAC region, including China, would have very minimal access to user data from the EU and US,” TikTok’s Chief Information Security Officer Roland Cloutier wrote.

Project Texas, once completed, is supposed to close this loophole for a limited amount of data. But many of the audio recordings reveal the challenges employees have faced in finding and closing the channels allowing data to flow from the US to China.

"Physical location does not matter if the data can still be accessed from China."

Fourteen of the leaked recordings include conversations with or about a team of consultants from Booz Allen Hamilton. One of the consultants told TikTok employees that they were brought on in February 2021 to help manage the Project Texas data migration, and a TikTok director told other TikTok employees that the consultants reported to TikTok's chief of US data defense. In recordings, the consultants investigate how data flows through TikTok and ByteDance’s internal tools, including those used for data visualization, content moderation, and monetization.

In September 2021, one consultant said to colleagues, “I feel like with these tools, there’s some backdoor to access user data in almost all of them, which is exhausting.”

When asked for comment, Booz Allen Hamilton spokesperson Jessica Klenk said something about the above information was incorrect, but refused to specify what it was. “[A]t this point I’m not in a position to further discuss or even confirm/deny our relationship with any client. But I can tell you that what you’re asserting here is inaccurate.”

Additionally, four of the recordings contain conversations in which employees responsible for certain internal tools could not figure out what parts of those tools did. In a November 2021 meeting, a data scientist explained that for many tools, “nobody has really documented, uh, like, a how-to. And there are items within the tools that nobody knows what they’re for.”

The complexity of the company’s internal systems and how they enable data to flow between the US and China underscores the challenges facing the United States Technical Services team, a new dedicated engineering team TikTok has begun hiring as part of Project Texas.

"Chinese nationals are not actually allowed to join."

To demonstrate the USTS team’s independence from Chinese-owned ByteDance, one team member told a colleague in January that “not everyone can join” the team. “Chinese nationals are not actually allowed to join,” he said. (A former employee who spoke to BuzzFeed News on condition of anonymity for fear of retribution corroborated this account.) When asked for comment on this practice, TikTok did not respond.

But while the mandate of this team is to control and manage access to sensitive US data, the USTS team reports to ByteDance leadership in China, as BuzzFeed News reported in March. In a recorded January 2022 meeting, a data scientist told a colleague: “I get my instructions from the main office in Beijing.”

ADVERTISEMENT

TikTok's goal for Project Texas is that any data stored on the Oracle server will be secure and not accessible from China or elsewhere globally. However, according to seven recordings between September 2021 and January 2022, the lawyer leading TikTok's negotiations with CFIUS and others clarify that this only includes data that is not publicly available on the app, like content that is in draft form, set to private, or information like users' phone numbers and birthdays that is collected but not visible on their profiles. A Booz Allen Hamilton consultant told colleagues in September 2021 that what exactly will count as "protected data" that will be stored in the Oracle server was "still being ironed out from a legal perspective."

In a recorded January 2022 meeting, the company's head of product and user operations announced with a laugh that unique IDs (UIDs) will not be considered protected information under the CFIUS agreement: "The conversation continues to evolve," they said. "We recently found out that UIDs are things we can have access to, which changes the game a bit."

What the product and user operations head meant by "UID" in this circumstance is not clear — it could refer to an identifier for a specific TikTok account, or for a device. Device UIDs are typically used by ad tech companies like Google and Facebook to link your behavior across apps, making them nearly as important an identifier as your name.

As TikTok continues to negotiate over what data will be considered protected, the recordings make clear that a lot of US user data — including public videos, bios, and comments — will not be exclusively stored in the Oracle server. Instead, this data will be stored in the company's Virginia data center, which may remain accessible from ByteDance's Beijing offices even once Project Texas is complete. That means ByteDance's China-based employees could continue to have access to insights about what American TikTok users are interested in, from cat videos to political beliefs.

It also appears that Oracle is giving TikTok considerable flexibility in how its data center will be run. In a recorded conversation from late January, TikTok's head of global cyber and data defense made clear that while Oracle would be providing the physical data storage space for Project Texas, TikTok would control the software layer: "It's almost incorrect to call it Oracle Cloud, because they're just giving us bare metal, and then we're building our VMs [virtual machines] on top of it." Oracle did not respond to a request for comment.

ADVERTISEMENT

Meanwhile, TikTok’s national security lawyer hopes the negotiation will have ripple effects in the tech industry and beyond. “There is going to be national security law that comes down from the Commerce Department,” they said, referencing the Biden administration’s development of regulations to govern apps that could be exploited “by foreign adversaries to steal or otherwise obtain data.”

"The question is whether the company will go far enough."

“The law will be promulgated and codified in probably the next 18 months, I would say — and that’s how every Chinese company is going to be able to operate in the US,” the lawyer said.

TikTok’s efforts with Project Texas may ultimately pay off for the company. According to Graham Webster, a research scholar at Stanford’s Cyber Policy Center, if TikTok commits to being “transparent and high-integrity, and China-based employees won’t be able to access user data,” then “from a data security perspective, it should be possible to convince good-faith skeptics they have done enough.

“The question is whether the company will go far enough and whether skeptical authorities are truly open to being convinced,” he told BuzzFeed News.

The details of the arrangement between CFIUS, TikTok, and Oracle were still under discussion as of January 2022, when the recordings end. But even though Project Texas’s goal is to cordon off access to the most sensitive details about Americans that exist on TikTok’s servers, one policy employee had doubts that will actually prevent ByteDance’s employees in China from accessing this data.

“It remains to be seen if at some point product and engineering can still figure out how to get access, because in the end of the day, it’s their tools,” they said in a September 2021 meeting. “They built them all in China.” ●

Topics in this article

Corporate Accountability

Big Tech

TikTok



Emily Baker-White
BuzzFeed News Reporter

Contact [Emily Baker-White](#) at emily.bakerwhite@buzzfeed.com.

Got a confidential tip? 📧 [Submit it here](#)

incoming

Your weekday morning guide to breaking news, cultural analysis, and everything in between



INNOVATION DAILY COVER

A China-Based ByteDance Team Investigated TikTok's Global Security Chief, Who Oversaw U.S. Data Concerns

ILLUSTRATION BY STEPHANIE JONES FOR FORBES

Emily Baker-White Forbes Staff

Follow

Oct 25, 2022, 12:32pm EDT

Roland Cloutier, a U.S. Air Force veteran and former law enforcement officer, stepped down as TikTok's Global Chief Security Officer in July 2022 as the Biden administration continued to evaluate the national security risks posed by TikTok's Chinese ownership.

China-based ByteDance team led multiple audits and investigations into TikTok's U.S.-based former Global

Chief Security Officer who had been

TIKTOK'S CHINA PROBLEM



China-based employees' access to American user data, according to internal company materials reviewed by *Forbes*.

TikTok hired Roland Cloutier as its Global Chief Security Officer in March 2020, shortly after the Treasury Department's Committee on Foreign Investment in the U.S. (CFIUS) opened an investigation into TikTok's ties to China. In [public statements](#), TikTok touted the work of Cloutier, a U.S. Air Force veteran and former veterans affairs police detective, as evidence that TikTok was taking cybersecurity and data concerns seriously.

But according to current and former employees, as well as internal materials reviewed by *Forbes*, Cloutier's efforts to build out a robust security team were hamstrung by ByteDance's Internal Audit and Risk Control department, which is led by Song Ye, an executive in Beijing.

The materials show that Internal Audit launched multiple audits and investigations into Cloutier, alleging that he had pushed contracts worth millions of dollars to U.S.-based security vendors who were his personal friends. *Forbes* did not view materials that conclusively substantiated or refuted the veracity of these allegations.

Some current and former employees, though, characterized the probes into Cloutier as pretextual fishing expeditions designed to find a reason to push him out of the company. They noted that TikTok's Chief Internal Auditor, Chris Lepitak, had argued that some

work managed by Cloutier's TikTok team should instead be owned by ByteDance's Internal Audit team. The sources said Lepitak indicated that Internal Audit should oversee areas like digital forensics and insider risk, which are key to ensuring the security of user data. Lepitak reports to Song Ye, who reports to ByteDance cofounder and CEO Liang Rubo. *(Disclosure: In a past life, I held policy positions at Facebook and Spotify.)*

TikTok and ByteDance did not answer questions about why Cloutier was investigated, whether he was fired or whether he was pushed out of the company because of his work on data access controls. ByteDance spokesperson Jennifer Banks said that “[a]ny internal investigation is done with the intent to maintain a safe and compliant workplace,” but declined to comment on specific investigations.

One investigation into Cloutier focused specifically on the Global Security Organization's relationship with consulting giant Booz Allen Hamilton. Several former employees at Booz currently work on TikTok's security team. Among other things, Booz was [helping](#) TikTok manage China-based employees' access to U.S. user data. Previously, Booz declined comment on its relationship with TikTok, and did not immediately respond to a comment request.

TikTok is currently negotiating a national security contract with CFIUS which will govern the way the Chinese-owned social media app handles Americans' personal user data. Before he left his post at the company in July 2022, Cloutier had been working on reducing

China-based employees' access to data: In an April 2020 [blog post](#), he wrote, "Our goal is to minimize data access across regions so that, for example, employees in the APAC region, including China, would have very minimal access to user data from the E.U. and U.S."

BuzzFeed News reported in June that U.S. [user data had been repeatedly accessed](#) by employees in China into at least January 2022. *Forbes* reported last week that ByteDance's Internal Audit department — the same one that investigated Cloutier — planned to monitor [individual U.S. citizens' locations](#) using the TikTok app.

“Our goal is to minimize data access across regions so that, for example, employees in the APAC region, including China, would have very minimal access to user data from the E.U. and U.S.”

Cloutier did not respond to multiple requests for comment. TikTok [announced](#) that he was stepping down from his role as Chief Security Officer in July, and his LinkedIn profile says he left the company in September.

ByteDance spokesperson Banks said in a statement that the Internal Audit team is “responsible for objectively auditing and evaluating the company and our employees’ adherence to our codes of conduct.”

TikTok did not comment on a detailed list of points and questions from *Forbes* about the Cloutier investigations and other investigations conducted by ByteDance’s Internal Audit team. However, in response to *Forbes*’s [earlier report](#) about the team, TikTok’s communications department tweeted: “Our Internal Audit team follows set policies and processes to acquire information they need to conduct internal investigations of violations of the company codes of conduct[.]”

Despite TikTok’s claim that Internal Audit is “our” team, internal materials indicate that the Internal Audit team does not report to any members of TikTok’s executive team, and instead reports directly to ByteDance executives in China. TikTok did not answer a question about why it referred to the Internal Audit team in this way.

Materials also show that the probes conducted by Internal Audit have often been extensive, including contracts with outside security firms and reviews of many thousands of emails, employee correspondences and messages in Lark, ByteDance’s internal workplace management software. Materials also show that some investigations have been kept confidential from employees’ managers and from HR.

Cloutier is also not the only U.S. executive who was targeted by the Internal Audit department. Two sources

also said that at least one other executive, former TikTok Global Head of Marketing Nick Tran, was also pushed out over allegations of conflicts of interests due to personal relationships, which the sources characterized as an excuse to terminate the employee. Tran declined to comment.

Numerous senior employees felt “that themselves and their teams are just ‘figureheads’ or ‘powerless ombudsmen’” who are “functionally subject to the control of CN-based teams.”

Three current and former employees also described a list of TikTok employees — some of whom have now left the company — that ByteDance hoped to oust from their positions. Neither TikTok nor ByteDance commented on the existence of such a list. The Financial Times [previously reported](#) that TikTok had created a “kill list” for employees it wished to force out of the company. At the time, TikTok told FT that it was “unable to find any list that matched this description.”

TikTok has not yet named its next Chief Global Security Officer, but documents show that the company's Global Security Organization is currently in the middle of a corporate restructuring, meant to address "pain points" including redundancy across teams. TikTok and ByteDance declined to answer questions about whether the restructuring would change the division of responsibilities between TikTok's Global Security Organization and ByteDance's Internal Audit team.

In the past, TikTok has struggled with retention of U.S.-based executives. In September, *Forbes* reported that at least five senior leaders at TikTok had left the company because they felt they could not contribute to key decision making. ByteDance's Internal Audit department apparently found the same thing: A risk assessment prepared by the department in late 2021 found that numerous senior employees felt "that themselves and their teams are just 'figureheads' or 'powerless ombudsmen'" who are "functionally subject to the control of CN-based teams."

Neither TikTok nor ByteDance commented on the risk assessment.

Last month, President Biden issued an executive order instructing CFIUS to more closely consider the risks posed by foreign companies' access to Americans' private data. Yesterday, the Department of Justice held a [press conference](#) to announce indictments into two Chinese government intelligence officials who allegedly sought to impede a federal investigation into alleged wrongdoing

by the China-based telecom giant Huawei. (Huawei did not immediately respond to a request for comment.)

At the press conference, Deputy Attorney General Lisa Monaco, who is reportedly [among the officials reviewing the deal](#) between TikTok and CFIUS, said about the Huawei case: “This case exposes the interconnection between PRC intelligence officers and Chinese companies. And it demonstrates once again why such companies, especially in the telecommunications industry, shouldn't be trusted to securely handle our sensitive personal data and communications.”

Richard Nieva contributed reporting.

MORE ON TIKTOK AND BYTEDANCE

MORE FROM FORBES

TikTok Parent ByteDance Planned To Use TikTok To Monitor The Physical Location Of Specific American Citizens

By **Emily Baker-White**

MORE FROM FORBES

LinkedIn Profiles Indicate 300 Current TikTok And ByteDance Employees Used To Work For Chinese State Media-And Some Still Do

By **Emily Baker-White**

MORE FROM FORBES

TikTok Is Bleeding U.S. Execs Because China Is Still Calling The Shots, Ex-Employees Say

By **Emily Baker-White**

MORE FROM FORBES

Senate Intelligence Committee Calls On FTC To Investigate TikTok For 'Deception'

By **Emily Baker-White**

MORE FROM FORBES

TikTok, Hospitals And Tutoring Apps: The Many Tentacles Of Chinese Tech Giant ByteDance

By **Alexandra S. Levine**

Follow me on [Twitter](#). Send me a secure [tip](#).



Emily Baker-White

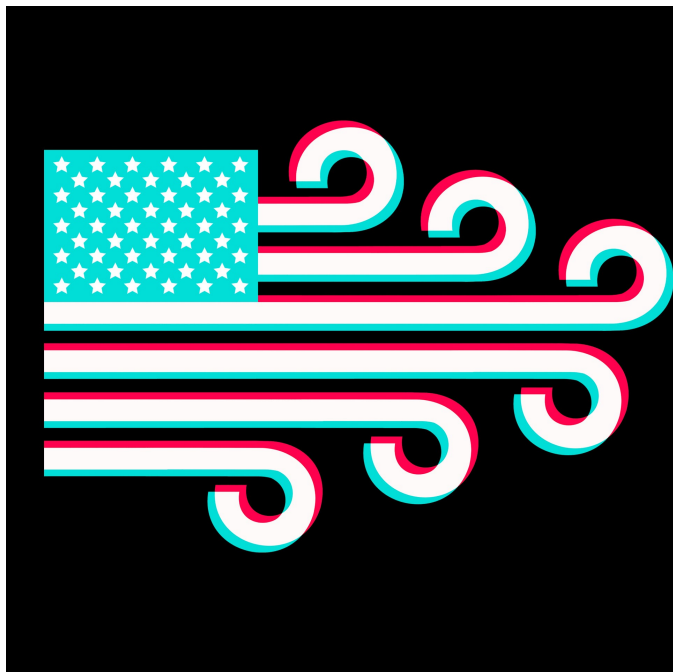
Follow

I'm a technology reporter and senior writer at Forbes based in San Francisco. Have a tip? Email me at ebakerwhite@forbes.com or emilybakerwhite@protonmail.com.

[Editorial Standards](#)

[Reprints & Permissions](#)

TIKTOK'S CHINA PROBLEM



INNOVATION EDITORS' PICK

TikTok Couldn't Ensure Accurate Responses To Government Inquiries, A ByteDance Risk Assessment Said

ILLUSTRATION BY FERNANDO CAPETO FOR FORBES

Emily Baker-White Forbes Staff

Follow

Nov 28, 2022, 07:00am EST

The internal risk assessment, completed in late 2021, also warned of rampant self-dealing, embezzlement, and potential indictment of executives.

In fall 2021, members of ByteDance's internal audit and risk control team prepared an urgent message for executives: Change your approach to fraud prevention — soon — or you could end up in jail.

The message came in the form of a standard Fraud Risk Assessment, reviewed by *Forbes*, which was based on a

review of TikTok and ByteDance policies, and on approximately 90 interviews — some educational and others investigatory — with TikTok and ByteDance employees from at least 17 different teams.

In its executive summary, the document laid out the stakes: “Unless ByteDance makes substantial, sustained, and rapid investments in its anti-fraud programs, it will likely be too late to prevent immense future fraud-related losses and liabilities — potentially including multi-billion dollar fines (\$USD), being forced to submit to the control of an external monitor, loss of the ability to operate in the U.S. and other major markets, and criminal indictments of ByteDance executives and managers (even if they did not actively participate in misconduct).”

Much of the risk assessment was devoted to discussion of basic risks present at any large company — things like embezzlement and conflicts of interest in vendor selection. But it also warned of additional risks caused by ByteDance’s Chinese ownership. At one point, it said that according to an employee with knowledge of the company’s data retention practices, it was “impossible” to avoid “sensitive and/or regulated data” from being “improperly” kept in servers in China. At others, it pointed to incomplete company policies, irregular document retention practices, and a “lack of formal clarity” about which executives and teams were in charge of various workstreams.

Because of that lack of formal clarity, the assessment said, “it is frequently difficult or impossible to verify the

correctness of information the Company reports to government agencies.”

At the time the risk assessment was written, TikTok was engaged (as it is today) in negotiations with the U.S. government about potential national security risks posed by the app’s ownership by Beijing-based ByteDance. Those risks intensified in June, after a [report](#) from BuzzFeed News showed that China-based ByteDance employees had repeatedly accessed U.S. TikTok users’ personal information, and again in October, after a [Forbes report](#) showed that a Beijing-based ByteDance team had planned to use the TikTok app to monitor the location of specific U.S. citizens.

The assessment did not recognize TikTok as a separate business entity from ByteDance, but drew from numerous TikTok-specific sources of information, including documents referencing TikTok operations, TikTok content moderation, the TikTok verification process and TikTok revenue products. *(Disclosure: In a former life, I held policy positions at Facebook and Spotify.)*

“[I]t is frequently difficult or impossible to verify the correctness of information the Company reports to government agencies.”

TikTok did not reply to a request for comment.

ByteDance spokesperson Jennifer Banks provided the following statement about the assessment: “ByteDance regularly conducts risk assessments to identify potential risks and improve compliance, but this report is not one of them. This document was created within one department nearly two years ago, never presented internally beyond that, and is largely inaccurate, with outdated details which are made irrelevant by regular updates to our practices in the years since.” Banks did not answer a follow-up question about which, if any, of the specific points included in this reporting were inaccurate, and did not offer details on how the company has updated its practices since the assessment was done.

The assessment was primarily authored by an attorney with experience in state and federal government who no longer works for ByteDance. The author responded “no comment” to an interview request.

The assessment also identified risks related to TikTok and ByteDance’s primary form of internal communication — a ByteDance messaging app called Lark — noting that Lark messages are stored in China. TikTok and ByteDance did not answer questions about whether the Lark messages of U.S.-based employees, including those in which employees discussed topics like the labeling of Chinese state media entities or the tracking of foreign influence operations, are viewable by ByteDance employees in China.

But the assessment's discussion of Lark did not stop at where messages were stored. It also said, "[t]he Company is currently incapable of extracting accurate, usable records of critically important internal communications, specifically, numerous information about and within internal Lark messages."

It then put that limitation into sharp relief, saying that as a result, "we lack the ability to assure even basic custodian-by-custodian preservation of communications that represent critically important investigative evidence and/or that the Company is responsible for maintaining and turning-over to outside parties in connection with government investigation and litigation subpoenas." In other words, ByteDance might not be able to turn over certain internal communications to the government, even in circumstances where it is legally required to do so.

“The Company is currently incapable of extracting accurate, usable records of critically important internal communications[.]”

Austin Hacker, press secretary for Republican Congressman James Comer, confirmed to *Forbes* that Comer's office has requested internal communications

from TikTok, including Lark messages. “At this time, TikTok has failed to provide the requested information, documents, and communications,” he said in an email. TikTok spokesperson Maureen Shanahan confirmed that TikTok received Rep. Comer’s request and said the company plans to respond.

Comer’s office is just one of numerous government entities that might seek Lark records from TikTok and ByteDance — and encounter the irregular data retention practices described in the risk assessment, if they have not changed since it was written. In July, the Senate Intelligence Committee [called on](#) the FTC to investigate whether TikTok had misled lawmakers about foreign access to U.S. user data, and regulators from the [EU](#) and [Australia](#) have also launched investigations into the company’s data practices. In a recent [update](#) to its European data policies, TikTok acknowledged that EU user data is accessible by China-based employees, “subject to a series of robust security controls and approval protocols.”

In addition to its warnings about ByteDance’s inability to comply with government requests, the assessment also pointed to problematic internal policies. One employee interviewed for the assessment said that for a set of new product launches, “nobody really confirm[ed] the product’s features were compliant with the law before launch.” Elsewhere, the assessment described a document called “Communications Guidelines,” which many managers and employees understood to be mandatory despite warnings from company lawyers that it “could likely not be enforced consistent with U.S. labor

laws.” TikTok and ByteDance declined to answer questions about why their lawyers gave this advice.

The assessment also described a vendor payments process that lacked even basic checks against self-dealing and embezzlement. “Based on expense data obtained for this FRA and verbal confirmations from system administrators,” the assessment said, “it appears that ByteDance’s data systems simply do not collect or retain data about multiple critically important matters related to company expense transactions.”

Moreover, it said company transactions often happened without contracts in place (it referenced almost 35,000 payments of this type), or with poor recordkeeping about what the payments were for. Between September 2019 and May 2021, the report said, “ByteDance made over forty-six thousand payments (collectively totaling over \$1.38 billion USD) for which the data field that is supposed to track which project a payment relates to says only ‘NULL.’” Also, because ByteDance tasks some employees with entering one another’s payments, the assessment noted that over \$1 billion in payments was attributable to just seven people.

The assessment cited various examples of alleged employee fraud at ByteDance, including embedded images of fraudulent invoices and a reference to 342 instances where “multiple different supplier names receiv[ed] payments at the same bank account number.” It described one case where an employee “abused his access to Company systems to improperly verify TikTok user accounts/handles” and “orchestrated a substantial

fraud scheme involving embezzlement, bribery, kickbacks among fictitious vendors, family members, and friends.”

“This FRA did not examine extensive high-risk related-party transactions involving potentially improper self-dealing between ByteDance and its own institutional investors[.]”

But it also noted the company’s limited ability to investigate incidents of this kind, saying: “Employees responsible for investigating potential procurement fraud encounter a pervasive absence of evidence that accurately, completely, and specifically describes important decisions, thought processes, and actions by employees and managers related to high-risk transactions, such as vendor selections on rushed, high-value, procurements where no competitive bidding occurs.”

Despite the assessment’s considerable length and detail, its authors were also careful to explain its limited scope. “This FRA did not examine extensive high-risk related-party transactions involving potentially improper self-dealing between ByteDance and its own institutional

investors,” it said. Moreover, because the assessment was conducted only by ByteDance employees, it noted that it lacked the independence and objectivity expected of fraud assessments at companies of ByteDance’s size. (According to the Association of Certified Fraud Examiners, Fraud Risk Assessments are standard for large companies and should be conducted [regularly](#).)

To underscore the stakes of ByteDance’s lack of fraud protections, the document referenced the criminal proceedings against Theranos founder Elizabeth Holmes as an example of how privately held companies can be criminally liable for fraud. It noted that people uninvolved in fraud can be personally indicted “for failing to report suspicions to internal and external authorities.”

MORE FROM FORBES

MORE FROM FORBES

A China-Based ByteDance Team Investigated TikTok's Global Security Chief, Who Oversaw U.S. Data Concerns

By **Emily Baker-White**

MORE FROM FORBES

TikTok Parent ByteDance Planned To Use TikTok To Monitor The Physical Location Of Specific American Citizens

By **Emily Baker-White**

MORE FROM FORBES

TikTok Is Bleeding U.S. Execs Because China Is Still Calling The Shots, Ex-Employees Say

By **Emily Baker-White**

MORE FROM FORBES

Senate Intelligence Committee Calls On FTC To Investigate TikTok For 'Deception'

By **Emily Baker-White**

Follow me on [Twitter](#). Send me a secure [tip](#).



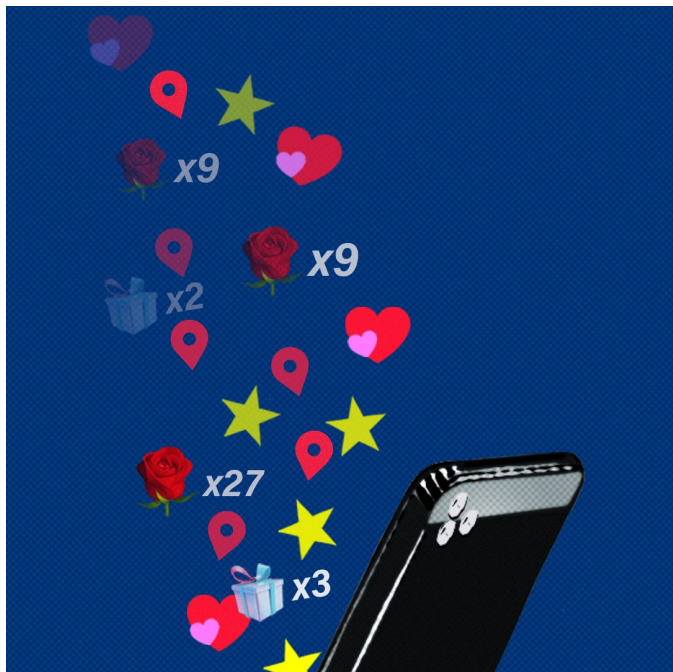
Emily Baker-White

Follow

I'm a technology reporter and senior writer at Forbes based in San Francisco. Have a tip? Email me at ebakerwhite@forbes.com or emilybakerwhite@protonmail.com.

Editorial Standards

Reprints & Permissions



INNOVATION DAILY COVER

TikTok Parent ByteDance Planned To Use TikTok To Monitor The Physical Location Of Specific American Citizens

ILLUSTRATION BY STEPHANIE JONES FOR FORBES; PHOTO BY GEORGE PETERS/GETTY IMAGES

Emily Baker-White Forbes Staff

Follow

Oct 20, 2022, 03:24pm EDT

The project, assigned to a Beijing-led team, would have involved accessing location data from some U.S. users’ devices without their knowledge or consent.

A China-based team at TikTok’s parent company, ByteDance, planned to use the TikTok app to monitor the personal location of

some specific American citizens, according to materials reviewed by *Forbes*.

The team behind the monitoring project — ByteDance’s Internal Audit and Risk Control department — is led by Beijing-based executive Song Ye, who reports to ByteDance cofounder and CEO [Rubo Liang](#).

The team primarily conducts investigations into potential misconduct by current and former ByteDance employees. But in at least two cases, the Internal Audit team also planned to collect TikTok data about the location of a U.S. citizen who had never had an employment relationship with the company, the materials show. It is unclear from the materials whether data about these Americans was actually collected; however, the plan was for a Beijing-based ByteDance team to obtain location data from U.S. users’ devices.

TikTok spokesperson Mouren Shenker said that

TIKTOK’S CHINA PROBLEM

on users’ IP addresses to “among other things, help show relevant content and ads to users, comply with applicable laws, and detect and prevent fraud and inauthentic behavior.”

But the material reviewed by *Forbes* indicates that ByteDance’s Internal Audit team was planning to use this location information to surveil individual American citizens, not to target ads or any of these other purposes. *Forbes* is not disclosing the nature and purpose of the planned surveillance referenced in the materials in order to protect sources. TikTok and ByteDance did not answer questions about whether Internal Audit has specifically

targeted any members of the U.S. government, activists, public figures or journalists.

TikTok is [reportedly close](#) to signing a contract with the Treasury Department's Committee on Foreign Investment in the United States (CFIUS), which evaluates the national security risks posed by companies of foreign ownership, and has been investigating whether the company's Chinese ownership could enable the Chinese government to access personal information about U.S. TikTok users. *(Disclosure: In a past life, I held policy positions at Facebook and Spotify.)*

In September, President Biden signed an executive order enumerating specific risks that CFIUS should consider when assessing companies of foreign ownership. The [order](#), which states that it intends to “emphasize . . . the risks presented by foreign adversaries’ access to data of United States persons,” focuses specifically on foreign companies’ potential use of data “for the surveillance, tracing, tracking, and targeting of individuals or groups of individuals, with potential adverse impacts on national security.”

The Treasury Department did not respond to a request for comment.

The Internal Audit and Risk Control team runs regular audits and investigations of TikTok and ByteDance employees, for infractions like conflicts of interest and misuse of company resources, and also for leaks of confidential information. Internal materials reviewed by *Forbes* show that senior executives, including TikTok CEO Shou Zi Chew, have ordered the team to investigate

individual employees, and that it has investigated employees even after they left the company.

The internal audit team uses a data request system known to employees as the “green channel,” according to documents and records from Lark, ByteDance’s internal office management software. These documents and records show that “green channel” requests for information about U.S. employees have pulled that data from mainland China.

TikTok and ByteDance did not answer questions about whether Internal Audit has specifically targeted any members of the U.S. government, activists, public figures or journalists.

“Like most companies our size, we have an internal audit function responsible for objectively auditing and evaluating the company and our employees’ adherence to our codes of conduct,” said ByteDance spokesperson Jennifer Banks in a statement. “This team provides its recommendations to the leadership team.”

ByteDance is not the first tech giant to have considered using an app to monitor specific U.S. users. In 2017, the New York Times [reported](#) that Uber had identified various local politicians and regulators and served them a separate, misleading version of the Uber app to avoid regulatory penalties. At the time, Uber acknowledged that it had run the program, called “greyball,” but said it was used to deny ride requests to “opponents who collude with officials on secret ‘stings’ meant to entrap drivers,” among other groups.

TikTok did not respond to questions about whether it has ever served different content or experiences to government officials, regulators, activists or journalists than the general public in the TikTok app.

Both Uber and Facebook also reportedly tracked the location of journalists reporting on their apps. A [2015 investigation](#) by the Electronic Privacy Information Center found that Uber had monitored the location of journalists covering the company. Uber did not specifically respond to this claim. The 2021 [book *An Ugly Truth*](#) alleges that Facebook did the same thing, in an effort to identify the journalists’ sources. Facebook did not respond directly to the assertions in the book, but a spokesperson [told](#) the San Jose Mercury News in 2018 that, like other companies, Facebook “routinely use[s] business records in workplace investigations.”

“It is impossible to keep data that should not be

stored in CN from being retained in CN-based servers.”

But an important factor distinguishes ByteDance’s planned collection of private users’ information from those cases: TikTok [recently told lawmakers](#) that access to certain U.S. user data — likely including location — will be “limited only to authorized personnel, pursuant to protocols being developed with the U.S. Government.” TikTok and ByteDance did not answer questions about whether Internal Audit executive Song Ye or other members of the department are “authorized personnel” for the purposes of these protocols.

These promises are part of [Project Texas](#), TikTok’s massive effort to rebuild its internal systems so that China-based employees will not be able to access a swath of “protected” identifying user data about U.S. TikTok users, including their phone numbers, birthdays and draft videos. This effort is central to the company’s national security negotiations with CFIUS.

At a Senate hearing in September, TikTok Chief Operating Officer Vanessa Pappas [said](#) the forthcoming CFIUS contract would “satisfy all national security concerns” about the app. Still, some senators appeared [skeptical](#). In July, the Senate Intelligence Committee [began an investigation](#) into whether TikTok misled lawmakers by withholding information about China-based employees’ access to U.S. data earlier this year,

following a June [report](#) in BuzzFeed News showing that U.S. user data had been repeatedly accessed by ByteDance employees in China.

In a statement about TikTok's data access controls, TikTok spokesperson Shanahan said that the company uses tools like encryption and "security monitoring" to keep data secure, access approval is overseen by U.S. personnel, and that employees are granted access to U.S. data "on an as-needed basis."

It is unclear what role ByteDance's Internal Audit team will play in TikTok's efforts to limit China-based employees' access to U.S. user data, especially given the team's plans to monitor some American citizens' locations using the TikTok app. But a fraud risk assessment written by a member of the team in late 2021 highlighted data storage concerns, saying that according to employees responsible for the company's data, "it is impossible to keep data that should not be stored in CN from being retained in CN-based servers, even after ByteDance stands up a primary storage center [sic] in Singapore. [Lark data is saved in China.]" (brackets in original).

Moreover, a leaked audio conversation from January 2022 shows that the Beijing-based team was, at that point, gathering additional information on Project Texas. In the call, a member of TikTok's U.S. Trust & Safety team recounted an unusual conversation to his manager: The employee had been asked by Chris Lepitak, TikTok's Chief Internal Auditor, to meet at an LA-area restaurant off hours. Lepitak, who reports to Beijing-based Song Ye,

then asked the employee detailed questions about the location and details of the Oracle server that is central to TikTok's plans to limit foreign access to personal U.S. user data. The employee told his manager that he was "freaked out" by the exchange. TikTok and ByteDance did not respond to questions about this conversation.

Oracle spokesperson Ken Glueck said that while TikTok does currently use Oracle's cloud services, "we have absolutely no insight one way or the other" into who can access TikTok user data. "Today, TikTok is running in the Oracle cloud, but just like Bank of America, General Motors, and a million other customers, they have full control of everything they're doing," he said.

This corroborates a January statement made by TikTok's Head of Data Defense in another leaked audio call. In that call, the executive said to a colleague: "It's almost incorrect to call it Oracle Cloud, because they're just giving us bare metal, and then we're building our VMs [virtual machines] on top of it."

Glueck made clear that this would change if and when TikTok finalizes its contract with the federal government. "But unless and until that's the case," he said, Oracle is not providing anything "other than our own security" for TikTok.

TikTok did not answer questions from *Forbes* about the status of the company's negotiations with CFIUS. But in a statement to Bloomberg published early this morning, TikTok spokesperson Brooke Oberwetter said: "We are confident that we are on a path to fully satisfy all reasonable U.S. national security concerns."

Richard Nieva contributed reporting.

MORE FROM FORBES

MORE FROM FORBES

Students Viewed This Type Of TikTok 412 Billion Times-And It's Not Porn

By **Emma Whitford**

MORE FROM FORBES

Facebook And Instagram Are Full Of Violent Erotica Ads From ByteDance- And Tencent-Backed Apps

By **Emily Baker-White**

MORE FROM FORBES

LinkedIn Profiles Indicate 300 Current TikTok And ByteDance Employees Used To Work For Chinese State Media-And Some Still Do

By **Emily Baker-White**

MORE FROM FORBES

TikTok Moderators Are Being Trained Using Graphic Images Of Child Sexual Abuse

By **Alexandra S. Levine**

Follow me on [Twitter](#). Send me a secure [tip](#).



Emily Baker-White



I'm a technology reporter and senior writer at Forbes based in San Francisco. Have a tip? Email me at ebakerwhite@forbes.com or emilybakerwhite@protonmail.com.

Editorial Standards

Reprints & Permissions

INNOVATION EDITORS' PICK

EXCLUSIVE: TikTok Spied On Forbes Journalists



ILLUSTRATION BY PHILIP SMITH FOR FORBES/IMAGE BY DRAFTER123 GETTY IMAGES

Emily Baker-White Forbes Staff

Follow

Dec 22, 2022, 02:53pm EST

6

ByteDance confirmed it used TikTok to monitor journalists' physical location using their IP

addresses, as first reported by *Forbes* in October.

An internal investigation by ByteDance, the parent company of video-sharing platform TikTok, found that employees tracked multiple journalists covering the company, improperly gaining access to their IP addresses and user data in an attempt to identify whether they had been in the same locales as ByteDance employees.

According to materials reviewed by *Forbes*, ByteDance tracked multiple *Forbes* journalists as part of this covert surveillance campaign, which was designed to unearth the source of leaks inside the company following a **drumbeat of stories exposing the company's ongoing links** to China. As a result of the investigation into **the surveillance tactics**, ByteDance fired Chris Lepitak, its chief internal auditor who led the team responsible for them. The China-based executive Song Ye, who Lepitak reported to and who reports directly to ByteDance CEO Rubo Liang, resigned.

“I was deeply disappointed when I was notified of the situation... and I’m sure you feel the same,” Liang wrote in an internal email shared with *Forbes*. “The public trust that we have spent huge efforts building is going to be significantly undermined by the misconduct of a few individuals. ... I believe this situation will serve as a lesson to us all.”

“It is standard practice for companies to have an internal audit group authorized to investigate code of conduct violations,” TikTok General Counsel Erich Andersen wrote in a second internal email shared with *Forbes*. “However, in this case individuals misused their authority to obtain access to TikTok user data.”

Forbes first reported the surveillance tactics, which were overseen by a China-based team at ByteDance, in October. Asked for comment on that story, ByteDance and TikTok did not deny the surveillance, but took to Twitter after the story was published to say that “TikTok has never been used to ‘target’ any members of the U.S. government, activists, public figures or journalists,” and that “TikTok could not monitor U.S. users in the way the article suggested.” In the internal email, Liang acknowledged that TikTok had been used in *exactly* this way, as *Forbes* had reported.

“This is a direct assault on the idea of a free press and its critical role in a functioning democracy.”

The investigation, internally known as Project Raven, began this summer after *BuzzFeed News* published a story revealing that China-based ByteDance employees had repeatedly accessed U.S. user data, based on more than 80 hours of audio recordings of internal TikTok meetings. According to internal ByteDance documents reviewed by *Forbes*, Project Raven involved the company's Chief Security and Privacy Office, was known to TikTok's Head of Global Legal Compliance, and was approved by ByteDance employees in China. It tracked Emily Baker-White, Katharine Schwab and Richard Nieva, three *Forbes* journalists that formerly worked at BuzzFeed News. (*Disclosure: In a previous life, I held policy positions at Facebook and Spotify.*)

“This is a direct assault on the idea of a free press and its critical role in a functioning democracy,” says Randall Lane, the chief content officer of *Forbes*. “We await a direct response from ByteDance, as this raises fundamental questions about what they are doing with the information they compile from TikTok users.”

After this story was published, TikTok spokesperson Hilary McQuaide said, "The misconduct of certain individuals, who are no longer employed at ByteDance, was an egregious misuse of their authority to obtain access to user data. This misbehavior is unacceptable, and not in line with our efforts across TikTok to earn the trust of our users."

ByteDance spokesperson Jennifer Banks added, “ByteDance condemns this misguided plan that violated the company's Code of Conduct.” She said that

ByteDance has not found evidence that the company surveilled *Forbes* journalists beyond Baker-White, but that the investigation is ongoing. Internal company materials reviewed by *Forbes* indicate surveillance of Schwab and Nieva as well.

Banks also noted that its head of Global Legal Compliance, Catherine Razzano, did not know about the surveillance of journalists until late October, although materials reviewed by *Forbes* show that she was aware of the Project Raven leak investigation before that time.

MORE FROM FORBES

TikTok's China Problem

By Emily Baker-White

“This new development reinforces serious concerns that the social media platform has permitted TikTok engineers and executives in the People’s Republic of China to repeatedly access private data of U.S. users despite repeated claims to lawmakers and users that this data was protected,” Senator Mark Warner told *Forbes*. “The DoJ has also been promising for over a year that they are looking into ways to protect U.S. user data from ByteDance and the CCP — it’s time to come forward with that solution or Congress could soon be forced to step in.”

According to an internal email sent Thursday by Andersen, ByteDance found that several of its employees obtained the data of “a former BuzzFeed reporter and a Financial Times reporter,” as well as a “small number of

people connected to the reporters” through their TikTok accounts. The audit was conducted by the law firm Covington & Burling, which has **represented** TikTok in litigation against the U.S. government. Covington did not respond to a comment request.

In addition to the firing of TikTok’s Chief Internal Auditor, Chris Lepitak, who was suspended after *Forbes*’ initial report about the surveillance scheme in October, ByteDance fired two additional TikTok employees in the United States and China as a result of the findings. Lepitak did not immediately respond to a request for comment. “None of the individuals found to have directly participated in or overseen the misguided plan remain employed at ByteDance,” Andersen wrote in the internal email.

“This new development reinforces serious concerns that the social media platform has permitted TikTok engineers and executives in the People’s Republic of China to repeatedly access private data of U.S. users despite repeated claims to lawmakers and users that this data was protected.”

The team that oversaw the surveillance campaign was ByteDance’s Internal Audit and Risk Control department, a Beijing-based unit primarily responsible for conducting

investigations into potential misconduct by current and former ByteDance employees.

TikTok chief executive Shou Zi Chew wrote in his own email to employees, “We take data security incredibly seriously,” adding that the company’s Project Texas, which would limit China-based access to U.S. user data (and which was **first reported by Baker-White at BuzzFeed News**) was a “testament to that commitment.”

In 2021, TikTok became the most visited website in the world, but the app’s ownership by Chinese tech giant ByteDance has raised serious concerns about the company’s access to the personal information of millions of U.S. citizens, as well as its capacity to manipulate and influence user content. The company is currently negotiating a national security contract with the Treasury Department’s Committee on Foreign Investment in the U.S. (CFIUS), which will govern the way the Chinese-owned social media app handles Americans’ personal user data. The company has also sought to assuage concerns about ties to China by working to move some U.S. user information stateside to be stored at a data center managed by Oracle as part of Project Texas.

“In this case individuals misused their authority to obtain access to TikTok user data.”

Forbes **reported** in October that the same China-based ByteDance internal audit and investigations team that oversaw the surveillance campaign against journalists

also investigated TikTok global security chief Roland Cloutier, a U.S. Air Force veteran, who was tasked with overseeing efforts to limit Chinese employees' access to American user data. Cloutier stepped down in July 2022. At least **five senior employees** who led departments at TikTok recently left the company over revelations that they could not meaningfully influence decision-making, *Forbes* also found.

TikTok and ByteDance declined to comment on specific employee investigations or on the departures.

In August, *Forbes* additionally found LinkedIn profiles for three hundred ByteDance employees that showed they previously worked for Chinese state media publications. Twenty-three of the profiles appeared to have been created by ByteDance directors. At the time, ByteDance spokesperson Jennifer Banks said the company makes "hiring decisions based purely on an individual's professional capability to do the job. For our China-market businesses, that includes people who have previously worked in government or state media positions in China. Outside of China, employees also bring experience in government, public policy, and media organizations from dozens of markets."

ByteDance is not the first tech giant to use an app to monitor specific users. In 2017, the New York Times **reported** that Uber had identified various local politicians and regulators and served them a separate, misleading version of the Uber app to avoid regulatory penalties. At the time, Uber acknowledged that it had run the program, called "greyball," but said it was used to deny

ride requests to “opponents who collude with officials on secret ‘stings’ meant to entrap drivers,” among other groups.

Both Uber and Facebook also reportedly tracked the location of journalists reporting on their apps. A **2015 investigation** by the Electronic Privacy Information Center found that Uber had monitored the location of journalists covering the company. Uber did not specifically respond to this claim. The 2021 **book** *An Ugly Truth* alleges that Facebook did the same thing, in an effort to identify the journalists’ sources. Facebook did not respond directly to the assertions in the book, but a spokesperson **told** the *San Jose Mercury News* in 2018 that, like other companies, Facebook “routinely use[s] business records in workplace investigations.”

But an important factor distinguishes ByteDance’s collection of private users’ information from those cases: TikTok **told lawmakers** in June that access to certain U.S. user data — likely including location — will be “limited only to authorized personnel, pursuant to protocols being developed with the U.S. Government.”

Brendan Carr, an FCC commissioner who called on Apple and Google to ban TikTok following the June BuzzFeed News report, said: “At the precise moment when TikTok is trying to convince U.S. officials that it can be trusted—when it has every incentive to ensure the security of user data—its Beijing-based parent company abused its systems to obtain data on reporters that are covering TikTok? This should be the final nail in the coffin for the idea that U.S. officials can trust TikTok.”

This story has been updated to incorporate additional information from TikTok and ByteDance.

MORE FROM FORBES

MORE FROM FORBES

TikTok Parent ByteDance Planned To Use TikTok To Monitor The Physical Location Of Specific American Citizens

By Emily Baker-White

MORE FROM FORBES

A China-Based ByteDance Team Investigated TikTok's Global Security Chief, Who Oversaw U.S. Data Concerns

By Emily Baker-White

MORE FROM FORBES

TikTok Is Bleeding U.S. Execs Because China Is Still Calling The Shots, Ex-Employees Say

By Emily Baker-White

MORE FROM FORBES

LinkedIn Profiles Indicate 300 Current TikTok And ByteDance Employees Used To Work For Chinese State Media-And Some Still Do

By Emily Baker-White

Follow me on [Twitter](#). Send me a secure [tip](#).



Emily Baker-White

Follow

I'm a technology reporter and senior writer at Forbes based in San Francisco. Have a tip? Email me at ebakerwhite@forbes.com or emilybakerwhite@protonmail.com.

Editorial Standards

Reprints & Permissions

India Banned TikTok In 2020. TikTok Still Has Access To Years Of Indians' Data.

F forbes.com/sites/alexandrarevine/2023/03/21/tiktok-india-ban-bytedance-data-access

March 21, 2023



In 2020, Indians burned posters with the TikTok logo in support of their government for banning the Chinese-owned app.

NOAH SEELAM/AFP/GETTY IMAGES

India's 150 million users were forced to stop using the Chinese-owned app in 2020. But an internal tool reviewed by *Forbes* showed that ByteDance and TikTok employees can still mine some of their most sensitive data. One employee called it "NSA-To-Go."

By Alexandra S. Levine, Forbes Staff

Almost three years after TikTok's largest market, India, banned the Chinese-owned social media app over geopolitical tensions, troves of personal data of Indian citizens who once used TikTok remain widely accessible to employees at the company and its Beijing-based parent, ByteDance, *Forbes* has learned.

The revelation comes as President Joe Biden's administration threatens to ban the platform used by more than 100 million Americans if TikTok's Chinese owner does not sell its stake. Officials in the highest levels of the U.S. government see a blanket TikTok ban as a possible solution to the country's national security concerns about the potential for China to surveil or manipulate Americans. Some have called India a "guide star," urging the U.S. to follow its lead.

"I don't think [Indians are] aware of how much of their data is exposed to China right now, even with the ban in place," a current TikTok employee told *Forbes*.

According to the employee and a review of internal TikTok and ByteDance programs by *Forbes*, almost anyone at the companies with basic access to their tools can retrieve and analyze granular data about past TikTok users in India. (ByteDance has more than 110,000 employees around the world, including in China and Russia, but reportedly fired its entire India staff last month.) Another source also independently confirmed that Indians' data has been accessible since the country banned the app.

"I don't think [Indians are] aware of how much of their data is exposed to China right now, even with the ban in place."

One social mapping tool—which the TikTok employee jokingly called "NSA-To-Go"—can spit out a list of any public or private user's closest connections on TikTok and personally identifiable information about them, and it still pulls up the TikTok profiles of people in India, according to a review by *Forbes*. Staff can plug in a TikToker's unique identifier or UID, a string of numbers tied to more detailed data about the person, to retrieve the TikTok usernames (often, first and last name) of hundreds of friends and acquaintances; the region where they live; and how they share TikTok content with phone contacts and users across other social platforms. The same UID can be used across TikTok and ByteDance's other internal tools to find even more information about the person—including their search behavior. The TikTok employee described it as a key to building a "digital dossier" on any user, including those with private accounts.

"We have steadfastly complied, and continue to remain in full compliance, with the Government of India order since it was implemented," TikTok spokesperson Jason Grosse said in an email. "All user data is subject to our robust internal policy controls surrounding access, retention, and deletion." ByteDance did not respond to a request for comment.

The purpose of India’s 2020 ban appears to have focused on preventing public access to TikTok in the country going forward, given concerns about the app potentially sending data it had collected on Indian users back to China. (Nikhil Gandhi, who was then head of TikTok in India, said at the time that TikTok had “not shared any information of our users in India with any foreign government, including the Chinese government.”) The ban did not seem to call for deletion of app data that had already been captured and stored.

As a result, the profiles of Indian users who once used TikTok can still be found online, though their owners haven’t been able to post since the 2020 ban. The company would not say how many Indian accounts can be viewed in the internal tool, but TikTok had roughly 150 million monthly active users there at the time it was shut down, according to data analytics firm Sensor Tower. The data in this particular tool appears to be frozen in time for the India users; for other countries like the U.S., where TikTok is widely used today, it updates in real-time.

The current TikTok employee told *Forbes* that nearly anyone with basic access to company tools—including employees in China—can easily look up the closest contacts and other sensitive information about any user. That includes everyone from prominent public figures to the average person, according to the employee and a *Forbes* review of the tool. In the wrong hands, the employee noted, that information could be dangerous.

“From [their social graphs], if you want to start a movement, if you want to divide people, if you want to do any kind of operation to influence the public on the app, you can just use that information to target those groups,” they said. This powerful demographic data, especially on TikTok’s unmatched Gen Z userbase, could also be highly valuable for commercial purposes, the employee added.

| “We can’t ban them from the data they already have.”

Beyond the India case, company-wide access to a tool like this could be highly problematic in the context of geopolitical conflict. Data on users from Ukraine and Russia, including details about who they communicate with on the app, has been available in the tool, according to the TikTok employee and internal materials obtained by *Forbes*. Though there is no known instance of this tool or others at TikTok being used against foreign adversaries, such information could jeopardize the safety of soldiers and citizens alike.

“When an authoritarian country like China is able to amass a lot of information about citizens in another country, that’s going to raise all sorts of red flags,” former National Security Agency general counsel Glenn Gerstell told *Forbes*. He said that while he thought it might be hard for China to actually weaponize that information in practice, it “absolutely raises concerns, heightens tensions [and] puts them in a position potentially to do mischief with the data. And that’s obviously a threat.”

TikTok has already used its arsenal of tools to target individuals and their networks. A December *Forbes* investigation revealed that ByteDance had tracked multiple journalists who cover the company, gaining access to their IP addresses and other data to try to uncover which ByteDance employees may have been in proximity to them and potentially leaking information. The company vehemently denied that report until its own internal investigation proved it to be accurate, heightening fears across the U.S. government that such surveillance could be conducted on Americans more broadly. The FBI and Justice Department are now investigating ByteDance's use of TikTok to spy on journalists, as *Forbes* first reported. The White House has also ordered federal agencies to wipe TikTok from government employees' devices by the end of this month.

Get a tip about TikTok or ByteDance? Reach out securely to the author, Alexandra S. Levine, on Signal at 306-326-1242, or email her at alex@forbes.com.

TikTok's retention of Indians' data shows why, stateside, a consensual agreement between TikTok and the Committee on Foreign Investment in the U.S. might be far more effective than a ban, Gerstell said. (CFIUS and TikTok have been in talks since 2019 on a deal to address national security concerns about the app.) He said a CFIUS deal could lock down historical data, which the India ban apparently failed to do, and that it would give the U.S. government the ability to set the terms around what happens to Americans' data from past and present. Though a consensual deal wouldn't guarantee that China won't find a way to access that old data, it could afford other protections, he explained.

"If it's a ban—which is the same thing in India—we can't ban them from the data they already have," Gertstell said. "Whatever the data is up to that moment of the ban is TikTok's, is ByteDance's...and we have no legal basis, if all we're doing is banning the thing, to tell them what to do with [it]." It gets even more complicated if the data is already stored outside U.S. jurisdiction, he added.

"The politicians, and the people pounding the table when they talk about bans, in their mind think they're solving a problem," he told *Forbes*, "and they absolutely aren't."

Emily Baker-White contributed reporting.

MORE FROM FORBES

[MORE FROM FORBES](#)[TikTok's China Problem](#)[By Emily Baker-White](#)[MORE FROM FORBES](#)[The FBI And DOJ Are Investigating ByteDance's Use Of TikTok To Spy On Journalists](#)[By Emily Baker-White](#)[MORE FROM FORBES](#)[TikTok CEO Is Quietly Meeting With Lawmakers Ahead Of First-Ever Testimony](#)[By Alexandra S. Levine](#)[MORE FROM FORBES](#)[In The Face Of Attacks, TikTok Tries To Charm Its Critics With Transparency](#)[By Alexandra S. Levine](#)[MORE FROM FORBES](#)[How A TikTok Ban Would Work - And How TikTok Could Fight Back](#)[By Emily Baker-](#)

White**MORE FROM FORBESEXCLUSIVE: TikTok Spied On Forbes Journalists**By Emily Baker-
White

Follow me on [Twitter](#). Check out my [website](#). Send me a secure [tip](#).



Alexandra S. Levine

I'm an investigative features writer at Forbes covering technology and society. I previously spent three years covering tech for Politico and three years as a staff columnist at The New York Times.

Phoebe Liu

Forbes Staff

Mar 21, 2023,12:00am EDT



Bezos with girlfriend Lauren Sánchez, who is the vice chair of the Bezos Earth Fund. (Photo by Steve ... [+] FilmMagic

The Bezos Earth Fund, a multi-billion dollar pledge by Jeff Bezos, the world's third-richest person, is putting \$34.5 million toward better climate reporting and sustainable food, the organization announced on Tuesday.

The new donations put the Earth Fund's total amount granted at \$1.66 billion. In early 2020, Bezos pledged to spend \$10 billion over a decade to fight the impact of climate change. One third of the way into that ten year period, the organization has accomplished nearly 17% of its goal.

The newly announced grants include \$19.1 million in funding for environmental impact reporting efforts. The Carbon Disclosure Project, or CDP, which is known for its A-F environmental impact ratings, will receive \$9.9 million. The GHG Protocol, an international standard for calculating and disclosing greenhouse gas emissions, is being granted \$9.25 million. The Earth Fund's grants aim to help CDP and the GHG Protocol refine their models and increase the transparency of climate impact data. A spokesperson for the Earth Fund did not disclose the time period over which the new grants will be paid out, saying that grant terms vary.

“The global demand for greenhouse gas accounting and disclosure is skyrocketing,” Andrew Steer, president and CEO of the Bezos Earth Fund, said in a press release, emphasizing the need for trust in climate accountability initiatives.

Amazon, which Bezos founded and now chairs, has historically declined to participate in CDP’s ratings surveys and thus received “F” ratings since 2016. Amazon did submit CDP surveys in 2021 and 2022, but its 2021 report is not disclosed publicly. (All first-time participants have the option not to disclose their score, and its 2022 submission is marked “not scored” because the company submitted its response after the deadline, per CDP guidelines.)

Instead, Amazon uses the GHG Protocol to calculate its carbon footprint and releases the information in its own sustainability reports. Notably, the GHG Protocol takes into account renewable energy purchases to offset some of Amazon’s grid electricity consumption. Amazon has come under fire for using offsets to shape its overall carbon footprint reporting, rather than reducing its overall carbon dioxide emissions. A spokesperson for Amazon told *Forbes* that the company aims to fully power its operations with 100% renewable energy by 2025.

The Earth Fund spokesperson emphasized that Amazon and the Earth Fund are separate entities, adding that the Earth Fund is supporting initiatives that address voluntary carbon market governance.







Will Trump Be Arrested Tuesday? Here's What We Know-But It's Unlikely

The remainder of the \$34.5 million in grants go to making meat less environmentally damaging to cultivate and consume—what the Earth Fund calls “climate-friendly” food. Cornell University’s College of Agriculture and Life Sciences will receive \$9.9 million for a virtual fencing project. In Cornell’s case, virtual fencing means equipping livestock with devices that keep them within designated grazing areas, lessening the need to chop down large swaths of forest to build physically fenced fields. The Earth Fund is also granting \$5.5 million to the Good Food Institute, which in turn funds research on plant-based meat alternatives.

After an initial announcement of \$791 million grants in 2020, the Earth Fund's grantmaking pace has slowed. In 2021, the organization announced approximately \$400 million in grants. In 2022, the amount was even smaller, falling just shy of \$300 million.

The Earth Fund's grantmaking pace is not necessarily linear, and the organization's work also includes guidance for grantees, the organization's spokesperson said, reaffirming that the Earth Fund will reach its \$10 billion commitment.

Bezos has spent more time making grants and talking about his philanthropy since stepping down as Amazon CEO in 2021. *Forbes* estimates that Bezos has given \$2.79 billion in his lifetime, prior to counting the newest grants. He gave away \$690 million in 2022 alone, to Earth Fund grantees as well as to Bezos Academies, which provides tuition-free preschools for low-income families; the Bezos Day 1 Families Fund, which helps families experiencing homelessness; and toward the Courage & Civility awards announced in 2021 for chef Jose Andres and activist Van Jones to charities of their choice.

Bezos does not have his own private charitable foundation. He funds at least some of his charitable giving via gifts of stock; in 2022, he donated \$735 million worth of Amazon stock to unnamed charitable entities. Some of it may have gone to donor-advised funds, which are like a charitable giving bank account that holds the assets until a donor wants to disperse some or all of the funds to a nonprofit group.

Past donations from the Bezos Earth Fund have gone to large climate organizations including the World Resources Institute, which is a partner of CDP, and the Environmental Defense Fund; a smattering of climate justice organizations; and landscape restoration and preservation groups, among others.

The news of the Earth Fund grants comes less than a day after Amazon announced a new round of 9,000 layoffs, following a January round of 18,000 layoffs.



Phoebe Liu

I'm a reporter at Forbes writing about the world's richest people with a focus on the tech sector. Send any tips to my email (pliu@forbes.com) or Signal

...

TikTok Insider: Zhang Yiming's Journey of Giant Waves

 mp.weixin.qq.com/s/1Dv17rDRto_1i_LdHEVARA

original Zhang Jun Zhang Xiaojun 2022-04-24 20:03

Included in collection #byte beat 3

Interface Contributing Author: Zhang Jun

Editor: Gao Yulei

- This article was first published on Jiemian News -

ByteDance founder Zhang Yiming bought a painting of "waves" just before the political storm that forced him to sell his business in the United States loomed .

It was early 2020, and he was living in the United States. The sudden political vortex put him in a high-load and sedentary state, which triggered old back problems. His body endured the pain.

In the eyes of many people, this is a Chinese entrepreneur who lacks artistic talent and has a strong sense of pragmatism. It's a little surprising that he buys art. People who know him say that the painting stems from his fondness for California.

In the past six years, ByteDance has gone through a chaotic and bumpy international journey. Now TikTok's global monthly activity peak has exceeded 1.2 billion, and its daily activity has surpassed the pace of Douyin in China, which is firmly above 600 million. This means that every day, more than 1 billion people on the planet open this entertainment short video app from China on their mobile phones.

The sudden emergence of Douyin and TikTok has increased the valuation of Byte by nearly 36 times; more importantly, **Chinese content platforms have penetrated into the hinterland of the West for the first time, and set a new model for Chinese companies to do business globally.**

The painting with the theme of "waves" not only reflects Zhang Yiming's ambition to go overseas, but also a true portrayal of his having to face the countercurrent of globalization.

01

Zhang Yiming's pure personality

The starting point for Zhang Yiming to lead the world is the AVIC low building located at No.

TIKTOK内幕 张一鸣的巨浪征途





48, Zhichun Road, Haidian, Beijing. At the beginning of 2016 , the employees moved with the high-level staff to this squat, square, off-white building with only two floors. This was originally the location of the Aviation Museum, and **helicopters can take off and land on the roof.**

Zhang Yiming, who has always been humble, sent an internal letter to remind all employees to pay attention: "We are one of the few companies in Zhichun Road in the center of the imperial capital."

At that time, Zhang Yiming was keen on handling administrative affairs, and he was very satisfied with this low building with a height of 14 meters and a sense of space in the interior. The founder has a lot of experience on office space: "Many companies will slump when they move to a good headquarters." He cited SUN, Yahoo, and Evernote as examples. It will breed comparisons - for example, some company executives actually want to be equipped with independent elevators. "Very tacky," he wrote.

Just moved in, only Zhang Yiming has an office in the whole company, which is located in the east of the second floor on the top floor. Employees often see him in and out of the elevator, wearing a T-shirt and jeans, walking with his head down and swiping his phone. When it's meal time, **he will take the public elevator to the cafeteria on the first floor, endure the hunger, and wait in line for delicious meals with the staff holding the plate.**

On the northwest and south sides near the center on the second floor, Chen Lin and Zhang Nan are sitting respectively, and they act as the "right-hand man" of the CEO. At this time, Byte's business was simple, with only two product lines—one was Toutiao, which Chen Lin was in charge of;

Sitting on the first floor is Zhang Lidong. He is the second person to get the privilege of an office, although the area is not large, it was converted from a storage room. Employees call Zhang Lidong the "Second Boss". His duty is to earn money and build a solid financial pillar for the company.

In 2016, in the eyes of many people, this company called "Today's Toutiao" was just an information platform that started from low-quality content, grabbing third-party information, and feeding algorithms. To make matters worse, the news client has long been a red sea of red seas.

Zhang Yiming, with a software engineer background, is less than 1.7 meters tall, has small eyes, wears glasses, and smiles when he meets everyone; he speaks a bit gibberish. Many people regard him as the spokesperson of data-oriented and machine rationality. This kind of statement embodies the pure line of technocracy, but ignores his side of dealing with people. He was mild-mannered and appeared to be a sincere, simple, harmless man. But he has a high emotional intelligence that is reflected in a pure personality. People who are familiar with him told me that **Zhang Yiming is good at understanding human nature, and can quickly convey goodwill and make the other party aware. "People who have been in contact with him often think that this young man is good and are willing to help him."**

Earlier in 2014, Toutiao was facing a public relations crisis. Zhang Yiming came to communicate with the media. A person close to the turmoil recalled to me that a highly respected veteran media person was very angry when he saw a controversial technology rookie. Consider him where he stands.

On the other hand, Zhang Yiming is not emotional, and is extremely precise about people and things, and his eyes can't tolerate gray and sand. This made him reveal a kind of ruthlessness. **In the early days, he sent people who took the company's code to prison.**

02

hidden line

For this founder with a pure personality, the global social overlord Facebook is an idol, an enemy, and even an object of imitation. On their subsequent journey to sea, Facebook was always with them.

Zhang Yiming once ordered employees to explore social products, one of which was called "Fly Chat". A product manager told me that Zhang Yiming frequently said in Feichat business meetings, such as: **"We can build Facebook."** **"Why don't we learn Facebook?"** **"Why don't we learn Facebook?"** The manager recalled: "I heard him talk about Facebook the most." "What is certain is that Yiming likes and even envies Facebook."

Just when the domestic foundation was not yet firmly established, Zhang Yiming had already set his sights overseas. In fact, TikTok, which is rising a few years later, is just a bright line of byte internationalization, and the dark line buried clues as early as 2015-2016. They hatched News Master, the overseas version of Toutiao, which was renamed Top Buzz for a while; and then launched Buzz Video, an overseas version of Xigua Video.

The idea of internationalization can be traced back to the expectation of the peak growth of Toutiao today. As we all know, Zhang Yiming is an out-and-out data superstitious person. Early members of the overseas team told me that the company estimated a set of data at that time: China's information flow market has a total daily activity of 240 million. Assuming that the winner takes all, half of the market will be divided, and the upper limit of daily activity is about 120 million. Zhang Yiming immediately realized the worry behind the numbers.

Reality fulfills the above inference. Toutiao exploded in all directions in 2016, with 30 million DAU in the middle of the year, and broke through 100 million in the Spring Festival of 2017; but after a short myth, it fell into fatigue (the peak DAU rose to 120 million, and now it has fallen to about 100 million). **"When there is growth pressure, I think of finding opportunities in the international market. This is one of the ways."**

For the countries going to sea, Toutiao preferred the United States, Japan and Latin America. "I asked Zhang Yiming directly," said a former middle-level person in Byte. "At that time, Chinese companies internationalized in Asian and African countries, but today's headlines are in the United States and Japan. Zhang Yiming said that the conditions in Asia and Africa are too bad. Even if it is very large, the volume is too small, and we cannot afford to wait for the market to grow. Although it is difficult for the United States and Japan, as long as they occupy a piece, the share will be large-so, to **be a first-world country, which market is the largest, which market to do .** "

Determining "which market is bigger" is a science. Zhang Yiming doesn't just look at DAU (daily activity), he will ask his subordinates to calculate DAU multiplied by ARPU value (Average Revenue Per User, average revenue per user) - that is, the total number of daily activity, how much money can be earned by multiplying a daily activity user, and thus draw a market The maximum commercial benefit that can be extracted.

Zhang Yiming never seems to set up a mental prison for himself. "Yiming believes that challenging Facebook and Google should be something that can be done," another person in charge of an overseas region told me. "For him, it is to stand firm and then kick the giants down." **Zhang Yiming said to employees, "We want to occupy this market", "If we want to grow bigger, we need..."**

Zhang Yiming once solemnly analyzed internally: "Facebook is launched from high to low, and we are launched from low to high." It means that Facebook is a social product, and whoever is the core of social interaction will affect the people around him. Going down; Byte is a recommended algorithm product. The algorithm and the masses go together and go hand in hand. As long as more people use the app because of the algorithm, they can hold their position, make it bigger and stronger, and finally surround Facebook. This so-called low go higher.

At the end of this year , Bytedance formulated its 2017 strategy, and there are only two Po (highest priority) strategies: mutual entertainment and internationalization.

In the next three years, people were amazed by the rise of Douyin, a line of mutual entertainment, but another thing was overlooked-the globalization of bytes has never stopped. This allows them to grab the second and third growth curves.

03

Failed

Every Sunday, Zhang Yiming walked out of the east office on the second floor, came to the meeting room, and found a good seat to sit. In 2017, he will attend the international bi-weekly meeting on time. The number of people in the meeting will be maintained at 20, and only middle-level and above will participate. **Mostly, he runs his hands over his touchscreen Surface computer, listening to meetings and typing without**

speaking. A middle-level person who was present recalled to me that among the sparse words left by Zhang Yiming, only one sentence still lingers in his mind.

Zhang Yiming said: "The most important thing is to run fast."

It didn't take long, however, for them to discover that trouble was on the way.

The first-generation person in charge of Byte Overseas is named Zhou Jingjin , who is the top science student in a county-level city in Zhejiang Province. Zhang Yiming recruited him early. Chinese Internet companies believe in the concept of "newcomers doing old business" and "old people doing new business". Zhou Jingjin took the initiative to invite Ying to go on an international business trip.

Copyright is the first mountain. In the United States and Japan, copyright protection is extremely strict, and they cannot rely on the old way of directly grabbing at home. An industry insider said that there are generally two sets of contingency policies in the market: for content that can identify the copyright owner (such as Disney) at a glance, they use the "red flag" mechanism to purchase honestly; Those who are not prone to lawsuits should use the "safe haven" mechanism - reposting with vests to avoid platform responsibilities. However, the two types of judgments are all based on human guessing, and there are many unlucky moments when guessing wrong, which led to Byte's early lawsuits.

Zhang Yiming realized that going overseas requires mature managers with international trading experience. In mid-2016, he recruited Liu Xinhua as the person in charge, and Zhou Jingjin reported to him. Liu Xinhua was originally the CMO of Cheetah Mobile, and he has long since gained fame and wealth and freedom. **Zhang Yiming gave the second-generation person in charge very high authority—from the first day he came, he gave the business department a courtesy.**

The International Business Unit is the first business unit (BU) established by Byte, referred to as "i18n". (The source is internationalization, i and n are the first and last characters, and 18 is the number of characters in the middle.) It enjoys independence, which is unique in the history of bytes, and it has not appeared in the next few years. But I didn't expect that in the company that still operated on the middle platform at that time, the business department became a great constraint.

After Liu Xinhua took office, he quickly promoted four things-building an overseas structure, setting up local operations, and downplaying copyright disputes; in addition, he led the renaming of the overseas version of Toutiao News Master. Their research at this time found that the users of American News products are people over the age of 45. To make the product younger, it is necessary to dilute the color of serious news and position light information. The American slang word, Buzz, represents something that generates buzz in social media, and

can refer to information and gossip; while Top Buzz refers to the best buzz. After the name change, Top Buzz transformed from PGC to UGC creator economy, and wanted to be an upgraded version of Medium, an American blogging platform.

According to a director of operations of the product, **in developed countries, it is growth that finally puts information products in a bind.** He told me that the monetization channels for mobile Internet growth in China and foreign countries are very different. In China, the mobile phone pre-installation market is huge, the exposure channels are dotted, and the overall price is fair; the overseas ecology is that user growth and monetization are monopolized by two giants: Facebook and Google. "The project is competing with them. Users come from these two lines, and the monetization channel also comes from these two lines. The growth model is an endless loop."

He settled an account for me. Toutiao finds mobile phone manufacturers in China to do pre-installation. A user realizes 3 cents per day, and can earn 15 yuan in the 50-day life cycle. The pre-installation cost is only 5 yuan, which makes them profitable. (The life cycle refers to how many days the user will uninstall the app after getting a new phone.) Overseas numbers are much different. For example, in the United States, a user costs \$3, but within 30 days of the entire life cycle, it can only earn nearly \$1. "If you can't make money back, the result is that you are paying taxes on it," the above-mentioned operator concluded. "Overseas, if you want to make content or social products, the ceiling is Facebook. It is a giant jaw."

In 2017, Byte spent anxiety due to the lack of new sexy stories. In July, the Strategy Department wrote a report and submitted it to Zhang Yiming. The report shows that there is little hope for the internationalization of information products, and transformation is urgently needed. But Zhang Yiming couldn't accept backing down—"Yiming firmly believes that great efforts can produce miracles." An employee of the International Business Department said that **in his mind, since this model has been verified in China, it should be able to go global.** The project lasted for another year.

On the other hand, Liu Xinhua believes that the general trend of graphics and texts is gone, and his interest has become less, so he shifted his energy to videos. According to people close to the high-level executives, when Liu went to Japan, he found that Japan Information had powerful products, and the chances were slim, so he gave up graphics and texts, and only made Buzz Video, which ushered in good growth in the early days. The small video gave him a taste of the sweetness. However, the disadvantages of the independent kingdom of the business department have become more and more prominent, and it is difficult to allocate resources from the middle office. And Liu wanted to make videos, which did not meet Zhang Yiming's expectations for him, and the video track was guarded by Byte. Therefore, under the multiple incentives of cultural integration and product direction, Liu left after only one year in office to join Kuaishou.

At the project meeting in 2018, the bigwigs sat around a square table, and the middle class sat around behind them. On weekdays, Zhang Lidong, who has mastered the source of banknotes, has a lot of weight in his words. He used to be a reporter and was the vice president of the Beijing Times. He is more emotional than Zhang Yiming, but he is sharp in judgment and decisive in killing. Participants relayed to me that **that day, Zhang Lidong suddenly spoke in a hoarse voice: "This project will not be done, and I will not be able to make money..."**

Suddenly, the whole room was silent, and no one dared to speak.

"This project is still promising, we can take another look." Zhang Yiming took up the conversation.

After Liu Xinhua left, the International Business Department fell apart. The products and operations were taken over by Chen Lin and Zhao Tian, who were in charge of Toutiao at that time, respectively, and the algorithms and technologies were reported back to their respective middle stations. Later, Kang Zeyu joined Byte from Baidu and took over international products. He hatched the Indian social product Helo here.



来源：基于作者访谈整理

制图：张小璐 jùn

张小璐

Until August 2018, the company made up its mind to cut off information internationalization. Top Buzz, an outdated product, ended tragically under the heavy mountain of copyright and growth. Byte's first business unit is coming to an end. The only fruit it left behind, Helo, did not escape the bad luck of being banned by the Indian government in the future.

In Zhang Nan's line, the internal jokes and small volcano videos also tried to go to sea. Also failed.

No one has ever seen sullen color climb up Zhang Yiming's face, he is like an emotional insulator. But the above-mentioned participants heard him say, **"I don't feel angry now. The biggest negative emotion I have towards a person is disappointment."**

Black and white double T

Zhang Yiming, who values return on investment (ROI) and is partial to pragmatism, will not worry too much about the meaning of a name, as long as the data rises well. "Douyin" originated from A/B testing and master fortune telling.

However, **the reason why TikTok is called TikTok is that Zhang Yiming made the decision himself.**

A key person who personally witnessed the start of TikTok told me that the team took many English names and did A/B tests, but none of them were finalized. They almost kicked TikTok out of the many cool English words. TikTok is the title of a European and American pop song released in 2009. It is pronounced from tick tock and describes the ultimate nightclub carnival. What makes people hesitate is that although this song is very popular, it is very similar to a saliva song, and it seems vulgar in American culture. **Its few advantages are: easy pronunciation.** Of course, the name was chosen by accident. Byte changed its strategy at the beginning of the internationalization of short videos, focusing on Japan and South Korea. In these two countries, TikTok is not only catchy, but also a bit playful.

"Yiming thinks this is it." The early team thought, since there is no better one, let's use it for now, anyway, it can be changed at any time. No one expected that this onomatopoeia, which has no meaning, is so powerful— **"It can be pronounced in all languages in the world, and it's all the same"** —and eventually became popular all over the world.

For content-based applications, byte's decisive weapon is the recommendation algorithm. It often finds a product shell and pours its well-trained algorithms into it, supplemented by user growth and commercialized system combat capabilities. As I explained in "Douyin Insider: The Birth of the Time Melting Pot", whether it is a recommendation algorithm, user growth, or commercialization, Byte used to be supported by the middle platform. It can be

considered that these three sets of capabilities have been verified and accumulated on Toutiao. But stop there, and the company is just another news client.

Musical.ly came just in time. It presents a second product body and massive content fuel for Byte. After merging with the Byte algorithm, it explodes with tenacious vitality. **However, on the eve of the smooth meeting between the two companies, both companies fell into a period of struggle.**

Musical.ly, a short music video product, was born in Shanghai. The two founders are like the opposite of Zhang Yiming: sensual, fluent in English, and full of artistic flavor—Yang Luyu (Louis) perms curly hair, loves cycling, and wears an earring in one ear; Zhu Jun (Alex) has long gray hair, Like a Taoist priest. The two are like artists in the Internet industry, with sharp product insights, but lack of algorithms and advanced technology research and development capabilities.

The birth story of Musical.ly was a game of misfire. It's hard to imagine that these two "artists" worked together at Epro Software, an insurance enterprise service company. This kind of to B track used to be at the bottom of the sexy contempt chain in the IT circle. Of course, standing at the starting point, they don't have a single idea of entertainment in their minds. What they prepare for starting a business is education.

The founder and actual controller of the company is Yang Luyu. He believes that the short video track has opportunities, and the way out is education. At that time, Jun Zhu went to the United States and moved to the enterprise service provider SAP to study the future form of education. When he went back to Shanghai to visit relatives, Yang Luyu lobbied him. Not long after, Zhu Jun joined as a co-founder, and the two began to explore a video mutual teaching and mutual learning community called "Zhi Liao". However, the threshold for educational video production is too high, stumbled, half of the financing was burned, and there was no hope.

Due to the situation, it can only be transformed into entertainment. They have accumulated a certain understanding of community products at this time, believing that "an excellent community is a collection of life attitudes" and "a tool for self-expression". So the two came up with a new idea to promote to young people: "Live like music." In 2012, they launched this app, and took a very blunt Chinese name: "Music Land". The result was the beginning of a second failure.

At this time, the status quo of the Internet industry is that 4G has not yet been popularized. Kuaishou, who started a business at the same time, has survived the long waiting period in China. However, Yang Luyu and Zhu Jun, who have international work experience, chose another path—they planned to try their luck in countries with strong Wi-Fi coverage. Going back to that node, only the United States and South Korea have Wi-Fi in public places in the

world. Finally, after two setbacks in China and two despairs, they decided to start their business in the United States.

This time the naming is like a godsend. An insider of Musical.ly told me that they wanted to find adverbs to express their attitude towards life. **"ly" was inspired by the initials of "Lu Yu" in pinyin**, and they hoped to express: "live music.ly". However, the music domain name has already been registered, so I chose music as a compromise. More coincidentally, **".ly" is a Libyan national domain name, which happened to coincide with the Libyan war that year and was sold at a particularly cheap price.**

The decadence of Yang and Zhu suddenly reversed. Musical.ly, which was launched in 2014, has been sought after by American teenagers. In just two years, the product achieved 20 million monthly and 5 million daily active users in the US market. Musical.ly has been dubbed a "white kid's toy."

Immediately afterwards, new troubles came again. From 2016 to 2017, Musical.ly has thoroughly grasped the American youth market, and its growth has been sideways for a whole year. There are two aspects to the dilemma: First, the brand of Musical.ly has formed a stereotype in Europe and the United States. It is a "teenage version of the App", and other age groups cannot do it; Brand Kuaishou and Douyin began to eat away at the market. What is particularly troublesome is that the Musical.ly algorithm is weak, and it is not enough to return to China for business. **Under the anxiety of growth, Musical.ly had the idea of selling.**

Byte wasn't the first choice for Musical.ly to sell. In the third quarter of 2016, the two founders made a special trip to Facebook headquarters in California, USA to meet with founder Mark Zuckerberg. Zuckerberg is a strong bidder, having spent \$1 billion to acquire Instagram, a 20-person team. Thanks to the blessing of Facebook, Instagram has grown into a photo community giant.

Zuckerberg is interested in capturing the teen market. In his view, Musical.ly is "Instagram for video". Zuckerberg sent Instagram founder Kevin Systrom to visit Shanghai several times to discuss the acquisition with the core team of Musical.ly. **People involved in the transaction told me that Systrom made at least three trips to Shanghai in person, and in the end, Facebook verbally made an acquisition offer of \$1.6 billion in pure cash.** However, in the later stage of the negotiation, Facebook's attitude became hesitant due to uncertainty about how high the ceiling of short videos was.

The second one who extended an olive branch is Kuaishou, the originator of Chinese short videos. Suffering from insufficient cash flow, Kuaishou offered an investment plan that expressed sincerity to the greatest extent. Musical.ly retains independence and becomes a subsidiary of Kuaishou, which holds more than 40% of the shares.

The last entry is ByteDance. At this time, Byte was eagerly looking for short video opportunities, and hatched small volcano videos and Douyin. Volcano reproduces Kuaishou, Douyin reproduces Musical.ly. The company's executives, including Zhang Yiming, prefer volcanoes—after all, they can't resist the temptation of data—Kaishou's gains are impressive, and Musical.ly's response in China is mediocre. The executives have always wondered whether Musical.ly is difficult to implement **in China**? Therefore, Douyin, which copied Musical.ly at the pixel level, also survived a long period of silence during the founding stage, and no one cared about it internally. (For the Douyin entrepreneurial story, see my previous article "The Inside Story of Douyin: The Birth of the Time Melting Pot".)

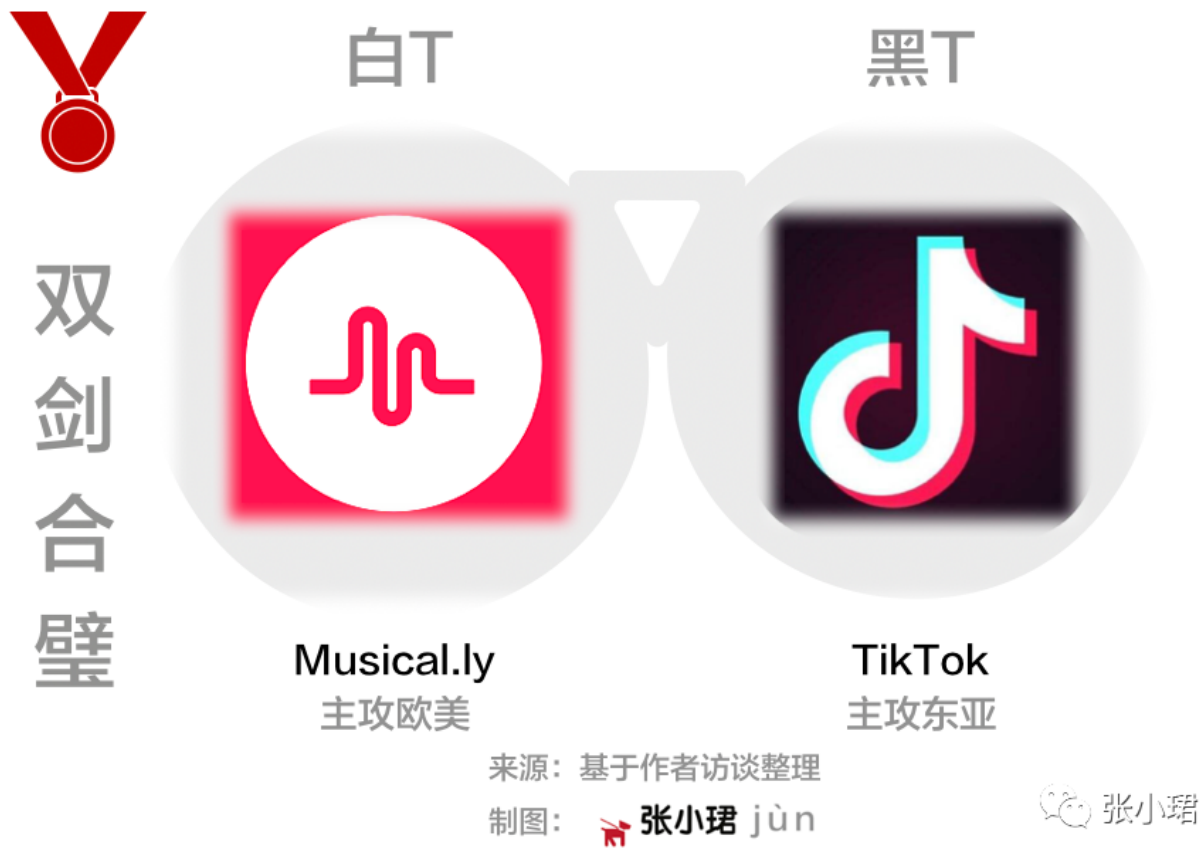
The intriguing turning point came in May 2017. Douyin's DAU has exceeded 1 million, just showing signs of growth. Although Zhang Yiming did not expect it at this time, this product will form a crushing trend for Kuaishou in the future. **However, he changed his indifferent attitude and immediately found the founding team of Musical.ly. "At that time, he said that we had passed 1 million DAU, and we were going to reach 5 million soon."** A core member of Musical.ly recalled to me. Zhang Yiming hopes that the two sides will cease fire and let Musical.ly agree to sell to Byte.

At that time, **the founding team of Musical.ly put forward three conditions: 1. Rename Musical.ly to reverse the minds of users who are teenagers App; 2. Access the byte algorithm; 3. Spend at least 1 billion US dollars on marketing.** Zhang Yiming agreed to all of them. According to people close to the transaction, Zhang Yiming's offer is lower than Facebook's, only \$1 billion, but the acquisition can be made in the form of cash + stock. Based on Byte's valuation of US\$22 billion that year, this figure has now doubled by 20 times (new news shows that Byte's valuation is US\$400 billion).

Also in May, which has the significance of reshaping the global short video landscape, the Douyin team can't wait to launch TikTok in South Korea and Japan. They called some people from the International Business Department who were working on video projects in Japan in the early days. At this time, Byte did not have any influence. The overseas team was to help young people who were newborn calves. Even "recruiting soldiers and buying horses" was difficult. The person in charge of TikTok's product and the head of Douyin's product at that time were the same person: Ren Lifeng, nicknamed "Juanjuan". He reported to Zhang Nan.

They chose a differentiation strategy—"fighting around North America"—and focused on developing Japan, South Korea, Southeast Asia, India, and Brazil. Among them, East Asia is the dominant area of TikTok. However, none of these regions is as important as the United States. **For content products, the United States is the high ground, "whoever wins the United States wins the world."** A TikTok start-up person said that whether it is the short video strategy for Byte or the globalization strategy, Musical.ly is too important, "it must be bought."

In November 2017, after half a year of repeated negotiations, Musical.ly and TikTok merged. At this time, even the people in the game would not have thought that this would be one of the most successful acquisitions in the history of China's Internet. The power of the joint explosion of the two is beyond everyone's imagination. Compared with Baidu's \$1.9 billion acquisition of 91 Assistant, this is really a bargain for Byte.



The origins of Musical.ly and TikTok have also been handed down. A person familiar with TikTok said that Musical.ly's icon is white as the main color, and TikTok is black, so: one is called "White T" and the other is called "Black T". "White T" focuses on Europe and the United States, and "Black T" focuses on East Asia. Later, the company spread a good story that the two products intend to "drain the river". Some later employees believed that this may also be Zhang Yiming's negotiating skills during the acquisition—playing an emotional card, "Let Musical.ly feel that you are not here to grab my site."

But the original core teams on both sides dismissed such humane rhetoric. The TikTok team said that focusing on East Asia is out of purely strategic considerations. **"Yiming wouldn't do such a stupid thing."** The Musical.ly team said that the team hadn't merged at the time, and the two sides felt like a horse race—two forces, black and white, were in confrontation.

Zhang Yiming relies on documents and meetings to drive organization and alignment of information. He deliberately guards against the opponent's spies, and when writing internal documents, he will deliberately set up secret codes to block the dissemination of information. The above-mentioned insider said that the password for "White T" is 1233, and the password for "Black T" is 1180.

05

The gist of Facebook

On the upper left of the low building of AVIC, there used to be four deep black characters of "Jiday's headlines". In mid-2018, the company removed them and put up a brand new blue signboard in the same color as Facebook - "ByteDance". Douyin has become popular this year, with a daily activity of over 200 million, surpassing Kuaishou.

The company has entered the next era, **and it will compete with Facebook in the same ocean.**

中航矮楼的变化



来源：基于作者访谈整理

制图：张小珺 jùn

张小珺

Nine months after the acquisition, Byte incorporated Musical.ly's more than 400-person team and integrated the algorithm into Musical.ly. The sideways data restarted growth, but not so fast.

At the same time, Zhang Yiming started the name change plan as scheduled. At this time, there was an alternative plan. The Musical.ly team proposed to Zhang Yiming to continue the "ly" tradition and change the name to Vedio.ly. But after the A/B test, the data is not as good as TikTok. Therefore, the unified name of the Douyin overseas version is TikTok. In August 2018, Byte announced with great fanfare the full integration of Musical.ly and TikTok.

In the decision-making chain, renaming is a major event that requires concentration. The huge user base has already recognized Musical.ly, and forced integration not only loses users in stages, but also consumes a lot of cash flow to rebuild the brand, which may "lose the wife and lose the army". The original Didi internationalization person said that Didi had been hesitant to unify the name for a period of time when it acquired the travel company 99 in Brazil, but it finally gave up due to complex considerations of multiple factors. Didi's decision is in contrast to Byte. In Zhang Yiming's eyes, on the global map, TikTok is beating a byte and a game of chess from beginning to end.

Integrate some detailed measures. "Black T" and "White T" have no combined product package. They uniformly replaced the Musical.ly icon with TikTok, and the corner logo retained the Musical.ly logo; and changed the title to: TikTok-including Musical.ly. The gear change lasted for more than half a year, and the "including Musical.ly" field was removed only after the brand mentality was established. It was only later discovered that "White T" performed better than "Black T" overall, so they replaced all applications with "White T" product packages. **This also shows that the new TikTok we see today is the combination and evolution of Byte Algorithm and Musical.ly products, each taking its own strengths.**

Next, a gorgeous money carnival debuted. Business wars driven by spending money have long been commonplace in China's tragic Internet arena, not to mention that the initiator is ByteDance, which is used to stirring up the situation. It is even more unsurprising. **Only this time, they will burn money and war overseas.** What is full of drama is that for a period of time, Facebook not only did not hinder TikTok, but also regarded the latter as its most valuable customer.

After the integration, TikTok gave an order and entered the frenzy of throwing money, throwing money, and throwing money crazily. Their most important distribution channel is of course their old friend Facebook. "From the third and fourth quarters of 2018 to the first quarter of 2019, TikTok's promotion budget has increased by more than 100% every quarter," a person close to Facebook told me. "Facebook's annual revenue in Greater China is about 5 billion US dollars. TikTok planned to contribute about US\$1 billion in three years."

The entire industrial chain has been involved in this dance of money. The sales person in charge of Facebook Asia Pacific is a Chinese. Thanks to TikTok, he became the global sales champion in glory. At the end of 2018, the company issued him an excess year-end bonus, "possibly a million level". "Colleagues in Singapore and Hong Kong are saying that he stepped on shit luck." - At this moment, Facebook did not raise its vigilance.

The reason for Facebook to let down its guard is simple: **TikTok's retention rate is simply too poor.** "Is this company stupid? The users who bought it basically ran away, and the retention rate was 30% the next day. Facebook's internal view is: I direct traffic to it, and it can't retain users anyway, and it doesn't pose any threat." The above sources said. At the beginning of 2019, Liu Zhen, the senior vice president in charge of the internationalization functional department of Byte at that time, took a special trip to bring the team to Facebook and signed an annual strategic cooperation agreement with its senior executives in Greater China.

In fact, the cost-effectiveness of buying volume on Facebook is extremely low. At this time, the amount of buying a user in the United States is exaggerated to about \$10. However, **Bytedance, a company that is good at accounting, has silently upgraded its strategy.** People close to Byte told me that they no longer worry about how long it takes to earn back the cost, but instead look at the ARPU value. Simply put, it is how much money a daily active user can earn.

This is the cunning of business warfare. Byte's goal setting is not designed out of thin air, they are aiming at Facebook. Byte paid a high salary to poach a group of management from Facebook, and some of them brought Facebook data out. The granularity of the numbers is fine, and some of them have not been disclosed in the financial report. For example, how much Facebook lives in each country and how much money it can earn... **Byte has made a**

beautiful table covering more than 100 countries based on this. Then, they cleverly used the Facebook ARPU value as the target, and reversed how much they needed to spend on advertising.

What Facebook cares about is that, unlike social networking, video content can cross borders. A short video in the United States can be consumed in Europe, Japan, and Latin America, and it is inherently scalable. Moreover, this product is so humane that it adds a layer of magic to it. Coupled with the confusing effect of global products, the data of each country is not outstanding, but Byte adopts the tactics of dispersing and disintegrating and breaking down one by one, and finally brings together more than 100 countries to make a blockbuster.

One of the reasons why TikTok and Top Buzz are so different is that the former can grow naturally. What's more, the business jungle has forged this enterprise quite shrewdly. They quickly knew that they had to reduce their dependence on Facebook as quickly as possible.

In the first half of 2019, after completing a beautiful sneak attack, TikTok shifted its launch position to Google and Snapchat. According to Byte, this is to prevent Facebook from "doing small and frustrating actions" - what can be thought of is spying on data, secretly raising costs, and artificially causing inaccurate recommendations. In the TikTok budget rankings, Facebook's share fell month by month, from 20% to less than 10%.

It is already mid-2019 when Facebook wakes up like a dream. TikTok's global daily activity has exceeded 100 million. Facebook is trying to thwart TikTok with Lasso, a short-form video app in Mexico and the United States. However, it didn't take long before a black swan event that affected the nerves of the world fell from the sky.

06

Bimonthly increase of 110 million!

—"Don't be complacent", "We are pigs on the wind"

Apart from Zhang Yiming, if TikTok is to be crowned with another soul figure, employees will not hesitate to vote for Musical.ly co-founder Jun Zhu. It is customary to call him by his English name Alex internally.

Zhu Jun has built influence in Byte at a slow pace. He is a rare manager who I have never heard of employees expressing negative emotions. Just after the acquisition, the company made constant adjustments to Jun Zhu. He initially reported to Zhang Yiming, but he was in a marginal situation. It is said that Zhang Yiming could not understand his foreign company style until he recognized his product capabilities; after a period of time, Zhu Jun reported to Zhang Nan, who was in charge of Douyin and TikTok; June 2019, Zhu Jun took over as the head of Douyin for a short time, and reported to Zhang Nan in name, and Zhang Nan continued to be in charge of overseas. In the above three stages, Zhang Yiming is not very satisfied with TikTok.

Until October 2019, the company adjusted again—Zhang Nan was in charge of the country, Jun Zhu took over overseas and reported directly to Zhang Yiming—this was a promotion of his influence. TikTok ushered in a period of rapid development.

Zhu Jun is older than most Byte executives, born in the 70s. He has a refined temperament, a goatee, and speaks English. He is from Anhui. After graduating from Zhejiang University, he worked in the field of corporate services. **He is also a man of temperament, who likes to drink and recite poems; he often wears a gray shawl in the office, with loose hair and wooden clogs. "Like a practitioner."**

There are legends about him. "I often meet him on the subway. He takes the subway in Shanghai. He is a financially free person," said an operator. "In the company, it is rare to see a person with gray hair like him. The female colleague held the door and let others go first." "A kind old man," said a product manager (Byte employees are mainly born in the 90s, so the post-70s are called "old people" in the company), "Alex likes Drinking, I wasn't so busy before, he would take us out for a drink." "Alex has stayed in the United States for many years, and since he came here, it's a combination of Chinese and Western," said a middle-level executive, "A bimonthly summary, every time Alex speaks, it's simply A kind of enjoyment. English is very authentic, and it can explain Chinese culture into English. Wow! It's really great!"

When he took over, TikTok Chinese employees and foreign employees were filled with antagonism, and Zhu Jun proposed the mission, vision and values. The employee said: "Alex has built a poetic expression." "Foreigners are especially buy in." **Alex said: "TikTok is commerce, a bridge, and a window."**

Jun Zhu's appointment was just at the right time. He sat in the driver's seat, gathered people's hearts and stabilized the morale of the army on this global fleet, and led everyone into the night together. At the beginning of 2020, TikTok had less than 250 million daily users. The people in the boat didn't realize at this time that a huge storm was brewing ahead.

The new crown virus spread rapidly-the global epidemic broke out, and TikTok also broke out.

First, at the end of February, an overseas interview went viral in the high-level byte group. Facebook COO Sheryl Sandberg said in an interview that the growth rate of TikTok worried her, "the growth numbers are faster than we have ever been before." What TikTok felt was not joy, but panic. Zhu Jun called an emergency meeting: "Sandberg has paid attention to us."

Immediately afterwards, the epidemic spread rapidly around the world, injecting a catalyst into TikTok. "From March to April 2020, in a two-month period, TikTok increased by 110 million DAUs," a TikTok person told me, "It is extremely exaggerated. " **App.)**

However, the rapidly rising numbers have made byte executives more and more worried. One day at noon, Zhu Jun pulled a group in the enterprise software "Flying Book" developed by Byte, including several key persons in charge. A person close to the management told me that Zhu Jun asked in the group: "What is the risk to us if we remove the Facebook SDK (login interface)?" Feedback to him after get off work at the latest.

The immediate question hanging over their heads is: should the Facebook login interface be removed immediately? Once these interfaces are connected, Facebook seems to have placed an eyeliner on TikTok, and you can have a panoramic view of how many users log in and how many users repost every day; but if you don't connect, the TikTok user experience will be hurt. These interfaces are like feeding machines.

Sure enough, the evaluations of various departments believe that there is a loss-removing the Facebook interface will result in the inability to obtain accurate portraits when acquiring users, which will affect growth and monetization efficiency. Zhu Jun asked everyone to further clarify the loss of user experience. The team came to the conclusion that no more than 20%.

Zhu Jun conveyed the order: cut it off immediately.

In the end, it took less than a week for TikTok to unplug all of the Facebook login interfaces. They decidedly weaned off the pacifier.

The uneasiness didn't dissipate. At the summary of the TikTok bimonthly meeting, Zhu Jun warned managers, "Don't be complacent" and "We are pigs on the wind".

When Zhu Jun was nervously taking TikTok to climb the globalization wave, his old partner Yang Luyu in Musical.ly went to the byte education line to continue his educational dream-

leading the team to develop the "Dali Intelligent Learning Lamp" ". He cut off his old curly hair and kept it cropped.

"An important node in the development of TikTok?" An employee who has worked in TikTok for almost two years without thinking, **"It is the epidemic. It soared into the sky."**

07

"Leave no gaps, comprehensive suppression"

Zhang Yiming, who sits on the easternmost side of the top floor, also regards internationalization as his heart's desire. At the beginning of 2020, Zhang Yiming redistributed the company's power structure—he handed over the China region, appointed Zhang Lidong and Zhang Nan as the chairman and CEO of the China region; and he took a big step forward and became the global CEO. The "three pieces" constitute the center of power.

At this time, Zhang Yiming's bimonthly OKR has a line that reads "no gaps". People close to the power told me that it is actually a code, the full name is: "Leave no gaps, comprehensive suppression." **These eight characters are the highest level that this taciturn, non-aggressive boss has given to TikTok. instruction.**

Under the eight-character policy, TikTok has two unwritten agreements: no matter which region, as long as competitors go, TikTok must advance and crush them; whenever a competing product ranks ahead of the list, it must be within a week, no matter what The price crushes the opponent. Even if you "kill one thousand enemies and lose eight hundred yourself", as long as you remain invincible, you will not hesitate to pay any price.

The user growth (UG, User Growth) center is the vanguard to undertake the highest order, and the person in charge is named Zhao Qi. He has a doctorate in computer science from Peking University. He looks gentle and wears black-rimmed glasses. He was once the co-CEO of the start-up company "Che Lai Lai". For him personally, this is a not-so-successful venture. **But big companies are so strange-sometimes they are especially partial to people with entrepreneurial experience, even if it is a failed entrepreneurial experience.** Maybe it's because of their tragic colors, or their courage to control the overall situation, or just the sincere words they confide after seeing the bottom of the business, which always makes the CEO feel sympathetic and sympathetic.

In Byte, colleagues called Zhao Qi "the person who spends the most money on the Internet in China." To put it simply, the UG middle platform managed by Zhao Qi spends money in

exchange for user growth, snowballing the product, and the commercialized middle platform managed by Zhang Lidong then earns money back by selling products. At this time, for TikTok, spending a lot of money to grow is the top priority, and it is too early to commercialize.

Starting from China, TikTok stretches like an octopus on the earth, and its globalization continues to expand. They divide the country into four levels: s, a, b, and c, and the strategic priorities are lowered in order——



TikTok国家战略级别

(每双月都会有变化…)

S级

美国、日本、英国、印度（下架）

A级

德国、巴西

B级

有15-20个。一般来说是西欧如法国、意大利、西班牙、荷兰；东欧如俄罗斯；亚洲如韩国；人口大国如印度尼西亚、墨西哥；发达国家如加拿大、澳大利亚……

注：B级主要是Facebook ARPU值排名较高的国家，或人口大国，或移动互联网渗透高的国家。

C级

有20-30个。如东南亚的泰国、越南；中东的沙特、阿联酋；非洲埃及；南美洲阿根廷……

注：C级比B级稍弱。

其他

其余160-170个国家。

注：其他国家几乎不用投放，能自然辐射到。比如在俄罗斯买量，乌克兰日活会起来；在法国买量，瑞士日活会起来。

Exactly the same as Toutiao's first attempt at internationalization, developed countries are the key to TikTok's capture. Once cultural products conquer the hub, they will radiate to other regions, which is a blow to cultural dimensionality reduction. (Douyin also implements this idea in China, starting from first- and second-tier cities.)

People familiar with the matter told me that in the global budget market, developed countries such as the United States, Britain, Germany, and Japan have taken most of the banknotes. India invested strategically because of its large territory; Latin America and Russia went because of competitors Kuaishou and Likee (under the Huanju Times) respectively, and had to invest out of the four-character policy of "leaving no gaps" (Russia originally belonged to c, and later rose to b).

The potential for cultural dimensionality reduction is too great. Southeast Asia is the lower reaches of Chinese culture. TikTok only made a small amount of advertising, and it topped the App Store list in Thailand, and won the top spot in both the App Store and Google Play in Vietnam. "It came up in a flash." In the Middle East, TikTok only launched in Saudi Arabia and the United Arab Emirates, and the surrounding countries also rely on natural radiation. Like Iraq, TikTok has never spent a penny. However, during the epidemic, TikTok surged to 6 million daily active users, and Iraq's mobile Internet population was about 25 million, with a daily active penetration rate of 24% and a monthly active penetration rate of 40%.

"Everyone was stunned," the above-mentioned employee concluded, **"The biggest difference between TikTok and Kuaishou and Likee is that it occupies developed countries. It has a public pool, and American content is supplied to the world, and Douyin content is supplied to East Asia and Southeast Asia. Power is particularly big."**

In contrast, the internationalization of Kuaishou has taken many detours. Former Kuaishou employees said that they used the so-called "horse racing mechanism" and changed their names in various regions-Kwai, Snack Video, Zynn (closed). These small teams took root everywhere like bamboo shoots and fought independently. The person in charge has changed like a lantern, and the person in charge who has just announced his resignation, Qiu Guangyu (Tony), is from Didi, which is the fifth wave of the team.

During Qiu's term of office, he tried to gather and focus as much as possible. They also thought about whether it is time to learn the unified name of TikTok, but they have been wandering and shelved. First, Kuaishou's capital warehouse is not as substantial as Byte;

second, the cross-regional radiation potential of content is not as good as TikTok. Now it is only in the Brazilian market and maintains its voice.

In order to explain the rise of TikTok in various countries, it is necessary to introduce a little business knowledge. Generally speaking, TikTok has to cross four stages, and the "turning point" is the most wonderful moment.

The first stage is brainlessly throwing resources. Douyin has verified the extraordinaryness of this business story, and it is nothing more than a copy in the world. The so-called "simple belief, foolish persistence".

The second stage is content ecological construction. If a competitor spends 10,000, TikTok will spend 20,000. The two ends of the machine are users and content. The user growth end continuously sends users, and the content end continuously sends talents, a chemical reaction occurs on both sides, and the user experience spirals upward.

The third stage is the milestone moment - the inflection point has arrived. Byte has a "inflection point theory" and will pay extra attention to the "DAU penetration rate" (daily active penetration rate). The higher the daily active penetration, the higher the user stickiness, and the retention rate that previously plagued TikTok and caused Facebook's misjudgment will naturally increase. **According to experience, the penetration rate of each country reaches 20%-30%, which can meet the inflection point.**

Inflection points are magical moments. As soon as it comes, App popularity mainly depends on interpersonal communication and natural growth. "Buying volume: natural volume" transitions from buying volume to natural volume, and the number moves backward one by one. From a global perspective, purchases accounted for 70% to 80% at the beginning, but now it has dropped to 20% to 30%, "forming a natural and healthy growth state."

The fourth stage is brand building and commercialization.

The s/a/b/c classification will not remain static, and each country may get on the "elevator" at any time. The determinants are complex. It is not only related to hard indicators such as population base, per capita GDP, Internet penetration, and the market ceiling of digital marketing advertising, but also inseparable from soft factors. **TikTok is a mirror of the cultures of various countries.**

Indonesia originally belonged to b, and it went straight to a for a while, because Southeast Asians have a strong desire to express. The release rate of TikTok is as high as 10% in Indonesia, compared to less than 5% for Douyin in China, and only 2%-3% in Japan. "East Asians are more restrained," said a person in charge of national strategy.

South Korea initially belonged to a, but fell to c due to sluggish daily activity growth, and was raised to b after a while. Some employees judged that it might be related to "Koreans are more xenophobic". "You can see that 85% of the market share in South Korea is Samsung and LG, not China or Apple." Another factor is "there are too many entertainment options in South Korea."

In this way, TikTok used its rapid speed and abundant funds to carve out a moat with a heavy hammer. People close to the strategy formulation told me that in the three years from 2018 to 2020, TikTok has a lot of cash in hand, mainly in four directions: marketing growth brand spending about 5 billion US dollars, content construction subsidies spending about 2 billion US dollars, server broadband It took about \$1.5 billion to \$2 billion, and finally the cost of personnel. It is estimated that **10 billion U.S. dollars have been invested in the total.** (Here's how much money 10 unicorns valued.)

The above-mentioned person believes that if any platform wants to make resistance products, the cost of user migration must be multiplied by at least 2 or 3, which is 20 to 30 billion US dollars. No matter which giant crocodile it is, it is a huge sum of money, enough to make him frown and hesitate for a while.

Zhang Yiming is bold and has the courage to spend money, and he still has to rely on Zhang Lidong who sat downstairs when he was in the low building of AVIC. Zhang Lidong is the company's "banknote making machine" and "God of Wealth". He has enriched the company's pocketbook by cashing in on Toutiao and Douyin.

o8

political adventure

However, the joy of blowout growth was immediately submerged in the political storm.

Back in 2016, the EU passed the General Data Protection Regulation (GDPR). The outside world interprets it as the most stringent bill in history, with a staggering maximum penalty of 4% of global annual turnover or 20 million euros. At the beginning of the implementation of GDPR, the relevant competent authorities targeted Facebook, which was fined 10 million euros in 2018. The adoption and implementation of GDPR has caused countries to pay more

attention to personal privacy. **Under the increasingly strengthened supervision, the global data network has begun to move from common to fragmented.**

With the decline of Western economic growth and the rise of populism, local protectionism has become prevalent. TikTok also ushered in the first shot of political censorship.

At the end of 2019, then US President Trump launched an attack on the grounds that Byte's acquisition of Musical.ly had not been reported to the Committee on Foreign Investment in the United States. In order to cope, Zhang Yiming stayed in the United States for several months.

In fact, Zhang Yiming recognized the situation ahead of time. That was before the political storm knocked on the door. In order to prevent data hidden dangers, the "localization" of TikTok overseas has started in an orderly manner. A TikTok person told me that at the beginning of 2019, Byte began to assess the risk of isolation internally and made a plan; from the third quarter, "localization" was officially launched. This movement is by no means as simple as the switching of optical technology. From auditing, operation, server, to technical product personnel, the complex process lasted for more than a year.

In the face of quietly relocating, the work of the parties suffered heavy losses. The first wave is the reviewers. At this time, the review team of more than 300 people was abolished, former Byte employees said. Most of these employees are bilingual workers who specialize in minor languages. Although they are allowed to transfer jobs, they are limited by the type of work, so the chances of winning are not great.

In the first quarter of 2020, when the haze of the epidemic spread to the world, TikTok launched the second wave of migration for operational personnel. Their duty is to find talents and control the content and style of painting. Overnight, the power of many regions was transferred from China to overseas. For example, the European operation team was almost disbanded, or transferred, or left. Only regions that do not involve geopolitical risks, such as Southeast Asia, can remain domestic.

Among those who left, there are many meritorious ministers. After two Musical.ly members merged into TikTok, they were in charge of Western and Central European operations. The general manager of TikTok Europe is named Rich Waterworth. He ordered two people to quickly hand over the work to the European team within a week. "The two girls are very wronged. We have worked so hard here for three or four years. You asked me to hand over in a week, and the team had to cut it off." A person who had contact with them said that the two were transferred later, and one was playing games. One is for charity.

After completing the first two waves of "localization" intensively, the situation in the United States has intensified. Around March 2020, Zhang Yiming, the President's Office, and Liu

Zhen returned to China on a chartered flight. At this time, Zhang Yiming was already a technology tycoon that attracted worldwide attention, and his every move could create headlines. **He entered the country for quarantine, was locked in a hotel, and commanded the company in turmoil through video.**

After returning to China, Zhang Yiming soon took further action. In May of this year, Byte Global announced a high-profile personnel appointment, which caused an uproar in the Chinese and American technology circles. In Byte, Kevin Mayer (Kevin Mayer) is the first American to gain supreme power, not only as COO, but also as TikTok CEO. The appointment is effective June 1. Mayer's legacy is built on Disney. In the kingdom of Mickey Mouse, he led the promotion of large-scale acquisitions such as Pixar Animation and Marvel, and launched the streaming service Disney+, with a remarkable record. Zhang Yiming hopes that his American identity and local influence will help Byte mediate among the intricate American forces.

At the same time, "localization" proceeds to the third stage, and the migration target is the server. It seems that at this time, the Trump administration has regarded TikTok as an obstacle on the road to re-election, and the drums of the political storm have become more intensive.

A person who participated in the TikTok biweekly meeting remembers that Zhu Wenjia, who is in charge of algorithm technology, said: "It will take two months to cut the algorithm code." "**Can it be done within 15 days?" Zhang Yiming couldn't wait.** The answer is yes. And the fourth and final wave of migration is for products and technologists. TikTok executives, including Zhu Wenjia, have all transferred to Singapore.

2020 is the year when Byte encountered political failure. The epidemic not only brought tiktok a hurricane, but also cut them apart. Before the turmoil in the United States Just in June when Mayer first took office, the Indian government issued a ban.

Within days of the incident, Mayer called an all-hands meeting, the most hasty all-hands meeting in Byte's history. **In less than five minutes, Mayer told everyone not to worry, the Indian team is actively communicating and the situation is not yet under control. However, he broke his promise.**

It is quite gratifying that the second short video app in India is Snack Video under Kuaishou. With the ban on TikTok, its data ushered in a rapid climb, and its daily activities surpassed the 150 million mark; but the secret joy did not last long. It was also blocked in India a month later .

Back to TikTok in the United States, the critical situation took a turn for the worse-in July 2020, high-level U.S. government officials stated that TikTok would be banned; in August,

Trump 45-day ultimatum, ordering TikTok to spin off its American business, or close down. Zhang Yiming was forced to negotiate a sale, with potential transaction partners including business giants such as Microsoft, Oracle, and Wal-Mart, as well as Byte's American investors. On the surface, Zhang Yiming participated in the spin-off negotiations, but secretly upholds the belief of a global game of chess.

Less than three months after taking office, Mayer suddenly announced her departure. There are different opinions in the company. Some people say that his abacus is to sell TikTok in the United States with the shareholders, which seems to be in his personal interest; Vanessa Pappas, general manager of TikTok North America, became interim CEO.

During this period of time, the three words that the company uttered the most from top to bottom were: geopolitics, Sino-US confrontation, and force majeure. In fact, 99.9% of people don't know what the company is going through, let alone where their personal fate is going. The uninformed mid-level and high-level comforted the uninformed grassroots: "Do your best and obey the destiny."

"Internet Poet" and has served as the head of Byte Strategy Zhu Jun delivered a speech: "In this era of high walls, TikTok's mission is to build bridges so that people all over the world can connect with each other and enjoy happiness." Generous remarks inspired a group of people.

The complicated and confusing American turmoil was finally relieved by Trump's election defeat. **"What does this look like? I just lay there and felt that they would 'die', and they would really 'die'." A senior industry person who followed the incident closely said, there was a slight difference,** Byte Assets in the United States lost everything. Zhang Yiming survived the U.S. election because the negotiations objectively prolong the time. After the new U.S. President Biden took office, he revoked the ban, and byte thus avoided disaster.

He believes that this incident is much more difficult than Byte's previous "escaping the pursuit of giants" in China. It has played well among the giants, and fell in love with the giants, but it has not fallen into any camp, and has developed the ability to "have both ways". **In the TikTok incident, Byte faced a more passive situation, and the game object was larger, "It's like a leaf of duckweed in the sea."** The person compared a car driving into a narrow alley in Beijing, which made everyone unexpected: "It passed through once, drove in this time, and came out again."

Governments vary in their control over data security. In order not to put himself in danger again, Byte has set up an extremely strict isolation mechanism. According to a legal person with knowledge of this, for sensitive data such as personal account numbers, addresses, social security cards, and consumption records, the general principle is "China's data is in

China, and overseas data is in overseas." In the United States, Europe, Singapore, etc., TikTok has data centers. Which data center the data from different parts of the world flows into will be based on the law first, and then the principle of proximity. For example, in the United States where the situation is special, even if other data centers are geographically more advantageous, data will not flow out of the US border.

"This is a huge project." A person close to Byte's senior management said that the company spent a lot of money to improve this matter, isolating data from all levels, encrypting data, and designing a high-complexity verification mechanism so that people with different permissions " It can not only support the work, but also cannot look at the data."

Byte has also become the most thoroughly localized Chinese technology company. "There is no Internet company in China that can rely on local so much." An employee said. Even the middle office that relies on the headquarters needs to be localized. For example, the user growth middle office that has the key to growth is actually very difficult to recruit overseas. But the US, UK, Japan, Brazil, and Germany all have growth strategy teams. In some markets, for a period of time, the teams on both sides will PK.

The purpose of this is not to compete, but to replace training with competition, so that the Chinese can help the locals grow. The most painful thing is this. The Chinese team expands the market and accumulates methodologies, and then they personally go to the field to recruit local teams and pass on their skills. He clearly knew that the result would be "beat the master to death with random punches". "We worry about whether it will come to us every day," said a witness, "but it is a slow penetration."

Chinese employees complained: "Their work is far less diligent than the Chinese, generally 965 (start at 9 o'clock, leave work at 6 o'clock, and work for 5 days)." "We do what the locals don't do, and they get into trouble." , We want to wipe our ass." And now, "TikTok basically does not recruit people in China, and only those who cannot be recruited abroad are recruited in China."

Globalization has squeezed job opportunities for Chinese people. **The massive "localization" has caused a Chinese citizen to have three choices if he wants to be on the big ship of byte internationalization.** One is to change the permanent residence to Singapore, Los Angeles, etc., so that local data can be accessed; the other is to obtain a U.S. green card and access local data through VPN, but there are permission restrictions; the third is to move from the core department that contacts data to an area that does not need to rely on data , relatively away from the decision center.

After experiencing a great political adventure, although they know that localization is the right path and the only way to go, they are still the sad people on this fleet. Before long, the sad man disembarked.

fleet on the waves

After escaping from the political cracks and realizing that Mayer's appointment was a mistake, Zhang Yiming further pondered his global fleet. **Organization is a delicate art, and the glint of an eye behind a lens is a measure of humanity.**

After May 2021, the top leaders of TikTok are neither Chinese Zhang Nan and Zhu Jun, nor Americans Mayer and Pappas. Zhang Yiming hand-picked Zhou Shouzi, who is of Chinese descent, Singaporean nationality, study abroad background in Britain and the United States, and a handsome and friendly oriental face, as the general manager of TikTok. Many employees told me that this is the result of careful consideration and a "balanced result" in all aspects. "A balance has been found between the West and China."

After arriving at the post, Zhou Shouzi delivered a speech at the all-hands meeting. His handsome appearance and elite background captured the hearts of the people. Employees who did not show up at the scene watched the video, and **the comment section appeared: "So handsome", "A critical hit for appearance", "Maximize my avatar"**. "The funding was perfect," said one employee.

Some employees shrugged and said that what he said was nothing more than "smart talk." "I've listened to it three times."

The script is always: go to school in Singapore, join the army, and go to university in the UK; get acquainted with the famous Russian boss Yuri Milner by chance, and invest in Chinese companies such as Xiaomi, Didi, and Ali during the five years of working in DST; The offer from the business school, regardless of Yuri's persuasion to return to school, Yuri cast a coveted big list during this period, and he expressed his envy and regret. "It's a bit of Versailles, but not annoying." Of course, he focused on how he met Zhang Yiming. The speech was also mixed with a little personal story of meeting a life partner, which boosted the goodwill.

On the fleet pyramid, Zhou Shouzi is at the top. As the chief helmsman, he has two most important generals under his command: one is Chinese Zhu Wenjia, and the other is American Pappas. Zhu Wenjia leads the production and research, and Pappas is in charge of the regional general manager (GM, General Manager), who spends his energy on localized operations.

More intuitively speaking, Zhu Wenjia governs most of the Chinese people, and Pappas governs most of the foreigners; Zhou Shouzi is superior to the two, controlling and balancing

the Chinese and foreigners with his elegant figure of diversity.

Let's first look at the left half of the fleet map.

Zhu Wenjia has dark skin and wears black-rimmed glasses. He is an old Byte employee. He first reported to Yang Zhenyuan, the person in charge of the recommendation algorithm center, and was in charge of Data IES (Interactive Entertainment Community). **This high-tech senior trained in byte culture has a charm similar to Zhang Yiming. He once said in an internal sharing meeting that he could not drive and thought it was a waste of time. He takes a taxi to and from get off work. During the one and a half hours of commuting day after day, Zhu Wenjia would sit in the back seat of a taxi and study his thesis.** Every two weeks, you can finish a doctoral dissertation of a good standard. Doctoral dissertations are more systematic and easy to understand than literature, and are more than 100 pages of English-language readings.

On Byte's management ladder, it was Douyin that allowed him to take a big step forward. When Douyin was far from booming, Zhu Wenjia, as a middle-level staff, led a team to settle in to make recommendation algorithms, and achieved "armed to the teeth" growth. **When Douyin's daily activity exceeded 100 million, he got the highest performance "O" (outstanding) in Byte.** Only those who have made outstanding contributions to the company and who are outstanding can win this honor. It is said that the year-end bonus can be won for 100 months-many colleagues mentioned this and thought it would be a mouth-watering sky-high amount. Then, Zhu Wenjia took the initiative to ask Ying to transform into products and serve as the CEO of Toutiao. Everyone knows that the growth of Toutiao has long since stagnated, and the rise of Douyin has even eroded Toutiao in reverse. But with this training ground, Zhu Wenjia has grown from a person in charge of a simple recommendation



algorithm to a leader with both product and technical capabilities. In February 2021, Zhu Wenjia moved to TikTok with a legend.

The map goes down one level, and several key people report to Zhu Wenjia's solid line or dotted line, namely:

- Liang Yuming, the person in charge of R&D (formerly the head of Hulu China's data and advertising team), reported to Hong Dingkun, the person in charge of Byte Engineering, and reported to Zhu Wenjia with a dotted line.
- Xu Jie, the person in charge of the recommendation algorithm, reported to Zhu Wenjia in real line.
- Tan Siqi, the person in charge of the product (who once worked for Huobi and Xiaohongshu), reported to Zhu Wenjia in real line.
- Wang Leding, the person in charge of the content and style of painting, reported to Zhu Wenjia in real line.
- Wang Yinglei, the person in charge of the live broadcast (who used to start a business and worked in Snapchat), reported to Han Shangyou, the person in charge of Byte Live, and reported to Zhu Wenjia with a dotted line.
- Liu Hanyu, the person in charge of growth (who once worked for Baidu and Tencent), reported to Zhao Qi, the person in charge of Byte User Growth Center, with a solid line, and reported to Zhu Wenjia with a dotted line.

During Zhu Jun's time, TikTok had two popular product leaders: Wang Yinglei (Adam) and Tan Siqi. Wang Yinglei used to be in charge of strategy at TikTok, including "country" and operating products (content understanding and content style); Tan Siqi was in charge of product features.

Byte is a company that is keen to support young people. Wang and Tan can represent the typical portraits of this kind of people—post-90s, winners who have emerged from the education selection system, returnees from prestigious schools, smart and clever; most importantly, Have a sincere heart for the company. Also more obedient.

Among them, Wang Yinglei built a "national" product manager team with more than ten people, acting as a bridge. They stand horizontally in the GM centers in China and various places, channeling divisions and emotions, and carrying business indicators on their shoulders. However, this team seems to be an intermediate form of power transition from China to overseas. When Zhu Wenjia took office, he had already existed in name only. Currently, Wang Yinglei is in charge of TikTok live broadcast; Wang Suiding takes over his remaining operating products (content understanding and content painting style).

Look again at the right half of the map.

Pappas was a tall, powerful woman with short blond hair. **"Her aura makes you feel like a Hollywood star."** She has a strong personality and a meticulous style of handling things. She is one of the few American professional managers who work hard and can swallow the bitter fruit of 996 in Chinese companies. Byte poached her from YouTube.

Employees recalled that in the United States, once night fell, the huge office on the first floor that could accommodate one or two hundred people was empty. In the end, only the Chinese staff, Pappas and the security guard remained in the empty house. "It was like this for almost seven or eight days. I got off work at nine or ten o'clock, and took the lead," the Chinese employee who placed the order said with emotion. "Americans really don't care about the boss's face. Not a single GM left, and all the people below left. gone."

Under Pappas, most of those reporting to her are Local GMs, who hold local jurisdiction:

- The general manager of North America is held by Pappas.
 - The general manager of Europe (excluding Eastern Europe), Rich Waterworth, is a white man with black-rimmed glasses and a burly figure. At the end of 2020, he issued an open letter in the British "Evening Standard", stating that the monthly life in Europe exceeded 100 million.
 - The general manager of Australia is Lee Hunter, who has worked for Google for more than ten years, served as the global brand director of YouTube, and was also the CEO of an ASX-listed company.
 - Yoichi Sato, general manager of Japan, is a Japanese who has worked in Google and Yahoo for many years and is a veteran who has witnessed the changes in Japanese marketing.
 - Qi Qianqian, the general manager of Eastern Europe, is a rare Chinese among GMs. He has working experience in Russia and was once the head of Alibaba Culture Media in Russia.
- ...

On top of the TikTok fleet, there is another person who is a special exception-Erich Andersen. Andersen is American, white-haired, over fifty years old. He serves as the global general counsel of Byte, at the helm of legal affairs, government relations, and public relations. In fact, he took over most of Liu Zhen's power map (Liu Zhen left in May 2020). Andersen shrouded in an aura of mystery. An employee specifically pointed to his name and said to me: **"He can directly contact Zhang Yiming."**

At Byte, Andersen didn't show up right away. Thanks to the political storm, he helped Byte sue the US government and won Zhang Yiming's trust. Andersen once worked for Microsoft, from a legal person, he climbed to the top level step by step, and served as the chief

intellectual property consultant. According to people who know him well, Andersen is based in New York. He is a dignified yet kind leader who tends to understand and encourage his employees. Compared with Liu Zhen, he has more experience from a global perspective—he **used to help American companies enter the Chinese market, and now he helps Chinese companies try to expand the American market.** He might be able to serve as a ballast stone for the fleet when it is subjected to huge waves.

In addition, Blake Chandlee, TikTok's commercial director, and CSO Roland Cloutier also reported to Zhou Shouzi. Before 2021, TikTok did not emphasize commercial indicators such as ad load, and focused on growth; after 2021, TikTok accelerated commercial realization, which made Chandlee play an increasingly important role. His global sales team is like Zhang Lidong's army in Byte China.

In this exquisitely crafted structure, Byte has set up some additional mechanisms with good intentions, which are used to balance human nature and speed up the operation of this giant fleet.

In the past two years, Byte has emphasized the "virtual and real two-line reporting" mechanism. Among them, the balance between the middle office and various business lines is the top priority. Take the user growth center as an example—the person in charge of European growth reports to Zhao Qi, the person in charge of user growth center with a solid line, and reports to Rich Waterworth, the European general manager with a dotted line, so that "Rich can feel safe."

An analyst who has researched TikTok said that the essence of Byte's global management is to "be able to manage and let go." For example, in India, TikTok has done basically every small language. This can only be done by local people - it requires both organizational tolerance and organizational error correction ability.

The wind of PMO (Project Management) has also been popular in Byte in the past two years. The enterprise expands too fast, and departmental walls and poor communication emerge. PMO is countermeasures. Project management personnel serve specific projects, manage project planning and scheduling, and act as "firefighting captains" in case of emergencies. They are like the little motors of the fleet, the lubricants of the main engines. After Zhu Wenjia arrived, he set up a PMO department (Project Manage Office) and established more than 20 project teams.

PMO gives flexibility to business warfare. In April 2021, Kuaishou Overseas will use coins to do fission and usher in a wave of growth. TikTok has set up a special project to block Kuaishou to support user growth in the middle platform. They stare at the rankings of various countries and spend money to implement the order of "list suppression". TikTok is gradually regaining the upper hand.

However, on this fleet, many seemingly high-ranking managers have "limited powers". People who really hold great power keep themselves in mysterious security all the time. The company has set up an information layering mechanism.

It seems that the GM who is in charge of one party has no right to check the s/a/b/c classification of the country under its jurisdiction, especially when the bottom of the level is b/c/other; the company will not let them know that it has allocated other countries how much budget. These will breed internal imbalances and add obstacles to management-Byte sweeps the barriers with one hand to ensure smooth operation; it also buryes barriers with the other hand, putting power under the control of a very small number of people.

10

Plaid shirts, mooncakes, cosmic strips

On the fleet going to sea, Zhou Shouzi is the fifth helmsman. **Zhang Yiming always knows what kind of people should be reused at what stage.**

Row upon row of professional managers —Zhou Jingjin and Liu Xinhua tried and made mistakes for him on the road to internationalization; Liu Zhen helped him build early contacts; Zhang Nan and Zhu Jun alternately straightened out products for him, especially Zhu Jun sewed up part of the cultural barrier; It was supposed to use Mayer's American identity to settle the US government, but the plan fell through; Pappas temporarily filled in the crisis. Employees have long been accustomed to the coming and going of high-level executives, and they sum it up as "completed the phased mission". Now, the ship is in the hands of Zhou Shouzi.

At the beginning, people in business were worried that Zhou only understood finance, strategy and investment, and lacked business understanding, but after a period of time, they found that "a bit exceeded expectations". Moreover, Zhou Shouzi has a high EQ. After he arrived at Byte, he made imperceptible changes.

The most obvious one is that he immediately downgraded from the style of suits and leather shoes and CFO when he was in Xiaomi - he changed into a plaid shirt. One employee even told me exactly that the change happened in his second month on the job. Because in the first month, the company expected him to send the company to the capital palace like Xiaomi did; but in the second month, Byte urgently announced that the listing plan was canceled and extended indefinitely, and he immediately changed his style. . "Like a chameleon."

In order to integrate into Zhang Yiming's culture, many employees observed that Zhou Shouzi quietly emptied Twitter and Instagram. "He is imitating and blending in with the executives here." Lei Jun, his former employer and founder of Xiaomi, is an enthusiastic person who likes high-profile publicity, while Zhang Yiming is the opposite. Zhou Shouzi understood this.

He rarely commented on business details. However, last year, **he proposed a key direction-"depoliticization"**. "Become a pure entertainment product." A person close to TikTok said.

Another thing he ponders over is how to further adjust the organization to reduce cultural shock under the framework of globalization.

Among Chinese companies, ByteDance has become the content platform . Unlike the internationalization , which send Chinese people to leave their hometowns and travel across oceans, and reward them with generous salaries; content products have cultural attributes and regional genes, and Byte recruits a large number of locals. This has led to constant cultural conflicts between Chinese and foreigners—even a few boxes of mooncakes can cause disputes.

Should mooncakes be distributed to Chinese employees only during the Mid-Autumn Festival, or should they be distributed equally to global employees?

In the past, byte chose the previous one. A group of foreign employees complained about being treated unfairly. Later, Byte learned to be smart, and sent a questionnaire in advance to let overseas employees voluntarily choose whether they want mooncakes. There is nothing to criticize about this approach—it provides warmth and leaves room for detours. Unexpectedly, another group of employees headed by Americans stood up and questioned: "This is spreading Chinese culture." Later, the company appeased them.

Chinese emphasize collectivism and are easier to obey; Americans pay attention to individuals since childhood and have a strong sense of individuality. **This forces TikTok to subdue demons and eliminate demons on the way to the sea, and to do spiritual massage in accordance with the unique culture and values of each country** -the latter is a new topic for most Chinese companies.

Some employees said that Byte Overseas, especially American employees, thought in their hearts that they were working for TikTok, not ByteDance. One symptom is that their LinkedIn generally only writes TikTok jobs and does not mention ByteDance.

Therefore, Byte pays special attention to the management of overseas personnel. The TikTok China member meeting is sometimes postponed due to various reasons, but the American member meeting will definitely guarantee it on time. At the same time, Byte is equipped with internal communication personnel in each region. Questions from overseas employees often involve corporate responsibility, human rights, gender equality, and racial equality, and the communicators should coordinate and polish the answers according to local characteristics. In order to cope with the challenges of globalization management, in 2020, Zhang Yiming added a new item to Byte's cultural code: diversity and compatibility.

"TikTok is an excellent case of globalization," a chief analyst at a well-known brokerage told me. "Many overseas users may not know which country TikTok is from."

Byte internationalization has no headquarters. Although the news frequently exposed that they were considering setting up a new headquarters, it has not been settled for a long time. "It hasn't been decided yet, and there may not be a headquarters." An employee said. Even Singapore—where Zhou Shouzi, Zhu Wenjia, and important industry and research personnel are based—is not called a headquarters. Like Zhou Shouzi's glue effect, Singapore is also a place of balance between Eastern and Western civilizations.

Step by step, TikTok has grown into a giant virtual network with invisible nodes, hovering over the world.

In terms of data, TikTok once struggled to catch up with Douyin. Just when it was approaching, India was suddenly blocked, and the daily activities fell by more than 100 million. It took more than a year for TikTok to catch up again. Based on a number of people familiar with the matter, as of the beginning of 2022, TikTok has exceeded 700 million daily active users, and "the growth rate is still very fast." However, Douyin has seen little growth in the past year, with about 670 million daily active users, and TikTok has surpassed it in an all-round way as it wishes. With the combination of the two, this product has broken 1.3 billion daily activities worldwide. At the same time, its download volume has surpassed the overlord Facebook, ranking first in the global social products.

Organizationally, Byte is undergoing a transformation from a mid-stage drive to a business unit drive. Under the background of weakening the middle platform and strengthening the business department, Zhao Qi, the person in charge of the user growth center, handed over the growth of domestic mature business to each business department, and only brought overseas growth; at the same time, he took over the commercial product Pangolin, He was also incorporated into Zhang Lidong's system. "The person in charge of a department that spends the most money has started commercialization, and UG has become a secondary department." People close to byte commercialization believe that this is not only in line with

the current environment of reducing costs and increasing efficiency, reducing fat and reducing weight; Reflects the evolution of TikTok's business stage.

After leapfrogging the most exciting "turning point" in the four stages of business, TikTok no longer relies on the UG middle platform, and the growth flywheel can rotate naturally, and it has come to the final stage: accelerated commercialization. At present, TikTok still has a lot of room for commercialization. According to foreign media reports, TikTok may reach \$11 billion in revenue in 2022. According to the above-mentioned sources, there is a more aggressive target internally, which is between 11 billion and 20 billion US dollars.

And its biggest risk remains geopolitics.

Looking back, after the birth of Douyin and TikTok, Byte employees exploded from 3,000 to more than 130,000 (including outsourcing), more than 40 times; the valuation skyrocketed from 11 billion US dollars to nearly 400 billion US dollars, a rapid increase 36 times. **It "takes off" from the low building where the helicopter can be parked.** This company, which is constantly promoting the reduction of ego, has a spectacular title: the universe strip.

In mid-2021, due to the gratifying data of Douyin and TikTok, Byte held a small-scale celebration. According to people familiar with the matter, when reporting to American shareholders, the president's office staff brought a small cake with a lit candle on it. **Although Zhang Yiming didn't like such a clichéd situation, he still leaned over and blew out the candle.**

After completing the global expansion at a high speed, Zhang Yiming has stepped down as CEO and will retreat to the second line at the end of 2021. Liang Rubo, the current CEO of ByteDance, followed Zhang Yiming to start a business from the university dormitory. He is a more modest, restrained and low-key co-founder than Zhang Yiming. Some insiders reminded me that Liang Rubo has a technical background, which is beneficial to ByteDance's global brand image. His English has improved a lot, and he can already communicate with foreigners fluently. Moreover, the accent is much smaller than that of Zhang Yiming.

Finally, back to twelve years ago, Zhang Yiming and Liang Rubo had just founded their last company, Jiujiufang, and 2010 was the second year of the company. This Christmas, Zhang Yiming watched a movie that influenced a generation of mobile Internet entrepreneurs - the Zuckerberg biopic "Social Network". The founder of the social network who became famous at a young age is born in the 1980s like Zhang Yiming, and Zuckerberg is even one year younger than Zhang Yiming.

After watching the movie, Zhang Yiming clicked on the Douban App and typed a short comment: **"The most impressive word in "The Social Network" is paranoia."** He gave this movie a four-star recommendation.

One year and three months later, Zhang Yiming founded Bytedance. For many years to come, Facebook has been buried in his heart. Now, though, he doesn't mention the company so often.

Just like Zhang Yiming led TikTok to fight against the waves, in this world, **if you are not swallowed by desire, maybe you can swallow desire in one bite.**

- End -

Special thanks: I sincerely appreciate the trust and support of those who are willing to share information with me. **Without your help, the world will know a lot less about TikTok, a milestone product for China to go overseas.**

Notes to the article: 1. The above daily and monthly active data of Douyin and TikTok have not been deduplicated, and there is a situation where a user has multiple accounts. 2. The Facebook company mentioned in the article has changed its name to Meta.

Citation statement: The material is obtained from the author's first-hand interview. If you want to quote the content of the video/article, you need to indicate the source: According to "TikTok Insider: Zhang Yiming's Journey to the Giant Wave".

- You may be interested -

[Douyin Insider: The Birth of the Melting Pot of Time](#)

Modified on 2022-04-25



NCSC under the MOND
Innovation and Training Division
support@ims.nksc.lt

2021-08-23

Assessment of cybersecurity of mobile devices supporting 5G technology sold in Lithuania

ANALYSIS OF PRODUCTS MADE BY *Huawei*, *Xiaomi* and *OnePlus*

Introduction

To ensure the use of secure software and hardware in the country, the National Cyber Security Centre (NCSC) under the Ministry of National Defence carried out a cyber security assessment of mobile devices supporting 5G technology sold in Lithuania by Chinese manufacturers. This analysis presents the results of the assessment of smartphones manufactured by Huawei, Xiaomi and OnePlus.

Huawei, Xiaomi and OnePlus are Chinese IT and consumer electronics manufacturers with an international presence¹ and a strong presence in the European market². In 2020, these manufacturers introduced to the Lithuanian market smartphones supporting fifth-generation (5G) mobile technology. The security assessment was carried out for widely available Huawei P40 5G³, Xiaomi Mi 10T 5G⁴ and OnePlus 8T 5G⁵ mobile devices. Images of the devices examined in the assessment are shown in Figure 1.



Huawei P40 5G

Xiaomi Mi 10T 5G

OnePlus 8T 5G

Figure 1: The devices examined in the assessment. Front and rear panel views

¹ CNET. “Huawei, OnePlus and beyond: China’s biggest smartphone brands you should know about”. <https://www.cnet.com/news/huawei-oneplus-china-biggest-smartphone-brands-you-should-know-about-lenovo-meizu-xiaomi-oppo-vivo/>

² Counterpoint. European Smartphone Market Down 14 % YoY in 2020; Xiaomi Gains While Huawei and Samsung Lose. <https://www.counterpointresearch.com/european-smartphone-market-2020/>

³ Huawei. Technical parameters of Huawei P40 5G. <https://consumer.huawei.com/en/phones/p40-pro/specs/>

⁴ Xiaomi. Technical parameters of Xiaomi Mi 10T 5G. <https://www.mi.com/global/mi-10t-pro/specs/>

⁵ OnePlus. Technical parameters of OnePlus 8T 5G. <https://www.oneplus.com/lt/8t/specs>



Despite these brands being well-known, in the 2017-2021 period the corporations faced security challenges for the equipment being developed; according to the CVE database (Common Vulnerabilities and Exposures), 9 vulnerabilities⁶ related to the risk of personal data leaking were identified for Xiaomi's production (8 of these vulnerabilities could be realised by remote means), 144 vulnerabilities⁷ were identified for Huawei's products during this period (28 vulnerabilities were identified in 2020; 23 in the first half of 2021), most of which were related to disruption of device functionality, and one vulnerability was identified in 2020 allowing an attacker to use third-party software to send SMS text from a mobile device when the mobile device was locked.⁸

Various sources assess that these manufacturers have a leading position^{9,10} in the mobile device market, and their wide assortment of products, their development of new technologies and their noticeable growth in Lithuania undoubtedly make them an appropriate object for cyber security research.

Conclusions of the study

Decomposition analysis performed on mobile devices manufactured by Huawei, Xiaomi and OnePlus identified 10 instances of increased cybersecurity risk. This cybersecurity assessment analyses 4 cybersecurity risks related to the general security of factory-installed applications in the devices, threats of leakage of personal data, and restrictions on freedom of expression. It is planned to describe in detail the other cybersecurity risks identified in this comprehensive study, and to present the assessment of such risks by the end of 2021. This analysis examines issues related to the security of personal data.

The analysis showed that the process of installing mobile applications on Huawei devices is characterised by cybersecurity uncertainties. For the installation of mobile applications on Huawei phones, a manufacturer-based infrastructure is used, which consists of the official electronic application store AppGallery and peripheral application distribution platforms.

When the user intends to install the mobile application on a Huawei device, a search for the mobile application is performed in the AppGallery store; when the application is found, it is downloaded and installed on the mobile device. However, if the application is not found in the official store, the user is automatically directed to peripheral application distribution platforms, from which the mobile application is downloaded to the mobile device for installation. It is worth noting that most of the application distribution platforms are located in countries not covered by the General Data Protection Regulation, which creates a corresponding risk of leakage of user metadata. The study found that a portion of the mobile applications contained on the application distribution platforms are imitations of the original applications, with malicious functionality or virus infestation; such applications can be downloaded and installed by the user on the mobile phone, thereby jeopardising the security of the device and the data contained in it.

Data security risks have also been identified in the Xiaomi device; factory-installed system applications send statistical data on the activity of certain applications installed on the device to servers of the Chinese cloud service provider Tencent, located in Singapore, the USA, the

⁶ CVE database. Publicly announced vulnerabilities in Xiaomi products. https://www.cvedetails.com/vulnerability-list/vendor_id-19038/MI.html

⁷ CVE database. Publicly announced vulnerabilities in Huawei products. <https://www.cvedetails.com/vendor/5979/Huawei.html>

⁸ CVE database. Publicly announced vulnerabilities in OnePlus products. <https://www.cvedetails.com/vendor/16036/Oneplus.html>

⁹ BusinessChief. <https://businesschief.asia/technology/chinese-smartphone-brand-xiaomi-beats-apple-europe-sales>

¹⁰ Fortune. <https://fortune.com/2020/11/25/xiaomi-third-quarter-results-largest-western-europe/>



Netherlands, Germany and India.

It was found that the original browser of the device, Mi Browser, uses two data collection modules: Google Analytics and Sensor Data. The Google Analytics module installed on the device allows the browsing and search history to be read, to send this data to analytics servers which Xiaomi accesses and the data of which Xiaomi uses¹¹. This functionality is activated by registering the mobile phone into the Xiaomi User Experience marketing programme. By default, this is automatically done during the phone's first activation or when reset to factory settings.

The Sensor Data module used in the device has been found to collect statistical information on 61 parameters (time of activation of application, language used, etc.) about the activity of applications used. The collected statistics are sent via an encrypted channel to Xiaomi servers in Singapore, which is not covered by the General Data Protection Regulation. According to international sources, clear cases of unauthorised collection of user data by Xiaomi have been identified^{12,13}. Potentially excessive collection and use of analytical data can be said to pose a threat to the privacy of personal data.

It has also been established that when a user chooses to use Xiaomi cloud services, the user's mobile phone number is registered on servers located in Singapore. This is done by the device sending an encrypted SMS message to a special phone number. After receiving the SMS message, the server synchronises it with the Xiaomi server in Singapore, from which the phone downloads a confirmation via mobile internet, allowing the user to connect to the Xiaomi cloud service. It has been established that the registration of a telephone number is carried out regardless of whether the user chooses to be authenticated by phone number or by e-mail address. It is important to note that the encrypted and sent SMS message and its addressee are not visible to the user.

The automated sending of messages and the software functionality of their concealment pose potential threats to the security of the device and personal data; in this way, without the user's knowledge, device data can be collected and transmitted to remote servers.

The Xiaomi Cloud service is designed to store and synchronise the data stored on the device (data stored in the contact book, call history, SMS messages, photos, notes, Wi-Fi settings and browsing history, etc.) on remote servers. Using this service, user data is sent to servers located in Singapore.

Xiaomi system applications (Security, MiBrowser, Cleaner, MIUI Package Installer and Themes) have been found to regularly download the manufacturer's updated configuration file MiAdBlacklistConfig from a server located in Singapore. This file contains a list composed of the titles, names and other information of various religious and political groups and social movements (at the time the analysis was performed, 449 records were identified in the MiAdBlacklistConfig file). Analysis of the Xiaomi application code showed that the applications have implemented software classes for filtering the target multimedia displayed on the device according to the downloaded MiAdBlacklistConfig list.

This allows a Xiaomi device to perform an analysis of the target multimedia content entering a phone: to search for keywords based on the MiAdBlacklist list received from the server. When it is determined that such content contains keywords from the list, the device blocks this content. It is thought that this functionality can pose potential threats to the free availability of information.

NCSC recommends that users take an interest in the software and hardware used, and responsibly evaluate the proposed functionality of the equipment.

¹¹ Xiaomi. Privacy Policy. https://privacy.mi.com/all/en_IN/

¹² Forbes information. <https://www.forbes.com/sites/thomasbrewster/2020/04/30/exclusive-warning-over-chinese-mobile-giant-xiaomi-recording-millions-of-peoples-private-web-and-phone-use/>

¹³ Android Authority information. <https://www.androidauthority.com/xiaomi-privacy-cheap-phone-1118444/>



Details of the research

The main software characteristics of the mobile devices included in the analysis are listed in Table 1, indicating the operating system (OS) basis, the manufacturer's modification of the operating system basis, the version of the operating system kernel and the dates of security updates.

Table 1. Main software characteristics of mobile devices included in the analysis

Name of device	Huawei P40	Xiaomi Mi 10T	OnePlus 8T
Factory-installed OS basis	Android 10	Android 10 (QKQ.200419.0P2)	Android 11
Manufacturer's modification of factory-installed OS basis	EMUI 10.1.0	MIUI Global 12.0.10 (QJDEUXM)	Oxygen OS 11.0.5.6.KB05BA
Latest available OS basis	Android 10	Android 11	Android 11
Manufacturer's modification of the latest available OS basis	EMUI 11.0.0.151 (C432E5R5P3)	MIUI Global 12.0.2.0 (RJSEUXM)	Oxygen OS 11.0.8.13.KB05AA
Latest available OS release date	2020-12-24	2021-05-25	2021-04-08
OS kernel version	4.14.116	4.19.81-pref-gef23740	4.19.110-pref+
Initial security update package level	2020-04-01	2020-09-01	2020-10-01
Date of most recent security update	2021-06-01 ¹⁴	2021-03-01 ¹⁵	2021-04-01 ¹⁶
Number of security updates	9	3	4

All mobile devices examined are based on the Android operating system; Huawei P40 and Xiaomi Mi 10T use system version 10, while OnePlus 8T uses what is currently the latest system version, 11. It is worth noting that by default the standard Android 11 operating system has wider access control capabilities,¹⁷ enabling the user to better control the access of applications to data stored on the device.

Android operating system security updates are updates to the components of the operating system, designed to correct software vulnerabilities that threaten the security of the device or the data stored on it. These updates are focused on software vulnerabilities allowing remote code execution, elevation of privilege, information disclosure (information leakage), denial of service and other types of attacks. Each of these security updates fixes between 20 and 60 security vulnerabilities listed in the CVE database. It is worth noting that the harmfulness of vulnerabilities ranged between 5.4 and 10.0 points (out of a possible 10 points).

For this reason, it is important for mobile device users to install these updates regularly. These Android operating system security updates are released periodically, every 1-3 months. Xiaomi has committed to delivering these updates to its devices for 2 years¹⁸, and OnePlus has made such a commitment for a period of 3 years¹⁹. Huawei's commitments to supply updates of the operating

¹⁴ Huawei information. <https://consumer.huawei.com/en/support/bulletin/>

¹⁵ Adimorah blog information. <https://adimorahblog.com/new-stable-update-for-the-mi-10t-and-mi-10t-pro/>

¹⁶ OnePlus information.

<https://www.oneplus.com/global/support/softwareupgrade/details?code=PM1605596915581>

¹⁷ Android Authority information. C. Scott Brown, *The best Android 11 features you need to know* <https://www.androidauthority.com/android-11-features-1085228/>

¹⁸ Xiaomi information. <https://www.mi.com/global/service/support/security-update.html>

¹⁹ OnePlus information. <https://forums.oneplus.com/threads/oneplus-software-maintenance-schedule.862347/>



system or operating system security updates were not found. It is worth noting that the maker of the Android operating system, Google, releases security updates for unmodified versions of the Android Open Source Project. For this reason, operating system updates and operating system security updates are available earliest for devices manufactured by Google.

On the other hand, device manufacturers such as Huawei, Xiaomi, OnePlus and others have to adapt the operating system updates or operating system security updates to the manufacturer’s modifications of the operating system basis, so such updates are only available later for these manufacturers’ mobile devices. It is particularly important to emphasise that the latest security updates are available only for the Huawei P40 mobile device. The analysis found that the latest security update for the Xiaomi Mi 10T was 3 months old, and the latest security update for the OnePlus 8T mobile device was 2 months old.

The NCSC notes that, in accordance with the above information, timely security updates for existing devices are essential.

1. Huawei’s official store AppGallery directs users to third-party e-shops in which the applications are malicious or virus-infected

The analysis showed that the process of installing mobile applications on Huawei devices is characterised by cybersecurity uncertainties. For the installation of mobile applications on Huawei phones, a manufacturer-based infrastructure is used, which consists of the official electronic application store AppGallery and peripheral application distribution platforms (APKMonk, APKPure, Aptoide, etc.). A diagram of the Huawei e-shop is shown in Figure 1.

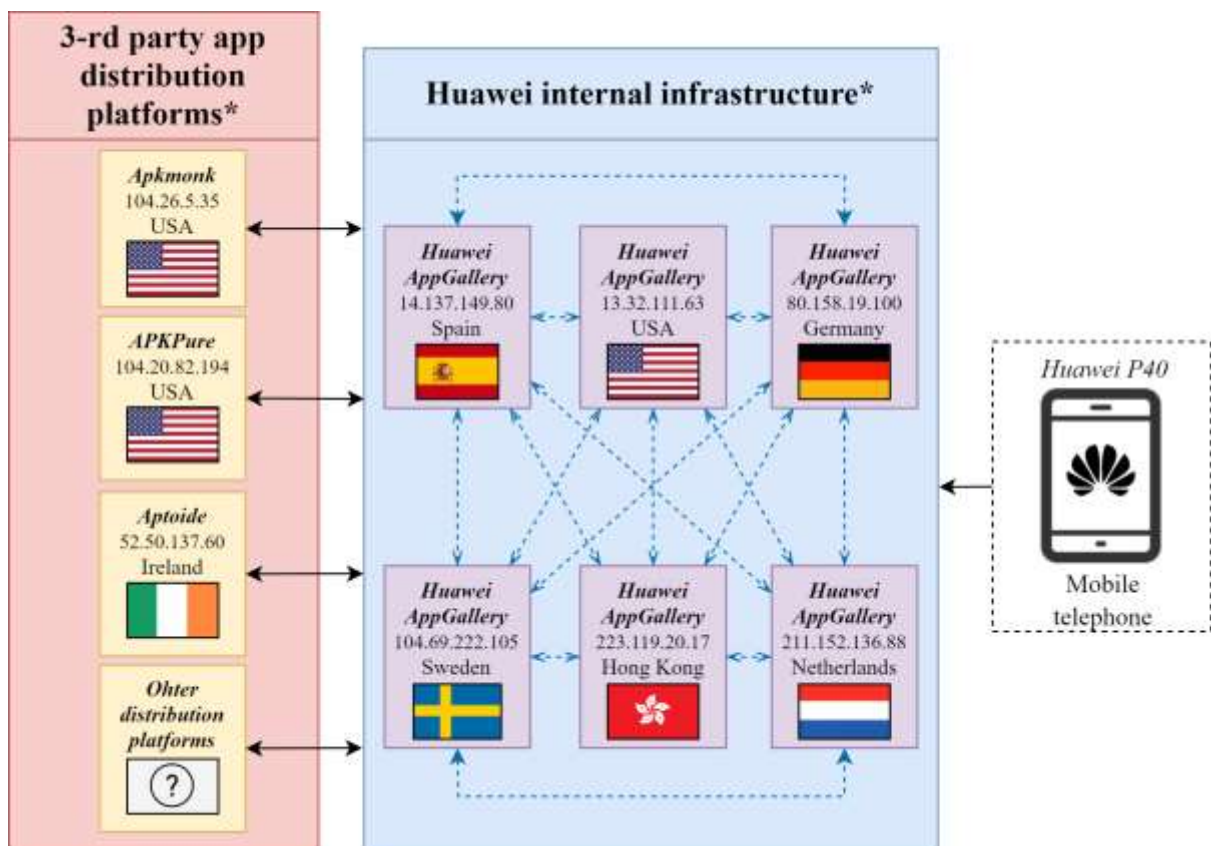


Figure 1: Diagram of Huawei’s mobile-application e-shop



Huawei’s mobile-application e-shop infrastructure consists of two blocks: the internal Huawei AppGallery infrastructure and third-party application distribution platforms. Its own Huawei AppGallery infrastructure has been determined to be located in Spain, the USA, Germany, Sweden, the Netherlands, Hong Kong and Thailand. This infrastructure is integrated with third-party distribution platforms, of which the three best-known operate in the USA, Ireland and the Netherlands. According to various sources²⁰, Huawei’s mobile-application distribution infrastructure currently includes 6-8 third-party distribution platforms. Information about Huawei’s mobile-application distribution infrastructure is presented in Table 2.

Table 2. Information about the Huawei mobile-application distribution infrastructure, indicating the parameters for the internal Huawei AppGallery and the three best-known integrated external distribution platforms

Line No.:	Infrastructure	Address:	IP address	State
1	Internal Huawei AppGallery	appdl-1-drcn.dbankcdn.com.c.dnhwc1.com	223.119.20.17	Hong Kong
2		pay7.hicloud.com	14.137.149.80	Spain
3		appdl-11-dre.dbankcdn.com	13.32.111.63	the USA
4		appdl-11-drcn.dbankcdn.com	65.9.52.144	the USA
5		appdl-2-drcn.dbankcdn.com.cdn.dnsv1.com	211.152.136.88	the Netherlands
6		uc3.hispace.hicloud.com	23.14.13.247	Sweden
7		sdkservice-dre.op.hicloud.com	104.69.222.105	Sweden
8		HWID-dre.platform.hicloud.com	104.69.222.145	Sweden
9		appdl-12-drcn.dbankcdn.com.akamaised.net	184.31.15.17	Sweden
10		appdl-12-dre.dbankcdn.com.akamaised.net	184.31.15.51	Sweden
11		appdl-1-dre.dbankcdn.com.c.dnhwc1.com	119.46.76.15	Thailand
12		appdl-1-dre.dbankcdn.com.c.dnhwc1.com	119.46.76.17	Thailand
13		appstore.huawei.com	80.158.2.135	Germany
14		metrics2.data.hicloud.com	80.158.2.190	Germany
15		www.hicloud.com	80.158.19.100	Germany
16		query.hicloud.com	80.158.19.121	Germany
17		grs.dbankcloud.com	80.158.20.103	Germany
18		Jos.hicloud.com	80.158.23.247	Germany
19		iap.hicloud.com	80.158.40.92	Germany
20		appdl-2-dre.dbankcdn.com.cdn.dnsv1.com	101.33.11.29	Germany
21		appdl-2-drcn.dbankcdn.com.cdn.dnsv1.com	101.33.11.45	Germany
22		appdl-4-drcn.dbankcdn.com	163.171.128.127	Germany
23		appdl-4-drcn.dbankcdn.com	163.171.128.129	Germany
24	External platform APKMonk	www.apkmonk.com	104.26.4.35	the USA
25	External platform APKPure	download.apkpure.com	104.20.83.194	the USA
26	External platform Aptoide	en.aptoide.com	34.249.219.183	Ireland
27		ws75.aptoide.com	34.254.115.204	Ireland
28		ws75.aptoide.com	52.17.222.230	Ireland
29		en.aptoide.com	52.50.137.60	Ireland
30		rakam-api.aptoide.com	52.209.136.146	Ireland
31		pnp.aptoide.com	54.194.247.193	Ireland
32		en.aptoide.com	54.220.86.7	Ireland
33		ws75.aptoide.com	54.229.235.132	Ireland
34		CDN-mobile.aptoide.com	172.67.29.206	the USA
35		pool.apk.aptoide.com	5.79.110.134	the Netherlands
36		apkins.aptoide.com	95.211.168.137	the Netherlands
37		apkins.aptoide.com	95.211.223.52	the Netherlands

²⁰ XDA-Developers information. <https://www.xda-developers.com/petal-search-download-apps-huawei-honor-smartphones-hms/>



When the user installs a mobile application on a Huawei device, a search for the mobile application is performed in the AppGallery store; when the application is found, it is downloaded and installed on the mobile device. The mobile-application installation scheme using the Huawei AppGallery platform is presented in Figure 2.

When the name of an application is entered in the search box of the Huawei AppGallery application, a list of search results is generated. The search results window contains the Petal Search section. When the Petal Search is selected, the user is shown a list of applications accessible through third-party application distribution platforms (1). When a user selects an application from this section, a warning message (2) is displayed. The warning message indicates that further actions will occur outside the Huawei AppGallery application.

When the user closes the warning window, the web browser is opened on the device, the user is redirected to the third-party application distribution platform. If the user selects the application-installation file download option (3) on the platform, the file is downloaded and saved in the device's internal memory (4, 5). Once the device completes the process of downloading the application-installation file, the installation of the application starts.

Since in this case the installation of the application is initiated by the web browser of the device, the user is shown an information window (6) requesting authorisation to initiate the application installation procedure using the web browser. Once the user has given permission, an application-installation window (7) is shown, which again requests user input to start the installation. Once the user has reconfirmed the application-installation, the application is installed (8, 9) and an icon for the newly-installed application is added to the main window (10).

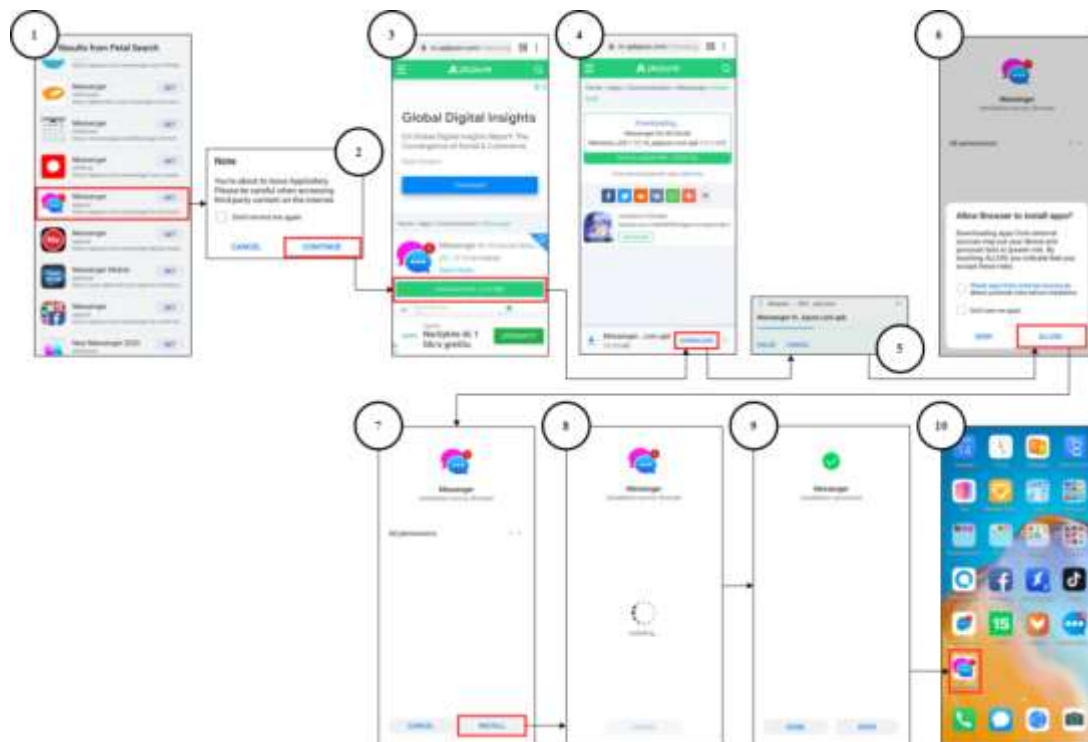


Figure 2: Mobile application installation scheme using the Huawei AppGallery platform

If the application being searched for is not available in the Huawei AppGallery store, the user is



automatically redirected to peripheral third-party application distribution platforms, from which the mobile application is downloaded to the phone for installation.

The analysis found that a portion of the mobile applications available at such distribution platforms are fakes of the authentic applications, with malicious functionality or virus infestation; such applications can be downloaded and installed by the user on a mobile phone, thereby jeopardising the security of the device and the data contained in it.

A schematic diagram of the installation of a Huawei application, including third-party distribution platforms for their installation, is shown in Figure 3.

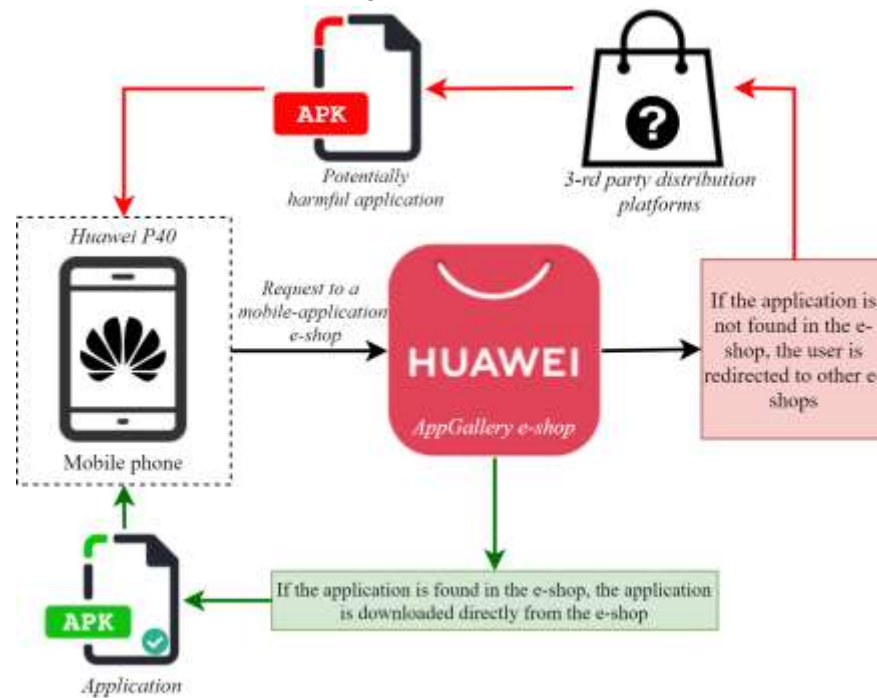


Figure 3: Schematic diagram for the installation of a Huawei application, including third-party distribution platforms

It is worth noting that part of the application-distribution infrastructure used by Huawei is located in countries not covered by the General Data Protection Regulation. It is important to note that a mobile device downloading an application from a mobile-application e-shop located in a country covered by the GDPR can execute requests to third countries not covered by the Regulation. This creates a corresponding risk of leakage of user metadata.

The analysis examined the AppGallery e-shop operating in the Huawei infrastructure and three of the best-known integrated third-party distribution platforms, APKMonk, Aptoide and APKPure. It is worth noting that information on APKMonk and APKPure developers could not be found in freely-available sources. According to Aptoide²¹, the headquarters of the distribution platform is registered in Portugal (Lisbon), and the company's branches operate in China (Shenzhen) and Singapore.

The analysis monitored traffic as applications were downloaded from sources used in the Huawei infrastructure. During the research, applications were searched for in the Huawei AppGallery e-shop, without changing the sequence for download of applications as originally set by the manufacturers; the applications were downloaded directly from the original e-shop and from the third-party application distribution platforms provided by AppGallery.

When recording the number of connections, it was found that during the downloading of an application from the original AppGallery e-shop, requests to 38 addresses were identified, and in the

²¹ Aptoide information. <https://en.aptoide.com/company/about-us>



case of APKMonk, 56 addresses. The highest number of requests was identified for Aptoide and APKPure; respectively, 74 and 73 addresses.

Information illustrating Huawei mobile device requests during application download procedures is shown in Figure 4.

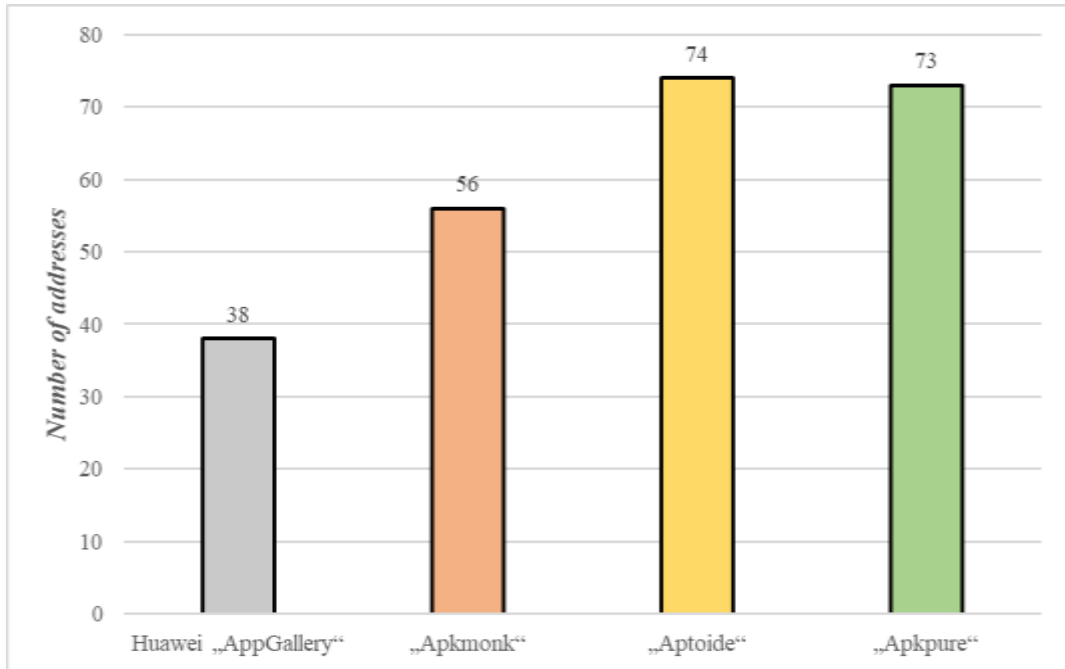


Figure 4: Number of Huawei mobile device requests during application download procedures

More detailed information on the countries to which the requests were directed and the number of such requests is given in Figures 5 through 7.

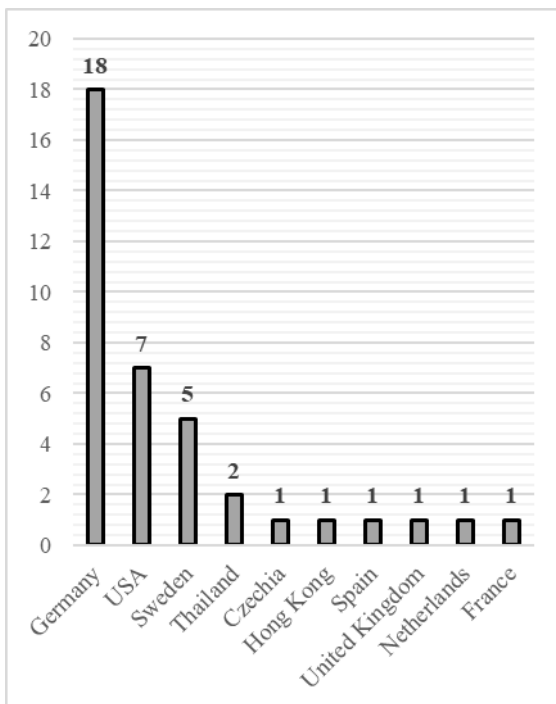


Figure 5: Huawei AppGallery request information

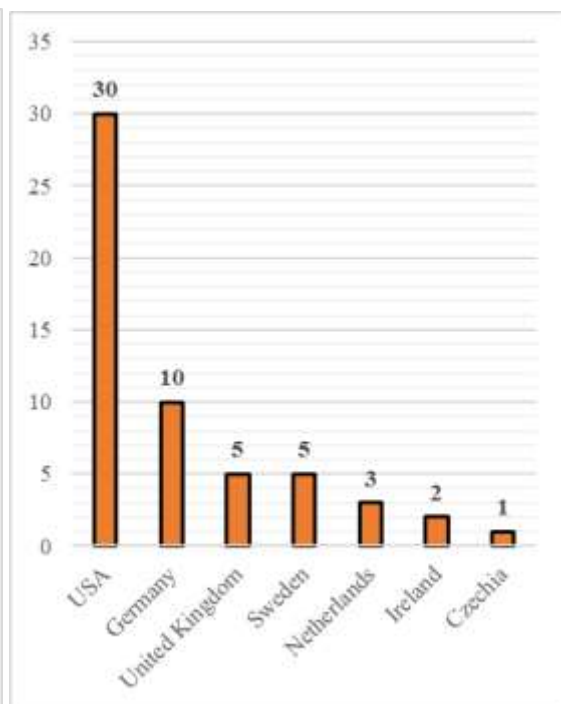


Figure 6: Distribution platform APKMonk request information

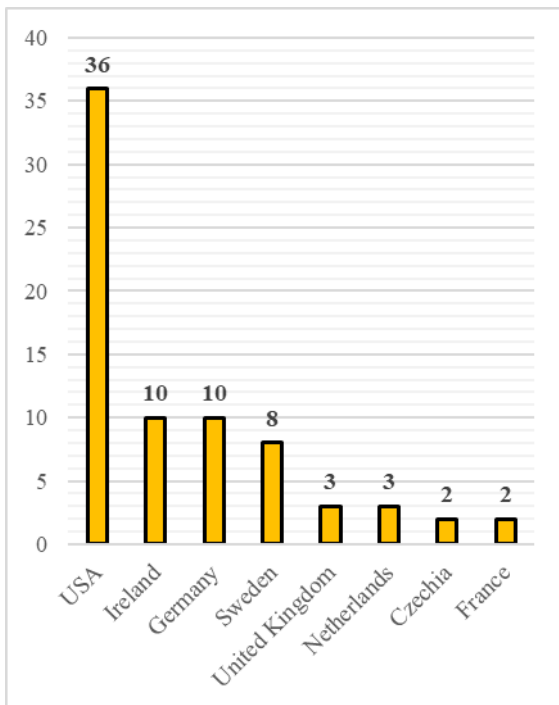


Figure 7: Distribution platform Aptoide request information

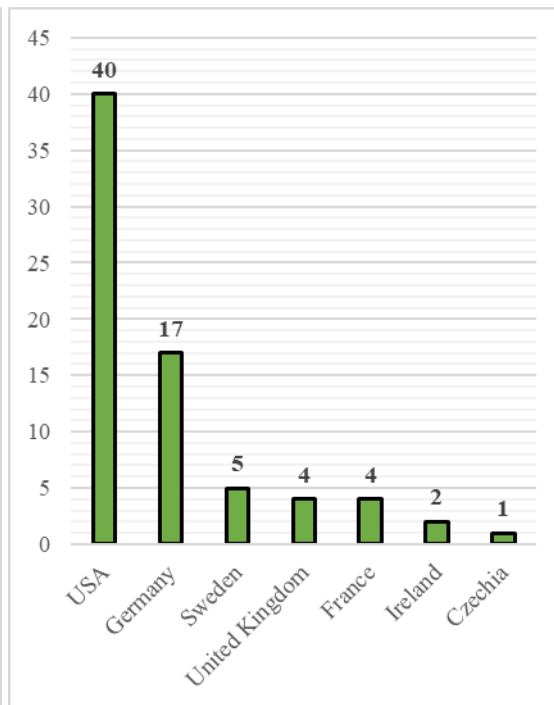


Figure 8: Distribution platform APKPure request information

More detailed analytical information with specific IP addresses and countries is provided in Table 3.

Table 3. More detailed analytical information with specific IP addresses and countries

Line No.:	Huawei AppGallery		APKMonk		Aptoide		APKPure	
	Address	State	Address	State	Address	State	Address	State
1	apkrep.ns1.ff.avast.com	Czechia	34.250.145.50	Ireland	i.w.inmobi.com	Ireland	apkrep.ns1.ff.avast.com	Czechia
2	appdl-1-drcn.dbankcdn.com.cdnhwel.com	Hong Kong	52.209.136.146	Ireland	en.aptoide.com	Ireland	sync.crwdcntrl.net	Ireland
3	pay7.hicloud.com	Spain	5.62.53.15	Czechia	ws75.aptoide.com	Ireland	52.209.246.140	Ireland
4	8.8.8.8	the USA	appimg3.dbankcdn.com	the USA	ws75.aptoide.com	Ireland	13.32.111.63	the USA
5	appdl-11-dre.dbankcdn.com	the USA	13.33.242.107	the USA	webservices.aptwords.net	Ireland	feeds.apyhi.com	the USA
6	13.33.242.98	the USA	auction.unityads.unity3d.com	the USA	en.aptoide.com	Ireland	34.98.67.61	the USA
7	13.107.213.44	the USA	odr.mookie1.com	the USA	rakam-api.aptoide.com	Ireland	34.236.65.196	the USA
8	52.177.138.113	the USA	auction.unityads.unity3d.com	the USA	pnp.aptoide.com	Ireland	rtb.openx.net	the USA
9	appdl-11-drcn.dbankcdn.com	the USA	auction.unityads.unity3d.com	the USA	en.aptoide.com	Ireland	35.244.159.8	the USA
10	152.199.21.230	the USA	EU-u.openx.net	the USA	ws75.aptoide.com	Ireland	35.244.174.68	the USA
11	5.62.36.56	the UK	id.rlcdn.com	the USA	apkrep.ns1.ff.avast.com	Czechia	65.9.52.144	the USA
12	appdl-2-drcn.dbankcdn.com	the Netherlands	52.85.48.221	the USA	5.62.53.117	Czechia	download.apkpure.com	the USA



	n.com.cdn.dnsv1.com							
13	www.petalsearch.com	France	52.154.69.245	the USA	wv.inner-active.mobi	the USA	104.26.4.35	the USA
14	uc3.hispacelcloud.com	Sweden	65.9.53.128	the USA	wv.inner-active.mobi	the USA	partner.googleadservices.com	the USA
15	sdkservredre.op.hicloud.com	Sweden	104.21.35.78	the USA	8.8.8.8	the USA	pagead2.googleadsyndication.com	the USA
16	HWID-dre.platform.hicloud.com	Sweden	www.apkmonk.com	the USA	test.quantcast.mgr.consensu.org	the USA	142.250.74.100	the USA
17	appdl-12-drcn.dbankcdn.com.akamaised.net	Sweden	104.197.172.31	the USA	quantcast.mgr.consensu.org	the USA	s0.2mdn.net	the USA
18	appdl-12-dre.dbankcdn.com.akamaised.net	Sweden	partner.googleadservices.com	the USA	auction.unityads.unity3d.com	the USA	firebaseemotefconfig.googleapis.com	the USA
19	appdl-1-dre.dbankcdn.com.c.cdnhwcl.com	Thailand	142.250.74.35	the USA	Publisher-config.unityads.unity3d.com	the USA	app-measurement.com	the USA
20	appdl-1-dre.dbankcdn.com.c.cdnhwcl.com	Thailand	adservice.google.com	the USA	www.datadoghq-browser-agent.com	the USA	adservice.google.com	the USA
21	appstore.huawei.com	Germany	142.250.74.100	the USA	sdktm.w.inmobi.com	the USA	Firestore-settings.crashlytics.com	the USA
22	80.158.2.189	Germany	142.250.74.102	the USA	rules.quantcount.com	the USA	142.250.74.136	the USA
23	metrics2.data.hicloud.com	Germany	142.250.74.129	the USA	104.21.35.78	the USA	142.250.74.142	the USA
24	80.158.16.161	Germany	142.250.74.130	the USA	config.inmobi.com	the USA	Sync-tm.everesttech.net	the USA
25	www.hicloud.com	Germany	um.simplifi	the USA	142.250.74.2	the USA	152.199.21.230	the USA
26	query.hicloud.com	Germany	172.67.29.206	the USA	www.googletagmanager.com	the USA	172.67.68.182	the USA
27	grs.dbankcloud.com	Germany	tpc.googleadsyndication.com	the USA	partner.googleadservices.com	the USA	172.217.20.33	the USA
28	80.158.20.104	Germany	googleads4.g.doubleclick.net	the USA	connectivitycheck.gstatic.com	the USA	googleads.g.doubleclick.net	the USA
29	Jos.hicloud.com	Germany	www.gstatic.com	the USA	firebaseinstallations.googleapis.com	the USA	172.217.20.35	the USA
30	iap.hicloud.com	Germany	172.217.21.161	the USA	cdn.ampproject.org	the USA	tpc.googleadsyndication.com	the USA
31	80.158.54.98	Germany	ade.googleadsyndication.com	the USA	adservice.google.com	the USA	172.217.21.130	the USA
32	appdl-2-dre.dbankcdn.com.cdn.dnsv1.com	Germany	cm.g.doubleclick.net	the USA	www.google.com	the USA	www.gstatic.com	the USA
33	appdl-2-drcn.dbankcdn.com.cdn.dnsv1.com	Germany	192.48.236.3	the USA	pagead-googlehosted.l.google.com	the USA	ade.googleadsyndication.com	the USA
34	160.44.194.86	Germany	Pixel-sync.sitescout.com	the UK	142.250.74.130	the USA	www.google.com	the USA
35	160.44.199.4	Germany	openx2-match.dotomi.com	the UK	Firestore-settings.crashlytics.com	the USA	172.217.21.166	the USA
36	160.44.207.213	Germany	91.228.74.189	the UK	softonic.map.fastly.net	the USA	172.217.21.170	the USA
37	appdl-4-drcn.dbankcdn.com	Germany	image6.pubmatics.com	the UK	api.facebook.com	the USA	172.217.22.162	the USA



38	appdl-4-drcn.dbankedn.com	Germany	188.125.94.206	the UK	connect.facebookk.net	the USA	raw.githubusercontent.com	the USA		
39			81.171.20.104	the Netherlands	www.facebook.com	the USA	216.58.207.206	the USA		
40			95.211.137.160	the Netherlands	CDN-mobile.aptoide.com	the USA	www.gstatic.com	the USA		
41			ib.adnxs.com	the Netherlands	tpc.google syndication.com	the USA	firebaseinstallations.googleapis.com	the USA		
42			store3.hispaced.icloud.com	Sweden	fonts.gstatic.com	the USA	cm.g.doubleclick.net	the USA		
43			104.73.93.58	Sweden	pagead-googlehosted.l.google.com	the USA	216.58.211.130	the USA		
44			tls.adobe.com	Sweden	adservice.google.com	the USA	ad.turn.com	the UK		
45			sdkservers-dre.op.hicloud.com	Sweden	fonts.googleapis.com	the USA	185.29.135.233	the UK		
46			sdkservers-dre.op.hicloud.com.edgekey.net	Sweden	ads.mopub.com	the USA	185.64.190.78	the UK		
47			j.mrpdata.net	Germany	ads.mopub.com	the USA	212.82.100.176	the UK		
48			23.193.116.193	Germany	app-measurement.com	the USA	51.75.146.159	France		
49			metrics2.data.hicloud.com	Germany	pixel.quantserve.com	the UK	pixel.onaudience.com	France		
50			platform.hicloud.com	Germany	185.64.190.78	the UK	D-08.winudf.com	France		
51			grs.dbankcloud.com	Germany	data.flurry.com	the UK	green.erne.co	France		
52			appgallery.cloud.huawei.com	Germany	pool.apk.aptoide.com	the Netherlands	dsum-sec.casalemedia.com	Sweden		
53			JFS-dre.jos.hicloud.com	Germany	apkins.aptoide.com	the Netherlands	store3.hispaced.icloud.com	Sweden		
54			80.158.34.57	Germany	apkins.aptoide.com	the Netherlands	sdkservers-dre.op.hicloud.com.edgekey.net	Sweden		
55			160.44.199.4	Germany	id5-sync.com	France	HWID-dre.platform.hicloud.com	Sweden		
56			160.44.202.175	Germany	51.255.81.18	France	sdkservers-dre.op.hicloud.com	Sweden		
57							2.18.33.213	Sweden	3.66.135.160	Germany
58							z.moatads.com	Sweden	tracking.justpremium.com	Germany
59							store3.hispaced.icloud.com	Sweden	49.51.130.46	Germany
60							d.applovin.com	Sweden	pixel.rubiconproject.net.akadns.net	Germany
61							sdkservers-dre.op.hicloud.com	Sweden	80.158.2.189	Germany
62							sdkservers-dre.op.hicloud.com.edgekey.net	Sweden	metrics2.data.hicloud.com	Germany
63							cdn2.inneractive.mobi	Sweden	OAuth-login-dre.platform.dbankcloud.com	Germany
64							webview.unityads.unity3d.com	Sweden	80.158.19.69	Germany
65							api.vungle.com	Germany	80.158.19.100	Germany



66			ads.api.vungle.com	Germany	80.158.19.121	Germany
67			metrics2.data.hicloud.com	Germany	80.158.20.104	Germany
68			OAuth-login-dre.platform.dbankcloud.com	Germany	JFS-dre.jos.hicloud.com	Germany
69			JFS-dre.jos.hicloud.com	Germany	80.158.34.57	Germany
70			cloud.hicloud.com	Germany	grs.dbankcloud.com	Germany
71			80.158.40.21	Germany	80.158.44.234	Germany
72			appdlssl.hicloud.com	Germany	101.33.11.48	Germany
73			160.44.199.4	Germany	160.44.199.4	Germany
74			connectivitycheck.platform.hicloud.com	Germany		

The analysis found that when downloading an application from the Huawei infrastructure, a redirection to third-party application distribution platforms was carried out, from which applications with potentially malicious code were downloaded. A summary of the security analysis of mobile applications downloaded by a Huawei device from the Huawei infrastructure is presented in Table 4. The security analysis was performed with the well-known file analysis tool VirusTotal²².

Table 4. Summary of downloaded mobile applications after inspection using VirusTotal

Line No.:	Application name	Identifier	Application version	VirusTotal result
1	Social Media	com.social.messenger.allinoneapps	14	<i>Malicious software:</i> A.gray.andrsca.f
2	Web Machinist Mobile Pro Tapping	com.webmachinist.cncmachinisttappingcalculator	1.0	<i>Virus:</i> Trojan.Trojan.Banker.AndroidOS.Agent.ed
3	Messenger All in One	comm.essagechat.listing	28.0	<i>Malicious software:</i> Adware/Loead for Android.fyben.a

The research analysed three mobile applications downloaded from Huawei mobile application distribution infrastructure servers. According to VirusTotal scanning data, it was determined by one antivirus system that potentially malicious software, A.gray.andrsca.f, was installed in the Social Media application. After examining another mobile application, Web Machinist Mobile Pro Tapping, downloaded from Huawei infrastructure servers, one VirusTotal antivirus system identified a potential virus, Trojan.Trojan.Banker.AndroidOS.Agent.ed. This virus can carry out²³ theft of data for connection to banking systems. In the third application that was analysed, Messenger All in One, two antivirus systems found that the application uses potentially malicious software, the packages Adware/Loead and Android.fyben.a.

This raises serious concerns about the security of the device, as not all third-party application distribution platforms perform verification of uploaded applications.

This infrastructure security vulnerability can be exploited by obtaining original (authentic) applications from the Google Play Store, decompiling the application and then applying the necessary modifications to the content of the decompiled application by adding malicious code. The application code with malicious content is then recompiled, packaged and signed with a new private key. The modified application is uploaded to the above-mentioned third-party application distribution

²² VirusTotal information. <https://www.virustotal.com/gui/>

²³ Clavister information. <https://www.clavister.com/advisor/antivirus/view/?id=544073>



platforms. An associative diagram of this process²⁴ is given in Figure 9.

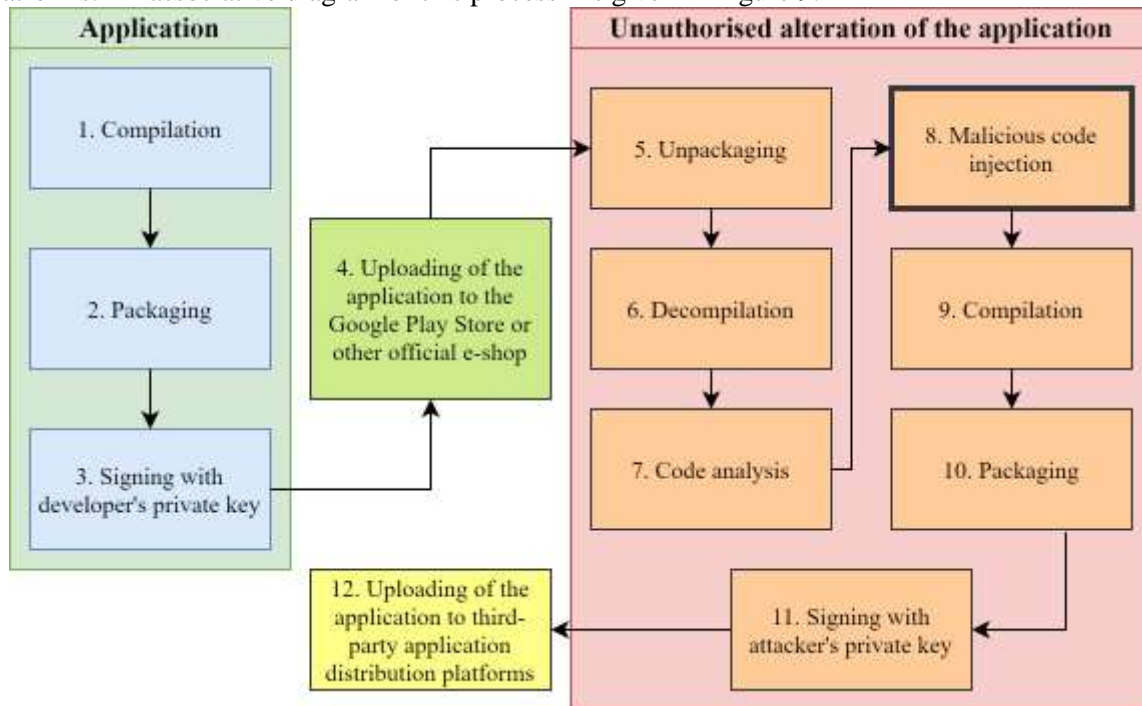


Figure 9: Associative diagram of malicious code insertion into a mobile application

An application developer compiles the code during application development and thus forms a functioning application. This application is packaged in the installation file and signed with the application developer's private key. The signed installation file for the application can be uploaded to application stores such as Google Play Store.

An attacker, like all users of application stores (except for relevant regional restrictions) can download this application; once received from official sources, it is unpacked and decompiled into the application code. This allows an attacker to perform analysis of the application, to determine the viability of the installation site of the malicious code and the installation technology to be used, and to insert malicious code into the application. After completion of malicious code insertion procedures, the application code is recompiled and packaged into an installation file, which is signed with the attacker's private key. The generated malicious application installation file is uploaded to third-party application distribution platforms, where not all uploaded applications are checked.

Virus-containing e-shops have been found to be a serious problem for these stores²⁵. A user who installs a virus-infected application may suffer from the collection or leaking of data stored in the device or an associated cloud service, or from damage to the mobile device.

The analysis found that a portion of the mobile applications available in the application distribution platforms are fakes of original (authentic) applications, with malicious functionality or virus infestation; such applications can be downloaded and installed by the user on a mobile phone, thereby jeopardising the security of the device and the data contained in it.

²⁴ Springer info. Repackaging Attack on Android Banking Applications and Its Countermeasures. <https://link.springer.com/article/10.1007/s11277-013-1258-x>

²⁵ P. Kotzias et al. How Did That Get In My Phone? Unwanted App Distribution on Android Devices. <https://arxiv.org/pdf/2010.10088.pdf>



2. Devices designed and manufactured in China access servers in third countries. This allows for the collection and aggregation of user metadata, and based on such data to monitor users

Analysis of decompiled software and data flows showed that Mi Browser uses two data collection modules: Google Analytics and Sensors Data. Sensors Data is a platform of Chinese origin, in functionality close to Google Analytics. According to the Sensors Data company,²⁶ it has more than 1,500 customers, including some of the largest corporations in the People's Republic of China, such as China Telecom, Baidu, CYTS, Sichuan Airlines, etc.

Google Analytics is an analytics platform for programmers or administrators to access information allowing them to evaluate the use of applications in the iOS, Android or web environments²⁷. Google Analytics automatically generates an event log allowing evaluation of the performance of an application. It is worth noting that developers have the technical ability to select the parameters to be analysed, and to set the depth of the analysis of such parameters.

It was found that this module can collect data about user browsing, clicks, etc., and send information for possible analysis to Google servers. It should be noted that these modules are activated at the time of initial switching-on of the device, upon consent to participate in the Xiaomi User Experience programme.

Having decompiled the Xiaomi device's factory-installed system applications, it was found that the functionality of these analytics applications was installed and operated in the standard internet browser of the Xiaomi phone, Mi Browser. Table 5 shows a fragment of Mi Browser code, denoting the Google Analytics functionality.

Table 5. Fragment of Mi Browser code, denoting the Google Analytics functionality

```
public static void reportAsync(String str, Map<String, Object> map) {  
if (!TextUtils.isEmpty(str) && !BrowserSettings.getInstance().isNotAllowCollectData) {  
BrowserReportUtils.stripUrlIfNecessary(map);  
BackgroundThread.postOnIOThread(new Runnable(str, map)  
{  
public final /* synthetic */ String f$0;  
public final /* synthetic */ Map f$1;  
{  
this.f$0 = r1;  
this.f$1 = r2;  
}  
Public final void run {  
FirebaseReportHelper.report(this.f$0, this.f$1);  
}  
});  
}  
}
```

In the code fragment displayed in the table, the function for sending data to the Firebase analytics platform on Google servers is implemented. Table 6 shows a fragment of Sensors Data code installed in the Mi Browser application. In the code fragment, the function that launches Sensors Data functionality in the Mi Browser application is presented.

Table 6. Fragment of Sensors Data startup code in the Mi Browser application

²⁶ Sensors Data information. <https://www.sensorsdata.cn/about/aboutus-en.html>

²⁷ Google Firebase information. <https://firebase.google.com/docs/analytics/get-started>



11	swipe_up	What function is registered for the swipe-up motion
12	current_default_search_engine	Current search engine used
13	language	Language set in the system
14	language_browser	Language setting in the browser
15	icon_reddot_status	—
16	user_newsfeed	Is the news stream disabled
17	user_download_videos	—
18	user_night_mode	Whether the browser uses night mode
19	dark_mode	Whether the system uses night mode
20	user_data_save_mode	Whether data-saving functionality is activated in the browser
21	user_incognito_mode	Is Incognito Mode enabled
22	user_desktop_mode	Browser's user-agent
23	user_checkbox_4G	Is browser updating via 4G allowed
24	user_push_agree	Whether browser notifications are activated
25	user_facebook_notification	Whether Facebook messages have been activated in the browser
26	user_youtube_signin	Whether the user is logged in to YouTube
27	user_click_interest	Shows how many times the user clicked on cards in the browser (news, YouTube recommendations, etc.)
28	user_login	Whether the user is logged in to Mi Account
29	adblock_switch	Is the ad-blocking function activated
30	adblock_show_notification	Is Adblock enabled
31	first_enter_newsfeed_way	Is the news stream window enabled for the first time
32	Fandst_appstart_source	—
33	first_appstart_third_party	—
34	Miu_personalised	Whether personalised advertising is activated
35	personalised_services	Whether personalised content recommendations have been activated
36	browser_ads	—
37	protection_type	—
38	app_boot_third_party	—
39	app_boot	Start-up time of the programme
40	feed_default_channel	—
41	experience_improve	Is Xiaomi User Experience activated
42	platform	Platform. Always Android
43	Miu_version	MIUI version
44	log_miaccount	Whether the user is logged in to the Mi account
45	MUI_region	Mi region
46	EID	—
47	apk_name	Application APK name
48	browser_install_referrer	—
49	Autocomplete_switch	Is AutoComplete in the search window activated
50	No_track_switch	Is the Do Not Track function enabled
51	bookmark_sync	Is synchronisation of bookmarks with the Mi server activated
52	history_sync	Is synchronisation of browsing history with the Mi server activated



53	feature_report_switch	Whether the user participates in the Xiaomi User Experience programme
54	clear_history_switch	Whether browsing history is deleted when the application is closed
55	personal_service_switch	Whether the functionality of user recommendations is enabled: personalised YouTube clips, etc.
56	enhanced_incognito_switch	Is Incognito enabled
57	user_tab_news	Has the user enabled the news tab
58	user_tab_games	Has the user enabled the games tab
59	search_optimization_switch	Constant, always equal to 1
60	cookie_status	Provides data about user cookie settings
61	subscription	Indicates whether a VPN is used and, if so, its identifier

During the analysis, full decoding and decryption of Xiaomi encrypted messages was carried out. Xiaomi’s phone has been found to send Sensors Data data in a Base64 dataset, which is additionally encoded using the *urlencode* algorithm. An example of a fragment of encoded data sent is given in Table 8.

Table 8. Fragment of data sent by a Xiaomi phone

zzvhrYfjw6d%2FA8RXtmQLWd2RTDyUWp5DBsFc55eI9yBbDRONrH12GSsq8SRDUtyJ8PquOrUqpsID g6qvSg%2FksVvDG3gcl6SWzk9uL4hWhOCpEw%2B%2BzMBq0KctqdOkn4kljhDgt CfdRixfrJe8PHTjr8x1cK5xMHHISL0MK%2FWu3utqKnuhf1UQGi64uYDCp%2FeEZ1MdakDE%2BLXsF 4wZKGiftO64 %2B8liP1NvxV1%2BsgTutVEbroI%2FWJUJkz9MfZyvL6OAPG6z9rRbJ354mUo6 %2BOMwZdN%2BAuWSzRz8IKITU6HwNZGMB0xmPDB8tSTM7ehnya%2FyAiHPqOIXD7IYzrvupBJT rZLCXLQzbTgIxtZG65KvV7yfgiwMhCxY%2Bkg0t3d0LXlJOOorQqFfsqJW%2B6LnWvE6lKdm7 %2BCPydhautVIgiMSZDi94iH%2FuYL%2B2dkmLxSjQFQh51FSBA%2BygRzfCItmL87KjjgT0t3 %2BmtvO%2Bs93IH72rC6ai0Y5kdIIdSuIg6A%2BomC73JYOeHygMR0jmjCjM5 %2FiUANqsH XPfoeaGBn8F%2FV1vik03CPbetK3yzfwLn9ZpkmzO64Ic%2BEsRNTgNk7jc0mKZrsisWs4IPO1e

Table 9 shows the decrypted content of data sent by Xiaomi’s phone to Sensors Data servers located in Singapore. Data sent for analysis: application version, application name, current region, device manufacturer, etc.

Table 9. Content sent by a Xiaomi phone to Sensors Data servers in Singapore

<pre>{ "_track_id": 1687170607, for Time: 1623852507838, for 'type': track, for 'distinct_id': '7d03ab71-91b1-47ca-8f56-0ce2d77f6c86', for Lib: { For \$Lib: Android, For \$lib_version: "4.0.3-pre", For \$app_version: '12.4.1-g', For \$lib_method: 'code', "\$lib_detail": "com.android.browser.BrowserActivity#####", }, for Event: "\$AppStart", for Properties: { For \$Lib: Android, "\$os_version": '10',</pre>
--



```

For $lib_version: "4.0.3-pre",
For $Model: 'M2007J3SY',
'$s': Android,
"$screen_width": 1080,
For $screen_height: 2400,
For $Manufacturer: 'Xiaomi',
For $app_version: '12.4.1-g',
for Platform: AndroidApp,
for 'miui_version': 'V12.0.18.0.QJDEUXM',
"log_miaccount": 0,
'miui_region': "LT",
for EID: "channel_en_youtube-web",
"apk_name": "com.mi.globalbrowser",
"browser_install_referrer": Google-play,
"autocomplete_switch": 1,
"no_track_switch": '2',
bookmark_sync: 1,
for 'history_sync': 1,
'feature_report_switch': 1,
"clear_data_switch": 0,
"personal_service_switch": 1,
"enhanced_incognito_switch": 0,
'hashtag_follow_count': 0,
'hashtag_follow_list': "",
"account_follow_count": 0,
"account_follow_list": "",
"feed_default_channel": "",
For $WiFi: True,
For $network_type: WIFI,
"$resume_from_background": True,
"$is_first_time": false,
"$screen_name": "com.android.browser.BrowserActivity",
For $title: 'Mi Browser',
"$is_first_day": True
}
    
```

Sensors Data data was found to be sent to the address <https://sa.api.intl.miui.com>. Table 10 provides information that characterises the analytical data transmitted over the network to servers located in Singapore.

Table 10. Characteristics of data sent by Sensors Data

Line No.:	IP address	Data sent, <i>B</i>	Data received, <i>B</i>	Total data, <i>B</i>	State
1	47.241.109.186	11789	0	11789	Singapore
2	161.117.9.4	4318		4318	
3	161.117.84.89	13386		13386	
4	161.117.189.14	1230		1230	
5	161.117.230.146	5294		5294	

The collected statistics are sent through an encrypted channel to Xiaomi servers in Singapore, which is a country not covered by the General Data Protection Regulation. Potentially excessive collection and use of analytical data can be said to pose a threat to the privacy of personal data.

Figure 10 shows the Sensors Data data encryption mechanism that was recreated during the



analysis, used to establish the data link between the device and the servers located in Singapore.

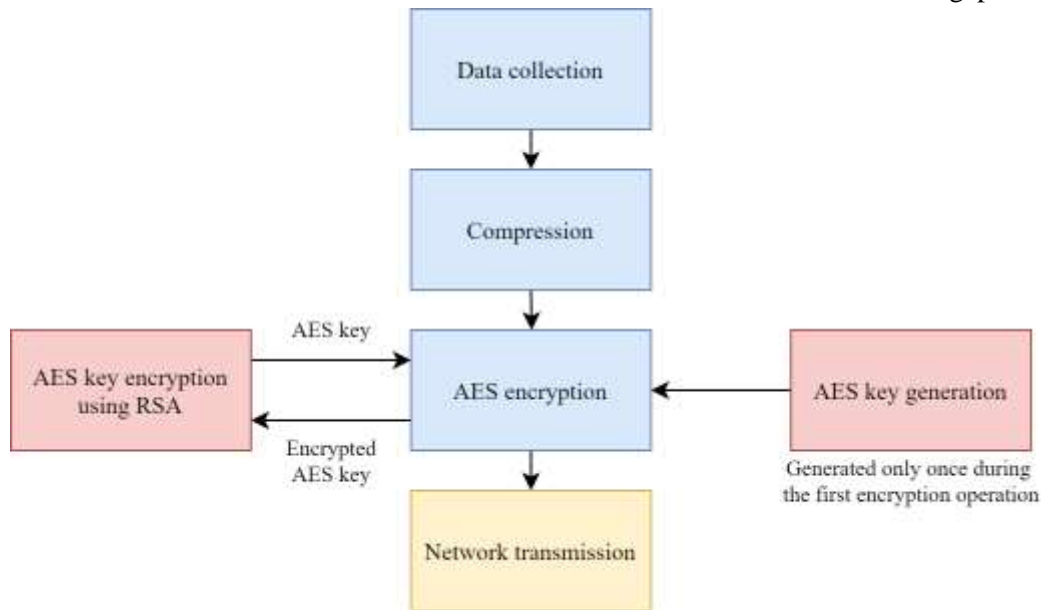


Figure 10: Data encryption mechanism used by Xiaomi

The encrypted dataset is generated by calling Sensors Data software installed in the Mi Browser: *registerSuperProperties* and *registerDynamicSuperProperties*. These functions are responsible for data collection and preparation of the JSON object. When the dataset is to be sent, it is first converted into a byte expression and archived using the *gzip* algorithm.

This is done to reduce the amount of data sent. The result is encrypted using the AES128-CBC algorithm. A key is generated using the device's pseudorandom number generator. After that, the key used in the AES encryption is encrypted by the RSA algorithm, using a public key downloaded from Xiaomi servers. The resulting dataset is packaged into a JSON object and sent to servers in Singapore.

The application calls the functions *registerSuperProperties* and *registerDynamicSuperProperties*. These functions are responsible for collecting data and preparing JSON objects. It can be said that the Sensors Data encryption mechanism ensures a relatively high level of data security when transmitting such data to the analytics servers located in Singapore.

The Google Analytics module installed on the device allows the Mi Browser browsing history, search results and other parameters of application activity to be read, and to send this data to the analytics servers. Data is sent via an encrypted TLS channel using Protobuf encoding. Decoding data without a Protobuf configuration file is impossible or difficult, but certain data can be discerned in the encrypted stream: the internet address opened in MI Browser, data entered in the search field or an action performed by the user (e.g., a click on the search field).

This data can be accessed and used by the application developer, Xiaomi.²⁸ An encoded fragment of data sent to Google Analytics servers is presented in Table 11.

²⁸ Xiaomi information. https://privacy.mi.com/all/en_US/



Table 11. Encoded fragment of outgoing data sent by a Xiaomi device to Google Analytics servers

```

event_network r:LT|285
_oapp_scBrowserActivity_siçÈ³¼å°òT

“urlr
:LT|https://nksc.lt/çb|;/ý Âicon_oapp op

r:LT|wifi_ifremind r

:LT|remind languager
:LT|en
is_system_languager
:LT|1sourcer:LT|search_icon_oapp op

r:LT|show_scBrowserActivity_siçÈ³¼å°òTweb_translate_op²

“ýæ/ñ@ý/event_network

r:
LT|wifiënter_wayr:LT|searchBar_website_oapp_scBrowserActivity_siçÈ³¼å°òT imp_search_page Ìæýæ
event_network r

:LT|323
_oapp_scBrowserActivity_siçÈ³¼å°òT urlr:LT|https://kam.lt
    
```

Table 12 presents information characterising the analytical data transmitted by the Xiaomi device through the network to Google Analytics servers.

Table 12. Characteristics of data sent to Google Analytics servers

Line No.:	IP address	Data sent, B	Data received, B	Total data, B	State
1	142.250.74.110	2545	0	2545	the USA
2	172.217.16.14	1282		1282	
3	216.58.207.206	12699		12699	

Based on the findings, it can be said that Xiaomi collects a relatively large amount of information about the processes running on the device, the behaviour of installed software packages, the actions performed by users and the configuration parameters of applications. Two analytics systems, Sensors Data and Google Analytics, are used to implement this process. An overview of sources found that Xiaomi devices collect a wider range of data compared to other manufacturers of



mobile devices^{29, 30, 31}.

Potentially excessive collection and use of analytical data can be said to pose a threat to the privacy of personal data.

3. The functionality implemented on a Xiaomi device can limit the free availability of information

It has been established that during the initialisation of the system applications factory-installed on a Xiaomi Mi 10T device, these applications contact a server in Singapore at the address `globalapi.ad.xiaomi.com` (IP address 47.241.69.153) and download the JSON file `MiAdBlacklistConfig`, and save this file in the metadata catalogues of the applications. A list of applications for which the `MiAdBlacklistConfig` file was found in metadata catalogues is presented in Table 13.

Table 13. List of mobile applications using the `MiAdBlacklistConfig` file

Line No.:	Application name	Application identifier	Device
1	Security	<i>com.miui.securitycenter</i>	Xiaomi Mi 10T
2	Mi Browser	<i>com.mi.globalbrowser</i>	
3	Downloads	<i>com.android.providers.downloads.ui</i>	
4	Music	<i>com.miui.player</i>	
5	Themes	<i>com.android.thememanager</i>	
6	MIUI Package Installer	<i>com.miui.global.packageinstaller</i>	
7	Cleaner	<i>com.miui.cleanmaster</i>	

Once the applications have downloaded the file, the download date is recorded in order to facilitate periodically updating the list. The scheme for downloading the `MiAdBlacklistConfig` file is shown in Figure 11.

²⁹ Apple Privacy Policy. <https://www.apple.com/legal/privacy/en-ww/>

³⁰ Douglas J. Leith. Mobile Handset Privacy: Measuring the Data iOS and Android Send to Apple and Google. https://www.scss.tcd.ie/doug.leith/apple_google.pdf

³¹ Xiaomi Privacy Policy. https://privacy.mi.com/all/en_IN/

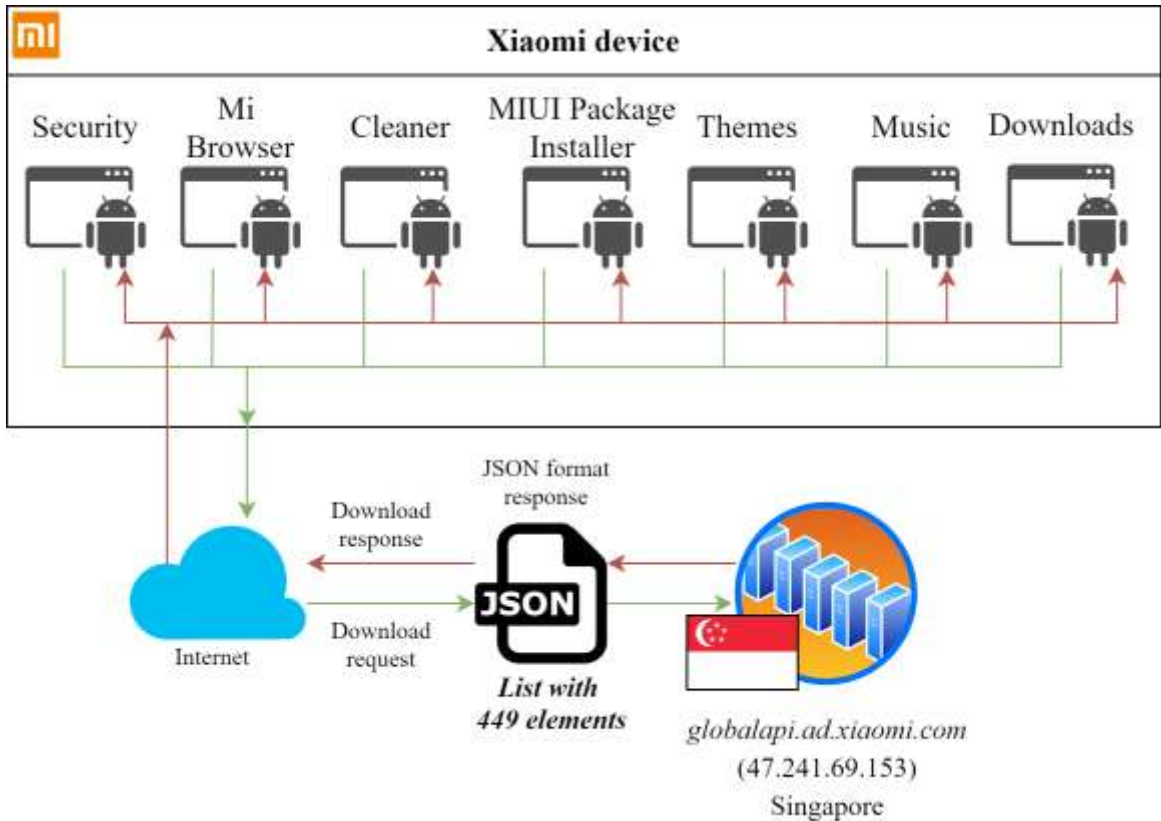


Figure 11. MiAdBlacklistConfig download scheme

This file contains a list composed of the titles, names and other information of various religious and political groups and social movements (at the time of the analysis, the MiAdBlacklistConfig file contained 449 elements). A fragment of the MiAdBlacklistConfig file is shown in Table 14.

Table 14. Fragment of the MiAdBlacklistConfig file

Line No.:	Original	Approximate translation
1	"宗教虔信者阵线",	"Front of religious believers",
	...	
22	"西藏自由",	"Free Tibet",
	...	
60	"蒙古独立",	"Independence of Mongolia",
61	"89民运",	"89 Democracy Movement",
62	"基督灵恩布道团",	"Christian charismatic mission",
	...	
145	"伊斯兰联盟",	"Islamic League",
	...	
201	"民运",	"Democratic Movement",
202	"妇女委员会",	"Women's Committee",
203	"伊斯兰马格里布基地组织",	"Al-Qaida in the Islamic Maghreb",
204	"人民报",	"People's daily newspaper",
205	"巴勒斯坦解放组织",	"The Organisation for the Liberation of Palestine",



		...
313	"台独万岁",	"Long live Taiwan's independence",
		...
369	"美国之音",	"The Voice of America",
		...
420	"89运动",	"89 Movement",
		...
449	"夏米斯丁艾合麦提·阿布都米吉提"	"Xia Misteen Ahemet Abu Dumijiti"

Analysis of the Xiaomi application code showed that the applications have implemented software classes for filtering the target multimedia displayed on the device based on the downloaded list in the MiAdBlacklistConfig file. A fragment of this code is shown in Table 16.

Table 16. A fragment of content filtering code used in a Xiaomi device

```
public boolean mo76794a(INativeAd iNativeAd, C8380a Avar) {
    if (iNativeAd == null) {
        return true;
    }
    Long currentTimeMillis = System.currentTimeMillis();
    for (String str: new HashSet(this.f11160b))
    {if (iNativeAd.getAdTitle!= null &AMP; &m12161a (iNativeAd.getAdTitle, str)
    ) {MLog.m6439d(MiAdBlacklistConfig, Ads: “ + iNativeAd.getAdTitle + “is blocked by title word: “ + Art);
    IF (Avar!= null) {
    aVar.f11165a= Art;
    }
    this.f11161c = Art;
    return true;
    } other if (iNativeAd.getAdBody!= null &AMP; &m12161a (iNativeAd.getAdBody, str))
    {MLog.m6439d(MiAdBlacklistConfig),Ads: [” + iNativeAd.getAdBody + “] is blocked by desc word: “ +
    Art);
    IF (Avar!= null) {
    aVar.f11165a= Art;
    }
    this.f11161c = Art;
    return true;
    }
    MLog.m6443i
    (MiAdBlacklistConfig, isAdsBlocked—> totalTime=” + (System.currentTimeMillis – currentTimeMillis)+
    “&threadId=” + Thread.currentThread.getId);
    return false;
    }
```

After analysing the Mi Browser, it was found that the application performs the download functionality of the MiAdBlacklistConfig file, but does not filter the content according to the list in the MiAdBlacklistConfig file. Based on the Xiaomi code, this functionality has been deactivated in “the European Union region”. The event registration content generated by the Mi Browser is presented in Table 17.

Table 17. Event registration content generated by the Mi Browser

Line No.:	Name of function	Parameter 1	Parameter 2
1	MLog.d	MiAdBlacklistConfig	start to request url
2	MLog.d	ConfigRequestCommon	UserAgent: Dalvik/2.1.0 (Linux; U; Android 10;



			M2007J3SY MIUI/V12.0.18.0.QJDEUXM)
3	MLog.d	MiAdBlacklistConfig	handleResponse
4	MLog.d	MiAdBlacklistConfig	request retry: success reset times
5	MLog.d	MiAdBlacklistConfig	response parsed success
6	MLog.d	MiAdBlacklistConfig	updateAdConfig
7	MLog.d	MiAdBlacklistConfig	notifyAllObservers
8	I:	NativeAdManagerInternal	posid[1.306.1.3],requestAd isPreload: false
9	I:	NativeAdManagerInternal	AdSwitch expired: new query from remote
10	I:	AdSwitchUtils	AdSwitchOFF is false
...			
23	I:	AdReportTask	{“mEvent”：“LOAD_AD”,“mPositionId”：“1,306.1.3” ;“mAppId”：“10000”,“mChannelId”：“miui”,“mOpera tor”：“246_01”,“mClientVersion”：“100492”,“mSdkV ersion”：“130200”,“mAdTime”：“1621431087190”, mModel: M2007J3SY,mGaid:“d3a32b43-6e7e- 4306-82ca- 0f65f1586511”,“mLanguage”：“en_US”,“mBuildSdk Version”：“29”,“mDoNotTrack”：“false”,“mBuildTyp e”：“stable”, muiVersion:“V12.0.18.0.QJDEUXM”,“mRegion”：“ LT”,“mTriggerId”：“9d1f86e3-579e-4110-b71e- 065f520c1fa3”, “mIsPreload”：“false”,“mCustomKey”：“adsCnt”,“mC ustomValue”：“0”,“mInstaller”：“com.xiaomi.discover ”,“mIsPreInstall”：0,mElapsed:0,mIsid:0}
24	I:	MIADSDK	Personalised ad is disabled in the EU region, reporting is not allowed
25	I:	MIADSDK	Personalised ad is disabled in the EU region, reporting is not allowed
...			
38	I:	AdReportTask	{“mEvent”：“PAGE_VIEW”,“mPositionId”：“1.306.1 .3”,“mAppId”：“10000”,“mChannelId”：“miui”,“mOp erator”：“246_01”,“mClientVersion”：“100492”,“mSd kVersion”：“130200”,“mAdTime”：“1621431420870” , mModel: M2007J3SY,mGaid:“d3a32b43-6e7e- 4306-82ca- 0f65f1586511”,“mLanguage”：“en_US”,“mBuildSdk Version”：“29”,“mDoNotTrack”：“false”,“mBuildTyp e”：“stable”, muiVersion:“V12.0.18.0.QJDEUXM”,mRegion:“LT ”,“mTriggerId”：“9d1f86e3-579e-4110-b71e- 065f520c1fa3”,mInstaller:“com.xiaomi.discover”,“m IsPreInstall”：0,“mElapsed”：0,“mIsBid”：0,“mCost”：3 33682}

It is believed that this functionality allows a Xiaomi device to perform an analysis of the target multimedia content entering the phone; to search for keywords based on the MiAdBlacklist list received from the server. Once the device determines that the content contains certain keywords, the device performs filtering of this content and the user cannot see it. The principle of data analysis allows analysis not only of words written in letters; the list that is regularly downloaded from the



server can be formed in any language. It is important to emphasise that this functionality is activated remotely by the manufacturer. It is believed that the existence of such functionality may jeopardise free access to information and limit its accessibility. It can be said that this is important not only for Lithuania, but also for all countries using Xiaomi devices.

4. On Xiaomi devices, to connect to the cloud, it is necessary to register a SIM card. Sent messages are not displayed on the phone. The risk of leakage of user data

Studies have shown that when a user chooses to use Xiaomi Cloud services, the user's mobile phone number is registered on servers located in Singapore. This is done by the device sending an encrypted SMS message to a special phone number. The registration procedure for Xiaomi Cloud services is performed on the Xiaomi device by sending an SMS message as shown in Figure 12.

When a user attempts to connect to the Xiaomi Cloud service for the first time, the device requests access to a (1) Xiaomi Account. After entering login data and successfully logging in to the account, a menu window (2) opens in which it is possible to enable and disable the main Xiaomi Cloud functions: data synchronisation and device geolocation in case of loss of a device.

After selecting the desired functions, the service operating in the background starts the SIM card data collection procedures (3, 4 and 5). After the service completes the SIM card data collection procedures, the user is shown an information window (6) indicating that in order to enable the functionality of call history and message synchronisation, the device must send an SMS to check the phone number.

It is also indicated in the information window that the user may be charged for sending an SMS message at the standard rates of the mobile telecommunications operator (provider). When the user closes the information window, the user is shown an operating system window (7), which asks the user whether to allow the SIM card registration service to send SMS messages automatically. With the user's consent, an automated telephone number registration procedure is launched (8).

The device downloads from the **general** server the configuration data structure for the procedure, which includes the address of the server with which further network communication is to be carried out, the phone number of the SMS addressee and other parameters. The device then generates an SMS message and sends the message to the phone number specified in the configuration data structure (9). The sent message is immediately deleted from the sent message log.

At the same time, the collected SIM card data is stored in the internal service database (10). After sending the SMS message, its content is encrypted and sent to a server, the address of which is specified in the configuration data structure, together with a query for confirmation of registration (11).

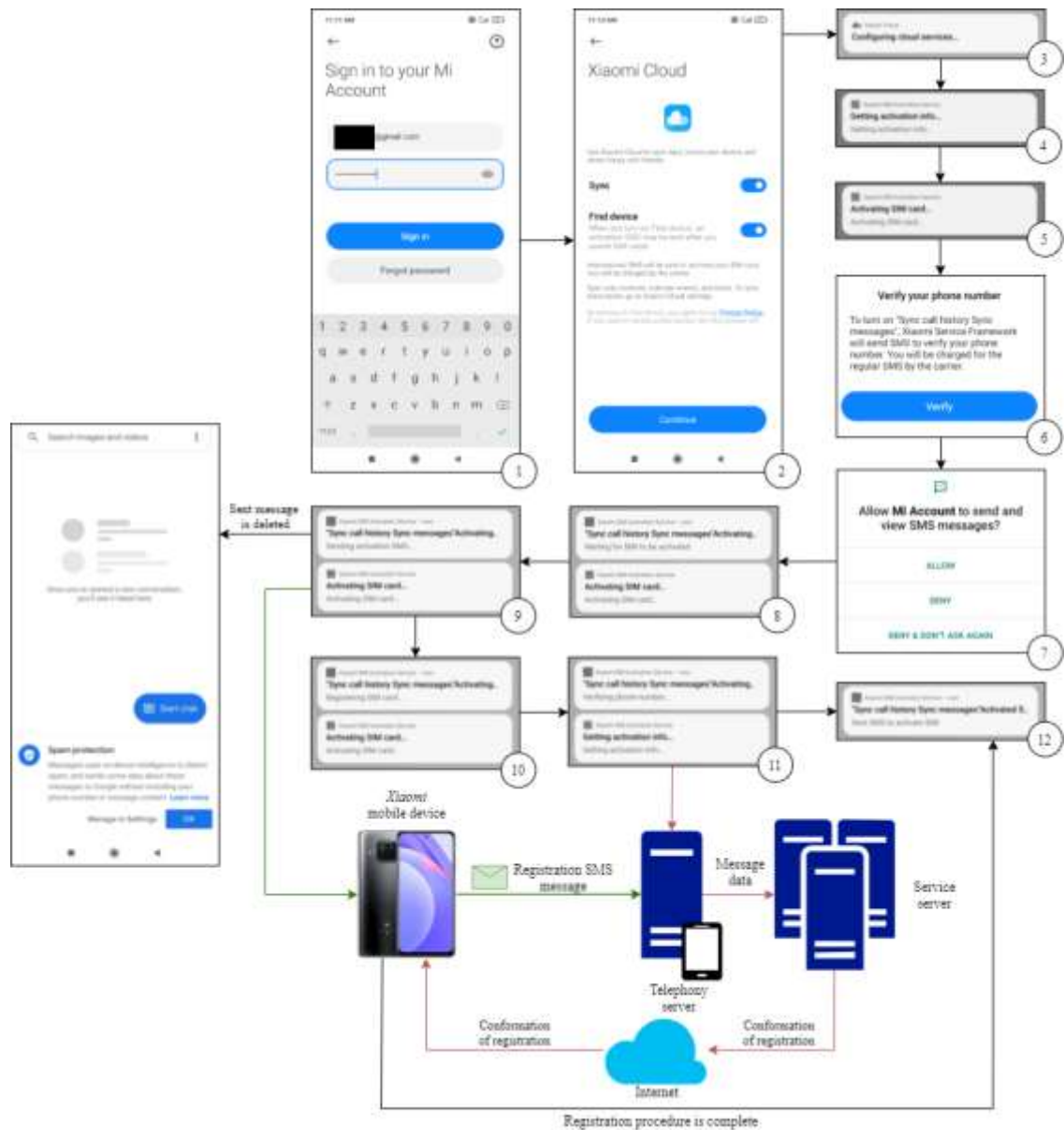


Figure 12. Registration procedure for Xiaomi Cloud services performed on a phone by sending an SMS message

After sending a registration query to the server, the device receives a response to the query, displaying a registration result (positive or negative) (12).

It has been established that the registration of a telephone number is carried out regardless of how the user chooses to be authenticated, either by phone number or by e-mail address. It is important to note that the sent encrypted SMS message and its addressee are not visible to the user. At the time of the analysis, after disabling the functionality of the Xiaomi Cloud service, the sending of messages was not observed. A more detailed network flow diagram is given in Figure 13.

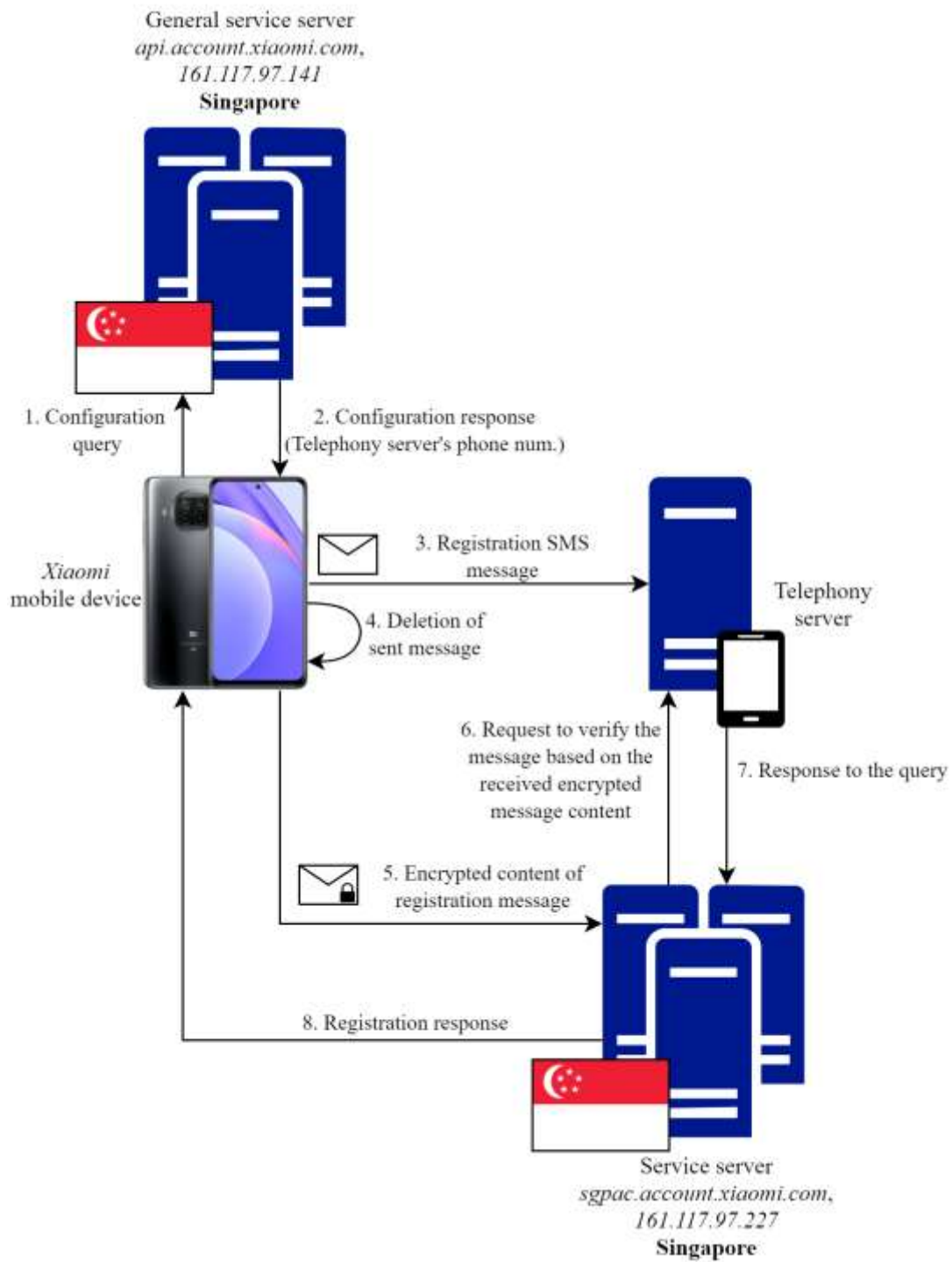


Figure 13. Registration scheme for the Xiaomi Cloud services network

Once the phone number registration process has started, the device sends a query to a general server located in Singapore (1), from which it receives a data structure as a response. This data structure includes the address of the target server for this service, the number of the telephony server and other parameters used for the registration procedure (2). The device then generates and sends an SMS message to the phone number specified in the received data structure (3). The message sent is immediately deleted from the sent message log (4). After sending the message, the device contacts the server located in Singapore and sends to the telephony server the encrypted content of the sent



structure.

During the analysis of the phone number registration service Xiaomi SIM Activation Service, it was established that the device performs the function of automatic sending of an SMS message. The addressee of the SMS message and the content of the message are shown in Figure 14.

```
[M2007J3SY::com.xiaomi.simactivate.service]-> com.xiaomi.activate.sys.MiuiSysImpl --- sendTextMessage  
com.xiaomi.activate.sys.MiuiSysImpl --- +37066803015 --- null --- AC/7ae6742e79d0b5937c3c7Feba2bc:60bf88c59725e8e8/8  
:MI
```

Figure 14. Content of the SMS message and process of sending

After analysing the decompiled factory-installed system service Xiaomi SIM Activation Service, it was found that the application performs the function of automatic sending of an SMS message using the external software class `miui.telephony.SmsManager`, which is not compiled and is archived in the service installation file.

A fragment of the code for sending the SMS message is given in Table 19.

Table 19. Fragment of the code for sending the SMS message

```
public void sendTextMessage(int i, String str2, String str3, PendingIntent pendingIntent, PendingIntent  
pendingIntent2) {  
    try {  
        class<?> cls = Class.forName(miui.telephony.SmsManager);  
        Object raise = cls.getDeclaredMethod(getDefault, new Class {Integer.TYPE}).invoke((Object) null, new  
Object {Integer.valueOf(i)});  
        CLS.getMethod(sendTextMessage, new Class {String.class, String.class, String.class, PendingIntent.class,  
PendingIntent.class}).invoke(raise, new Object {str, str2, str3, pendingIntent, pendingIntent2});  
        Log.d(MiuiSysImpl, "successfully send text message");  
    } catch (NoSuchMethodException e) {  
        Log.e(MiuiSysImpl, "error when send text message: NoSuchMethodException, e);  
        throw new RuntimeException(e);  
    } catch (IllegalAccessException e2) {  
        Log.e(MiuiSysImpl, "error when send text message: IllegalAccessException, e2);  
        throw new RuntimeException(e2);  
    } catch (InvocationTargetException e3) {  
        Log.e(MiuiSysImpl, "error when send text message: InvocationTargetException, e3);  
        throw new RuntimeException(e3);  
    } catch (ClassNotFoundException e4) {  
        Log.e(MiuiSysImpl, "error when send text message: ClassNotFoundException, e4);  
        throw new RuntimeException(e4);  
    } catch (SecurityException e5  
) { ActivateLog.m24w(MiSysImpl, sendTextMessage, e5);  
    }  
}
```

It is worth noting that in the above-mentioned external software class `miui.telephony.SmsManager`, there is an implemented functionality allowing deletion of SMS messages. The functions of sending and deleting SMS messages, and other functions implemented in the external software class `miui.telephony.SmsManager`, are shown in Figure 15.



```

public boolean miui.telephony.SmsManager.copyMessageToIcc(byte[],byte[],int)
public boolean miui.telephony.SmsManager.deleteMessageFromIcc(int)
public java.util.ArrayList miui.telephony.SmsManager.divideMessage(java.lang.Str
ing)
public boolean java.lang.Object.equals(java.lang.Object)
public java.util.ArrayList miui.telephony.SmsManager.getAllMessagesFromIcc()
public final java.lang.Class java.lang.Object.getClass()
public static miui.telephony.SmsManager miui.telephony.SmsManager.getDefault()
public static miui.telephony.SmsManager miui.telephony.SmsManager.getDefault(int
)
public int java.lang.Object.hashCode()
public final native void java.lang.Object.notify()
public final native void java.lang.Object.notifyAll()
public void miui.telephony.SmsManager.sendMultipartTextMessage(java.lang.String,
java.lang.String,java.util.ArrayList,java.util.ArrayList,java.util.ArrayList)
public void miui.telephony.SmsManager.sendMultipartTextMessage(java.lang.String,
java.lang.String,java.util.ArrayList,java.util.ArrayList,java.util.ArrayList,int
,boolean,int)
public void miui.telephony.SmsManager.sendTextMessage(java.lang.String,java.lang
.String,java.lang.String,android.app.PendingIntent,android.app.PendingIntent)
public java.lang.String java.lang.Object.toString()
public final void java.lang.Object.wait() throws java.lang.InterruptedException
public final void java.lang.Object.wait(long) throws java.lang.InterruptExcept
ion
public final native void java.lang.Object.wait(long,int) throws java.lang.Interr
uptedException
[Ljava.lang.reflect.Method;@f852a37
function d() {
    [native code]
}
[M2007J17G::com.xiaomi.simactivate.service]-> |
    
```

Figure 15. Functions of sending and deleting SMS messages, and other functions, implemented in the external software class miui.telephony.SmsManager

When the device sends an SMS message to the phone number specified in the configuration data structure, the device sends the encrypted content of the SMS message to the address sgpac.account.xiaomi.com (Singapore).

The server performs content verification against the received encrypted data with the SMS message data received by the telephony server and sends the activation result to the mobile device. An extract of the network traffic is given in Table 20.

Table 20. Communication with the server located in Singapore

Post/pass/activation/report HTTP/1.1 Content-Type: application/x-www-form-urlencoded User-Agent: Dalvik/2.1.0 (Linux; U; Android 10; M2007J3SY MI/V12.0.18.0.QJDEUXM) APP/unknown MK/TWkgMTBU Cookie: sdkVersion=accountsdk-2020.01.09 Host: sgpac.account.xiaomi.com Connection: Keep-Alive Accept-Encoding: gzip Content-Length: 346 DevID=VqFuDPTDczp39bXc&features=CALL_LOG_SYNC++MMS_SYNC+&mnc=24601&activationMode=uplink&simId=F_9M83JIJb_VOKce&smsBodyEncrypted=fu_5ODSHBbJv5XO6wRTIUfNCEerj978hkm5RhLrK19IYsgPUeVQoXbY9Di8-B9WaMvgJeAVwudc_nYD9LWJww28gYA9A9V1kqzNCf8e1tfLftN_Y0UXpvy4cXIHISL5yiGj2sI77KFzS20PgKtoc1xNcleEuLITEjTY_38%3D& action=vkey%3Aok%2Cverify%3A14%2Cdone%3A14HTTP/1.1 200 OK Date: Wed, 05 May 2021 09:50:27 GMT Content-Type: application/json Transfer-Encoding: chunked Connection: keep-Alive Content-Encoding: gzip {"result":"ok","code":0,"date":{},"description":"..."}

During the analysis, it was established that the device communicated with servers located in



Singapore. The list of identified communications is given in Table 21.

Table 21. Information about communications with servers located in Singapore

Line No.:	Domain	Address	Data, Bytes	State	Purpose
1	api.account.xiaomi.com	161.117.97.141	9200	Singapore	General server <i>Configuration for authentication is sent from the server to the phone: SMS tel. number, server address, etc.</i>
2	sgpac.account.xiaomi.com	161.117.97.227	48990	Singapore	Server <i>Based on the SMS message received from the phone, a registration response is generated and sent to the phone.</i>

IP addresses belonging to the domains api.account.xiaomi.com and sgpac.account.xiaomi.com are registered with Alibaba.com Singapore E-Commerce Private Limited. Alibaba is an information technology company established in 1999 in the People’s Republic of China. It is known that Chinese IT companies are obliged to transfer any form of information under the companies’ control to the Chinese government or its intelligence agencies³².

Automated sending of messages and its concealment by means of software pose potential threats to the security of the device and personal data; in this way, without the user’s knowledge, device data can be collected and transmitted to remote servers.

³² The Diplomat. <https://thediplomat.com/2019/02/the-real-danger-of-chinas-national-intelligence-law/>

Cornell Brooks Public Policy

Tech Policy Institute

Banning TikTok: What's At Stake and Would a Ban Address the National Security Risk?

[Sarah Kreps](#)

Director, Tech Policy Institute
Cornell University

Joshua Clark

Cybersecurity Fellow, Tech Policy Institute
Cornell University

Introduction

In the last several years, the bilateral relationship between the United States and China has become increasingly fraught. Although the growing tensions manifest across all issues, nowhere are they more clearly manifested than in the technology space. Consequently, the United States Government has taken a series of precautionary measures aiming to slow China's tech advancement, specifically in the area of artificial intelligence, semiconductor chips, and 5G technologies. Alongside these measures, the United States has taken notice of the potential for China to misuse data of American citizens. In 2016, a Chinese company bought a gay dating app, Grindr, and the Committee on Foreign Investment in the United States (CFIUS) concluded that Chinese ownership was a national security risk and required that China sell the app, which took place in 2020. In the meantime, TikTok has become a popular social media platform, with 150 million Americans on the platform. Congress has proposed a ban on TikTok, the White House has said it welcomes a bill that would allow it to ban the app, and the TikTok CEO is testifying on Capitol Hill on March 23, 2023.

This policy brief seeks to answer the key questions at stake with a possible TikTok ban. It considers the national security questions motivating debates about the ban, whether a ban would address these risks, whether proposed alternatives—a sale of TikTok or an initiative that would move the data to Texas—would mitigate these risks, the legal grounds for a ban, and how, technically, a ban might work.

What national security concerns does TikTok represent?

TikTok reports over 150 million American users and is owned by the Chinese company ByteDance. A 2017 Chinese National Intelligence Law requires that Chinese entities “support, assist and co-operate” with Chinese intelligence efforts, which has been interpreted to suggest that Chinese-owned companies might be required to share user data with the government. Chinese government access to user data presents two major categories of concern:

Privacy and user data protection

- TikTok collects vast amounts of user data, including location, device information, and user interactions, which could be exploited to build detailed profiles on individuals or to track user activities and preferences.

- TikTok’s ownership by ByteDance, a Chinese company, raises concerns about the potential for the Chinese government to access or misuse users’ data for espionage or surveillance purposes. Although TikTok says that “since beginning transparency reporting in 2019, we have received zero data requests from the Chinese government,” interpretations of the national intelligence law suggest that the company would indeed have to turn over data if asked in the future.
- Certain American individuals hold high intelligence value based on their occupation, location, and interests. While government employees and service members are prohibited from using TikTok on their devices, industry leaders, journalists, researchers in strategic industries, or relatives of government employees are still at risk of foreign intelligence leveraging their personal data.

TikTok as a vector for information warfare

- TikTok has a powerful aggregate user data model that reflects the general preferences and psychology of 150 million American users. By understanding the average mindset of, for example, a 22-year-old American college student, foreign actors are better positioned to manipulate that person psychologically through targeted messaging and curated content.
- TikTok’s algorithmic content distribution, young audience, and inherent access to user data and psychological profiles make it a powerful platform for targeted misinformation and propaganda campaigns.
- Foreign actors have proven capable of leveraging social media to attempt to influence elections or exacerbate social division. Inside access to the TikTok algorithm or specific user data would be a powerful tool to achieve these ends, though no evidence of influence operations occurring through TikTok exists.

Would a TikTok ban significantly reduce these risks?

A ban would not significantly reduce data privacy risks. While it would prevent TikTok from collecting new data on US users, it would not eliminate the data already collected, which is backed up to servers in Singapore and potentially accessible from China. This ban would also not address the broader issue of data privacy risks posed by the lack of US privacy and data security regulation. Leaked user data from American social media apps is readily available online, and brokers sell data obtained from these American apps with no regulatory supervision to buyers that could easily include Chinese intelligence. Foreign actors do not need TikTok’s data or continued operation to engage in disinformation or influence campaigns.

A ban on TikTok would significantly reduce the short-term risk of TikTok specifically being used as a vector for information warfare, as removing access would reduce the virality of misinformation or propaganda on the platform. However, given the existing historical aggregate data on American preferences obtained by TikTok since 2018 and the ready availability of data from other social media apps online, the long-term information warfare risks represented by having the models of American citizen’s preferences available for purchase will remain with or without TikTok until more comprehensive privacy legislation is enacted, or accountability mechanisms for all tech companies are strengthened.

Does Project Texas significantly reduce these risks?

Project Texas is the proposal by TikTok to mitigate privacy concerns by storing all American user data in a Texas data center operated by US-based Oracle and 3rd party auditors. From a policy standpoint, Project Texas represents the most stringent set of privacy requirements any social media company has ever been required to comply with. These measures would include localizing all US data, careful access control over

data passing in and out of Oracle's cloud, full visibility into the recommendation system, and making Oracle responsible for compiling the app source code and delivering it to app stores. These steps are inarguably all positive.

However, there are some technical concerns about the feasibility of auditing TikTok's codebase, which is reportedly millions of lines. The prevailing understanding within the cybersecurity community is that there are "always backdoors" within a system this large, and that auditing such a codebase could turn into a "cat and mouse game." Additionally, these measures do not mitigate the risks represented by China using TikTok as a vector for propaganda or disinformation, and do not remove what historical data may have been collected. Finally, as the Chinese division of ByteDance has a full copy of the source code that drives TikTok, their current or ex-employees are uniquely positioned to understand and take advantage of any legacy security vulnerabilities, even after the codebase is transitioned over to US control.

Is a TikTok ban legal?

The Trump White House issued an Executive Order on August 6, 2020 that aimed to ban TikTok. The proposed ban met with a series of legal obstacles. One US District judge stated that "the Government's own descriptions of the national security threat posed by the TikTok app are phrased in the hypothetical" and that the president had overstepped his emergency economic powers that the Trump Executive Order had cited. Another District Judge determined that the Administration had not considered alternatives other than a ban on TikTok.

When President Biden took office, he formally rescinded the ban, but the Committee on Foreign Investment in the US (CFIUS) began examining whether a Chinese-owned social media company can adequately safeguard Americans' data. As the process has dragged on, members of Congress and increasingly President Biden have become impatient. In March 2023, a bipartisan group of Senators announced the Restricting the Emergence of Security Threats that Risk Information and Communications Technology (RESTRICT) Act, the type of statutory reform that would pave the way for a legal and therefore more successful ban than was attempted in 2020. The bill, endorsed by the White House, would grant the Commerce Department the power to regulate technology produced by countries "adversarial" to the United States. Importantly, the bill would circumvent the Berman amendments, Cold War-era measures that restricted the president's authority to regulate or ban imports of "informational materials" from adversarial nations, by authorizing the Commerce Secretary to prohibit "transactions." Further, rather than focusing on an individual app, its emphasis on transactions means that hardware, software, quantum computing, synthetic biology, and robotics would all be included, giving it more longevity than an app-specific bill. Constitutional law history generally suggests that the courts give considerable latitude to the executive branch on issues of national security and that the legislative statutory reform would provide a more unassailable path toward a ban compared to when the ban was attempted in 2020.

What are the technical options to enforce a TikTok ban? Is this feasible?

While some tools exist to enact a TikTok ban, motivated users will be able to find ways to continue to use the app. As TikTok relies on network effects and user-generated content, adding friction to the user experience will likely decrease the total user count and reduce the amount of new data collected by ByteDance. However, the US government does not have an existing technical infrastructure to enforce these bans, and would need to lean on partners in the tech industry to implement these changes.

Three major mechanisms for bans are detailed below, along with the feasibility and effectiveness.

Network ban: Direct Internet Service Providers (ISPs) to block traffic to and from TikTok

- ISPs route traffic for mobile devices via cellular and WiFi networks. By denying access to TikTok IP addresses, no content can be sent to or received from existing TikTok apps or via browser. This practically renders the app useless.
- This method can be circumvented using VPNs, or tools that allow users to route their traffic through 3rd party intermediaries hosted outside the US and therefore not required to block TikTok IPs. VPNs are easily downloadable on iOS and Android.

App Store ban: Direct Apple and Google to remove TikTok from app stores

- Apple and Google remove apps that break the law or their terms of service, and have complied with similar orders in India.
- App store bans limit new downloads, and gradually degrade the stability of existing users by blocking application updates.
- This method can be circumvented through sideloading or downloading apps directly from 3rd party stores or websites. Sideloading is currently possible on Android devices and jailbroken iPhones, though recent EU legislation will require sideloading for all EU iPhones with iOS 17.

Financial ban: Direct US companies to suspend business relationships with TikTok

- By suspending these relationships, TikTok would be unable to monetize via advertising, pay creators, or have server or content delivery infrastructure within the US.
- This method can be circumvented by moving server operations to Canada, South America, or Europe. This would result in some degree of latency, but not so much as to be unacceptable to users.
- This method will not necessarily reduce the incentive for influencers to create content, as the majority of content creators monetize through bespoke brand deals and growing their audience on higher-paying social media platforms such as Youtube, not through TikTok's ad program.
- This method was successfully challenged on legal grounds during the Trump administration, though the new RESTRICT legislation may re-enable this approach.

Are there examples of apps or technology being banned? How successful were these efforts?

India implemented network and app store bans for more than 56 Chinese apps, including TikTok, successfully. In the aftermath, local apps replicating the functionality of the banned apps were adopted, and replaced the use of the banned apps, despite the ability for motivated or technical users to circumvent the bans.

China blocks practically all American owned social media apps through their national firewall. They also act as vendors for internet censorship technology to other countries interested in limiting assembly online. Nearly all social media is centralized to large players, such as WeChat, and are required to provide backdoor access to Chinese intelligence. Individuals can still access sites through VPNs but there is no doubt that the firewall complicates access, which achieves the intended goal.

The US has issued a ban on PokerStars/internet poker, which led to a massive user drop, though a smaller community remains in states where it remains legal. For almost a century the United States has restricted the

export of data encryption technology as it would a bomb or missile, although encryption software is nearly ubiquitous. The US has instituted export controls on artificial intelligence to China to slow the military and economic advancement of the country. Export controls, or in this case bans, are not intended to prevent the use but slow the spread or make it more inconvenient to the point that users choose alternatives.

Should the US impose a TikTok ban?

American citizens seem to have decided that they value user experience and personalized content more than their privacy, which is resulting in a growing national security concern. To address this issue, steps need to be taken across the social media landscape to better protect private user data and incentivize tech companies to take on that responsibility. Motivated users would likely continue to find ways to use the app after a ban, but as with other social media platforms, TikTok is characterized by strong network effects. If major influencers find it inconvenient or less financially attractive, they may migrate elsewhere and draw their followers with them, denting the potential national security value of user data.

A TikTok ban will not fully address the underlying national security concerns around user data and privacy, however. Moreover, the United States, as a democracy, will be taking steps that impede the ability of the TikTok constituency (young Americans), to express themselves and earn a livelihood. Given the potentially limited benefits and costs of a TikTok ban, legislators should consider establishing more comprehensive data privacy protections, and push for mitigation strategies such as Project Texas, before resorting to a ban.

TikTok, ByteDance, and their ties to the Chinese Communist Party

Submission to the Senate Select Committee
on Foreign Interference through Social Media

14 March 2023

Rachel Lee
Prudence Luttrell
Matthew Johnson
John Garnaut

Contents

About this Submission.....	3
Executive Summary	7
1. Why TikTok Matters	9
2. TikTok and Xi’s External Propaganda Plan	16
3. The ByteDance Origin Story	25
4. The Party-State Transforms ByteDance	32
5. Tracing Communist Party Control Through ByteDance and TikTok	37
6. ByteDance Serves Party Propaganda	51
7. ByteDance in China’s Military-Industrial-Surveillance Complex.....	61
8. Analysing the App: Content Quality and Access to Sensitive User Data	67
9. Taking Stock of the Evidence.....	77
Appendix 1: Static Analysis Methodology.....	84
Appendix 2: Device Data Accessible to TikTok App.....	85
Appendix 3: ‘android.permission’ Strings in TikTok Code	86
References	88

About this Submission

This submission is addressed to:

Committee Secretary
Select Committee on Foreign Interference through Social Media
Department of the Senate
PO Box 6100
Canberra ACT 2600

The authors of this report* express thanks to the Australian Senate Select Committee on Foreign Interference through Social Media for the opportunity to make this submission.

Our submission is motivated by concerns that TikTok (and potentially other platforms subject to authoritarian political leverage) pose risks not only to the data privacy of individual users, but to social cohesion, democratic functioning, and the national security interests of democratic nations including Australia and its partners and allies.

The analysis in this report is anchored in open-source material, as can be examined in the hundreds of endnotes. Many of our references point to Chinese-language sources that have been overlooked by the public debate to date. Some of our most important sources have been excavated from digital archives after being taken offline by TikTok's parent company, ByteDance, or authorities in the People's Republic of China (PRC).

Our research confirms beyond any plausible doubt that TikTok is owned by ByteDance, ByteDance is a PRC company, and ByteDance is subject to all the influence, guidance and de facto control to which the Chinese Communist Party (CCP, the Party) now subjects all PRC technology companies. We show how the CCP and PRC state agencies (together, the Party-state) have extended their ties into ByteDance to the point that **the company can no longer be accurately described as a private enterprise.**

These findings draw on previously unexamined sources and contradict many of TikTok's public statements. The most significant findings, in our view, relate to how TikTok's capabilities may be integrated with what China's leader Xi Jinping describes as the Party's "external discourse mechanisms".

TikTok has recently generated attention among politicians and policymakers for its potential use as a data access and surveillance tool, leading to multiple national and state governments banning the app's use on government-issued devices.¹ Mostly missing, however, has been discussion of how TikTok provides Beijing with the **latent capability to**

* Rachel Lee is a pseudonym as requested by the author and agreed by the Committee.

“weaponise” the platform by suppressing, amplifying and otherwise calibrating narratives in ways that micro-target political constituencies abroad.

TikTok undoubtably possesses the requisite capabilities, and a close examination of Chinese-language sources reveals the Chinese leadership’s intent. Our research shows how **ByteDance’s 10-year development journey tracks with Xi Jinping’s efforts to “meticulously build an external discourse mechanism [and] utilise the role of emerging media”**, as Xi told a “Study Session” of China’s top leaders in December 2013.²

In 2017, ByteDance launched TikTok and acquired the U.S. company Musical.ly. At the same time, Beijing launched a six-year regulatory campaign to build Party control systems inside ByteDance and accelerated the integration of senior corporate leaders into its “public opinion guidance” regime. Over this same period, Beijing has blocked the TikTok app inside China while enabling it to flourish outside China – to the point that it is now one of the most sophisticated and powerful social media platforms in the world.

In May 2021, Xi returned to another Politburo “Study Session” and instructed his colleagues to use the “external discourse mechanisms” that they had built in order to **“target different regions, different countries, and different groups of audiences”** with **“precise communication methods”** in order to **“make friends, unite and win the majority, and constantly expand our circle of friends who know China and are China-friendly.”**³

Xi did not name TikTok in the official meeting readout, published by Xinhua. Subsequently, however, the People’s Daily (Overseas Edition) elaborated on Xi’s message in an article (republished by Xinhua) that called for China to **“allow short video platforms to become ‘megaphones’ for telling Chinese stories well and spreading Chinese voices well”**.⁴ The article mentioned TikTok specifically as the representative example of short video platforms.

In Washington, in the pre-TikTok era, Russian intelligence actors “interfered in the 2016 presidential election in sweeping and systematic fashion”, according to the Mueller report.⁵ They did this by waging “a social media campaign that favoured presidential candidate Donald J. Trump and disparaged presidential candidate Hillary Clinton”, while seeking to “provoke and amplify political and social discord in the United States”.⁶

Mueller found no evidence that Russia caused the election of Trump or that Trump had colluded with Russia. Nevertheless, Russia’s interference fed perceptions that bitterly divided Americans and wounded the faith of many that the election had been free and fair.

In Canberra, the spectacle of Russian interference in the U.S. presidential election provided impetus to an Australian Government investigation into authoritarian interference in the Australian political system. According to media reports, the classified inter-agency report delivered in 2017 found that “the CCP’s operations are aimed at all levels of government and designed to gain access and influence over policy making.”⁷

According to the then-Prime Minister, Malcolm Turnbull, this analytical work “galvanised” the Australian Government to deliver a comprehensive counter foreign interference strategy, with bipartisan support.⁸ It also generated conversations in other Five Eyes nations, catalysed Australia’s strategic recalibration with respect to China,⁹ and contributed to decisions such as blocking Huawei from 5G networks (2018), elevating the Quadrilateral Security Dialogue to leadership level (2021), and forging the three-nation AUKUS agreement to jointly develop emerging technologies and deliver nuclear-powered submarines to Australia (2021 and 2023).

In Ottawa, intelligence agencies reportedly found in 2017 that the CCP was interfering at “all levels of government”.¹⁰ In contrast with Australia, however, Canada’s political leaders did not act, and the problem of CCP interference continued to grow.¹¹

Last week, while battling allegations of turning a blind eye,¹² Prime Minister Justin Trudeau announced two probes into foreign interference and a special rapporteur who will have “a wide mandate to make expert recommendations on protecting and enhancing Canadians’ faith in our democracy”.¹³ Whatever is revealed, the damage already caused to Canadian democracy is real.

In the absence of policy action, TikTok could be the next challenge to democracies’ resilience against authoritarian interference. As ever, the challenge is to deal with the potential for foreign interference before ‘elite capture’ becomes ‘state capture’.

It is possible that TikTok has already become so entrenched in some jurisdictions that politicians fear that banning TikTok might amount to political self-sabotage. As U.S. Secretary of Commerce Gina Raimondo told Bloomberg earlier this month: *“The politician in me thinks you’re gonna literally lose every voter under 35, forever.”*¹⁴

If the risks remain unaddressed, **the integrity of future elections could be vulnerable to allegations from both analysts and opportunists that elections have been “rigged” by a condominium of politicians and China’s super-app TikTok.** Much of it might be overstated, but – in the absence of effective policy action – there will be enough truth to make the allegations stick, leaving the credibility of democratic processes in doubt.

Our purpose in submitting this report is not to prescribe legislative or administrative actions, but to contribute constructively to public conversations and regulatory deliberations by identifying relevant empirical source material and filling analytical gaps.

In recent years, Australia has been a pioneer among democratic countries in building a bipartisan foundation for analysing and building resilience against authoritarian foreign interference. We submit this work to the Australian Senate because we believe Australia could play a similarly constructive role again.

Disclaimer

Our report relies on a wide range of online and other publicly available sources on TikTok, ByteDance, their relationship to China's Party-state, and risks they may pose to data privacy, national security, and the integrity of democratic systems globally.

To our knowledge, many of the most significant Chinese-language sources cited in this report have been overlooked in the public debate surrounding these companies. We consider our analysis to be sound and factual, and present it in the good faith belief that it is, but we are not in a position to independently verify the accuracy of the information contained in any public records.

Executive Summary

1. **A Powerful Public Platform – Not Just Dance Videos:** TikTok’s claims that it is about entertainment, not politics, are untenable. Last year, a third of adult users got their news from it, while one in six American teens say they are on the platform “almost constantly”. The platform has significance far beyond playful short videos.
2. **The True Origin Story:** A formative experience absent from founder Zhang Yiming’s official biographies is Beijing’s 2009 decision to shut down a Twitter clone he founded, Fanfou. The lesson, as later told by a ByteDance censor: *“Failing to delete politically sensitive content . . . is a life-and-death matter.”*
3. **Airbrushing the Parent:** The website of TikTok parent ByteDance today is bare bones, lacking detail about the company founder, corporate structure or partners. Excavating four years of archived snapshots reveals layers of disappearing information – including proof that TikTok is the wholly owned corporate child of ByteDance.
4. **TikTok’s Chinese Twin:** While TikTok is a household name, its analogue in China, Douyin, is not. TikTok claims to be its own insulated entity, but our research indicates that TikTok and Douyin share personnel and technological resources, have parallel management structures, and permit data sharing with each other.
5. **Not a Private Entity:** If ByteDance was once a private enterprise controlled by its founder, then it is no longer. The company’s status began to change in 2017, when it launched TikTok and acquired Musical.ly. The Chinese Communist Party commenced a program of co-option, infiltration, and legal and extra-legal coercion. In our view, ByteDance should now be understood as a “hybrid” state-private entity.
6. **The Chief Editor is also the Communist Party Boss:** ByteDance does not publicise that its editor-in-chief, Zhang Fuping (no relation to Zhang Yiming), is also its Communist Party Secretary. His guidance is clear: *“Transmit the correct political direction, public opinion guidance and value orientation into every business and product line.”*
7. **“Positive Energy” for China’s Military Police:** Chief-Editor-and-Party-Secretary Zhang Fuping was pictured at a 2017 signing ceremony with the director of the Political Work Department of the People’s Armed Police, the CCP’s domestic paramilitary force. According to a 2019 announcement, Douyin would help to *“spread the positive energy of the People’s Armed Police”*.
8. **Military-Security-Propaganda Collaboration:** ByteDance says it *“does not produce, operate or disseminate any products or services related to surveillance”*. But we found Douyin, TikTok’s analogue in China, directly aids Party propaganda and repression and its top leaders are ‘double-hatted’ in official propaganda organisations.

9. **Founder Stripped of His Shares?** Our review of Chinese-language sources indicates that ByteDance founder Zhang Yiming hasn't just relinquished his role as CEO, but has also given up all his shares in Douyin, after years of Party pressure. This recalls Jack Ma, who gave up his role at Alibaba before giving away his Ant Group shares.
10. **Two Key Risk Categories:** We assess six key threats, divided into two categories: data security concerns (privacy violations, data harvesting, espionage/surveillance) and political influence concerns (censorship, narrative control, political interference).
11. **Technical Evidence of Data Vulnerabilities:** Our preliminary technical analysis of the TikTok Android app identifies privacy and security risks stemming from sensitive user data vulnerable to Party-state requests for access.
12. **Intelligence Profiling:** There is significant risk the CCP could harness TikTok data to profile and target individuals around the world. Such activity could involve compromising material, device fingerprints, location-tracking or other data.
13. **Mass Narrative Control Power:** The biggest risks involve TikTok's unprecedented potential for shaping narratives and curating overseas political landscapes. ByteDance has a demonstrated capacity to develop automated content filters, calibrate content distribution, and adopt norms in service of Party propaganda.
14. **Xi's External Propaganda Intent:** TikTok's capabilities appear to neatly match Xi's edicts to build new media "external discourse mechanisms" and target differentiated foreign audiences with "precise communication methods".
15. **Propaganda and Election Misinformation:** Our original content analysis reveals higher proportions of pro-CCP content and political misinformation on TikTok than on some other platforms. There is evidence that Beijing's Party-state is interested in using social media to produce targeted propaganda for purposes including political interference.
16. **Political Interference:** The CCP's leverage over TikTok gives it vast potential to sway elections and undermine the will of open societies to compete against China's authoritarian model globally. Beijing could use these platforms' data on overseas public opinion to generate highly effective targeted disinformation, aided by AI.
17. **The "Project Texas" Gambit:** We show how TikTok's plan for "Project Texas" (the Oracle deal) fails to address the fundamental risks to data security posed by CCP infiltration of a parent company and China's national intelligence laws.
18. **The Meaning of Beijing's Overseas Veto:** The CCP signaled in 2020 that it would counter a U.S. attempt to force ByteDance to divest TikTok. Clearly Beijing wants to retain control over the app. So long as it does, TikTok poses risks to democracies.

1. Why TikTok Matters

This section sets out national security risks posed by TikTok to democratic nations, and the essential context for understanding those risks.

- a. **TikTok Is a News Platform:** TikTok’s claim that it is only an entertainment platform is untenable. Last year a third of adult users got their news from it, while one in six U.S. teens say they are on the platform “almost constantly”.
- b. **Opacity and Obfuscation:** TikTok is one of the world’s most important media platforms and yet remarkably little is known about it – thanks in part to parent company ByteDance’s efforts to airbrush basic information about the company’s founder, corporate structure, partners, and activities.
- c. **Narrative Control:** Concerns about Beijing using TikTok for data harvesting and surveillance are well-founded. In our view, however, bigger risks involve TikTok’s unique potential for shaping global narratives and curating a CCP-friendly political landscape.

1.1. The Rise of TikTok, the App that “Gazes Back”

It is news to no one that TikTok – as an app and a business – has exploded since its inception. The scale of the platform’s deep insights into users’ tastes and preferences has revolutionised the way societies (and young people in particular) access information. It has ushered in what could be described as the latest epochal shift in broadcast media. As TikTok proclaimed, “*relevance is the new reach*”.¹⁵

With this shift, social media is moving away from reliance on the user to actively decide what kind of content they want to see (by curating their own feed), toward personalised content recommendations through algorithms that respond to cues such as watch time, with only passive participation required of the user.

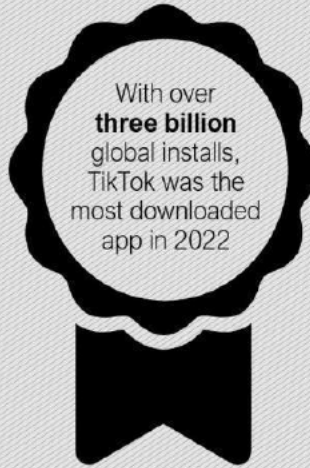
It is these algorithms, and the artificial intelligence that powers them, that led one tech blogger in 2020 to write, “*When you gaze into TikTok, TikTok gazes into you.*”¹⁶ Paired with the short video format that delivers both instant gratification for the viewer and exponential volumes of data about user interests to the app, the algorithm can deliver content recommendations with uncanny accuracy. It is no wonder then that other companies have sought to learn from and compete with the TikTok model (see Meta’s Instagram Reels and Alphabet’s YouTube Shorts).

TikTok By The Numbers

The most downloaded app in history



1 in 3
Americans uses TikTok



A staggering 20.8% of the world's 4.8 billion internet users use TikTok.



1 billion

monthly active users globally in September 2021

Addictive algorithms make for constant consumption



40 times

TikTok users open the app on average around 40 times per day. (By comparison, the average Twitter user opens the Twitter app roughly 15 times each day.)



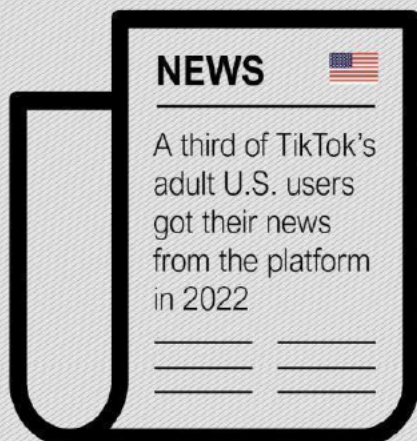
2 in 3

American teenagers aged 13 to 17 have used TikTok before. One in six say that they use the app "almost constantly".

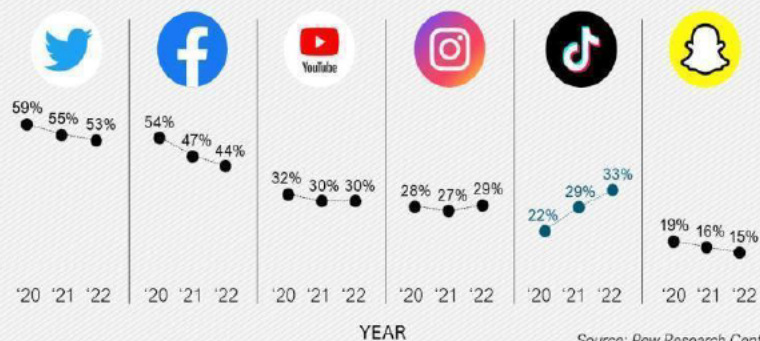
Last year, TikTok was second only to YouTube as the most used social media platform by American teenagers.



Young people use TikTok as a source of news



Social media sites by portion of users who regularly get news there



Comprehensive statistics for the Australian user base are hard to come by, but there is ample data on TikTok consumers both globally and in the U.S.

*"The latest [global] data suggest that TikTok has been adding an average of more than 650,000 new users every day over the past 3 months, which equates to almost **8 new users every second**."*¹⁸

TikTok has become the crucial medium for political actors to reach younger demographics, especially Gen Z. "There's no way that we can be a youth organisation trying to reach young people and not be on TikTok," said Cristina Tzintzún Ramirez, president of U.S. progressive political action committee NextGen America.¹⁹

Politicians, of course, face the same dilemma. U.S. Secretary of Commerce Gina Raimondo recently told Bloomberg of her own concerns:

*Passing a law to ban a single company [TikTok] is not the way to deal with this issue. **The politician in me thinks you're gonna literally lose every voter under 35, forever**. However much I hate TikTok – and I do, because I see the addiction in the bad s*** that it serves kids – you know, this is America.*²⁰

TikTok has revolutionised the attention economy. And yet TikTok describes itself only as an "entertainment platform" on a mission to "inspire creativity and bring joy".²¹ According to TikTok's VP and Head of Public Policy for the Americas, Michael Beckerman:

*We are not the go-to place for politics. . . . The primary thing that people are coming and using TikTok for is entertainment and joyful and fun content.*²²

But the claim that TikTok is about entertainment rather than politics is untenable in light of the facts. (See figure on previous page.) Increasing volumes of social media users are getting their news from the platform and using it as a search engine to navigate key issues. The numbers tell a story of an unimaginably successful algorithm, and an app that has gained unmatched sway over society and politics seemingly overnight.

To understand how this was possible, we must delve into the creation stories of TikTok, its China analogue and precursor, Douyin, and their USD 400 billion parent company, ByteDance, which is the most valuable startup in the world.²³ Understanding ByteDance, Douyin and TikTok requires understanding China's ruling Communist Party and its guiding ideology, organisational structures, and legal and extra-legal mechanisms for influencing, coercing and controlling China's nominally privately-owned technology companies.

1.2. Opacity and Obfuscation

Answering basic questions about how the app works, how it is controlled, and who controls it is not straightforward. ByteDance's company website contains just the bare bones, shorn of details about the company's founder, corporate structure, partners, and sizeable investment into AI.

Media reporting has emphasised the opacity of TikTok's algorithm in producing virality, even to some of TikTok's own employees. Chris Stokel-Walker, author of *TikTok Boom*, said:

*One person at TikTok in charge of trying to track what goes viral and why told me in my book that 'There's no recipe for it, there's no magic formula.' The employee even admitted that 'It's a question I don't think even the algo team have the answer to. It's just so sophisticated.'*²⁴

Leaked internal advice from TikTok on public relations talking points encapsulates the company's evasive self-presentation. The document instructs TikTok spokespersons to **"downplay the parent company ByteDance, downplay the China association, downplay AI"**.²⁵ The memo directs spokespersons to say, *"There's a lot of misinformation about TikTok right now. The reality is that the TikTok app isn't even available in China."*²⁶

This opacity and obfuscation is now compounded by what appears to be a concerted campaign to airbrush what little material was available online. Excavating four years of archived snapshots of ByteDance's company website reveals layers of disappearing information.²⁷ Pages that once recounted Communist Party activities inside ByteDance have been deleted from the website of Beijing Internet Association (an industry association charged with guiding the Party-building work of internet companies in Beijing).²⁸

1.3. Demystifying the TikTok-Douyin-ByteDance Relationship

While TikTok is a household name across much of the world, its China analogue, Douyin, is not. Our research points to a functional fusion of TikTok and Douyin under the control of a single corporate entity – ByteDance, a conglomerate registered in the Cayman Islands but headquartered in Beijing until November 2020.

Douyin's tagline exhorts users to *"record a good life"*. Its earlier establishment in China offers a roadmap for TikTok's global development (see [Section 3](#)). In [Sections 4](#) and [5](#), we set out how TikTok and Douyin share personnel and technological resources and have parallel management structures, all of which link back to ByteDance. TikTok admits in its latest Privacy Policy for Australia: *"We also share [user] information with [...] other companies in the same [corporate] group as TikTok."*²⁹

In [Sections 5 and 6](#), we show how the CCP exerts control over ByteDance (and TikTok) through a 'golden share' arrangement, export restrictions and cybersecurity review mechanisms. These sections outline key collaborations between ByteDance and Party-state propaganda and security organs, and the presence of Party members in key executive positions at ByteDance. We examine sources that show ByteDance striving to serve Party interests through censorship, public opinion-shaping and surveillance.

1.4. The Propaganda-Security Nexus

It is well-known that the Party's security apparatus absorbs and repurposes technology and data for surveillance, social control and repression. The logic of Beijing's interlocking data security laws applied to ubiquitous surveillance means that all customer data held by China-controlled companies will be accessible to the Party's security services.

Clearly the potential for Beijing to exploit TikTok for global surveillance is vast. In our view, however, the most significant risk posed by TikTok is its unprecedented potential for censoring and proactively shaping public opinion overseas – in the United States, Australia, and other countries around the world.

1.5. How the Chinese Communist Party Could Wield TikTok

Intelligence agencies in jurisdictions including the U.S.,³⁰ U.K.,³¹ Australia,³² European Union,³³ Canada,³⁴ New Zealand,³⁵ the Netherlands,³⁶ Estonia,³⁷ and the Czech Republic³⁸ have signaled clear concerns regarding China's data cultivation, influence, and political interference activities. The U.S. National Intelligence Council, a formal panel of intelligence officers and independent scholars, assesses that:

*Beijing will be able to exploit Chinese companies' expansion of telecommunications infrastructures and digital services, these enterprises' growing presence in the daily lives of populations worldwide, and Beijing's rising and global economic and political influence. Beijing has demonstrated its willingness to enlist the aid of Chinese commercial enterprises to help surveil and censor regime enemies abroad.*³⁹

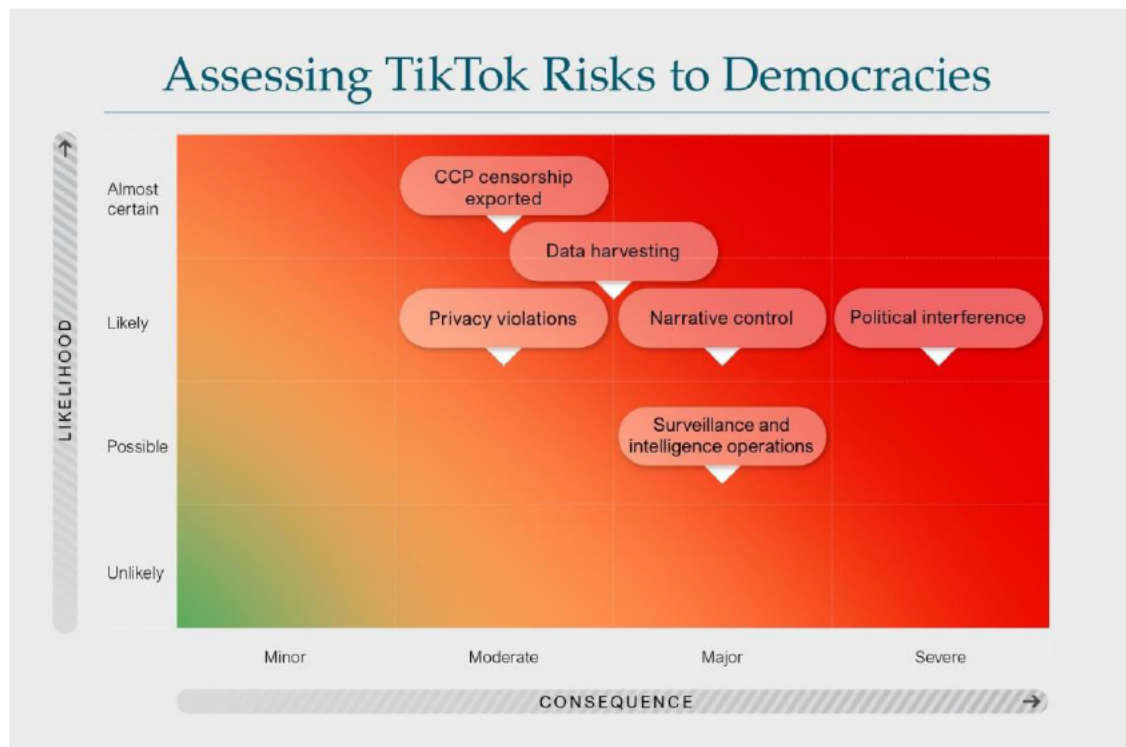
In [Section 2](#), we set out evidence of Beijing's capabilities and intent relating to influence, interference and intelligence activities. This includes not only data harvesting and surveillance activities, but also the deployment of targeted propaganda designed to shape global discourses and influence overseas policymaking on issues related to China, with short video platforms identified as a key arena for exploitation.

In [Sections 6 and 7](#), we show how the Party's global propaganda and surveillance activities inform our risk assessment of TikTok.

1.6. Taxonomy of TikTok Risks

We have identified six key risks posed by the app, divided into two categories:

Data security concerns	Political influence concerns
Privacy violations	CCP censorship exported
Data harvesting	Narrative control
Surveillance and intelligence operations	Political interference



Taxonomy of TikTok Risks to Democracies

- Privacy Violations:** TikTok could be used for unauthorised access to or theft of sensitive user data. Access could be gained through security breaches, including via backdoors or China-based staff's retrieval of data, whether of their own volition, at the behest of intelligence agencies or simply in compliance with Beijing's data laws.⁴⁰ ByteDance admitted in December that some China-based staff had surveilled U.S. journalists and TikTok employees through the app's geolocation function, intending to discover who was speaking with the journalists from inside the company.⁴¹

- **Data Harvesting:** Beijing could harness large datasets like those offered by TikTok to support the Party-state in its competition with liberal democracies and its development of critical capabilities in big data, AI, supercomputing, and predictive modelling.⁴² These technologies have important military and intelligence applications, including in profiling, analysing and targeting individuals or population segments.
- **Surveillance and Intelligence Operations:** Data collected by TikTok could be used to target individuals (or population segments) for intelligence purposes such as surveillance, recruitment, manipulation, and repression.⁴³ Targets could include key officeholders or critics of Beijing. Activity could involve the collection of compromising material about individuals, device fingerprints, or location data.⁴⁴
- **CCP Censorship Exported:** Elements of the CCP’s censorship preferences could be implemented at TikTok, infringing on individuals’ rights to expression and impacting the quality of free and open debate in democracies globally.
- **Narrative Control:** TikTok could be used to disrupt social cohesion and democratic processes through censorship, misinformation or propaganda. The TikTok-curated information environment – with its fast-growing significance for social and political discourse – could be manipulated through the selective promotion or demotion of certain topics, narratives or creators, including political figures.⁴⁵ Measures could range from blunt “content moderation” to hard-to-detect manipulation of recommendation and search algorithms (or ad hoc interventions by certain staff). It remains to be seen whether and how the rollout of TikTok’s “state-affiliated media” policy will ameliorate these effects.⁴⁶
- **Political Interference:** Information operations may be conducted in a more deft and disruptive manner. For instance, big data analysis of public opinion based on platform activity could be used to generate highly effective propaganda, using AI to automate the production and dissemination of targeted materials designed for specific purposes.⁴⁷ Moreover, bad actors could use the app for large-scale, coordinated campaigns for harassment or disinformation, in particular those that employ inauthentic, seemingly grass-roots accounts – a tactic known as “astroturfing”.⁴⁸ The Party could apply “agitprop” mobilisation campaigns to shape and manipulate geopolitical discussions, political debates and elections.

2. TikTok and Xi's External Propaganda Plan

This section details the deep drivers of the Party's efforts to control the media environment and the online "propaganda and ideology battlefield".

- a. **Propaganda Goes Digital:** Xi Jinping has intensified the Party's long-running efforts to adapt the Party's propaganda and ideological systems to the digital age, deploying media companies as instruments of an "external discourse mechanism" to shape global information and ideas.
- b. **Military-Surveillance Complex:** China's intelligence agencies are bringing data storage and processing capabilities under their control. The People's Liberation Army (PLA) – the armed wing of the Communist Party – studies the use of AI/ML to manage public opinion on social networks.
- c. **Political Interference:** TikTok – an app that now pervades the waking lives of many Australian and American teenagers – has latent potential to sway elections, corrode people's faith in democracy, and undermine the will of open societies to compete against China's authoritarian model globally.

Party writings and speeches by Xi Jinping stress the importance of "cultural security" for China's national unity and the survival of its socialist political system – which it defines as a single-party dictatorship.⁴⁹ Cultural security is an element of political security – Xi calls it a "guarantee" – and refers to ideological power (including propaganda, media, opinion, education, and law) and control over information networks.⁵⁰

The Party assumes that all external flows of information, thought, and values represent potential risk to China's socialist system, and that conflict with Western democracy requires submitting more of the world's data systems to Party norms of "internet governance" and "data security". Propaganda, ideological-political "thought work", and "international public opinion struggle" are the civilian tools of waging this conflict in peacetime.

Moreover, China's military and security apparatuses seek global advantage in key technologies to support the Party's ability to confront the West and wage 'grey zone warfare' (or 'political warfare'), including through information manipulation. The technologies given emphasis include those that enable mass surveillance and information operations.

We have observed the Party using social media tools to wage this "peacetime conflict". Based on our evaluation of the Party-state's access to and control over ByteDance and TikTok, we assess as high the risk that the Party will seek to leverage the company's innovative algorithms and access to key data to develop its own big data harvesting and analysis capabilities for targeted propaganda and political interference.

2.1. Leveraging New Media to Target Global Audiences

The Party has paid close attention to new media's influence on public opinion since the internet first started gaining traction in China in the mid-to-late 1990s. By September 2004, during the Fourth Plenary Session of the 16th Central Committee of the Communist Party of China, the Party passed its Decision on 'Enhancing the Party's Governance Capability', which formally designated the internet as a domain for Party control and influence:

*Attach great importance to the influence of new types of media channels, such as the internet, on public opinion. . . .Strengthen the construction of internet propaganda teams and form a strong online positive public opinion.*⁵¹

During his decade in power, Xi has intensified the Party's long-running efforts to refine its propaganda and ideological systems and adapt them to the digital age.⁵² He has frequently instructed the Party to utilise "new media" – a term that encompasses short video platforms – to "strengthen the promotion of the Chinese Communist Party" and "strive to create an image of China that is credible, lovable and respectable".⁵³

In November 2013, the Third Plenary Session of the 18th Central Committee of the Communist Party of China introduced its Decision on 'Some Major Issues Concerning Comprehensively Deepening Reform'.⁵⁴ It stipulated:

*We will straighten out the mechanism for both domestic and overseas propaganda, and support key media groups to develop both at home and abroad. We will foster external-facing cultural enterprises and support cultural enterprises to go abroad and expand markets there.*⁵⁵

In order to effectively carry out this international propaganda effort, Xi has called for the creation of "flagship" propaganda outlets for transmitting Party messages and enhancing "international discourse power".⁵⁶

In December 2013, at a Politburo Collective Study Session, Xi told cadres:

*We should meticulously build an external discourse mechanism, utilise the role of emerging media, enhance the creativity, appeal, and credibility of our external discourse, tell the China story well, spread Chinese voices, and explain Chinese characteristics effectively.*⁵⁷

Then, in 2016, at a Symposium on the Party's News and Public Opinion Work, Xi reiterated:

*We should strengthen the development of international communication capacity, enhance our international discourse power, focus on telling the China story well, and ... **strive to build flagship external propaganda media outlets with strong international influence.***⁵⁸

In December 2020, Xi convened a Politburo Collective Study Session to deliberate on plans to strengthen and enlarge China's national security system.⁵⁹ Yuan Peng, head of the China Institutes of Contemporary International Relations (CICIR), a Ministry of State Security think tank, also attended the session.⁶⁰ While the content of Yuan's lecture was not revealed, in a subsequent publication he argued that **the Party should leverage a 'post-truth' information environment in its struggle for ideological security:**

What is truth and what is a lie is already unimportant, what is important is who controls discourse power, this is nothing other than the twisted nature of the 'post-truth era'. In the face of this strange phenomenon without precedent in the past century, it is only by maintaining resolve, 'not fearing the floating clouds', and refusing impulsivity, that we will ultimately be able to emerge victorious from amidst this strategic game.⁶¹

(In February 2023, Hong Kong newspaper Ming Bao reported on Yuan Peng's emergence as vice minister of the Ministry of State Security, under what is apparently his real name, Yuan Yikun.⁶²)

In May 2021, at another Politburo Study Session, Xi referred specifically to his ambitions for promoting pro-China policymaking abroad through the deployment of targeted propaganda for overseas audiences:

*We should build an external discourse mechanism and improve the art of communication. **We should adopt precise communication methods that target different regions, different countries, and different groups of audiences, promote the globalised, regionalised, and differentiated expression of Chinese stories and Chinese voices, and enhance the affinity and effectiveness of international communication. We should [strive to] make friends, unite and win the majority, and constantly expand our circle of friends who know China and are China-friendly.***⁶³

Xi's language of making friends, winning the majority and expanding China's circle of friends is rooted in the Party's history of "united front" work.⁶⁴

In August 2021, the People's Daily published an article that elaborated on Xi's comments and identified short video platforms as a key arena for deploying propaganda to enhance

China's "international discourse power" overseas.⁶⁵ An excerpt from the article, which was republished by Xinhua, reads:

*As one of the windows of China's foreign exchanges, short video platforms also have a large audience abroad. **Various short video apps represented by TikTok** have emerged one after another, and many cultural short videos with rich content and well-made are loved by foreign internet users. ... In promoting the transformation and upgrading of China's international communication and building a strategic communication system with distinctive Chinese characteristics, **we should make good use of short video platforms that are open, inclusive, interactive and their advanced technological advantages, innovate communication methods, empower cultural communication, and allow short video platforms to become "megaphones" for "telling the China story well and spreading Chinese voices well."***⁶⁶

2.1.2. Propaganda and Power in Party Ideology

The sophistication, magnitude and force of Xi's efforts to dominate the "propaganda and ideology battlefield" are rooted in a classical tradition of Chinese statecraft in which *wu* (weapons, violence) and *wen* (words, culture) go hand-in-hand. This classical Chinese emphasis on discursive power has been strengthened, institutionalised and re-purposed by Marxism-Leninism, **an ideology that posits "systematic, all-around propaganda and agitation" as the "chief and permanent task"**.⁶⁷

The Party's obsession with controlling communication platforms stems from a belief that what people talk about and how they choose their words shape the way they think and ultimately act. Authors are seen as "weapons"⁶⁸ and words described as "bullets"⁶⁹ that can shape perceptions, define choices, subvert governments and sharpen battle lines between enemies and friends.⁷⁰

Once Xi completed his leadership accession in 2013, he directed his General Office to issue a communique on "The Current State of the Ideological Sphere". This April 2013 directive, known as Document No. 9, directs cadres to prioritise an "intense struggle" against seven key vectors of ideological threat.⁷¹ **The first five vectors of ideological threat that must be "struggled" against are foundational institutions for liberal democracies and the rules-based system which gave rise to the global internet.**

**“Communique on the Current State of the Ideological Sphere”
(Internal CCP Memo known as “Document No.9”, published 2013)**

The seven ideological threat vectors that must be “struggled against” are rule of law, individual rights, civil society, market (“neoliberal”) economics, independent media, “historical nihilism” and “questioning ‘reform and opening’”.

Threat Vector No.3: Promoting civil society in an attempt to dismantle the ruling party’s social foundation . . . The idea of civil society has been adopted by Western anti-China forces and used as a political tool.

Threat Vector No.4: Promoting the West’s idea of journalism, challenging China’s principle that the media and publishing system should be subject to Party discipline. The ultimate goal of advocating the West’s view of the media is to hawk the principle of abstract and absolute freedom of press, oppose the Party’s leadership in the media, and gouge an opening through which to infiltrate our ideology.

2.1.3. “Struggling” against Western “Infiltration”

Xi’s agenda of “struggling” against the institutional foundations of open societies was converted into an action plan at the Party’s National Propaganda Work Conference in August 2013.⁷² According to a leaked outline of Xi’s speech to the conference, Xi remarked that the West was carrying out “cultural infiltration” against China and that the “*struggle and contest we face in the ideological domain is long-term*”. He identified the internet as the “**main battlefield**”, calling for a “strong internet army” to resist the “Western anti-China forces” who were using the internet to subvert China and destroy it from within.⁷³

Since then, China’s quasi-commercial media has been comprehensively “disciplined”,⁷⁴ foreign news platforms have been locked out, and Chinese social media platforms that have taken the place of foreign platforms are grafted into the state propaganda system.⁷⁵ They are required to host “cybersecurity police stations” inside their organisations.⁷⁶

Outside China, propaganda is reinforced by the United Front Work Department, the International Liaison Department, diplomatic missions, intelligence agencies and even “triad” organised crime networks.⁷⁷ Together they provide inducements and threats that motivate people to talk, think and act in ways that serve the interests of the Party. It is a system of political-psychological conditioning, on a global scale.⁷⁸

The internet – which once threatened the Party’s grip on power – has become its most important tool of social and political control. In 2022, Reporters Without Borders ranked

China 175 out of 180 countries in its press freedom index.⁷⁹ All of this is important because China's media and internet controls do not stop at the physical border.

Ostensibly private companies play a key role in this vision. As media technology has continued to evolve, Xi has articulated plans to develop more refined and targeted methods of harnessing media for international propaganda in order to influence audiences to adopt more pro-China, pro-Party stances.⁸⁰ Viewed through Xi's paradigm of "international discourse power", new media companies – with their vast reach, data-harvesting abilities, and optimisation for targeting discrete segments of foreign societies – represent among the most important weapons in the Party's media arsenal.

2.2. Codifying a Propaganda-Security Nexus

In parallel with externally facing media and national security policy, **Xi and his leadership team have engineered a new legal regime mandating that individuals and corporations support the ideological security interests of the Party-state.** The Party's regulatory regime has made it the legal responsibility of companies to advance socialist thought, tighten control in cyberspace, and propagate the right information and values.⁸¹

The rapid development of the new media sector's responsibilities now dovetails with more specific policy prescriptions for the management of external propaganda, the collection of user data, and security-focused innovation.

2.2.1. Beijing Dreams of Data Riches

In 2013, in the early months of his reign, Xi began to speak of data in the way Mao had spoken of domestic oil production in the 1950s, when seeking to break reliance on the Soviet Union. Xi told the state-run Chinese Academy of Sciences:

*The vast ocean of data, just like the oil resources during industrialisation, contains immense productive power and opportunities. **Whoever controls big data technologies will control the resources for development and have the upper hand.***⁸²

Beginning in 2014, Xi Jinping created new institutions (such as the Central National Security Commission and the Cyber Administration of China) to manage internal and external risk across multiple overlapping domains.

The Party's 13th Five-Year Plan, published in 2016, and its "big data industry development" sub-plan, outlined national goals of applying big data across domains including: government supervision and efficiency; social control; data integration and centralisation; first-mover advantage in big data and emerging industries; cross-sector transfer, including Military-Civil Fusion; and cyber defence and risk prevention.⁸³

2.2.2. Intelligence Agencies Building Big Data Capabilities

These priorities are the direct outgrowth of Xi's leadership and the Party's decision to harness data for strategic purposes. They are also the inspiration for recent and ongoing attempts by the Ministry of State Security (China's lead external intelligence agency) and the Ministry of Public Security (the lead internal security agency) to bring the entirety of China's data storage and processing capabilities under the control of the security services – a move that heralds the agencies' intrusion into the operations of both domestic companies and foreign multinationals.

China's laws mandate that individuals and entities cooperate with intelligence agencies:

- **The National Security Law (2015)** requires citizens and organisations to report acts harming national security and to support national security bodies, public security bodies, and military bodies in their work.⁸⁴
- **The National Intelligence Law (2017)** compels PRC entities and individuals to support China's intelligence services by secretly turning over data collected in China or overseas.⁸⁵
- **The National Cybersecurity Law (2017)** compels companies and individuals to make networks, data, and communications available to the police and security services.⁸⁶
- **The Data Security Law (2021)** asserts state powers to access and control private data, including China's "national" data processed overseas.⁸⁷
- **The Personal Information Protection Law (2021)** requires companies handling Chinese citizens' personal data to minimise collection, disclose uses of personal data, and obtain prior consent in certain cases (involving the use of biometric data, for example), while forbidding the unapproved transfer and storage of personal information overseas.⁸⁸

2.2.3. "Seizing the Strategic Advantage"

The Party-state's ability to target individuals for intelligence operations and develop world-leading surveillance technologies has been fuelled by its access to huge amounts of data and expertise in deciphering it efficiently. The data is collected both legitimately and through breaches and spying operations, on both foreign and domestic targets.

Tech firms such as Baidu, Alibaba and Tencent are reportedly instrumental in assisting China's spy agencies to process "pilfered and otherwise obtained data".⁸⁹ U.S. National Counterintelligence and Security Center ex-chief William Evanina has said that this data:

. . .gives [China] vast opportunities to target people in foreign governments, private industries, and other sectors around the world – in order to collect additional information they want, such as research, technology, trade secrets, or classified information.⁹⁰

Beijing has recognised data harvesting as a critical capability in the Party-state’s race with the West to seize the “strategic commanding heights” of emerging technologies.⁹¹ The evidence points strongly to Beijing’s interest in leveraging private sector data – including foreign data and that of firms like ByteDance – to grow its stores and become the world’s most data-rich power. The U.S. National Intelligence Council assessed in April 2020:

*Beijing's commercial access to personal data of other countries' citizens, along with AI-driven analytics, will enable it to **automate the identification of individuals and groups beyond China's borders to target with propaganda or censorship**. Such access and analytics also will enable Beijing to tailor its use of a range of online and offline carrots and sticks to its targets outside China – potentially on a large scale.⁹²*

2.2.4. Social Media and Information Warfare

Xi’s China has gained a reputation for leveraging technology for influence and intelligence work, whether through AI for online censorship and “smart city”-style surveillance or through mass hacks of foreign data. What is less immediately obvious is how the Party may be thinking about leveraging AI to shape narratives online and carry out social media-based psychological operations and political interference far from China’s shores.

The emergence of China’s contemporary political warfare strategy begins with the People’s Liberation Army Political Work Regulations in 2003, which describe ‘public opinion warfare’, ‘psychological warfare’, and ‘legal warfare’ as elements of national defence and military combat effectiveness.⁹³ According to the most recent revision of the Regulations, issued in 2010, the purpose of peacetime political warfare (‘liaison work’) is to:

*Carry out the work of disintegrating enemy militaries and liaising with friendly militaries. Launch work related to Taiwan. Investigate and research conditions [related to] foreign militaries and ethnic separatist forces. **Launch psychological warfare work.**⁹⁴*

More recent sources confirm the PLA is reinvigorating its practice of political warfare. The *Science of Military Strategy*, a primary PLA doctrinal publication, states that the boundaries between peacetime and wartime have been permanently blurred, increasing the necessity of deeper military-civilian integration.⁹⁵ The *Strategy* describes **media, information,**

psychological deterrence and propaganda as elements of military activity, particularly in the early stages of a confrontation, such as that over the sovereignty of Taiwan.⁹⁶

Indeed, political warfare was one of the focuses of the significant military reforms undertaken during Xi's leadership. In his first term (2012-2017), Xi created a 'Strategic Support Force', which incorporated five core functions: intelligence, technological reconnaissance, electronic countermeasures, network attack and defence ('information warfare'), and psychological warfare functions.⁹⁷ **The PLA General Political Department's 311 Base, a specialised unit for psychological warfare operations, was placed under the Strategic Support Force, a move that appears designed to streamline the integration of cyber and psychological warfare.**⁹⁸

The PLA has spoken more explicitly about the opportunities posed by social media in recent years. A 2019 paper in a Chinese military journal, *National Defence Technology*, argues that AI can be leveraged to achieve "intelligentised online public opinion guidance".⁹⁹ Elsa Kania, an expert on the Chinese military's AI capabilities, predicts that:

*The PLA will likely leverage big data analytics, machine learning, and automation to support information warfare, including cyber warfare and electronic warfare. Potentially, these techniques will also enable precision psychological warfare that leverages big data to profile targets and customise attacks to shape individuals' emotions and behaviour.*¹⁰⁰

With this in mind, the concern is not just that an app with TikTok's data harvesting and targeted recommendation capabilities could be used as a platform for disseminating propaganda, disinformation, and other messages designed to influence democratic societies. Rather, it is that TikTok has the potential to sway elections, corrode people's faith in democracy, and undermine the will of open societies to compete against China's authoritarian model globally.

3. The ByteDance Origin Story

This section collates fragments of publicly available information to trace the source of ByteDance’s most important asset: political reliability.

- a. **A Founder’s Lesson in Red Lines:** A near-existential encounter with the propaganda system over the Xinjiang riots of 2009 taught Zhang Yiming to pre-emptively comply with Beijing’s censorship in order to survive.
- b. **Patronage Ties:** Frequently overlooked in ByteDance’s success is the founder’s relationships with Silicon Valley venture capitalist Neil Shen and (now-fallen) CCP internet czar Lu Wei.
- c. **Made By... Musical.ly:** Before ByteDance acquired its biggest competitor in November 2017, Musical.ly co-founder Louis Yang said that Douyin was almost a pixel-level replica of Musical.ly.

3.1. Invisible Red Lines

The official ByteDance origin story begins in 2012, when the company launched in an apartment near the Zhongguancun tech hub, China’s version of Silicon Valley. Zhang Yiming, following stints at less-successful startups and a short turn at Microsoft, had won investor backing for his idea to commercialise big-data and machine-learning in response to the tectonic shifts brought on by the proliferation of smartphones.¹⁰¹ The founding team included Zhang’s former colleagues from travel site Kuxun and real estate platform 99Fang.com.¹⁰²

Arguably, however, Zhang’s formative moment was a few years earlier. He had co-founded Fanfou, a Twitter clone, in 2008.¹⁰³ On 7 July 2009, Beijing destroyed Fanfou as it sought to control coverage of anti-government riots and a deadly police crackdown in Xinjiang.¹⁰⁴ Just after 10pm that night, Zhang’s business partner (future Meituan founder) Wang Xing posted: *“Harmonised by Fanfou, or Fanfou is harmonised.’ This is an uncomfortable choice, but one that has to be made.”*¹⁰⁵

By 11pm, Fanfou had become inaccessible and stayed that way for more than 500 days.¹⁰⁶

This was Zhang Yiming’s first collision with the invisible but existential red lines of the Propaganda Department. The lesson he learned – arguably just as important as his insights into artificial technology, big data and mobile apps – was that, to survive, social media providers needed to pre-emptively comply with the invisible red lines of the propaganda system. He learned that what might seem innocuous in the eyes of users could be viewed as subversive in Beijing. He would need to learn this lesson again with ByteDance.

Timeline of Zhang Yiming's Biography

- **1983** – Born in Longyan, Fujian province.
- **2001** – Began undergraduate studies in Nankai University, Tianjin.¹⁰⁷
- **2005** – Graduated with a software engineering degree and started a collaborative software company with two schoolmates. The business failed within six months due to flawed market positioning.¹⁰⁸
- **2006** – Joined online travel search engine Kuxun as the first engineer and the fifth employee. Kuxun asked users to input their travel plans and returned ticket options in real-time. Zhang's innovation was to code a program that repeated the same search at regular intervals and, when a ticket became available, send the user an SMS alert.¹⁰⁹
- **2008** – Left to work briefly for Microsoft Beijing. PRC tech media reported that Zhang wanted to learn how large organisations were managed but left because he found the work boring.¹¹⁰
- **2008** – Partnered with Wang Xing to start Twitter clone Fanfou, which was shut down for more than 500 days following protests in Xinjiang.¹¹¹ This was Zhang's first collision with the invisible but existential red lines of the Party.
- **2009** – Became CEO of online real estate portal, 99Fang.com, when Susquehanna International Group's China-based partner Joan Wang (Wang Qiong) approached him to take over Kuxun's side business in real estate search.¹¹² Joan Wang later became ByteDance's angel investor.¹¹³
- **2012** – Left 99Fang.com to start ByteDance.¹¹⁴



ByteDance founder Zhang Yiming, who stepped down as chairman in 2021.¹¹⁵

3.2. How ByteDance Became an “App Factory”

ByteDance soon developed a reputation as an “app factory”. Until November 2021, the company was structured around a large “central platform” that facilitated **resource-sharing** of the technology stack, the recommendation algorithm, and the user database **across the company’s different apps**.¹¹⁶ The first ByteDance app to take off was Today’s Headlines (in Chinese, *Jinri Toutiao*, or simply *Toutiao*), a news aggregator that used big data to drive its personalised recommendation engine. **The AI that powered this engine was the precursor to TikTok’s “For You” algorithm**.¹¹⁷



*Liang Rubo (left, circled) and Zhang Yiming (right) with ByteDance colleagues in 2013.*¹¹⁸

The ByteDance Crew



Liang Rubo and Zhang Yiming shared a room at Nankai University. They co-founded 99Fang.com and later also ByteDance.¹¹⁹ Liang became ByteDance CEO and Chairperson in 2021.



Zhang Lidong joined ByteDance as Senior VP and Partner in 2013, contributing to early successes with Today’s Headlines. He was previously VP at Beijing Times and Director of its advertising centre.¹²⁰ Zhang Lidong is now Chairperson of Douyin Group.



Kelly Zhang (Zhang Nan) joined ByteDance in 2013 to oversee user-generated content. She previously helped found two tech companies and started a photo-sharing app, Picture Bar, which ByteDance later acquired. Kelly Zhang is now CEO of Douyin Group.¹²¹



ByteDance was struggling to lure investors until the company was introduced in 2013 to Digital Sky Technologies (DST). When then-DST partner **Shouzi Chew** heard Zhang Yiming’s pitch, he signed off on USD 10 million in Series B funding for ByteDance.¹²² Shouzi Chew is now CEO at TikTok.

3.3. From Musical.ly to TikTok

For all of ByteDance's ingenuity in building consumer apps, Douyin and TikTok's success hinged in part on a rival app called Musical.ly.¹²³ ByteDance launched TikTok in May 2017 as an overseas analogue of Douyin, before acquiring TikTok's North America and Europe competitor Musical.ly in November 2017.

TikTok and ByteDance said in a 2020 petition to U.S. regulators that the recommendation algorithm came from TikTok, not Musical.ly.¹²⁴ Prior to the acquisition, however, Musical.ly co-founder Louis Yang reportedly complained that Douyin had copied Musical.ly. Yang told Chinese media that whether in market positioning, functions, or user interface, Douyin was almost a pixel-level replica of Musical.ly.¹²⁵

TikTok's Origins in Musical.ly

- **2014** – Alex Zhu and Louis Yang, former directors of a Shanghai platform for the insurance industry, released the first version of Musical.ly.¹²⁶
- **2016** – The Musical.ly app – launched in China, the U.S., Europe, and Japan – failed in China but grew popular among American teens through viral challenges and lip-sync videos.¹²⁷ Musical.ly attracted attention for its young user base. Its three most popular content creators in late 2016 were between the ages of 13 to 15, while the platform's audience was even younger.¹²⁸
- **Sep 2016** – At a conference, Zhang Yiming called short videos the next frontier of content innovation and emphasised the value of personalised recommendation algorithms for short videos. He also announced the allocation of RMB 1 billion to short video creators on Today's Headlines.¹²⁹ The same month, ByteDance launched Douyin as a clone of Musical.ly, according to early Douyin employees.¹³⁰
- **May 2017** – ByteDance launched TikTok overseas as an analogue of Douyin.¹³¹
- **Nov 2017** – Struggling to commercialise the platform and break into the China market, Musical.ly's growth plateaued.¹³² ByteDance acquired Musical.ly, its market share and user data, for around USD 800 million to 1 billion.¹³³
- **Aug 2018** – ByteDance merged TikTok and Musical.ly, making the new TikTok available in the United States for the first time.¹³⁴ In 2018 alone, ByteDance spent over USD 1 billion on advertising on major social media competitors such as YouTube, Instagram and Snapchat to attract new users to TikTok.¹³⁵

3.4. Party-Enabled Global Expansion

While media have cast ByteDance's expansion abroad as a tale of Zhang Yiming's daring and ambition, he also had evidently close relations with Beijing's internet regulator Lu Wei and leading venture capitalist Neil Shen (Shen Nanpeng). Both Lu and Shen served as gatekeepers for the expansion of tech companies, calibrating access to capital, social ties, and, crucially, Party support. Lu's ties to Zhang Yiming have become clearer in hindsight.

Zhang Yiming's Early Encounters with Party Gatekeepers Lu Wei and Neil Shen

- **Pre-Mar 2012** – Sequoia Capital China's Neil Shen rejected an offer from Zhang Yiming to invest in ByteDance first round financing. (In May 2021, when on the ByteDance board, Shen said he regretted that decision.¹³⁶)
- **Oct 2013** – Lu Wei and Zhang Yiming attended the 2nd China-South Korea Internet roundtable conference, one of their earliest public meetings.¹³⁷
- **Nov 2014** – Lu Wei, Neil Shen, and Zhang Yiming attended the first Wuzhen World Internet Conference.¹³⁸ Zhang Yiming spoke about machines liberating people in media.¹³⁹
- **Dec 2014** – Lu Wei attended the 7th U.S.-China Internet Industry Forum in Washington, D.C.¹⁴⁰ He then visited Tim Cook, Mark Zuckerberg, and Jeff Bezos at their company headquarters.¹⁴¹



Lu Wei with Jeff Bezos, Tim Cook, and Mark Zuckerberg at their respective offices in 2014.

- **Sep 2015** – Xi Jinping, Lu Wei, Neil Shen, Zhang Yiming, and the titans of the tech world attended the 8th U.S.-China Internet Industry Forum at Microsoft HQ near Seattle.¹⁴² Zhang did not make it to the group picture but joined a panel (with the CEOs of LinkedIn, Sina, and Expedia) about the differences between U.S. and Chinese internet users.¹⁴³ In an interview with Global Times after the forum, he proclaimed that the model of “copying to China” had given way to PRC enterprises expanding abroad.¹⁴⁴



Left to right, circled: Xi Jinping, Lu Wei, and Neil Shen at the 8th U.S.-China Internet Industry Forum. Zhang Yiming attended the forum but did not appear in the group photo.¹⁴⁵

- Dec 2015 – Xi Jinping, Lu Wei, Neil Shen, and Zhang Yiming attended the second Wuzhen World Internet Conference.¹⁴⁶



Left to right, circled: Zhang Yiming, Neil Shen, Xi Jinping, and Lu Wei at the 2015 Wuzhen World Internet Conference.¹⁴⁷

3.4.1. The Downfall of the Internet Czar

Lu Wei was dismissed from his position as director of the Cyberspace Administration of China in June 2016. He remained as Deputy Director of the Central Propaganda Department until November 2017, when the Communist Party's Central Commission for Discipline Inspection (CCDI) announced that he was suspected of serious violations of discipline.¹⁴⁸ In December 2018, the CCDI expelled Lu Wei from the Party for a laundry list of crimes, before the court sentenced him to 14 years in prison in March 2019.¹⁴⁹

In April 2018, the State Administration of Press, Publication, Radio, Film and Television (SAPPRFT) shut down Implied Jokes (one of ByteDance's community apps – Chinese name *Neihan Duanzi*) for hosting off-colour humour.¹⁵⁰ A U.S.-based watchdog group, China Digital Times, alleged that, on the night of SAPPRFT's decision, a chat screenshot circulated on WeChat, claiming there had been a transfer of benefits between Zhang Yiming and Lu Wei, and that this transfer of benefits had propelled ByteDance to the top tier of tech companies within four years.¹⁵¹

Two years later, in 2020, Chinese media outlet Caixin reported that Today's Headlines' suspected involvement in Lu Wei's downfall had generated concern on the market.¹⁵²

4. The Party-State Transforms ByteDance

This section examines the Party's campaign to subordinate ByteDance.

- a. **Opaque Party Control:** The past five years of ByteDance history is a story of increasing Party control, amid an industry-wide campaign of state regulation and Party pressure.
- b. **Zhang Yiming's Fall from Grace:** After ByteDance acquired Musical.ly in 2017, the Party intensified pressure to transform the company into a vehicle for Party interests, reaching its denouement with Zhang Yiming's high-profile public apology and resignation as CEO in 2021.
- c. **Zhang's Confession (2020):** *"I have deeply reflected on the roots of the problem that the company faces . . . a lack of education on socialist core values, and deviation from guiding public opinion."*

When TikTok Inc. and ByteDance Ltd. sued the Trump administration in August 2020 for banning the TikTok app, they stressed in court papers that the company is and has always been a wholly private entity:

*The TikTok application began as a product of private-sector entrepreneurship. . . .No foreign government, or person controlled by or acting on behalf of a foreign government, owns any significant interest or any other affirmative or negative rights or powers in ByteDance.*¹⁵³

This claim is misleading. A longer-term, **centrally directed shift toward imposing hidden but powerful structures of Communist Party control inside private enterprise** has developed at the expense of more transparent structures of corporate control. The power of the Party's internal systems of committees and cells used to wield control over companies is reinforced by external levers, both legal (through mechanisms of the state) and extra-legal (through the Party's own mechanisms, which sit outside the legal system).

4.1. Party Control in Private Companies

The divide between private and public companies in China has narrowed in recent years through the Party's aggressive expansion of Party organisations within private firms and its use of extra-legal measures to purge prominent leaders within those firms. The Party's multiple channels of control operate alongside legal channels in relation to strategic

decision-making and management of risks. **Party structures are not designed to be visible or accountable to international regulators, partners, investors, or consumers.**

Party members in Chinese private companies are required to establish Party cells in all organisations with three or more full Party members, according to the CCP Constitution.¹⁵⁴ The CCP Constitution stipulates that Party members are required to privilege Party interests and protect its secrets in all circumstances. All Party members take an oath to this effect.

In practice, this means the activities of Party cells, committees and individual members are visible and accountable only to those in the Party organisation. An understanding of the Party's operations inside ByteDance can only be gleaned by analysis of fragmentary open-source information, interpreted in the context of the Party's history, doctrine and practices.

4.2. State Media Scrutiny

ByteDance's transformation into a Party-state-controlled entity was systematic and protracted. The signs of misalignment with Party-state directives began in 2014, two years after the founding of the company. Zhang Yiming was vocal about his vision for Today's Headlines as a tech company, not a media company. This attracted criticism from competitors and some in the Party that Today's Headlines was a "news porter" stealing material from other producers and feeding users "vulgar content".¹⁵⁵

Company officials told critics the app was a search engine that recommended content from other outlets.¹⁵⁶ But in June 2014, China's National Copyright Administration (NCA) launched an investigation into the platform.¹⁵⁷ By September 2014, the NCA found Today's Headlines guilty of copyright infringement, though it acknowledged the platform had removed infringing media and developed cooperation agreements with content producers.¹⁵⁸

Internet czar Lu Wei's relationship with Zhang Yiming may have shielded the company for some time from the heat. The New York Times reported:

*[When] other internet companies complained that [Today's Headlines] was stealing their content, **one of Mr. Lu's top lieutenants told them that he was a fan and that they should stop complaining and work with the company.***¹⁵⁹

In a landmark 2016 interview with Caijing, Zhang Yiming insisted that ByteDance was not a media company and was therefore free from any obligation to "educate users":

*The difference between [Today's Headlines] and the media is this: The media must have values and it must educate people. . . . **We will bear corporate social***

*responsibility, but we do not want to educate users. . . I may have my opinions, but I don't want to impose my judgment on Today's Headlines.*¹⁶⁰

Zhang Yiming did not want ByteDance to operate like a newspaper with an editor-in-chief curating content. His approach was similar to the way Silicon Valley tech firms operate, where digital platforms are treated differently under U.S. law than traditional publishers, and are not liable for the content that human users or algorithms post and promote.

But his vision didn't sit well with Communist Party leadership.

4.2.1. Party Crackdown Prompts Greater Alignment

The scrutiny ByteDance faced over copyright infringement and its hosting of “vulgar content” was a prelude for a frontal encounter with the Party which left ByteDance a permanently changed company.

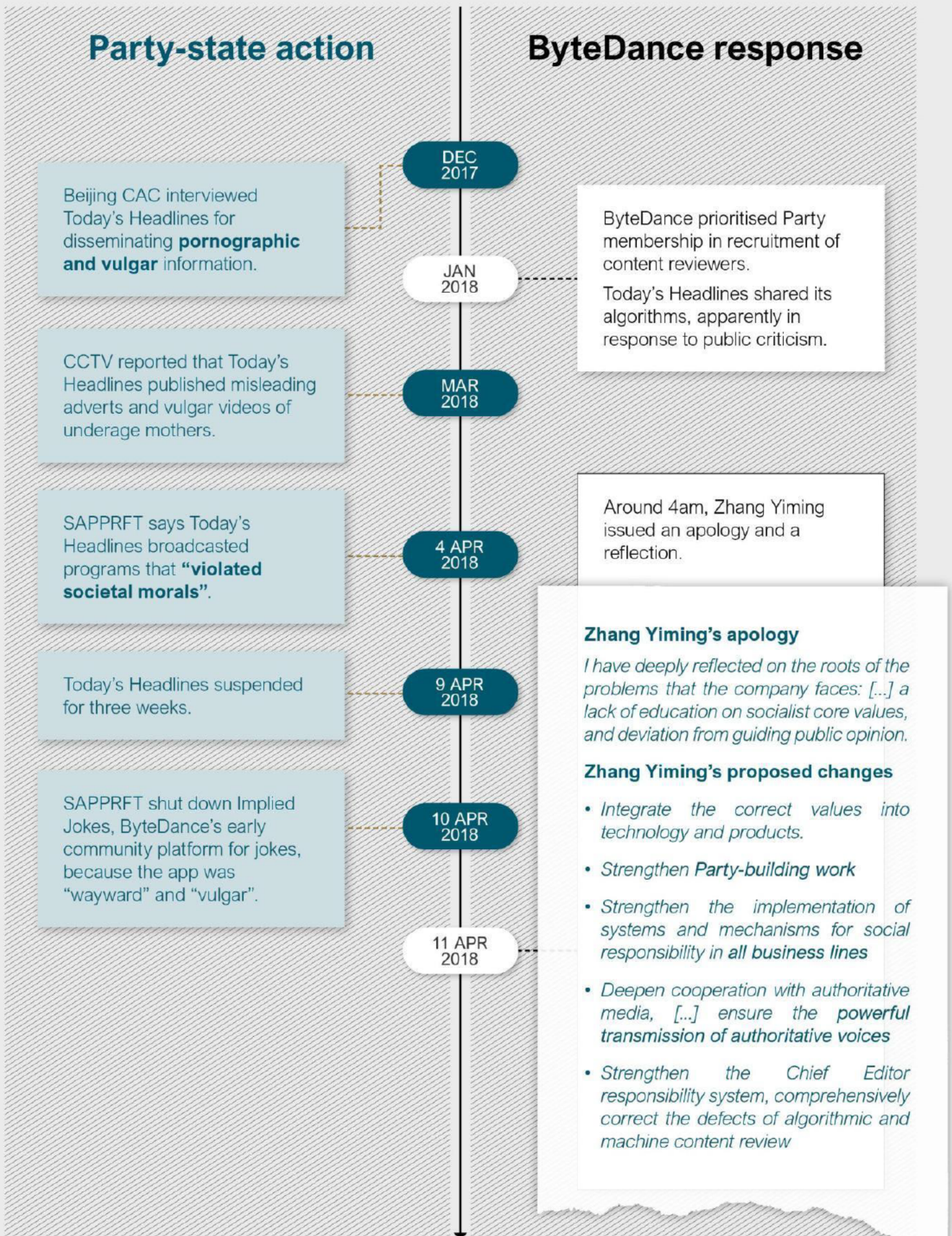
Beginning around 2017, a series of actions from the Party elicited reactions from the company to align itself more with the Party.¹⁶¹ In 2017 Party regulators scrutinised Today's Headlines for disseminating “vulgar” information. In 2018, the platform was criticised by state media and suspended for three weeks.¹⁶²

4.2.2. Pressure Leads to Zhang Yiming's Resignation

In 2021, like the founder-CEOs of Alibaba and Pinduoduo, Zhang relinquished his seat.¹⁶³

The graphics on the following two pages detail how, over time, the Party has forced ByteDance into greater political alignment.

The Transformation of ByteDance (Part 1)



The Transformation of ByteDance (Part 2)

Party-state action

ByteDance response

The National Anti-Pornography and Anti-Illegal Publications Office fined Douyin for its pornographic and vulgar content.

JAN
2021

SAMR fined ByteDance for failing to report a previous merger.

ByteDance and peers ordered to conduct a security review of deepfake technology.

MAR
2021

MAR
2021

Zhang Yiming shelved IPO plans after meeting cyberspace and securities regulators, according to Wall Street Journal.

Zhang Yiming began floating the idea of Liang Rubo taking over as CEO.

SAMR, the CAC, and the State Taxation Administration summoned ByteDance and its peers, warned them to heed Alibaba's example, and required public pledges to comply with anti-monopoly laws.

APR
2021

Financial regulators imposed tighter data and lending regulations on ByteDance and other internet companies.

MAY
2021

Zhang Yiming announced his resignation as ByteDance CEO, and appointed Liang Rubo as his successor.

Zhang Yiming's letter to the company

I've decided to resign as CEO and place aside the day-to-day responsibilities of management. As founder of the company, I will focus on important things for the long-term such as strategic vision, corporate culture, and social responsibility.

5. Tracing Communist Party Control Through ByteDance and TikTok

This section shows how, contrary to official talking points, ByteDance and TikTok are part of the same corporate group, with ByteDance executives directly controlling and shaping key TikTok functions.

- a. **Distinction without a Difference:** TikTok is a 100% owned subsidiary of ByteDance, bound by ownership ties, management structure, personnel overlap, and shared technological resources.
- b. **The CCP's Golden Share:** It is misleading to discuss corporate leadership without Party leadership. The Party-state's 1% 'golden share' gives legal form to the extra-legal access and influence which it already enjoyed.
- c. **ByteDance's 'Red Leaders':** We identify the leaders at ByteDance who integrate company management with Party organisation, particularly the propaganda and 'united front' systems.

5.1. Obfuscating Relations between TikTok and ByteDance, TikTok and Douyin

As TikTok continues to be scrutinised overseas for its links to the CCP – which it flatly denies – the company has also downplayed its ties to parent company ByteDance and emphasised the separateness of Douyin from TikTok:

- **Asserting TikTok's distinction from Douyin:** To magnify the apparent differences between TikTok and Douyin, ByteDance and TikTok spokespersons emphasise that TikTok is operated separately from Douyin and that TikTok is not available in mainland China.¹⁶⁶
- **Hiring 'global' leadership:** Since 2020, TikTok has had three CEOs from outside China. Kevin Mayer, a former Disney executive, was brought on as TikTok CEO in May 2020, reporting to Zhang Yiming, before resigning after just four months.¹⁶⁷ Vanessa Pappas then became interim CEO, until Shouzi Chew's appointment in April 2021.¹⁶⁸
- **TikTok sans headquarters:** TikTok engages in what has been called "Singapore-washing" to deflect the increased scrutiny facing companies from China.¹⁶⁹ Leaders have asserted that TikTok is not headquartered in China but is a "distributed" company with offices all around the world and a significant

presence in Singapore.¹⁷⁰ In addition to native Singaporean TikTok CEO Shouzi Chew, multiple ByteDance executives are now at least partially based there: founder and former CEO Zhang Yiming, CEO Liang Rubo, CFO Julie Gao, and TikTok’s global R&D head Zhu Wenjia.¹⁷¹

- **Changes to company name:** ByteDance renamed several subsidiaries from “ByteDance” to “Douyin” in May 2022.¹⁷² TikTok CEO Shouzi Chew explained in a 30 June 2022 letter to the U.S. Congress that *“multiple corporate entities share the ‘ByteDance’ name, [therefore] several China-based ByteDance entities were renamed earlier this year to keep the names of businesses and entities more consistent. Beijing ByteDance Technology Co. Ltd is now called Beijing Douyin Information Service Limited.”*¹⁷³ Observers have read this as another move to distance TikTok from its China operations.¹⁷⁴

5.2. TikTok Belongs to ByteDance

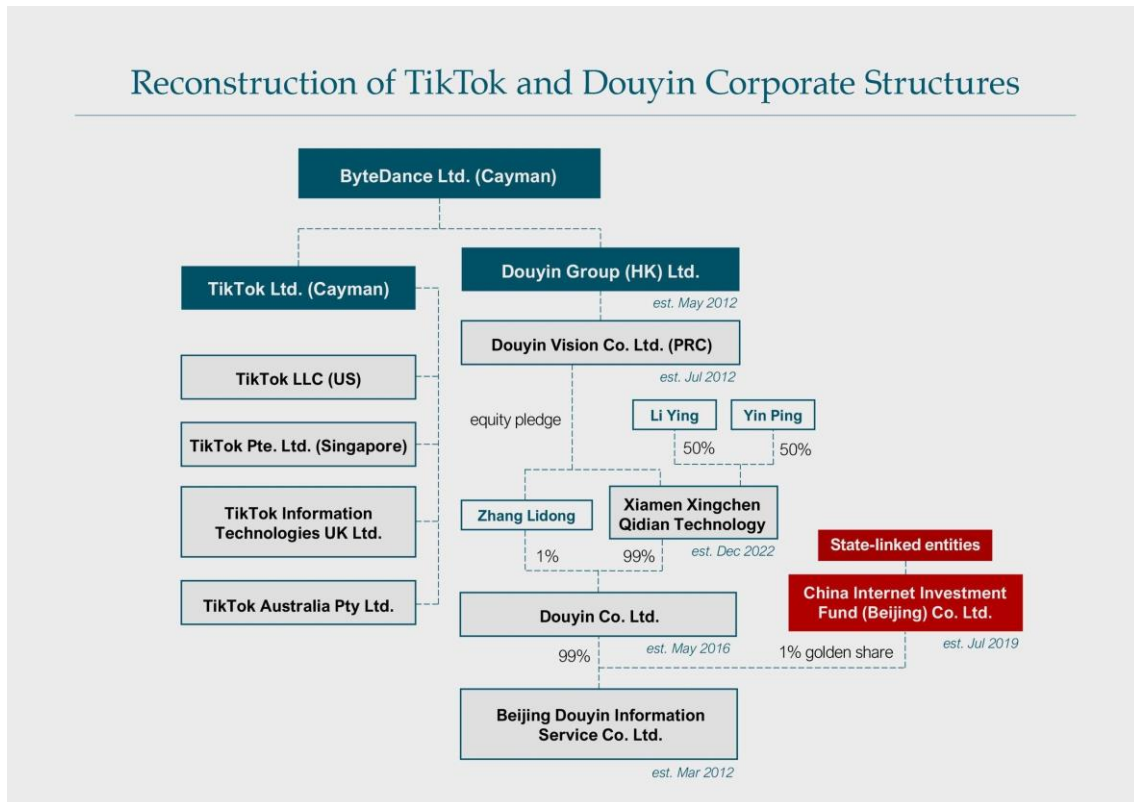
Legal documents and archived versions of the companies’ websites offer some insight into the corporate group’s opaque structure.

5.2.1. ByteDance is the Parent Company of TikTok and Douyin

According to a legal petition that TikTok Inc. and ByteDance Ltd. filed on 10 November 2020, ByteDance Ltd. (Cayman), owns TikTok Ltd. (Cayman), which wholly owns TikTok LLC, a Delaware limited liability company.¹⁷⁵ TikTok LLC holds “all of the outstanding shares of capital stock of TikTok Inc.”¹⁷⁶ An archived version of ByteDance’s website that shows a corporate structure last updated on 30 June 2020 confirms this chain of ownership.¹⁷⁷

Douyin and other PRC operations are likely held through a Hong Kong subsidiary, Douyin Group (Hong Kong) Ltd.¹⁷⁸ In January 2023, Hong Kong Economic Journal reported that Douyin Co. Ltd is an entity that ByteDance established in Mainland China under the variable interest entity (VIE) structure for business operations.¹⁷⁹

Reconstruction of TikTok and Douyin Corporate Structures



Sources: Evidence submitted to court by TikTok, ByteDance’s website, PRC (including Hong Kong) online corporate databases¹⁸⁰

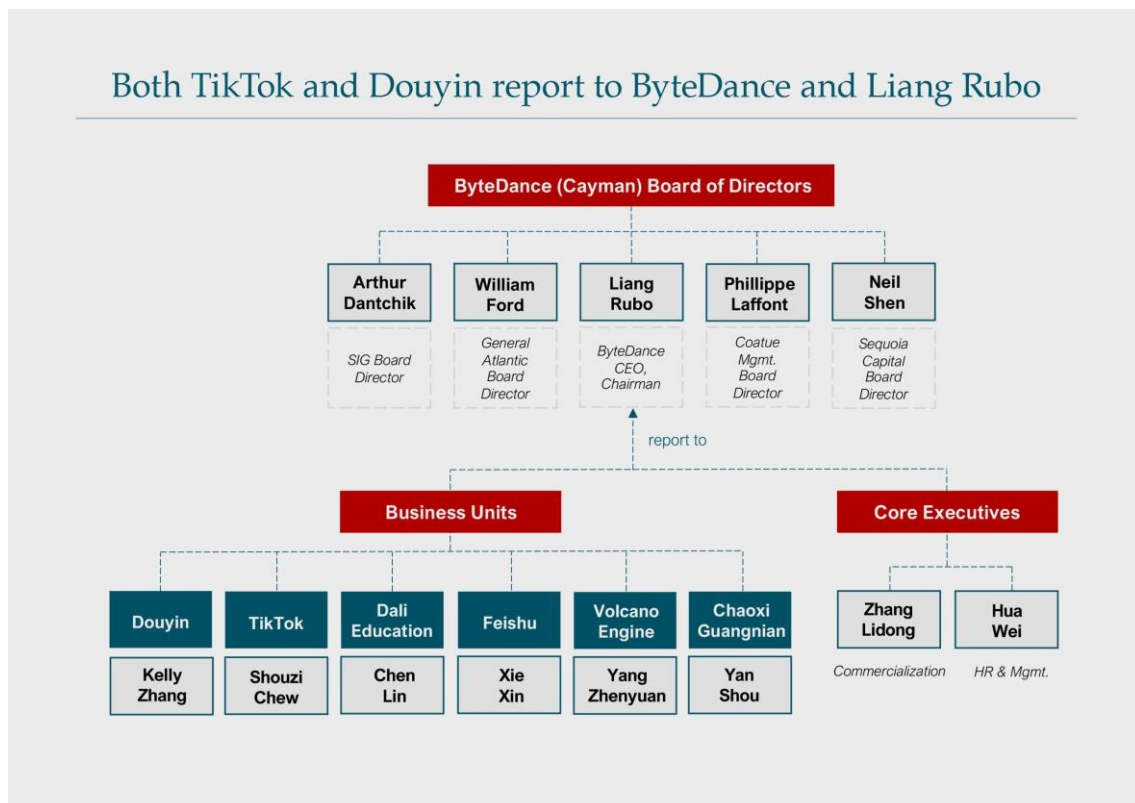
5.2.2. Headquartered in China

While the parent company that owns TikTok is incorporated in the Cayman Islands, ByteDance declared in November 2020 that its headquarters were in China. ByteDance referred to itself as a “Chinese-headquartered company” multiple times in its appeal against the U.S. official Divestment Order and CFIUS action:

*[TikTok Inc. and ByteDance Ltd.] did not submit the Musical.ly transaction to CFIUS for review in 2017 because **ByteDance was a Chinese-headquartered company and Musical.ly was also a Chinese-headquartered company.** . . . It is necessarily the case that whatever national security risks posed by the **Musical.ly app and its Chinese ownership** at the time of the acquisition were not enlarged or changed by the acquisition of the Musical.ly company by another **China-headquartered company, ByteDance.**¹⁸¹*

5.2.3. ByteDance Co-Founder Liang Rubo Leads Both TikTok and Douyin

Liang Rubo is CEO and Chairperson of the global ByteDance corporate group. ByteDance Ltd. (Cayman) currently lists Liang as one of its five directors on the Cayman Islands company registry.¹⁸² Both TikTok CEO Shouzi Chew and Douyin Group CEO Kelly Zhang report to Liang, at least nominally. On 2 November 2021, Liang announced the company’s organisational restructuring (in a letter published on Sina).¹⁸³ Liang stated that the individuals in charge of each of the six business units would report to him, including TikTok CEO Shouzi Chew and Douyin Group CEO Kelly Zhang.¹⁸⁴



Sources: Cayman Islands Registry, Shouzi Chew letter to U.S. senators, Liang Rubo letter to the company¹⁸⁵

Liang Rubo is a visible link between the Cayman company’s board and ByteDance’s China operations. He occupies various management positions in the company’s China-based subsidiaries, despite claims that the Cayman board is divorced from China operations.¹⁸⁶

Overlapping Leadership At TikTok And Douyin

Douyin



TikTok



Head of Operations at Douyin in 2017.



Ren Lifeng

Oversaw the launch of TikTok in 2017.

Douyin CEO in China.



Kelly Zhang

Put in charge of TikTok in October 2018.

Managed Douyin in March 2018, reported to Douyin CEO Kelly Zhang Nan.



Alex Zhu

Musical.ly founder; made "interim" CEO in October 2018, reporting to Zhang Yiming.

Current Douyin Group CEO.



Zhang Lidong

Leads TikTok's commercialisation; 'dotted line' manager to TikTok President of Global Business Solutions Blake Chandlee.

Responsible for the success of the Douyin algorithm.



Zhu Wenjia

Leads PRC-, Singapore-, and US-based teams working on product R&D, data infrastructure, and innovation.

Douyin President of E-Commerce Business.



Bob Kang

Oversees TikTok's e-commerce expansion.

5.3. Zhang Yiming's Retreat from ByteDance Appears Complete

On 19 January 2023, according to PRC corporate databases, Zhang Yiming transferred his 99% stake in Douyin Co. Ltd. to Xiamen Xingchen Qidian Technology Co. Ltd. (which was established just a month before).¹⁸⁸ Soon after the transfer, Xiamen Xingchen Qidian Technology Co. Ltd. pledged its equity in Douyin Co. Ltd. to Douyin Vision Co. Ltd., a wholly foreign-owned entity of Douyin Group (Hong Kong) Ltd.¹⁸⁹ (This transfer of shares has reignited rumours of an impending IPO.¹⁹⁰)

5.4. TikTok's Management Structure

Our reconstruction of the company's management structure indicates that TikTok leadership report up to their department leads in ByteDance (in addition to or instead of reporting to local TikTok managers), sometimes through 'dotted' reporting lines.¹⁹¹ Through department-specific reporting lines, it appears that ByteDance may be able to exercise significant and granular control over TikTok operations.

A ByteDance insider reportedly told China tech outlet LatePost last year that TikTok is not developed enough to be a self-contained business unit.¹⁹² Therefore, per the source, TikTok draws on personnel, experience, and methods of ByteDance's Douyin app, software, and commercial model to achieve "technology accumulation and business breakthroughs".¹⁹³

Whistleblower accounts from former and current TikTok employees attest to the closeness of the two companies. These accounts portray the ByteDance office in Beijing making decisions both large and small about TikTok's content moderation, product development, engineering, commercialisation, strategy and human resources.¹⁹⁴ Forbes reported in September 2022 that senior TikTok executives had left the company because of the degree of ByteDance control.¹⁹⁵

5.5. Shared Resources

In our assessment, it is not possible for TikTok to operate independently of ByteDance in Beijing for reasons including the sharing of technical and human resources across the global corporate groups. This has profound implications not just for TikTok's current relations with ByteDance, but for any *future possibility* of isolating TikTok operations – and foreign users' personal data – from ByteDance.

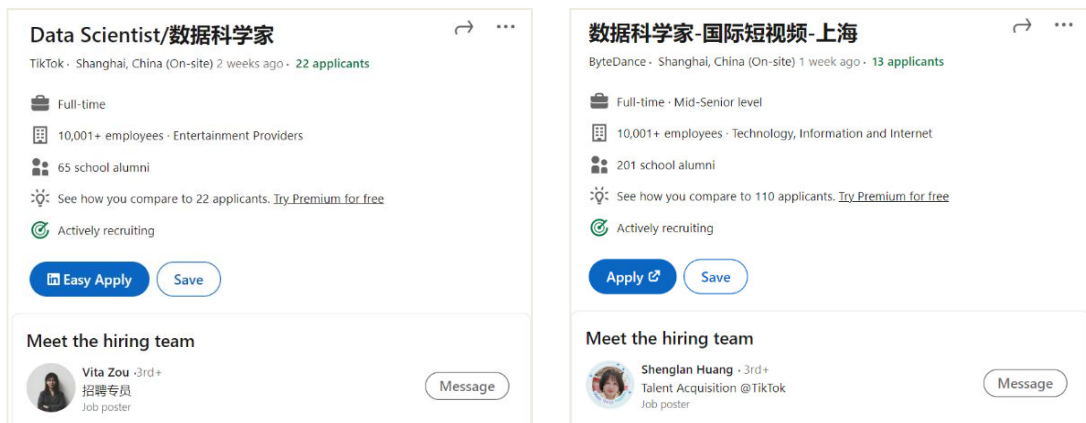
5.5.1. Personnel

The application of China's regulations to TikTok operations within its borders is unambiguous: ByteDance employees who are citizens must disclose information from TikTok relevant to national security and intelligence work.

Under Article 77 of the National Security Law, citizens and organisations have a duty to report acts harming national security, and to support national security, public security, and relevant military bodies.¹⁹⁶ Under Article 7 of the National Intelligence Law, citizens and organisations must support, assist, and coordinate with national intelligence work.¹⁹⁷ In our assessment, these laws codify what was previously extra-legal common practice.

Our research corroborates media reporting that [ByteDance continues to depend on employees in China to work on TikTok](#) and to recruit employees from China for roles at TikTok.¹⁹⁸

In November 2022, for example, TikTok posted a job ad for a “Data Scientist” based in Shanghai. A week later, an ad with the same description posted by ByteDance for a “Data Scientist – International Short Videos – Shanghai” showed that the hiring team belonged to “Talent Acquisition @ TikTok”.



*Cross-posting of job ads for TikTok/ByteDance roles.*¹⁹⁹

We found similar examples, not just for data scientists and analysts, but also for account directors (commercialisation), R&D engineers, and algorithm engineers.²⁰⁰ Both TikTok and ByteDance regularly cross-post job advertisements with the same position IDs.²⁰¹

5.5.2. Management and Employees See TikTok and ByteDance as Interchangeable

A simple search on LinkedIn shows at least 4400 people who list “ByteDance” and “TikTok” in a single profile.²⁰² A significant number of profiles list ByteDance and TikTok interchangeably, including prominent TikTok leaders such as Blake Chandlee, “President, Global Business Solutions at ByteDance/TikTok”.²⁰³

This echoes reporting by Forbes that TikTok employees had ByteDance listed on their pay checks and tax returns, and by CNBC as well as Forbes reporter Emily Baker-White that TikTok email aliases are simultaneously ByteDance email aliases.²⁰⁴ It points to the fungibility of ByteDance and TikTok as employer.

5.5.3. Shared Cloud Infrastructure Team

The cloud infrastructures for both TikTok and other ByteDance products appear to be administered by the same team. A role titled “Tech Lead (Database Administrator), Cloud Infrastructure” manages database services within ByteDance, providing “online storage service support for all types of products in ByteDance (TikTok, Douyin, [Today’s Headlines], etc)”.²⁰⁵ This role may be akin to a China-based “Master Admin” that BuzzFeed reporting refers to, who reportedly has access to U.S. user data.²⁰⁶

The ties that bind TikTok to ByteDance, coupled with the presence of robust Party control, raise the likelihood of Communist Party influence over TikTok.

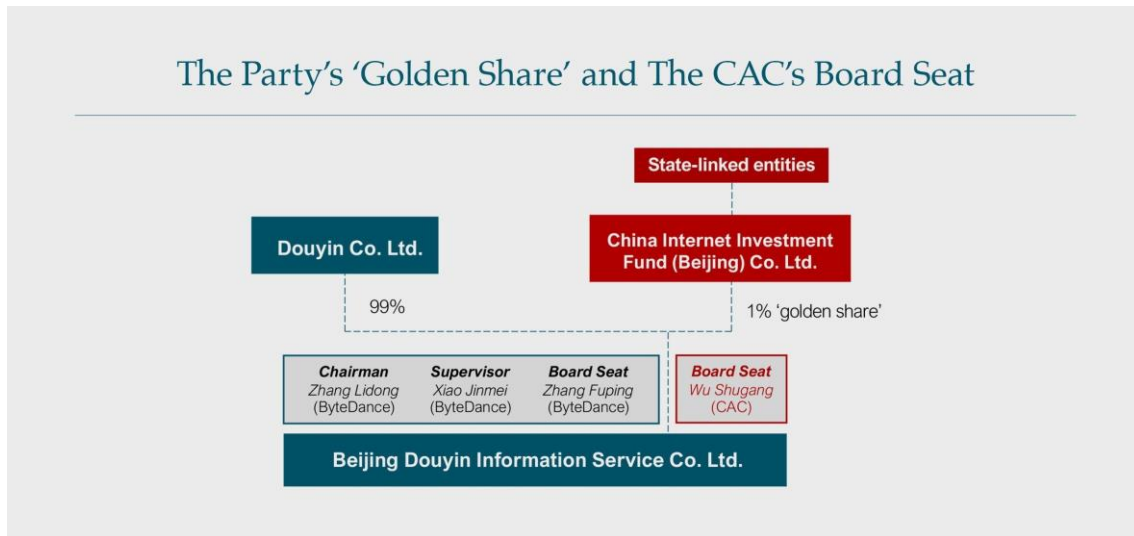
5.6. The Party-State’s Stake in Beijing Douyin

Beijing Douyin Information Service Limited, renamed from Beijing ByteDance Technology Co., Ltd. was established in March 2012 at the company’s founding.²⁰⁷ The Party-state formally registered a 1% stake in Beijing Douyin Information Service Limited in April 2021.²⁰⁸ The largest beneficial owners of this 1% stake are the State-owned Assets Supervision and Administration Commission (SASAC, which oversees state enterprises), China Media Group, and the Cyberspace Administration of China.²⁰⁹

The company’s own statements imply that the government stake was required by regulators. Responding to direct questioning in a letter to U.S. senators about whether the Chinese government owns a stake in TikTok, CEO Shouzi Chew clarified:

Beijing Douyin Information Service Limited is a separately held subsidiary of ByteDance Ltd. Beijing Douyin Information Service Limited does not have any direct or indirect ownership interest in or control over any TikTok entity. The Chinese state-owned enterprise’s acquisition of 1% of Beijing Douyin Information Service Limited was necessary for the purpose of obtaining a news license in China for several China-based content applications, such as Douyin and [Today’s Headlines].²¹⁰

The Party-state’s acquisition of “golden shares” in private tech companies gives it direct and open insider access to corporate decision-making, and influence through board seats and veto rights. This institutionalisation of Party alignment can limit or eliminate the need for subsequent state intervention.



Source: PRC online corporate databases²¹¹

In the case of ByteDance, the Cyberspace Administration of China (CAC) – China’s internet regulator and the external ‘nameplate’ and office of the CCP Central Cybersecurity and Informatisation Commission – appointed an official, Wu Shugang, to the board of Beijing Douyin Information Service Limited at the time of the ‘golden share’ acquisition.²¹²

A Financial Times review of the company charter provides details about Wu’s powers within the company: Wu reportedly gets a say over business strategy and investment plans, M&A, profit allocation, and a vote on the group’s top three executives and remuneration packages.²¹³ Wu can control the content on ByteDance’s media platforms in China, such as Douyin and Today’s Headlines, through his right to appoint the group’s editor-in-chief and the chair of a “content safety committee”.²¹⁴

Wu gained notoriety a decade ago from his June 2012 Weibo post:

I only have one wish – that one day I can cut off the dog head of traitors [i.e. liberal voices in China]. Let the Chinese traitors preaching so-called ‘human rights and freedom’ go to hell!!²¹⁵

Later, Wu became Party secretary of the Communist Youth League for organs directly under the Ministry of Education.²¹⁶



The notorious 2012 Weibo post of cyber regulator and now Douyin board member Wu Shugang.²¹⁷

Before joining ByteDance, Wu Shugang worked in the Local Guidance Office of the CAC's Online Commentary Work Bureau. He visited internet companies to give lectures to Party members about instructions from Xi Jinping and events such as the 19th Party Congress, particularly in relation to online public opinion and discourse power on the main “battlefield” of the internet.²¹⁸



Wu Shugang, who helps ensure Party alignment within ByteDance through his ‘golden share’ board seat.

5.7. Communist Party Organisation Members within ByteDance

In a 2022 hearing, U.S. Senator Josh Hawley questioned TikTok COO Vanessa Pappas about whether employees were affiliated with the CCP. Pappas responded that she “wouldn’t be able to tell [Hawley] the political affiliation of any individual”, but that among TikTok’s “U.S. and Singapore leadership, there are no CCP members. . . . **Everyone who makes a strategic decision at this platform is not a member of the CCP.**”²¹⁹

According to a Party newspaper, Study Times, ByteDance established its first Party branch in October 2014, followed by a Party committee in April 2017 with branches within Review and Operations, Public Affairs, and Technical Support.²²⁰

The Epoch Times reported that it obtained a list of ByteDance Party members.²²¹ Out of 138 Party committee members at the Beijing headquarters, most were born in the 1990s and many held management or technical positions.²²² We were not able to verify this list, but we note that the report has informed U.S. and Australian government approaches to questioning TikTok.²²³

The CAC has been pushing internet companies such as Alibaba and ByteDance to build up Party organisations.

The Cyberspace Administration of Beijing Municipality (Beijing CAC) mobilised ByteDance to establish a “public opinion research and evaluation small group” as well as an “internet content security committee”, with Party members serving as content “gatekeepers” and overseeing editing, auditing, technology, products, marketing, commercialisation, and other operational areas across the company.²²⁴

Beijing CAC also prescribed integrating the Party organisation with company management by creating a *“triple-hatted position incorporating the roles of Party Secretary, Editor-in-Chief, and Vice President.”*²²⁵

5.7.1. Red Leadership

TikTok executives refer to ByteDance Ltd.’s incorporation outside of China and the international composition of the board as evidence of their parent company’s independence from the CCP. This argument obscures the fact that key executives of parent company ByteDance – which we argue exerts continued influence on TikTok despite structural corporate boundaries – have close ties to the Party.

5.7.2. Party Secrecy Requirements

The Party’s systems for concealing its own control mechanisms begins with its rules and systems for governing itself. New Party members are required to pledge that they will “protect Party secrets”.²²⁶ The Party Constitution requires Party members to prioritise “the interests of the Party . . . before all else” (Article 16).²²⁷

These obligations of secrecy and primacy could conflict with legal obligations to disclose information to investors and regulators in rule-of-law jurisdictions.

Red Leaders at ByteDance

Bytedance Role

Party Role

Bytedance Role:
Founder and former CEO



Zhang Yiming

Party Role:
United front system

Zhang Yiming has links to provincial united front organisations in Fujian, including the Fujian People's Political Consultative Conference, the Fujian Province Overseas Friendship Association, and the Fujian Association for Members of Emerging Social Strata.

Bytedance Role:
Vice President, Chief Editor
of Douyin Group



Zhang Fuping

Party Role:
ByteDance Party secretary;
propaganda system

Before joining ByteDance, Zhang Fuping was Vice President and Deputy Chief Editor of state media Beijing Times.

Bytedance Role:
Vice President of Public
Affairs, Deputy Chief Editor



Feng Kaixu

Party Role:
ByteDance Deputy Party
secretary, united front system

Feng is a well-known calligrapher with links to the All-China Federation of Trade Unions (ACFTU), a united front organisation.

Bytedance Role:
VP of Government Relations



Chen Zhifeng

Party Role:
United front system

Like Feng Kaixu, Chen Zhifeng has been connected to the united front organisation ACFTU. Chen has discussed collaborating with CCP propaganda and united front figures in Fujian

5.7.3. Founder Zhang Yiming

ByteDance founder and former CEO Zhang Yiming told a reporter from The Atlantic in 2020 that he “isn’t a Party member”.²²⁹ However, our research has identified his links to several Fujian Province united front bodies.²³⁰ The purpose of the united front system is to increase Party influence outside the Party.

Zhang Yiming was present when the Central United Front Department began a new campaign engaging media professionals.²³¹ He attended the first ever training for new media professionals in 2015 that focused on how to conduct united front work online. While reflecting on the course, Zhang Yiming shared that the training course allowed him to “develop stronger self-confidence in rejuvenating the country through science and technology and strengthening the country through the internet.”²³²

5.7.4. Chief-Editor-and-Party-Secretary Zhang Fuping

Zhang Fuping joined ByteDance as Deputy Chief Editor of Today’s Headlines in 2016 and rose to Chief Editor the following year.²³³ Following the content crackdown on the company in March 2018, he started making public appearances not just as ByteDance Chief Editor but also as Party Secretary.²³⁴ He was appointed a board member of the Beijing Douyin Information Service Co. Ltd. in April 2021 alongside the CAC’s Wu Shugang.²³⁵

Zhang Fuping is not listed as the company’s Party Secretary on either the Chinese or English versions of ByteDance’s website. Nor does the company identify him as the business’s top-ranked official for political matters.

5.7.5. Board Member Neil Shen of Sequoia Capital

Notable also is Neil Shen, Global Steward of Sequoia Capital and Founder and Managing Partner of Sequoia Capital China, who serves on the board of ByteDance.²³⁶ Shen was a member of the 13th National Committee of the Chinese People’s Political Consultative Conference (CPPCC), a peak united front forum chaired by a member of the Politburo Standing Committee that brings together Party officials and Chinese elites.²³⁷ He was the CPPCC’s only representative from the venture capital sector.²³⁸

Shen is vice president of the Venture Capital Funds Committee of the Asset Management Association of China, which appears to exercise industry leadership in the venture capital field, and director of the Yabuli China Entrepreneurs Forum, which comes under the guidance of the All-China Federation of Industry and Commerce.²³⁹

Notably, Shen was absent from the line-up of the 14th National Committee of the CPPCC revealed in January 2023 (and he left the board of Chinese e-commerce giant Pinduoduo in late 2022).²⁴⁰ This may raise questions about his standing with the Party as it appears to shift its favour from tech firms toward state-owned enterprises.

Sequoia Capital China previously hired Wang Xisha, daughter of former Politburo Standing Committee member Wang Yang, as an investment partner.²⁴¹

6. ByteDance Serves Party Propaganda

This section examines the functional and personnel links between ByteDance and the Party's propaganda apparatus.

- a. **Coming to the Party:** ByteDance cooperates with Beijing's security services and organs of repression to guide public opinion and generate support for repressive activity.
- b. **Influence Through Personnel:** That ByteDance has a Party Secretary who is also "Chief Editor" is just one strand of a web of personnel connections designed to integrate ByteDance into the state propaganda system.
- c. **Narrative shaping:** The biggest risks involve TikTok's unprecedented potential for shaping narratives and curating overseas political landscapes. ByteDance has a demonstrated record of adopting norms in service of Party propaganda.

6.1. Whitewashing the Party-State's Security and Repression Apparatus

ByteDance claims that the company "*does not produce, operate or disseminate any products or services related to surveillance*".²⁴² However, our research shows that ByteDance platform Douyin, TikTok's analogue in China, serves Beijing's security and repression systems in direct and explicit ways.

Through its network of subsidiaries, ByteDance cooperates with military organs on propaganda work. In November 2017, the People's Armed Police, a paramilitary organisation that reports to the Xi-led Central Military Commission, signed a cooperation agreement with Today's Headlines.²⁴³ Chief Editor Zhang Fuping was pictured at a signing ceremony with the director of the Political Work Department in the People's Armed Police, Yan Xiaodong.²⁴⁴ A year and a half later, the People's Armed Police announced their forces would be joining Douyin to "*spread the positive energy of the People's Armed Police*".²⁴⁵

ByteDance also engages in formal cooperation with the Ministry of Public Security (MPS), supporting the MPS to influence and guide public opinion and to provide propaganda that portrays the MPS as being in service to citizens.

Built from the CCP's analogues of Stalin's secret police, the MPS combines traditional police roles with the prosecution of political dissent.²⁴⁶ It is tasked with investigating ideological crimes (including elastic interpretations of inciting the subversion of state power) alongside ordinary crimes recognised and prosecuted in liberal democracies.



*ByteDance Party Secretary and Chief Editor Zhang Fuping (right)
with People's Armed Police Political Work Department Director Yan Xiaodong.²⁴⁷*

ByteDance is not merely a passive host for public security accounts on its Today's Headlines and Douyin platforms. The company offers expert guidance and big data analysis to assist the MPS in its dissemination of propaganda.

In April 2019, the MPS Information and Propaganda Bureau signed a strategic cooperation framework agreement with ByteDance, as the Australian Strategic Policy Institute first reported.²⁴⁸ According to a social media account run by the Public Security Bureau of Yangshan County, Guangdong:

[T]he strategic cooperation agreement aims to maximise [Today's Headlines'] and Douyin's specialised technology and platform advantages in big data analysis, accuracy of push notifications, and creative strategy. The cooperation agreement would . . . elevate public security propaganda in its capacity to influence, guide, and gain public trust . . . creating positive public opinion as an environment for the development and progress of public security work in the new era.²⁴⁹

ByteDance's collaboration with the MPS extends to Xinjiang, where it plays a role in disseminating Party propaganda. According to a report by the Australian Strategic Policy Institute, Xinjiang local authorities received guidance to use Douyin to broadcast a sanitised depiction of state poverty alleviation policies in Hotan, a region of Xinjiang with roughly a dozen suspected detention centres for Uyghur Muslims and other minorities.²⁵⁰ This points to ByteDance's involvement in the Party-state's efforts to whitewash the internment of Uyghurs in Xinjiang.

The United Nations has found that the CCP's repression of non-Chinese ethnic groups may amount to "crimes against humanity" – the most serious allegation the body is able to make, absent an International Criminal Court investigation.²⁵¹

6.2. ByteDance Ties to the Propaganda System

ByteDance and key company executives are members of media associations established to ensure compliance with Party norms. Institutional ties include:

- Kelly Zhang, CEO of Douyin Group, is vice president of the **China Netcasting Services Association**, of which Beijing ByteDance Network Technology is a member.²⁵² Nie Chenxi, former deputy chief of the Central Propaganda Department and a member of the 19th CCP Central Committee, is president of the association.²⁵³ The CCP Central Committee's Propaganda Department controls the National Radio and Television Administration (NRTA), which supervises the China Netcasting Services Association.²⁵⁴ As the largest professional association in the industry, China Netcasting Services Association publishes mandatory standards for online short video platforms.²⁵⁵
- Party Secretary and Chief Editor Zhang Fuping serves as executive vice president at the **Beijing Communication Industry Association**, of which Beijing Douyin Information Service is a member.²⁵⁶ The association "*uses Xi Jinping Thought on Socialism with Chinese Characteristics for a New Era as an operational guide*".²⁵⁷
- ByteDance is a member of the **People's Daily Smart Media Research Institute**.²⁵⁸ One key purpose of the institute is to explore how to use AI in media operations, including "*using mainstream values to control the algorithm, so as to comprehensively improve capacity to guide public opinion*".²⁵⁹
- Beijing Douyin Information Service is an executive corporate member of the **Internet Society of China (ISC)**.²⁶⁰ One of ISC's goals is to "*participate in the formulation of global Internet policies, norms and standards, improve the global internet governance system, and maintain cyberspace order*".²⁶¹

Outside of institutional ties, a notable number of employees have worked for Party propaganda outfits before joining TikTok and ByteDance. In August 2022, Forbes reported that its analysis of public LinkedIn profiles showed "*300 current employees at TikTok and its parent company ByteDance previously worked for Chinese state media*".²⁶² ByteDance and TikTok did not challenge the report's findings.

We independently verified that 10 senior leaders (directors, VPs and managers) at ByteDance and its subsidiaries in China have come from traditional state media, particularly the Beijing Times. Senior leaders with a history in traditional state media include Zhang Lidong, current Chairperson of Douyin Group; Zhang Fuping, Party Secretary, Vice President, and Chief Editor of Douyin; and ByteDance managers in Marketing, PR, Content Moderation, Operations, and Overseas Markets. We identified another three TikTok managers with prior experience in China's state media.

6.3. Party Instruction and Supervision

Beijing's cyber authorities mobilise and monitor internet companies such as ByteDance in times of crisis, such as during Covid-19 and the protests against the government's Zero Covid restrictions. Examples:

- In February 2020, as the Party mobilised against Covid-19, the CAC placed ByteDance (among other internet companies) under "special supervision" to ensure support for "*a good internet environment for winning the battle of Covid prevention and control*".²⁶³
- ByteDance was responsive to Party calls from the Wuhan Internet Industry Party Committee – and from Xi Jinping himself – to crack down on Covid-19 misinformation, anti-government sentiment, foreign reporting and other "*harmful information*", as defined by the Party.²⁶⁴ By late February 2020, ByteDance had set up channels on Douyin, Today's Headlines and its other apps for "*broadcasting positive energy*" and information about the government's epidemic control efforts.²⁶⁵
- More recently, on 1 December 2022, after anti-lockdown protests across major cities in China, the CAC instructed tech companies such as ByteDance to "*expand censorship of protests*", pay attention to content about anti-government protests, and restrict information about how to use VPNs to circumvent state internet controls.²⁶⁶ At an internal meeting, the CAC instructed ByteDance to increase staffing of censorship teams, according to insiders who spoke to the Wall Street Journal.²⁶⁷

6.4. Party-State Control of ByteDance Intellectual Property

The Party-state has emphasised the importance of algorithms and their injection with "mainstream values" for the purposes of propaganda work.

In March 2019, Xi Jinping published an article in Qiushi on "*Accelerating the development of media integration and constructing an omni-media broadcast pattern*". He emphasised the importance of "*exploring the use of AI in news acquisition, production, distribution,*

*reception, and feedback, [while] using mainstream values to guide and harness ‘algorithms’, and comprehensively improving public opinion-shaping capabilities”.*²⁶⁸

By the end of the year, Xi’s words had been enshrined in official guidelines. The instructions came from the CAC and directed internet companies using personalised recommendation algorithms to promote propaganda and refrain from republishing illegal or harmful content.²⁶⁹

Since March 2022, ByteDance has been subject to Article 6 of the CAC’s Internet Information Service Algorithmic Recommendation Management Provisions, which reads:

*Algorithmic recommendation service providers shall uphold the mainstream value orientation, optimise the algorithmic recommendation service mechanism, actively disseminate positive energy, and promote the use of algorithms for good.*²⁷⁰

The Party-state has developed additional levers of control over ByteDance’s intellectual property, such as export restrictions on recommendation algorithms and requirements for algorithms to be submitted for review to cyber regulators.

6.4.1. Export Controls

On 28 August 2020, while discussions were underway with the U.S. government about ByteDance’s potential forced sale of TikTok, China’s Ministry of Commerce and Ministry of Science and Technology added new items to their list of sensitive technologies requiring export controls.²⁷¹ This list included AI interactive interface technology and data analysis-based personalised information push-service technology, both of which TikTok uses.²⁷²

Two days later, on 30 August 2020, state media Xinhua published an article titled “*Planned TikTok deal entails China’s approval under revised catalogue*”.²⁷³ Professor Cui Fan of the University of International Business and Economics advised ByteDance to:

*. . . carefully study the revised catalogue, seriously and carefully consider whether it is necessary to suspend substantive negotiations on relevant transactions, comply with statutory application and reporting procedures, and then take further actions as appropriate”.*²⁷⁴

ByteDance responded the same day that it had seen the Ministries’ announcement and would strictly abide by the regulations.²⁷⁵

On 13 September 2020, ByteDance reportedly informed the U.S. government that its algorithm would not be for sale. A source who spoke to the South China Morning Post said, *“The car can be sold, but not the engine.”*²⁷⁶

6.4.2. Transfer of Personalised Recommendation Algorithm to Cyber Regulators

In March 2022, the CAC, the State Administration for Market Regulation (SAMR), the Ministry of Public Security, and the Ministry of Industry and Information Technology issued new regulations on recommendation algorithms.²⁷⁷ In August 2022, ByteDance submitted its personalised recommendation algorithm to cyber regulators.²⁷⁸ The company professes to use this same algorithm for Douyin, Today’s Headlines, Xigua Videos and other products that recommend content.²⁷⁹

ByteDance likely uses a similar algorithm for TikTok. In 2017, Li Lei, then the head of ByteDance’s AI Lab, said: *“Many of the lessons we have learned can be shared for our international products. . . . We have built the largest machine-learning platform for content. That’s our weapon.”*²⁸⁰

6.5. Censoring Content, Promoting Propaganda

Leaked TikTok documents from 2019 and 2020 established that content moderators were instructed to suppress content about politically sensitive events, figures, and speech, while limiting the viewership of posts from users deemed “ugly”, “fat”, “poor”, “LGBT” or “disabled”.²⁸¹ These leaked documents show the discretionary power of the platform in its selective and opaque restrictions on content and users. Interviews with former or current ByteDance staff, plus whistleblower accounts from former internet censors, have provided glimpses of a content-moderation process combining machine and human review.²⁸²

The body of evidence about censorship on TikTok is credible and substantial. Without disputing the veracity of these accounts, ByteDance and TikTok spokespeople have insisted that offending content moderation guidelines have since been retired.²⁸³

The company has developed a formulaic response to public criticism of censorship on the platform: **Explain there was a technical or policy error (instead of an attempt at censorship), apologise for the error, and declare that the error is now fixed.**²⁸⁴ This applied to media reporting about TikTok’s promotion of racist and anti-LGBTQ+ content, censorship of posts about #BlackLivesMatter, and removal of teenager Feroza Aziz’s account from the platform when she called attention to China’s treatment of Uyghurs in a makeup tutorial.²⁸⁵

ByteDance and TikTok assert that censorship is not a threat, but a close examination of content moderation on Douyin (and other ByteDance platforms in China) suggests otherwise. Content moderation is an existential issue for internet platforms in China, as we have witnessed with Zhang Yiming’s formative experience with Fanfou, one of China’s early Twitter equivalents. Li An, former ByteDance censor, explains:

*What Chinese user-generated content platforms most fear is **failing to delete politically-sensitive content that later puts the company under heavy government scrutiny**. It's a **life-and-death** matter. . . .Content moderation policymakers, plus the army of about 20,000 content moderators, have helped **shield ByteDance from major political repercussions and achieve commercial success**.²⁸⁶*

We have demonstrated how key individuals in ByteDance's company structure ensure Party alignment. In the sections that follow, we map the levers of control over the actual content in Douyin and other ByteDance platforms in China – and their implications for TikTok.

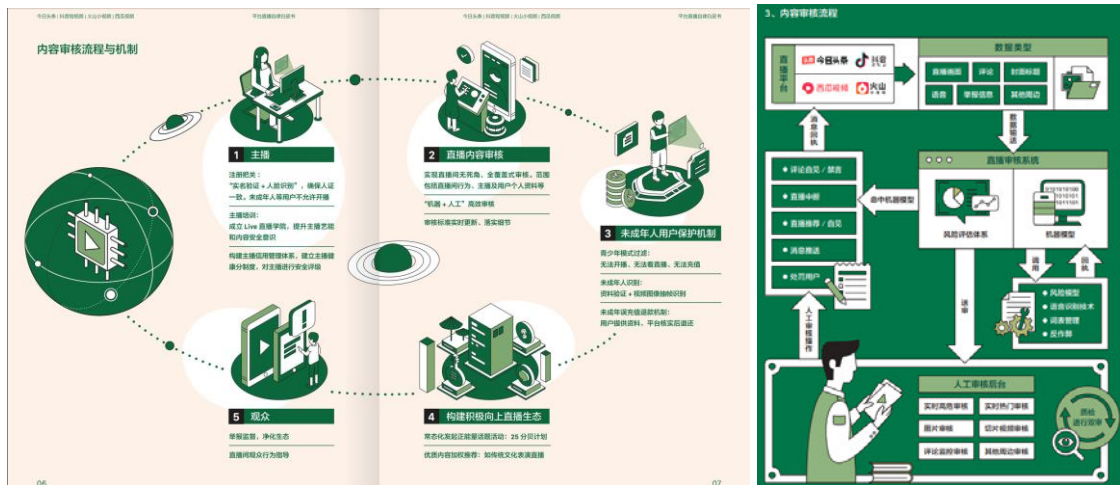
6.5.1. Automated Content Filters

Beijing uses the term “rumour” to label ideas and discourse critical of the Party-state.²⁸⁷ ByteDance notes in its 2018 Corporate Social Responsibility (CSR) report the measures it took to combat “rumours”:

- **Created large datasets:** *“Created a ‘rumour database’ of more than 300,000 articles, to filter old rumours. Agreed to cooperate with the CAC’s Illegal and Harmful Information Reporting Centre to work with authorities to share information on rumour databases.”²⁸⁸*
- **Developed targeted content distribution:** *“Launched an accurate rumour-dispelling function to accurately deliver rumour-dispelling articles to people affected by rumours.”²⁸⁹*
- **Harnessed technology:** *“Collaborated with the University of Michigan to establish an anti-rumour research alliance and develop anti-rumour technology.”²⁹⁰*

As recently as September 2022, the CAC led 12 internet platforms – including Douyin – in the tagging of online rumours as part of a dedicated campaign.²⁹¹ In September 2020, ByteDance attended a meeting with the National Anti-Pornography and Anti-Illegal Publications Office on its shared database for harmful information on the internet.²⁹²

A 2019 company White Paper on the “*Self-regulatory Mechanism of Live Video Streaming Platforms*” shows the breadth of ByteDance’s content-review models.²⁹³ ByteDance combines machine learning models (visual, audio, and textual models) with a risk model to vet livestreams in real time.²⁹⁴ It bans illegal and political content, inappropriate dressing, pornographic and vulgar content, abusive and provocative content, and superstitious content, among other categories of prohibited content.²⁹⁵ The rules further prohibit content involving deepfakes, slime, and all-you-can-eat contests.²⁹⁶



ByteDance’s content review process for livestreams includes a combination of machine and human review, as depicted in this diagram from ByteDance’s 2019 White Paper (which has since been taken down).²⁹⁷

The use of technology in content moderation extends to facilitating the work of state censors. Li An, former ByteDance censor, described the job as creating “*technology to make the low-level content moderators’ work more efficient*”.²⁹⁸ Li said:

. . . [the team] received multiple requests from [moderators] to develop an algorithm that could *automatically detect when a Douyin user spoke Uyghur, and then cut off the livestream session . . . because they didn’t understand the language*.²⁹⁹

The tech team decided not to pursue the solution because they “*didn’t have enough Uyghur language data points in [their] system, and the most popular livestream rooms were already closely monitored*”.³⁰⁰

6.5.2. Calibrating Content Distribution

In 2018, ByteDance Party Secretary and Chief Editor Zhang Fuping held a special Party class to study a National Work Conference on Cybersecurity and Informatisation. He declared then that ByteDance should “*transmit the correct political direction, public opinion guidance and value orientation into every business and product line, use values to guide algorithms, [and] create a Today’s Headlines that is more valuable to users and society*”.³⁰¹

ByteDance noted in its 2018 Corporate Social Responsibility (CSR) report that it identified users who received “rumours”, then pushed articles to them that dispelled such rumours.³⁰² This shows the control ByteDance retains over the targeting of content distribution and propaganda.

In November 2021, two employees at ByteDance subsidiaries were jailed by public security organs for accepting bribes to push specific content to Douyin’s trending list.³⁰³ A Douyin spokesperson responded that Douyin’s trending lists are generated by collating real-time trending content and applying content review mechanisms. The feature allows content editors to intervene in trending topics that violate laws and regulations, or public order and customs, or that are overly sensational.³⁰⁴ These charges foreshadowed Forbes reporting in January 2023 about TikTok’s “secret ‘heating’ button” that would help a video reach wider viewership and achieve virality.³⁰⁵

We found a September 2022 ByteDance investor report on a Chinese file-hosting site and assessed it to be authentic based on its visuals and substance.³⁰⁶ It reported that ByteDance *“adjusted its algorithm systems away from a purely commercial logic, strengthened the social value orientation of platform content, and ultimately strengthened control over content”*.³⁰⁷ According to the investor report, measures to control content included *“comprehensively analysing user behaviour and comment sentiment to crackdown on low-quality content such as clickbait and rumours”*; *“using machine learning to create risk identification and filtering models for pornography, vulgarity, and abuse, among others”*; and *“training the ‘positive energy model’ to strengthen the recommendation of content with mainstream values”*.³⁰⁸

6.5.3. Content Moderator Guidelines

In our assessment, the public-facing user service agreement for Douyin shows close alignment with norms promulgated by the China Netcasting Services Association (a state-backed professional association) and the National Radio and Television Administration.

The Association forbids *“content harming the socialist system with Chinese characteristics”*, *“separatist content”*, and *“content damaging the image of revolutionary leaders and heroes”*.³⁰⁹ Per the latest Douyin user service agreement, all *“created, commented, published and disseminated information”* on the platform *“must consciously abide by the law, socialist system, national interests, legal rights of citizens, social public order, morality and customs, and informational veracity”*.³¹⁰ Users must agree not to create or share content that *“threatens national security”*, *“incites separatism”*, *“breaks national unity”*, *“undermines the socialist system”*, or *“promotes evil cults and feudal superstitions”*.³¹¹

The Association further stipulates that, as internet platforms launch their short video services, they should build a content reviewer team of *“high political quality and strong professional capability”*.³¹² The team should undergo training by the National Radio and Television Administration, and there should be a ratio of at least one content reviewer per every thousand new short videos created each day.³¹³

Today’s Headlines prioritised Party members when hiring 2000 content reviewers in January 2018.³¹⁴ ByteDance noted in its 2018 CSR report that it ramped up the size of its content-

auditing team, with a focus on Party membership.³¹⁵ According to former censors, content moderation teams at ByteDance must apply directives received from authorities to new and existing content, often self- and over-censoring to avoid offending the Party.³¹⁶

6.5.4. Peddling Party Propaganda Abroad

Reuters reported that ByteDance censored content it perceived as critical of the Chinese government on its Indonesia news aggregator app, Baca Berita (BaBe), from 2018-2020.³¹⁷ Beijing headquarters reportedly instructed local moderators to delete articles critical of CCP authorities.³¹⁸ In July 2022, BuzzFeed reported claims from former employees that ByteDance pushed “soft” pro-China messaging on its news app TopBuzz, the international version of Today’s Headlines.³¹⁹ According to these employees, TopBuzz staff needed to provide evidence to ByteDance that they had placed the content on the app.³²⁰

The company tried to do the same on TikTok, too: In June 2022, Bloomberg reported that a Chinese government entity responsible for public relations attempted to open a stealth account on TikTok targeting Western audiences with propaganda”.³²¹

6.5.5. Implications for TikTok

ByteDance has demonstrated its capacity to develop automated content filters and calibrate content distribution in service of Party propaganda, apply Party-aligned content norms, and hire Party members as content moderators. Its capabilities to serve Party propaganda are manifold, including a public-opinion early-warning system, AI that automatically generates content, and “automatic targeting” that draws on signals outside its own app.³²²

ByteDance portrays TikTok and Douyin as distinct platforms with no relation to each other. Yet, as mentioned in [Section 6.5.2](#), content-related charges emerged against Douyin employees more than a year before Forbes’s explosive reporting on TikTok’s “secret ‘heating’ button”.³²³ Douyin offers fertile grounds for understanding TikTok, especially due to the current overlap in Douyin and TikTok personnel.

The lack of transparency around algorithm decisions creates additional vulnerabilities. ByteDance retains oversight over TikTok’s algorithms and their development through TikTok Global R&D Lead Zhu Wenjia’s reporting up to ByteDance VP Yang Zhenyuan.³²⁴

In our view, ByteDance has demonstrated sufficient capability, intent, and precedent in promoting Party propaganda on its Chinese platforms to generate material risk that they could do the same on TikTok.

7. ByteDance in China’s Military-Industrial-Surveillance Complex

In this chapter, we shift focus to the Party’s security apparatus, which intersects with ByteDance in significant ways that have to date gone uncharted.

- a. **An Academy for “Military-Civilian Fusion”:** ByteDance is a founding member of the Beijing Academy of Artificial Intelligence, which developed from a state-endorsed plan to harness civilian scientific research for AI-related national defence endeavours.
- b. **Defence Collaborations:** ByteDance researchers have collaborated with defence-linked universities on dual-use technologies such as person re-identification, deepfakes, quantum computing, and deep neural networks.

7.1. The Party-State Nurtures, Guides, and Benefits from ByteDance Tech

ByteDance’s technological advancements have benefited from the Party-state’s incubation of priority science and technology programs. Zhongguancun National Innovation Demonstration Dongcheng Park is one such program – a science and technology park in Beijing established as a government-backed incubation zone for startups. In 2017, ByteDance founder Zhang Yiming won the Zhongguancun Innovation and Entrepreneurship Youth Hero Award, acknowledging the science hub’s contribution to his success:

*Today’s Headlines is representative of enterprises that grew up in Zhongguancun. . . .The growth of Today’s Headlines has benefited from Zhongguancun’s talent and policy advantages.*³²⁵



Then-Science and Technology Minister Xu Guanhua (left) congratulates Zhang Yiming (right) on winning the Zhongguancun Innovation and Entrepreneurship Youth Hero Award in 2017.

Zhang Yiming acknowledged the symbiotic relationship he and his company enjoyed with the Party-state. His award acceptance speech, entitled “*Innovation and Responsibility of Technology Enterprises*”, described the special responsibilities companies like his were required to shoulder as they became more successful.³²⁶ He said:

*In the past, a company might be a node, but after becoming a platform, you are the infrastructure of the society, and the impact on the economy and society is bigger and you need to take on more responsibilities.*³²⁷

At the time, Today’s Headlines had begun cooperation with the Gansu Province Cyberspace Affairs Office to provide a sales platform to merchants in poor counties and assist in tracking down lost people.³²⁸

Party-state support and guidance is ongoing. The current 14th Five-Year Plan for Zhongguancun seeks to “*promote capacity for innovation*” by:

*Encouraging high-tech enterprises to strengthen technological R&D [...]. Through strategic cooperation with companies such as Xiaomi, **ByteDance**, and Tencent, advance the establishment of an innovation platform with **leading innovative internet tech companies as the main body, in-depth cooperation among industry, university, and research institutions**, and with high-tech industries that **connect the upstream and downstream.***³²⁹

ByteDance is pursuing technological advancement in areas the Party has prioritised. After the Party’s crackdown on the tech sector in 2021, ByteDance set out a plan for achieving “hard technological breakthroughs” in Extended Reality (XR), chips, life sciences, and enterprise intelligence tech. The language of ByteDance’s 2021 CSR report aligns closely with Party policy-speak.³³⁰ For example:

1. “*Based on accumulated advantages, extend upstream of the technological chain to AI chips, server CPU chips, and **strive to achieve the greatest degree of autonomy and controllability of the technological chain.***”
2. “*Continue to explore and apply the company’s accumulated AI tech to more fields and fields with **greater social value**, such as smart devices, medical care, and enterprise services.*”
3. “***Carry out basic research** and explore the frontiers at the intersections of AI+.”³³¹*

7.2. Beijing Academy of Artificial Intelligence

ByteDance was a founding member of the Beijing Academy of Artificial Intelligence, established by China’s Ministry of Science and Technology and the Beijing Municipal People’s Government in 2018.³³² Peking University, Tsinghua University, the Chinese Academy of Sciences, and AI giant Megvii are also members. The U.S. government placed Megvii on its export-control Entity List for enabling repression in Xinjiang in 2019, then blacklisted U.S. public investment into the firm in 2021.³³³

The Beijing Academy of Artificial Intelligence originated out of China’s 2017 Development Plan for New-Generation Artificial Intelligence, which aimed to “*build a first-mover advantage in the development of AI in China*”.³³⁴ The Plan stipulates that China will “*promote the formation of an all-element, multi-field, high-efficiency AI military-civilian fusion pattern*”.³³⁵ The Plan also includes instructions to:

*. . .encourage prominent civilian scientific research forces to participate in national defence for major scientific and technological innovation tasks in AI, to promote AI technologies to become quickly embedded in the field of national defence innovation.*³³⁶



7.3. Working with Defence Universities

Heeding guidance to serve national defence, ByteDance researchers have collaborated with defence-linked universities powering China's military. The Australian Strategic Policy Institute has rated Chinese universities' risk of ties to the People's Liberation Army,³³⁷ which we review below:

- **Huazhong University of Science and Technology:** Rated "very high risk" for its large number of defence laboratories and close links to the defence industry.³³⁸ A ByteDance researcher collaborated with scientists from this university's State Key Lab of Multi-spectral Image Information Processing Technology, a major defence lab, on person re-identification.³³⁹
- **People's Public Security University of China:** Rated "very high risk" for its affiliation with the Ministry of Public Security.³⁴⁰ ByteDance researchers collaborated with this university on deepfakes.³⁴¹
- **Tsinghua University:** Rated "very high risk" for its substantial involvement in defence research and alleged involvement in cyberattacks.³⁴² ByteDance researchers collaborated with Tsinghua on quantum computing and deep neural networks.³⁴³
- **Peking University:** Rated "high risk" for its involvement in defence research.³⁴⁴ ByteDance worked with Peking University researchers on intelligent text generation.³⁴⁵

State organisations that funded ByteDance's research would likely have access to their findings. Funders include the Beijing Academy of Artificial Intelligence, the Ministry of Public Security Technology Research Program, and the Natural Science Foundation of China.³⁴⁶

7.4. Surveillance Tech Partners

As detailed in [Section 6.1](#), ByteDance whitewashes Ministry of Public Security work in Xinjiang and broadcasts sanitised depictions of the region. In business operations and research, ByteDance has cooperated with companies identified as part of the military-industrial-surveillance complex enabling repression in Xinjiang:

- **Lion Technology:** On the U.S. Entity List since 2019 for ties to repression in Xinjiang.³⁴⁷ ByteDance cooperates with Lion Tech in data centers.³⁴⁸
- **SenseTime:** On the U.S. Entity List since 2019 for alleged ties to repression in Xinjiang.³⁴⁹ Sanctioned by Washington again in 2021 for ties to Beijing's

military-industrial complex. ByteDance used facial recognition technology developed by SenseTime.³⁵⁰

- **Dawning Information Industry, a.k.a. Sugon:** A subsidiary of the Chinese Academy of Sciences sanctioned for ties to Beijing’s military-industrial complex and enabling repression in Xinjiang.³⁵¹ ByteDance was a major client of Sugon cloud services. Sugon also makes data centers for ByteDance.³⁵²
- **iFlytek:** On the U.S. Entity List since 2019 for enabling repression in Xinjiang.³⁵³ ByteDance uses iFlytek for voice synthesis technology and music on Douyin and for office collaboration products on Feishu.³⁵⁴
- **Megvii:** Sanctioned by Washington in 2019 and 2021, as noted above.³⁵⁵ ByteDance collaborated with Megvii on computer vision research.³⁵⁶

7.5. Serving the Ministry of Public Security

ByteDance’s flagship China products – Douyin and Today’s Headlines – serve as resources for surveillance, particularly for China’s Ministry of Public Security (MPS).

In 2015, the MPS announced a raft of internet measures, including cybersecurity bureaus for major websites and major internet enterprises. The cybersecurity bureaus target cybercrime, including the Party-defined offence of spreading rumours.³⁵⁷

In September 2018, ByteDance Party Secretary Zhang Fuping announced Douyin’s integration with the MPS Network Security and Protection Bureau. The cybersecurity bureaus, together with Douyin and Douyin users, would collaborate to clean up cyberspace and promote the constructive environment of platform governance.³⁵⁸



*Douyin’s official ceremony marking its cooperation with the Ministry of Public Security.*³⁵⁹

The strategic cooperation agreement between ByteDance and the MPS signed in April 2019 includes a clause for *Douyin to cooperate with public security organs and jointly plan “offline activities”*.³⁶⁰ The agreement is vague on the meaning of cooperation and joint planning. But ByteDance’s 2019 CSR report documented the company’s efforts in establishing an *“integrated linkage mechanism [linking] behaviour recognition, online confrontation, and cooperation with public security agencies to crack down on behaviour offline”*.³⁶¹

There is evidence of arrests made as a result of ByteDance cooperation with the security services. ByteDance claims that it has aided in solving police cases, some involving hundreds of arrests, facilitated by an in-house official police cybersecurity team.³⁶² According to ByteDance’s 2022 Anti-Fraud Report, on which state media reported, between January 2021 and March 2022, Douyin helped public security organs apprehend 140 fraud-related criminal gangs, arrest 576 suspects, and solve more than 800 cases.³⁶³

8. Analysing the App: Content Quality and Access to Sensitive User Data

This section presents preliminary analysis of the TikTok app to assess its potential involvement in controlling narratives, and capacity to harvest user data.

- a. **TikTok as an Information Ecosphere:** Our original content analysis reveals higher proportions of misinformation and content favourable to the CCP on TikTok than on some other major social media platforms.
- b. **Data Harvesting Concerns:** Our analysis of TikTok's code shows that the app can access data beyond what is required for it to function, including sensitive data. This poses a risk to individual user data privacy, and lends itself to potential mass surveillance and intelligence applications.

8.1. Analysing Content on TikTok

In recent years there have been numerous examples of social media-based influence operations originating in China.

The Party and an army of state-backed cyber actors have led coordinated campaigns to harass journalists and human rights activists.³⁶⁴ They have also sought to shape global opinion on China's human rights record in Xinjiang and to interfere in multiple elections, including in the United States.³⁶⁵ U.S. officials warned before the 2022 midterm elections that Chinese agents of foreign interference were likely to "hinder candidates perceived to be particularly adversarial to Beijing".³⁶⁶

In late 2021, media reports identified a Shanghai Public Security Bureau soliciting bids for public opinion management services and seeking to register fake accounts on Western social media platforms, disguise and maintain them, and create original content.³⁶⁷

8.1.1. Prior Analyses of Content on TikTok

Media reporting and research by non-profit organisations present evidence that TikTok appears to censor content sensitive to the CCP, and hosts political misinformation. TikTok's coverage of issues considered sensitive by the CCP (such as Hong Kong's pro-democracy movement and China's human rights record in Xinjiang) appears to depart from that of Western-owned social media platforms, in ways that align with CCP interests.

In September 2019, the Washington Post reported that searches for *#hongkong* on Twitter and TikTok revealed starkly different results.³⁶⁸ On Twitter, the hashtag surfaced “*the city’s unavoidable protests, including pro-China agitprop, sympathetic memes and imagery from the hundreds of thousands of pro-democracy marchers who have braved police crackdowns*”.³⁶⁹ By contrast, TikTok surfaced “*playful selfies, food photos and singalongs, with barely a hint of unrest in sight*”.³⁷⁰

In November 2019, a Vice Germany journalist found that most of the videos he uploaded to TikTok with the hashtag *#Xinjiang* disappeared from search results.³⁷¹

The Australian Strategic Policy Institute (ASPI) followed up in August 2020 and found that the top 100 videos listed under *#Xinjiang* were 15% pro-CCP (denying the persecution of Uyghurs), 33% propaganda (“*[depicting] Xinjiang in an exclusively idyllic way*”), 12% critical of the CCP, and 40% entertainment.³⁷² ASPI noted that TikTok’s depiction of Xinjiang with “*smiling and dancing Uyghurs*” is a more “*politically convenient version for the CCP*”.³⁷³ The ASPI researchers wrote:

*While it’s unlikely that ByteDance would manipulate TikTok’s algorithm as blatantly as it does on its PRC-based equivalent, Douyin, there’s ample room for it to **covertly tweak users’ feeds, subtly nudging them towards content favoured by governments and their ruling parties** – including the CCP. . . . Even if ByteDance successfully ringfences TikTok from its China operations, censorship and information control can still be achieved via the **app’s opaque algorithm**, which is developed by ByteDance’s China-based engineering teams.*³⁷⁴

TikTok also faces allegations of propagating election misinformation.

TikTok says it does not allow political advertising on its platform.³⁷⁵ However, in October 2022, an independent investigation by rights group Global Witness and New York University’s Cybersecurity for Democracy (C4D) team found that TikTok failed to detect and remove advertisements containing election misinformation ahead of the 2022 U.S. midterms.³⁷⁶ TikTok approved 90% of the ads containing election misinformation that the researchers sought to upload:

*TikTok performed the worst out of all of the platforms tested in this experiment, with only one ad in English and one ad in Spanish – both relating to covid vaccinations being required for voting – being rejected. Ads containing the wrong election day, encouraging people to vote twice, dissuading people from voting, and undermining the electoral process were all approved. The account we used to post the election disinformation ads was still live until we informed TikTok.*³⁷⁷

8.1.2. Content Analysis

To test some of these claims, we designed and iterated over time a preliminary content analysis experiment that sought to identify the levels of pro-CCP content and misinformation present in top search results across TikTok, Twitter, Instagram and YouTube.

Given that TikTok functions uniquely (in that it generates recommended content without ever requiring the user to search for a topic or follow a creator), we focused our analysis on the content returned by each app's search function, thereby ensuring our experiment could be reliably repeated across platforms. This minimised the extent to which each app's content recommendation functions affected the content encountered. We also assessed that an analysis of the top search results returned for each term would provide valuable insight into the kinds of content users would likely encounter when seeking out information on certain topics via each app's search function.

The experiment tested two hypotheses:

1. TikTok hosts a higher proportion of content favourable to the CCP than competing social media platforms; and
2. TikTok hosts a higher proportion of misinformation than other platforms.

Based on our expertise in identifying PRC propaganda talking points, as well as a review of the existing literature on censorship, propaganda and misinformation on social media, we developed a list of 25 search terms across the two target issues and analysed the top 20 search results returned for each term. In total we analysed 2000 search results across the four platforms combined.

In the table below, we list the search terms examined, provide examples of the claims and representations we encountered, and note how we coded content. In order to reduce bias, we used fact-checking services such as Snopes and PolitiFact to assess the truthfulness of particular claims and coded content as 'disinformation' only if it presented untruths as fact.

We emphasise that this analysis is limited and preliminary in nature. It investigates the quality of content present in top search results for a limited set of terms, across a limited time period. Presence of pro-CCP content is not evidence that the app promotes propaganda or censors anti-CCP views. Similarly, presence of misinformation is not evidence that the app promotes this kind of content. Any assessment of the extent of propaganda, censorship or disinformation occurring on the platforms would require investigation into the origins of and intentions behind content appearing in top search results (on the content creator side) and evidence of the functions of TikTok's recommendation algorithm and content moderation processes (on the platform side).

Content Analysis Methodology

Assessing depictions of the CCP

Search terms

- "CCP"
- "China"
- "Mao Zedong"
- "China military"
- "PLA "
- "China human rights"
- "Tiananmen"
- "Tibet"
- "Hong Kong protest"
- "Uyghur"
- "Taiwan is a country"
- "Xi Jinping"
- "Xinjiang"
- "Wuhan lab"
- "Taiwan invasion"

Notes on how content was coded

Favourable depictions of the CCP

Content coded as such included refutations of so-called 'Western lies' about genocide in Xinjiang, rosy pictures of 'happy Uyghurs', criticism of Hong Kong's pro-democracy protest movement, PRC military propaganda, praise for the Chinese Communist Party, etc.

Unfavourable depictions of the CCP

Content coded as such included criticisms of Xi Jinping's leadership and China's human rights record, expressions of support for Tibetan and Taiwanese independence, content deriding CCP censorship practices, etc.

N/A

Content was coded as such if it was either unrelated to the target topic, or did not present either a favourable or unfavourable depiction of the CCP.

Assessing the presence of misinformation

Search terms

- "Mail ballot"
- "MAGA"
- "Uvalde TX conspiracy"
- "January 6 FBI"
- "Covid vaccine debunked"
- "Red wave"
- "Hunter Biden laptop"
- "Crisis actors"
- "mRNA vaccine"
- "Bucha fake"

Notes on how content was coded

Content containing misinformation

Content coded as such included misleading claims related to 'crisis actors' and the Uvalde, Texas school shooting, vaccine misinformation (including the claim that mRNA vaccines alter human DNA), false claims regarding the January 6 Capitol riots, etc.

Content absent misinformation

Content coded as such included factual reporting on election outcomes, expressions of personal political views (including personal opinion on the presence or absence of a "red wave" during the U.S. 2022 midterms), press reporting on investigations into the laptop that allegedly belonged to Hunter Biden, etc.

Content coded as N/A

Content was coded as such if it was unrelated to the target topic, or did not make any discernible claim.

8.1.3. Control Variables

We conducted this content analysis over a 48-hour period (20-22 November 2022). We performed the searches on newly created sock puppet accounts on an Apple device using a VPN to spoof the device IP's location, deleting accounts made for one app before making those for the next. This was done to reduce the potential for targeted recommendations generated by third-party user data sharing that may occur across apps.

8.1.3. Findings

Our experiment revealed that top search results on TikTok (and Twitter) featured higher proportions of content favourable to the CCP, compared to Instagram and YouTube.

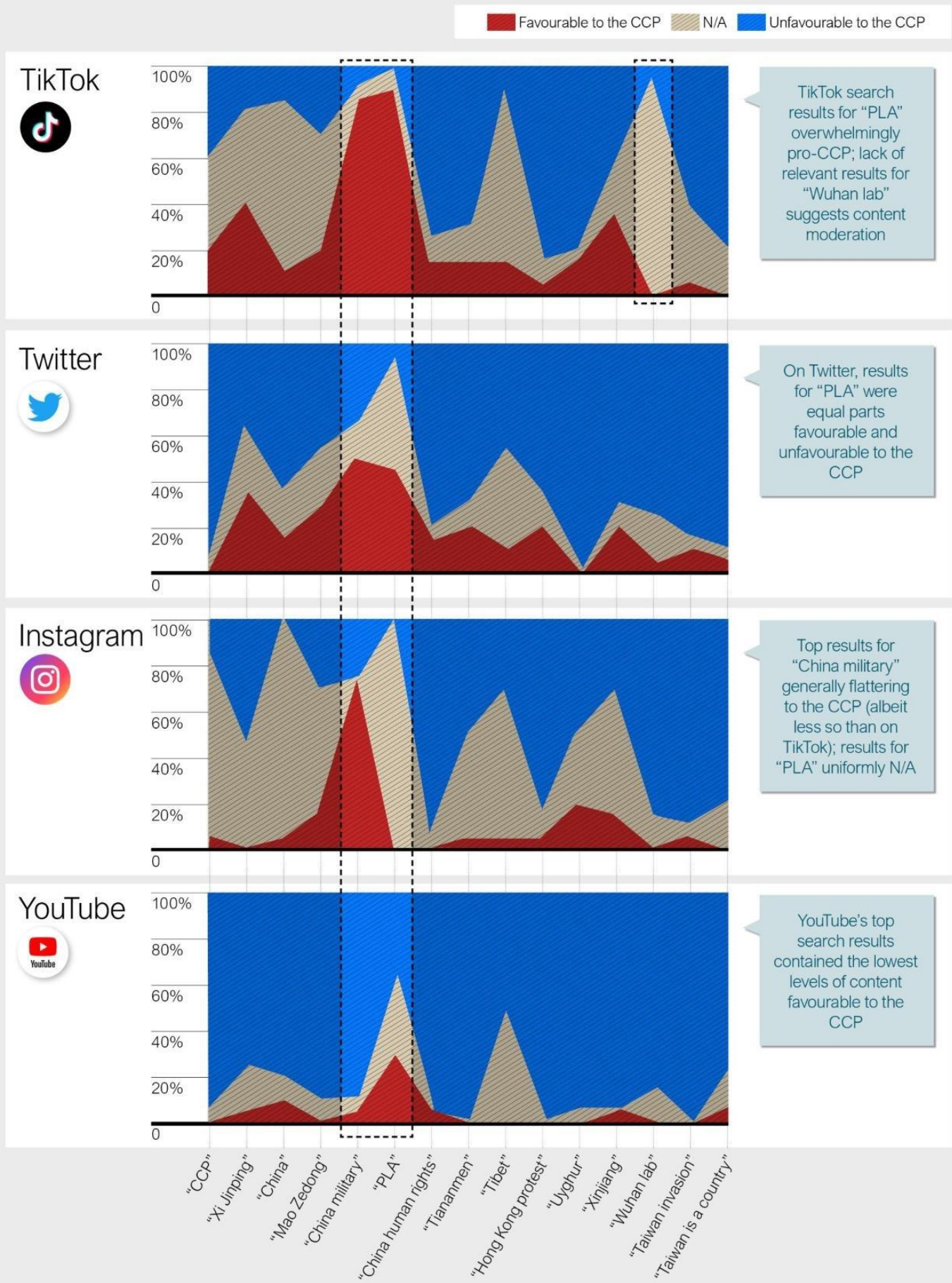
In the absence of direct evidence of policies, practices, and human or technical mechanisms for managing content on the platform, we cannot determine the specific causes of the elevated proportion of pro-CCP content and disinformation on TikTok vis-à-vis other apps. That is, our experiment does not enable us to determine whether this result stems from internal TikTok content moderation, algorithm manipulation, or a higher volume of pro-CCP content creators active on the platform.

Our findings do support a conclusion that, when searching for information on contentious topics related to China and, separately, to U.S. political issues, **the average TikTok (and Twitter) user is more likely to be exposed to content favourable to the CCP and misinformation in search results** than the average Instagram and YouTube user. These findings have significant implications for Gen Z users who increasingly use TikTok as a search engine to learn about political issues.³⁷⁸

We emphasise the limited and preliminary nature of this investigation, which focused on results returned for a limited set of search terms within a limited time period.

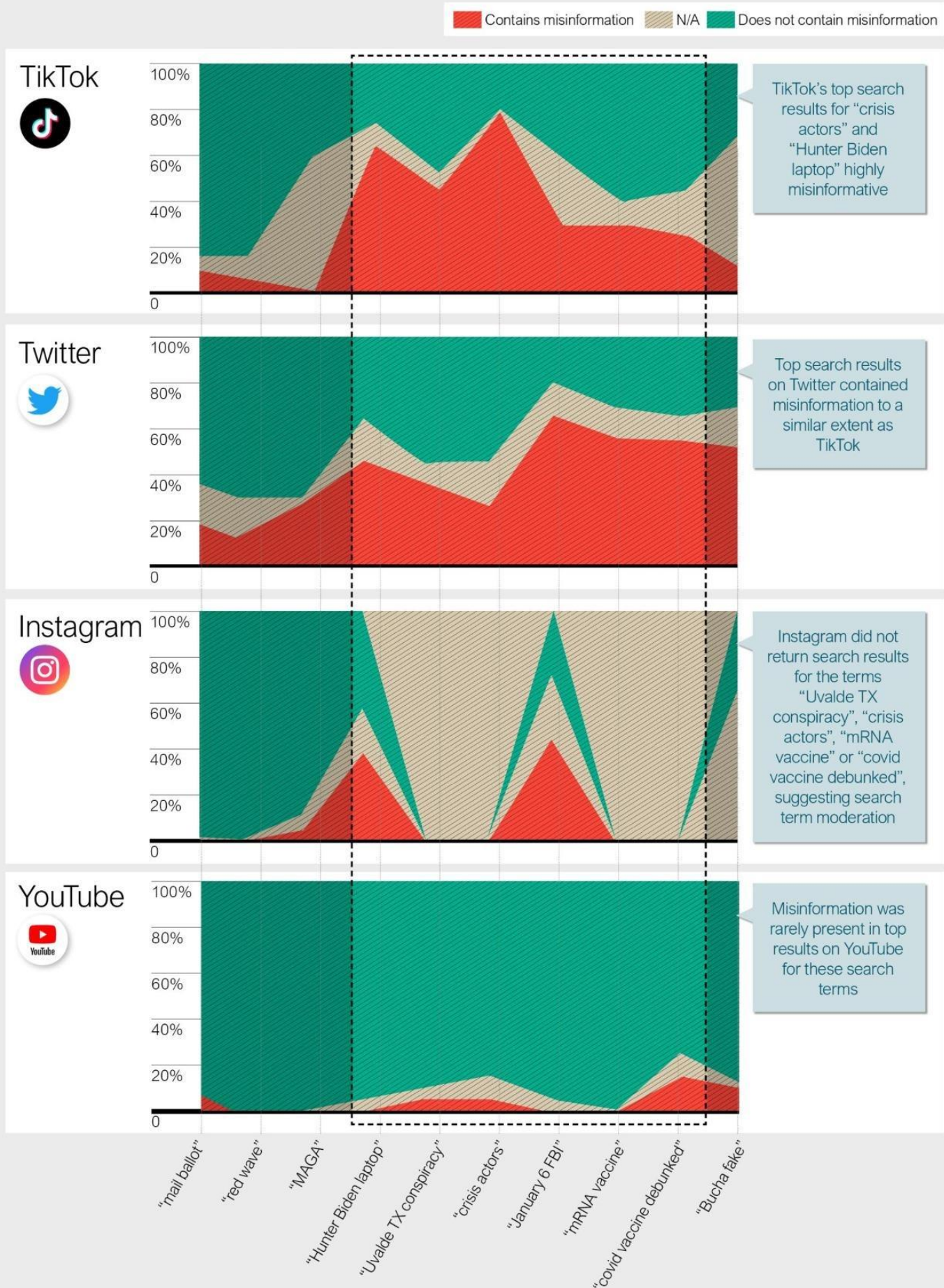
Preliminary Comparative Analysis of Content Across Major Platforms (Part 1)

We assessed depictions of the CCP present in the top 20 search results on TikTok, Twitter, Instagram and YouTube over a 48-hour period (20-22 November 2022):



Preliminary Comparative Analysis of Content Across Major Platforms (Part 2)

We assessed the presence of misinformation in the top 20 search results on TikTok, Twitter, Instagram and YouTube over a 48-hour period (20-22 November 2022):



8.1.4. Possible Intervening Variables: Twitter Takeover

This content analysis was conducted after Elon Musk completed his takeover of Twitter but prior to reports of substantial changes to content algorithms and moderation functions. In December, Twitter reportedly dismissed a number of key executives and, by some estimates, half of the workforce, including some of those working on content moderation.³⁷⁹

8.1.5. Suggestions for Future Analyses

These results capture only a snapshot of content on TikTok for a limited 48-hour period. Follow-up experiments could repeat the experiment multiple times, or over a longer period, examining a broader range of search terms, for more reliable results. This would allow stronger conclusions about the app's treatment of particular topics. For instance, in our experiment, almost all top search results for the terms "PLA" and "China military" contained favourable depictions of the CCP. However, we would require more robust evidence to draw firm conclusions about the reasons for and implications of this.

8.2. Technical Analysis: Data Accessed by the App

A July 2022 investigation by cybersecurity firm Internet 2.0 alleges abuses of data privacy and security by the TikTok app, including the claim that *"Permissions and device information collection are overly intrusive and not necessary for the application to function"*.³⁸⁰

The report cites a number of examples of data TikTok collects which the authors argue should be considered excessive, including information on other applications installed and running, hourly location data, persistent calendar access, contacts, and unique device identifiers such as the International Mobile Equipment Identifier (IMEI).³⁸¹

To independently verify some of these findings, we performed a limited technical analysis of the TikTok app designed to be verifiable and repeatable by others. Our technical analysis was conducted on the Android v25.1.3 app (the same version analysed by the Internet 2.0 investigation).³⁸² In summary, we found that the app requests permission to access a vast array of data, including sensitive data, and it also requests permission for data seemingly unnecessary for the functioning of the app (based on its current features).

Based on our understanding of the app's personalised recommendation algorithm, we assess that TikTok may be able to build user profiles that reflect personal proclivities relating to engagement with 'compromising' material. These user profiles could conceivably be used to publicly discredit or blackmail individuals for the purposes of political interference or transnational repression. Agents of the CCP regularly participate in campaigns of harassment and repression via social media.³⁸³

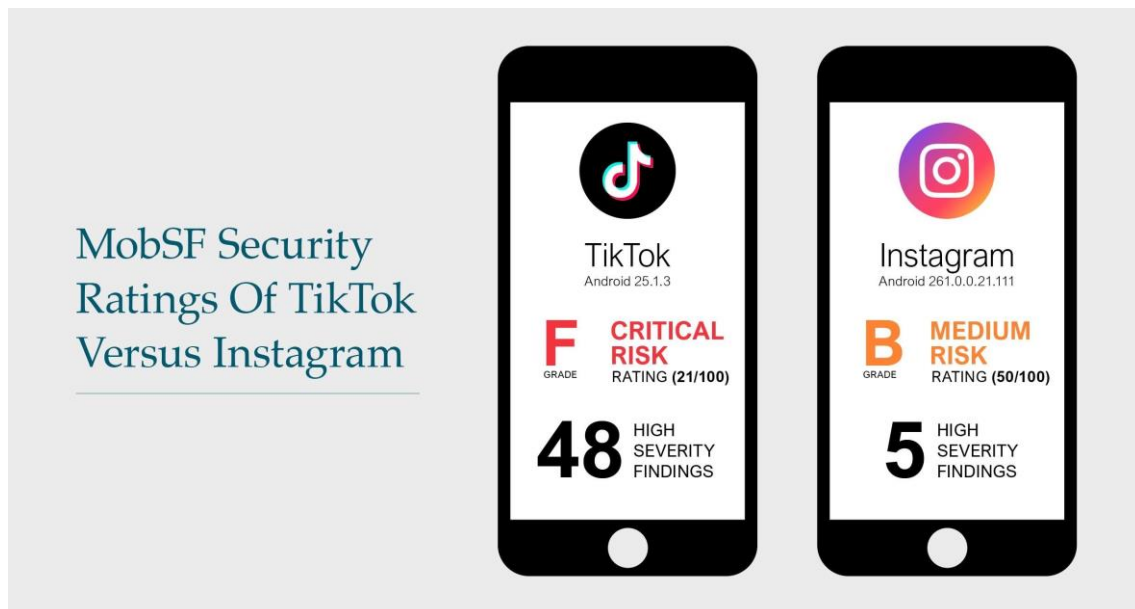
8.2.1. Static Analysis of the Android App

Our researchers performed a static analysis of the TikTok app (Android v25.1.3) in order to independently verify some of the findings of the Internet 2.0 report.³⁸⁴ (For our methodology for the purposes of replication, see Appendix 1.)

Our findings are based on an initial analysis of the decompiled code of the app. It is important to note that a significant proportion of the code is obfuscated, so we were unable to determine the functions of much of the code.

Moreover, static analysis is limited in its ability to inform definitive conclusions about whether data is being sent outside of the device. The TikTok Android app is a large, well-protected and complex program. Outside reference points would be required to determine whether TikTok’s collection and handling of data varies significantly from that of other popular social media applications. However, **third-party security evaluation services rate TikTok poorly compared with other social media platforms.**

We used the security analysis tool Mobile Security Framework (MobSF) to run two separate static analyses of the Android Package Kits (APKs) for TikTok (v25.1.3) and Instagram (v261.0.0.21.111). The MobSF reports scored TikTok’s security risks as “critical” (21/100) and gave the app an “F” grade with 5/428 trackers detected. Comparatively, Instagram scored as “medium” risk (50/100) and received a “B” grade with 2/428 trackers detected. MobSF flagged 48 “high severity findings” for TikTok and 5 for Instagram.



Risk ratings provided by Mobile Security Framework, based on an automated security evaluation.

8.2.2. Data Access

Our limited investigation of this particular version of the TikTok Android app found that it requests permission to collect a large number of datapoints about the user and their device.

We were unable to confirm whether the data is indeed collected, what it might be used for, or where it is sent. However, the data the app requests permission to collect contains numerous unique identifiers and would facilitate device “fingerprinting” – the practice of profiling a machine based on its unique software and hardware configuration.³⁸⁵ (For a list of device data the TikTok app is able to read, see Appendix 2.)

The app can perform checks for a user’s contacts, location and calendar information. (For the full list of ‘android.permission’ strings and the number of times each is observed in the decompiled code, see Appendix 3.) From this list, we can see that the app can collect users’ precise location, and collect location data even while the app is not in use.³⁸⁶

Given recent revelations regarding TikTok’s surveillance of American journalists using the app to monitor their locations, these findings present individual privacy and security risks that warrant further examination.³⁸⁷

9. Taking Stock of the Evidence

In this section, we show how TikTok’s attempts to defuse controversy and allay policymakers’ concerns have failed to address the fundamental risks facing democratic governments.

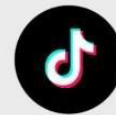
- a. **Recent Events Confirm the Risks Are Real:** Late-2022 revelations of data privacy violations by ByteDance, including the tracking of journalists reporting on TikTok, show the emptiness of supposed safeguards.
- b. **“Project Texas” Problems:** TikTok’s promises to house data in the United States cannot negate how Beijing’s comprehensive national security and intelligence laws weave ByteDance and TikTok into its global data goals and can obligate them to share any data the Party may demand, in secret.
- c. **Beijing’s Regulatory Veto:** Some U.S. regulators may want to stop short of a ban by instead forcing ByteDance to divest TikTok, but Beijing has repeatedly signaled that it would oppose such a solution, including by imposing export controls on algorithms.

9.1. TikTok’s Late-2022 Troubles

TikTok has faced increasing scrutiny in democratic capitals for several years, dating most significantly to the Trump administration’s August 2020 attempt to ban the app altogether. However, the month of December 2022 was especially eventful. The highlights:

9.1.1. Tracking U.S. Journalists

ByteDance admitted on 22 December that an internal-audit team – including employees in China – had inappropriately tracked journalists from the Financial Times and Forbes by accessing their location data in an attempt to identify their sources inside TikTok.³⁸⁸ While the Christmas-week timing of the news probably limited its immediate splash, this revelation hurt TikTok’s standing in Washington. Critics have long warned that ByteDance could access user data for abusive purposes, including to track and intimidate, whether on ByteDance’s initiative or on behalf of the Chinese government. This appeared to prove it.



Reporting On TikTok Reached Fever Pitch In Late 2022

JUN
2022

BuzzFeed News

Leaked Audio From 80 Internal TikTok Meetings Shows That US User Data Has Been Repeatedly Accessed From China

17 June

The leaks reveal that PRC-based engineers were able to access US TikTok users' app data, even while U.S. employees were not.

JUL
2022

FINANCIAL REVIEW

TikTok's 'alarming', 'excessive' data collection revealed

18 July

Technical analysis of the TikTok app by Australian cybersecurity firm Internet 2.0 judged the app's data access requirements excessive.

AUG
2022

Forbes

LinkedIn Profiles Indicate 500 Current TikTok And ByteDance Employees Used To Work For Chinese State Media—And Some Still Do

11 August

At least 500 TikTok and ByteDance employees—including those working in strategy and content—have previously worked for PRC state media.

OCT
2022

Forbes

TikTok Parent ByteDance Planned To Use TikTok To Monitor The Physical Location Of Specific American Citizens

20 October

An Internal Audit team at ByteDance intended to surveil specific U.S. citizens through the TikTok app's location tracking function, including some who had no employment relationship with either company.

NOV
2022

Forbes

TikTok May Be Suppressing Videos About The Midterms And Voting, New Research Suggests

7 November

TikTok is accused of censoring videos about the U.S. midterm elections, including politically-neutral content containing how-to-vote information.

DEC
2022

Forbes

EXCLUSIVE: TikTok Spied On Forbes Journalists

22 December

ByteDance confirms it used TikTok to track the locations of U.S. journalists reporting on the company, in an attempt to identify the sources of recent leaks.



U.S. Federal Communications Commissioner Brendan Carr highlights how TikTok parent ByteDance's pre-Christmas admission of snooping backs up allegations that have long dogged the company.

Democrat Mark Warner, chair of the U.S. Senate Intelligence Committee, said:

This new development reinforces serious concerns that the social media platform has permitted TikTok engineers and executives in the People's Republic of China to repeatedly access private data of U.S. users despite repeated claims to lawmakers and users that this data was protected.³⁸⁹

9.1.2. Intelligence Officials Sound the Alarm

Also toward the end of last year, key U.S. national security officials intensified their warnings about TikTok. In November, FBI chief Chris Wray stated that the FBI has "a number of concerns" regarding TikTok as a "national security threat":

They include the possibility that the Chinese government could use it to control data collection on millions of users or control the recommendation algorithm which could be used for influence operations if they so chose, or to control software on millions of devices which gives it the opportunity to potentially technically compromise personal devices.³⁹⁰

On 3 December, Director of National Intelligence Avril Haines addressed TikTok at the Reagan National Defense Forum:

It is extraordinary the degree to which China, in particular . . . are developing just frameworks for collecting foreign data and pulling it in and their capacity to then turn that around and use it to target audiences for information campaigns or for other things, but also to have it for the future so that they can use it for a variety of means that they're interested in.³⁹¹

On 16 December, CIA Director William Burns echoed such concerns:

I think it's a genuine concern, I think, for the U.S. government, in the sense that, because the parent company of TikTok is a Chinese company, the Chinese government is able to insist upon extracting the private data of a lot of TikTok users in this country, and also to shape the content of what goes on to TikTok as well to suit the interests of the Chinese leadership. . . . What I would underscore, though, is that it's genuinely troubling to see what the Chinese government could do to manipulate TikTok.³⁹²

9.2. "Project Texas" Doesn't Measure Up

TikTok has gone to great efforts to allay Western policymakers' data security concerns, and convince governments against a ban, forced divestment or other major action. In the U.S., the company has proposed and begun to implement a number of measures relating to data security, the most notable set of which is known as "Project Texas".³⁹³ However, these measures fail to address fundamental issues, as detailed below.

9.2.1. Oracle's Role Doesn't Address the Underlying Problem: While Oracle is responsible for the provision and maintenance of the data storage architecture under "Project Texas", the cloud servers themselves are administered by TikTok and, according to an Oracle official, TikTok maintains "*full control of everything they're doing*".³⁹⁴

Regardless of where data is stored, according to company spokesman Ken Glueck, Oracle would have "*absolutely no insight one way or the other*" into whether entities or individuals in China had access to TikTok data stored on the Oracle cloud, nor where it was being sent from there.³⁹⁵ As TikTok's Head of Data Defense said in leaked recordings:

It's almost incorrect to call it Oracle Cloud, because they're just giving us bare metal, and then we're building our [virtual machines] on top of it.³⁹⁶

9.2.2. Oracle's Financial Conflict: As TikTok's business partner, Oracle may not be in a position to serve as independent auditor of TikTok's algorithms as part of "Project Texas". Insiders told The Washington Post in late 2022 that "*audits have not been started or closely planned*" and that Oracle merely serves as TikTok's server provider "*with no authority to police operations*".³⁹⁷

9.2.3. ByteDance Policy Remains Clear on China Data Access: TikTok leadership have claimed that the company would not agree to government requests for data if asked.³⁹⁸ However, TikTok's privacy policy enshrines ByteDance access to U.S. (and European) user data.³⁹⁹ According to U.S. Senator Josh Hawley, when questioning TikTok executive Vanessa Pappas:

*You have hundreds of employees with access to U.S. user data that may very well be members of the Chinese Communist Party. **You have no way to assure me that they have no access to our citizens' data.** And you won't answer my question in a straightforward way about **whether a CCP member has ever gained access or not.** From my own point of view, that's a huge security problem.*⁴⁰⁰

TikTok shared an update to its Europe privacy policy in November 2022 that confirmed China-based employees have access to European user data:

*Based on a demonstrated need to do their job, subject to a series of robust security controls and approval protocols, and by way of methods that are recognised under the GDPR, we allow certain employees within our corporate group located in Brazil, Canada, **China**, Israel, Japan, Malaysia, Philippines, Singapore, South Korea, and the United States **remote access to TikTok European user data.***⁴⁰¹

TikTok's Pappas did not commit to stopping data flows to China.⁴⁰² Instead, TikTok has said that it will "*[minimise] employee access to US user data and [minimise] data transfers across regions*".⁴⁰³ TikTok describes these ostensible data flow-minimisation measures on its website:

*We have policies and procedures that limit internal access to user data by our employees, wherever they're based, based on need. Like many global companies, TikTok has **engineering teams around the world—including in Mountain View, London, Dublin, Singapore, and China** – and those teams might need access to data for engineering functions that are specifically tied to their roles. That access is subject to a series of robust controls, safeguards*

*like encryption for certain data, and authorisation approval protocols **overseen by our U.S.-based security team**. To facilitate those approvals, we also have an **internal data classification system**; the level of approval required for access is based on the sensitivity of the data according to the classification system.⁴⁰⁴*

These policies and procedures are internal, with oversight by a “US-based security team”. TikTok’s U.S. privacy policy says, *“We may share all of the information we collect with a parent, subsidiary, or other affiliate of our corporate group.”*⁴⁰⁵

TikTok’s refusal to implement an effective quarantine of U.S. user data from China-based staff, and from other entities in its global corporate group, means that this data will continue to be vulnerable to potential requests for access coming from Beijing made possible by the PRC’s National Intelligence Law (see [Section 2.2.2](#) and [Section 5.5.1](#)).

9.3. Biden’s CFIUS Decision – and Beijing’s Potential Countermove

TikTok may claim it is not controlled by the Chinese government but, if we revisit a series of key events in 2020, it is clear **the Chinese government cares about controlling TikTok**.

Amid the failure of “Project Texas” to address fundamental concerns, U.S. policymakers continue to consider stronger measures that Beijing would, based on the evidence, likely seek to thwart.

The most immediate policy landmark for TikTok globally was long expected to be the verdict of the Committee on Foreign Investment in the United States (CFIUS) review, led by the U.S. Treasury Department since 2019. Since late last year, CFIUS has reportedly been considering two approaches:

First, CFIUS could allow ByteDance to maintain ownership of TikTok as long as it moves TikTok’s U.S. operations (including its data) into a new subsidiary with a separate board composed of U.S. national security veterans. This approach, avoiding a ban, has reportedly been Treasury’s preference.⁴⁰⁶ (This would trigger criticism from Congress).

Alternatively, CFIUS could force ByteDance to sell TikTok’s U.S. operations altogether, **requiring it to relinquish ownership and control of this significant portion of the company, along with its algorithms and its data**. This is reported to be the preferred approach of the Defense Department, the Justice Department and the Intelligence Community. (TikTok critics in Congress have signalled that a forced sale could be satisfactory.⁴⁰⁷)

Beijing could balk at a forced sale. Back in 2020, as the Trump administration considered forcing a sale to U.S. buyers such as Microsoft, Beijing rolled out a series of countermeasures, including warnings and new export controls on algorithms (as outlined in [Section 6.4.1](#)). Official organs referred to a would-be forced sale as “bullying”, “robbery” and “contemporary piracy”:

- **24 August 2020:** TikTok and ByteDance sued the Trump administration for banning the app.⁴⁰⁸ China's Ministry of Foreign Affairs spokesperson said at a press conference: *"China supports relevant companies in taking up legal weapons to protect their legitimate rights and interests, and will continue taking all necessary measures to resolutely safeguard the legitimate rights and interests of PRC companies."*⁴⁰⁹ State outlet Xinhua published a commentary titled, "Say 'no' to economic bullying using legal weapons".⁴¹⁰
- **28 August 2020:** The PRC's Ministry of Commerce and the Ministry of Science and Technology announced new export controls pertaining to AI technologies relevant to TikTok.⁴¹¹ (See [Section 6.4.1.](#)) Xinhua spelled out the implications of the export controls for ByteDance's algorithms.⁴¹² ByteDance promised to strictly follow Beijing's rules.⁴¹³
- **12 September 2020:** Reuters reported that, according to sources, Chinese authorities would rather see TikTok shut down than forcibly sold.⁴¹⁴
- **20-26 September 2020:** Global Times and China Daily published at least seven editorials on TikTok.⁴¹⁵ One announced: *"China is prepared to prevent Chinese firm TikTok and its advanced technologies from falling into US hands at all cost, even if that means the vastly popular video sharing app risks being shut down in the US. . . .The case goes way beyond just a mafia-style robbery of a lucrative Chinese business and cutting-edge technologies, but a threat to its national security, because the US could find loopholes in those technologies to launch cyber and other attacks on China and other countries to preserve its hegemony."*⁴¹⁶

A similar crop of commentaries from Chinese state media emerged in response to late-2022 news of the Biden CFIUS review possibly pointing toward forced divestment.⁴¹⁷ There is no reason to think Beijing would be any warmer to the notion of a forced sale today than in 2020, even though blocking a sale would probably require TikTok to withdraw from the U.S. market at great commercial cost to ByteDance.

The attempts to regulate or restrict TikTok in 2020 revealed the CCP's interest in retaining control over the app. So long as that is the case, [TikTok poses risks to democracies](#).

Australia has a duty to consider these risks. In our view, Australian policymakers are well-placed to address this issue in a bipartisan way, as was the case when Australia developed and delivered a counter foreign interference strategy in 2017-18.⁴¹⁸ ■

Appendix 1: Static Analysis Methodology

To reconstruct our technical analysis and verify findings, follow the steps below:

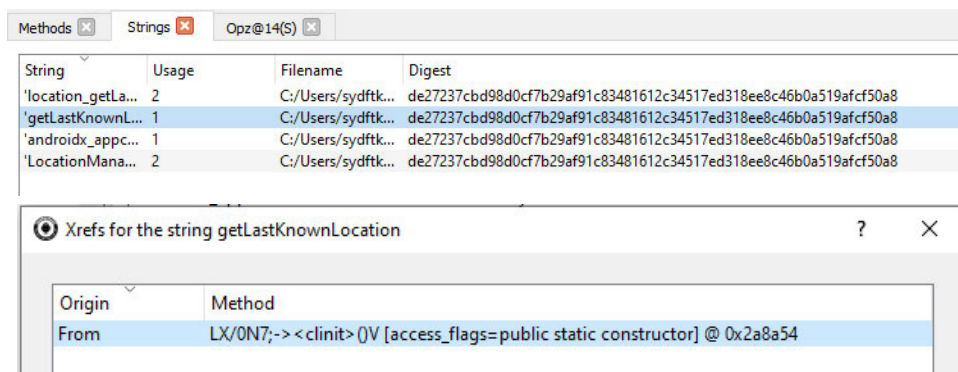
Download the TikTok Android v25.1.3 (ARM64) Android Package Kit (APK) from <https://www.apkmirror.com/apk/tiktok-pte-ltd/tik-tok-including-musical-ly/tik-tok-including-musical-ly-25-1-3-release/#downloads>.

Decompiling the APK

- Install Python at <https://www.python.org/downloads/>.
- Install Androguard (a tool and Python library for interacting with Android files) in Windows Command Prompt (CMD) (“*pip install androguard*”).
- Ensure that the Python scripts directory (C:\Users\[username]\AppData\Local\Packages\PythonSoftwareFoundation.Python.3.8\LocalCache\local-packages\Python38\Scripts) is located within the system environmental variables.

OR

- Navigate to “*entry_points.py*” in the Androguard install directory (Androguard/CLI) and run “*python entry_points.py gui*” in the CMD.
- Select “File” > “Open” > “.APK file”.
- Select “View” > “String”.
- Filter by desired string variable.
- Select the entry.
- Select the method.



Appendix 2: Device Data Accessible to TikTok App

The following table shows the device data that the TikTok app is able to read:

Type	Issue
Telephony Identifier	This application reads the ISO country code equivalent for the SIM provider's country code
Telephony Identifier	This application reads the ISO country code equivalent of the current registered operator's Mobile Country Code (MCC)
Telephony Identifier	This application reads the MCC and Mobile Network Code (MNC) of the provider of the SIM
Telephony Identifier	This application reads the Service Provider Name (SPN)
Telephony Identifier	This application reads the constant indicating the state of the device SIM card
Telephony Identifier	This application reads the device phone type value
Telephony Identifier	This application reads the numeric name (MCC and MNC) of current registered operator
Telephony Identifier	This application reads the operator name
Telephony Identifier	This application reads the radio technology (network type) currently in use on the device for data transmission
Location	This application reads location information from all available providers (WIFI, GPS etc.)
Connection Interfaces	This application reads details about the currently active data network
Connection Interfaces	This application tries to find out if the currently active data network is metered
Telephony Services	This application can make phone calls
PIM Data	This application accesses the calendar
PIM Data	This application accesses the downloads folder

Appendix 3: 'android.permission' Strings in TikTok Code

Below is the list of 'android.permission' strings and the number of times each is observed in the decompiled code (usage number). Usage number is not necessarily representative of the significance of the data to which access is requested. The usage numbers may also be underestimations, given the proportion of TikTok's code that is obfuscated (and therefore unreadable). For a string to be used in a command, it must first be defined. Therefore, '1' is the minimum number of times a used string can appear in code.

String	Usage
'android.permission.WRITE_CONTACTS'	1
'android.permission.WRITE_CALL_LOG'	1
'android.permission.WRITE_CALENDAR'	9
'android.permission.WAKE_LOCK'	3
'android.permission.VIBRATE'	1
'android.permission.USE_CREDENTIALS'	1
'android.permission.UPDATE_DEVICE_STATS'	3
'android.permission.SYSTEM_ALERT_WINDOW'	2
'android.permission.SEND_SMS'	1
'android.permission.REQUEST_INSTALL_PACKAGES'	2
'android.permission.RECORD_AUDIO'	38
'android.permission.RECEIVE_SMS'	1
'android.permission.RECEIVE_MMS'	1
'android.permission.READ_SMS'	2
'android.permission.READ_PHONE_STATE'	8
'android.permission.READ_PHONE_NUMBERS'	5
'android.permission.READ_EXTERNAL_STORAGE'	25
'android.permission.READ_CONTACTS'	18
'android.permission.READ_CALL_LOG'	1
'android.permission.READ_CALENDAR'	9
'android.permission.PROCESS_OUTGOING_CALLS'	2
'android.permission.MANAGE_EXTERNAL_STORAGE'	2
'android.permission.MANAGE_ACCOUNTS'	1

'android.permission.INTERNET'	5
'android.permission.GET_ACCOUNTS'	4
'android.permission.CHANGE_WIFI_STATE'	1
'android.permission.CHANGE_WIFI_MULTICAST_STATE'	2
'android.permission.CAMERA'	52
'android.permission.BROADCAST_SMS'	1
'android.permission.BODY_SENSORS_BACKGROUND'	1
'android.permission.BODY_SENSORS'	3
'android.permission.BLUETOOTH_ADMIN'	2
'android.permission.BLUETOOTH'	6
'android.permission.BIND_JOB_SERVICE'	2
'android.permission.ANSWER_PHONE_CALLS'	3
'android.permission.ACTIVITY_RECOGNITION'	3
'android.permission.ACCESS_WIFI_STATE'	4
'android.permission.ACCESS_NOTIFICATION_POLICY'	2
'android.permission.ACCESS_NETWORK_STATE'	10
'android.permission.ACCESS_MEDIA_LOCATION'	3
'android.permission.ACCESS_FINE_LOCATION'	10
'android.permission.ACCESS_COARSE_LOCATION'	21
'android.permission.ACCESS_BACKGROUND_LOCATION'	3
'android.permission.ACCEPT_HANDOVER'	2

References

- 1 Zen Soo, 'These Are the Countries That Have Bans on TikTok', Time, 2-Mar-2023, <https://time.com/6259718/countries-tiktok-banned/>
'Statement by Minister Fortier announcing a ban on the use of TikTok on government mobile devices', Treasury Board of Canada Secretariat, 27-Feb-2023, <https://www.canada.ca/en/treasury-board-secretariat/news/2023/02/statement-by-minister-fortier-announcing-a-ban-on-the-use-of-tiktok-on-government-mobile-devices.html>
'These 30 states have banned TikTok on government-issued devices, networks', The Daily Signal, 19-Jan-2023, <https://www.dailysignal.com/2023/01/19/these-30-states-banned-tiktok-government-issued-devices-networks/>
Max Mason, 'TikTok banned by 25 government departments and agencies', Australian Financial Review, 6-Mar-2023, <https://www.afr.com/technology/tiktok-banned-by-25-government-departments-and-agencies-20230303-p5cp4o>
Laura Dobberstein, 'Taiwan bans state-owned devices from running Chinese platform TikTok', The Register, 7-Dec-2022, https://www.theregister.com/2022/12/07/taiwan_bans_chinese_platform_tiktok/
Foo Yun Chee, 'EU Commission to ban TikTok on staff phones, citing security', Reuters, <https://web.archive.org/web/20230223120728/https://www.reuters.com/technology/eu-commission-staff-told-remove-tiktok-phones-eu-industry-chief-says-2023-02-23/>
Pieter Haeck, 'Don't use TikTok, Dutch officials are told', Politico, 25-Jan-2023, <https://web.archive.org/web/20230126222501/https://www.politico.eu/article/netherlands-dutch-government-work-tiktok-data-protection/>
'Danish defense ministry bans TikTok on employee work phones', AP News, 7-Mar-2023, <https://apnews.com/article/denmark-tiktok-ban-defense-ministry-c3f434fa46401ea93329e1f5cb132432>
'Belgium bans TikTok from government phones after US, EU', AP News, 11-Mar-2023, <https://apnews.com/article/tiktok-belgium-china-cybersecurity-b976fe2a56c58996e84c1040ddd7f1ad>
Todd Richmond, 'EXPLAINER: University of Wisconsin latest to ban TikTok', AP News, 25-Jan-2023, <https://apnews.com/article/technology-politics-united-states-government-china-privacy-26b0ee0d4c8421fa7f58b06f76651dc1>
- 2 '习近平：讲好中国故事，传播好中国声音', Qiushi, 2-Jun-2021, <http://archive.today/II79B>
- 3 '习近平：讲好中国故事，传播好中国声音', Qiushi, 2-Jun-2021, <http://archive.today/II79B>
- 4 '让短视频平台展示好中国形象传播好中国声音', Xinhua, 6-Aug-2021, <http://archive.today/qk00A>
- 5 Robert Mueller, 'Report on the investigation into Russian interference in the 2016 Presidential election', Mar-2019, <https://www.justice.gov/archives/sco/file/1373816/download>
- 6 Robert Mueller, 'Report on the investigation into Russian interference in the 2016 Presidential election', Mar-2019, <https://www.justice.gov/archives/sco/file/1373816/download>
- 7 Chris Uhlmann, 'Top-secret report uncovers high-level Chinese interference in Australian politics', Nine News, 28-May-2018, <https://www.9news.com.au/national/chinese-communist-party-interference-australian-politics/a6e8e4e0-28f6-4b7a-a94c-ba4b98ea8aa1>
- 8 'Speech introducing the National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2017', Malcolm Turnbull, 7-Dec-2017, <https://www.malcolmturnbull.com.au/media/speech-introducing-the-national-security-legislation-amendment-espionage-an>
- 9 'Speech introducing the National Security Legislation Amendment (Espionage and Foreign Interference) Bill 2017', Malcolm Turnbull, 7-Dec-2017, <https://www.malcolmturnbull.com.au/media/speech-introducing-the-national-security-legislation-amendment-espionage-an>
- 10 '2017 memo prepared for PM warns of Beijing election interference', Global News, 8-Feb-2023, <https://globalnews.ca/news/9464937/security-memo-trudeau-china-election-interference/>
'Cyber Threats to Canada's Democratic Process', Communications Security Establishment, 2017, https://publications.gc.ca/collections/collection_2017/cstc-csec/D96-2-2017-eng.pdf
- 11 'CSIS Public Report 2021', Canadian Security Intelligence Service, Mar-2022, <https://www.canada.ca/en/security-intelligence-service/corporate/publications/csis-2021-public-report.html>
- 12 Robert Fife and Steven Chase, 'CSIS documents reveal Chinese strategy to influence Canada's 2021 election', The Globe and Mail, 17-Feb-2023, <https://www.theglobeandmail.com/politics/article-china-influence-2021-federal-election-csis-documents/>
- 13 Robert Fife and Steven Chase, 'Trudeau orders two probes into Chinese election interference', The Globe and Mail, 6-Mar-2023, <https://www.theglobeandmail.com/canada/article-trudeau-calls-for-two-probes-into-chinese-election-interference/>
- 14 'Gina Raimondo becomes China player in a job where her predecessor used to nap', Bloomberg, 1-Mar-2023, <https://www.bloomberg.com/news/articles/2023-03-01/chips-tiktok-make-gina-raimondo-vital-to-biden-china-policy>

- 15 'Relevance is the new Reach', TikTok for Business, 6-Sep-2021,
<https://www.tiktok.com/business/en/blog/relevance-is-the-new-reach>
- 16 'TikTok isn't silly. It's serious', The Economist, 15-Jan-2022,
<https://www.economist.com/business/2022/01/15/tiktok-isnt-silly-its-serious>
- 17 'Teens, Social Media and Technology 2022', Pew Research, 10-Aug-2022,
<https://web.archive.org/web/20221206040910/https://www.pewresearch.org/internet/2022/08/10/teens-social-media-and-technology-2022/>
- 'More Americans are getting news on TikTok, bucking the trend on other social media sites', Pew Research Center, 21-Oct-2022, <https://web.archive.org/web/20221206145508/https://www.pewresearch.org/fact-tank/2022/10/21/more-americans-are-getting-news-on-tiktok-bucking-the-trend-on-other-social-media-sites/>
- 'Thanks a billion!', TikTok, 27-Sep-2021,
<https://web.archive.org/web/20221204042730/https://newsroom.tiktok.com/en-us/1-billion-people-on-tiktok>
- David Curry, 'TikTok App Report 2023', Business of Apps, 21-Feb-2023,
<https://www.businessofapps.com/data/tiktok-report/>
- Brian Dean, 'TikTok User Statistics (2022)', Backlinko, 05-Jan-2022, <https://backlinko.com/tiktok-users>
- 'Complaint for injunctive and declaratory relief, TikTok Inc. and ByteDance Ltd.', United States District Court, Central District of California Western Division, 24-Aug-2020,
<https://web.archive.org/web/20220416021500/https://s3.documentcloud.org/documents/7043165/TikTok-Trump-Complaint.pdf>
- 'Average daily activation count : 43 times a day ! Teenagers are addicted to "TikTok" !', App Ape Lab, 26-Jul-2018, <https://en.lab.appa.pe/2018-07/addicted-to-tiktok.html>
- 18 'Digital 2022', We Are Social, Feb-2023, <https://wearesocial.com/au/blog/2022/01/digital-2022-another-year-of-bumper-growth/>
- 19 'As midterms loom, TikTok faces its next political test', Washington Post, 31-Oct-2022,
<https://web.archive.org/web/20221101010758/https://www.washingtonpost.com/technology/2022/10/31/tiktok-faces-2022-midterm-elections/>
- 20 'Gina Raimondo becomes China player in a job where her predecessor used to nap', Bloomberg, 1-Mar-2023,
<https://www.bloomberg.com/news/articles/2023-03-01/chips-tiktok-make-gina-raimondo-vital-to-biden-china-policy>
- 21 'TikTok exec: We're not a social network like Facebook, we're an entertainment platform', CNBC, 16-Jun-2022,
<https://web.archive.org/web/20221127025649/https://www.cnbc.com/2022/06/16/tiktok-were-an-entertainment-app-not-a-social-network-like-facebook.html>
- 22 'Our Mission', TikTok, <https://web.archive.org/web/20221121044107/https://www.tiktok.com/about?lang=en>
- 23 'TikTok's Power Prompts Serious Questions About Security', CNN, 3-Jul-2022,
<https://web.archive.org/web/20220815120817/https://transcripts.cnn.com/show/rs/date/2022-07-03/segment/01>
- Salman Aslam, 'TikTok by the Numbers: Stats, Demographics & Fun Facts', Omnicore, 6-Jan-2023,
<https://www.omnicoreagency.com/tiktok-statistics/#:~:text=TikTok%20stats%20indicate%20that%20the%20platform%20cloaked%20its,a%20total%20of%20over%203%20billion%20downloads%20globally>
- 24 Alex Hern, 'How TikTok's algorithm made it a success: "It pushes the boundaries"', The Guardian, 24-Oct-2022,
<https://web.archive.org/web/20221209092204/https://www.theguardian.com/technology/2022/oct/23/tiktok-rise-algorithm-popularity>
- 25 'Inside TikTok's Attempts to 'Downplay the China Association'', Gizmodo, 27-Jul-2022,
<https://web.archive.org/web/20221109195455/https://gizmodo.com/tiktok-master-messaging-pr-playbook-china-music-1849334736>
- 26 'Inside TikTok's Attempts to 'Downplay the China Association'', Gizmodo, 27-Jul-2022,
<https://web.archive.org/web/20221109195455/https://gizmodo.com/tiktok-master-messaging-pr-playbook-china-music-1849334736>
- 27 ByteDance, <https://web.archive.org/web/20201130234613/https://www.bytedance.com/en/>
- 28 '党建新闻', Beijing Internet Association, <https://archive.ph/1CsgL>
- '协会介绍', Beijing Internet Association, <https://archive.ph/txvAr>
- 29 'Privacy Policy', TikTok, 2-Apr-2022, <https://archive.md/T2aL7>
- 30 'China cyber threat overview and advisories', CISA, <https://www.cisa.gov/china>
- 'The China Threat', FBI, <https://www.fbi.gov/investigate/counterintelligence/the-china-threat>
- 31 'National Cyber Strategy 2022', HM Government, 15-Dec-2022,
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1053023/national-cyber-strategy-amend.pdf
- 'UK condemns Chinese cyber attacks against governments and businesses', National Cyber Security Centre, 16-Sept-2020, <https://www.ncsc.gov.uk/news/uk-condemns-chinese-cyber-attacks-against-businesses-governments>

- 32 'ACSC Annual Cyber Threat Report 202-2021', Australian Cyber Security Centre, 15-Sep-2021, <https://www.cyber.gov.au/sites/default/files/2021-09/ACSC%20Annual%20Cyber%20Threat%20Report%20-%202020-2021.pdf>
- 'Australia joins international partners in attribution of malicious cyber activity to China', Senator the Hon Marise Payne, the Hon Karen Andrews MP, the Hon Peter Dutton MP, 19-Jul-2021, <https://www.foreignminister.gov.au/minister/marise-payne/media-release/australia-joins-international-partners-attribution-malicious-cyber-activity-china>
- 33 'Commission strengthens cybersecurity and suspends the use of TikTok on its corporate devices', European Commission, 23-Feb-2023, https://ec.europa.eu/commission/presscorner/detail/en/ip_23_1161
- 'JP-23-01 - Sustained activity by specific threat actors', ENISA and CERT-EU, 15-Feb-2023, <https://cert.europa.eu/files/data/TLP-CLEAR-JointPublication-23-01.pdf>
- 34 'National Cyber Threat Assessment 2023/2024', Canadian Centre for Cyber Security, 2022, <https://www.cyber.gc.ca/sites/default/files/ncta-2023-24-web.pdf>
- 'Statement by Minister Fortier announcing a ban on the use of TikTok on government mobile devices', Treasury Board of Canada Secretariat, 27-Feb-2023, <https://www.canada.ca/en/treasury-board-secretariat/news/2023/02/statement-by-minister-fortier-announcing-a-ban-on-the-use-of-tiktok-on-government-mobile-devices.html>
- Robert Fife and Steven Chase, 'CSIS documents reveal Chinese strategy to influence Canada's 2021 election', The Globe and Mail, 17-Feb-2023, <https://www.theglobeandmail.com/politics/article-china-influence-2021-federal-election-csis-documents/>
- 35 'New Zealand condemns malicious cyber activity by Chinese state-sponsored actors', Government Communications Security Bureau, 19-Jul-2021, <https://www.beehive.govt.nz/release/new-zealand-condemns-malicious-cyber-activity-chinese-state-sponsored-actors>
- 36 'Cyber Security Assessment Netherlands 2022', National Coordinator for Counterterrorism and Security, 4-Jul-2022, <https://english.nctv.nl/documents/publications/2022/07/04/cyber-security-assessment-netherlands-2022>
- 37 'Kaitsepolitsei Aastaraamat 2021-2022, KAPO, 12-Apr-2022, https://kapo.ee/sites/default/files/content_page_attachments/Aastaraamat_2021-22.pdf
- 'International Security and Estonia 2022', Estonian Foreign Intelligence Service, 31-Jan-2022, <https://www.valisluureamet.ee/doc/raport/2022-en.pdf>
- 38 'WARNING', National Cyber and Information Security Agency, 8-Mar-2023, https://www.nukib.cz/download/publications_en/2023-03-08_Warning-TikTok-App.pdf
- 39 'Cyber Operations Enabling Expansive Digital Authoritarianism', 7-Apr-2020, National Intelligence Council, <http://web.archive.org/web/20230217033234/https://www.dni.gov/files/ODNI/documents/assessments/NICM-Declassified-Cyber-Operations-Enabling-Expansive-Digital-Authoritarianism-20200407--2022.pdf>
- 40 See our technical analysis of the TikTok Android app in Section 8 for details of potential data collection overreach and user data security concerns. See also:
- 'Leaked Audio From 80 Internal TikTok Meetings Shows That US User Data Has Been Repeatedly Accessed From China', BuzzFeed, 17-Jun-2022, <https://www.buzzfeednews.com/article/emilybakerwhite/tiktok-tapes-us-user-data-china-bytedance-access>
- 'Privacy Analysis of TikTok's App and Website', Rufposten, 5-Dec-2019, <https://rufposten.de/blog/2019/12/05/privacy-analysis-of-tiktoks-app-and-website/>
- 41 'EXCLUSIVE: TikTok Spied on Forbes Journalists', Forbes, 22-Dec-2022, <https://www.forbes.com/sites/emilybaker-white/2022/12/22/tiktok-tracks-forbes-journalists-bytedance/?sh=5aebf8af7da5>
- 'TikTok Parent ByteDance Planned to Use TikTok to Monitor The Physical Location Of Specific American Citizens', Forbes, 20-Oct-2022, <https://www.forbes.com/sites/emilybaker-white/2022/10/20/tiktok-bytedance-surveillance-american-user-data/?sh=436b90e36c2d>
- 'Leaked Audio From 80 Internal TikTok Meetings Shows That US User Data Has Been Repeatedly Accessed From China', BuzzFeed News, 18-Jun-2022, <https://www.buzzfeednews.com/article/emilybakerwhite/tiktok-tapes-us-user-data-china-bytedance-access>
- 42 'Data brokers and national security', Lawfare, 29-Apr-2021, <https://www.lawfareblog.com/data-brokers-and-national-security>
- 'China harvest masses of data on Western targets, documents show,' The Washington Post, 31-Dec-2021, https://www.washingtonpost.com/national-security/china-harvests-masses-of-data-on-western-targets-documents-show/2021/12/31/3981ce9c-538e-11ec-8927-c396fa861a71_story.html
- 'How China harnesses data fusion to make sense of surveillance data,' Brookings, 23-Sep-2021, <https://www.brookings.edu/techstream/how-china-harnesses-data-fusion-to-make-sense-of-surveillance-data/>
- 'Baby Biocode: China's gene giant harvests data from millions of women,' Reuters, 7-Jul-2021, <https://www.reuters.com/investigates/special-report/health-china-bgi-dna/>
- Lotus Ruan, 'When the winner takes it all: Big data in China and the battle for privacy,' ASPI Report No. 5/2018, https://ad-aspi.s3.ap-southeast-2.amazonaws.com/2018-06/Winner%20takes%20it%20all_0.pdf?VersionId=r0DDh71qxQgqwHtX8z8tmScoz55JQVyc

- Samantha Hoffman and Nathan Attrill, 'Mapping China's technology giants: Supply chains and the global data collection ecosystem,' ASPI Report No. 45/2021, https://ad-aspi.s3.ap-southeast-2.amazonaws.com/2021-06/Supply%20chains.pdf?VersionId=56J_tt8xYXYvsMuhriQt5dSsr92ADaZH
- Emile Dirks and James Leibold, 'Genomic surveillance: Inside China's DNA dragnet,' ASPI Report No. 34/2020, https://ad-aspi.s3.ap-southeast-2.amazonaws.com/2020-06/Genomic%20surveillance_1.pdf?VersionId=QhPFyrNVaSjvblmFT24HRXSuHyRfhpmI
- 'Why TikTok is the latest security threat,' Center for Internet Security, <https://www.cisecurity.org/insights/blog/why-tiktok-is-the-latest-security-threat>
- 43 'Five Individuals Charged Variously with Stalking, Harassing and Spying on U.S. Residents on Behalf of the PRC Secret Police', US Department of Justice, 16-Mar-2022, <https://web.archive.org/web/20221231145316/https://www.justice.gov/opa/pr/five-individuals-charged-variously-stalking-harassing-and-spying-us-residents-behalf-prc-0#:~:text=United%20States%20v.%20Qiming%20Lin>
- 44 'TikTok Parent ByteDance Planned To Use TikTok To Monitor The Physical Location Of Specific American Citizens', Forbes, 20-Oct-2022, <https://www.forbes.com/sites/emilybaker-white/2022/10/20/tiktok-bytedance-surveillance-american-user-data/?sh=746cf0266c2d>
- 'Why TikTok is the latest security threat', Center for Internet Security, <https://www.cisecurity.org/insights/blog/why-tiktok-is-the-latest-security-threat>
- 45 'Social Media and News Fact Sheet,' Pew Research, 20-Sep-2022, <https://www.pewresearch.org/journalism/fact-sheet/social-media-and-news-fact-sheet/>
- 46 'TikTok's state-affiliated media policy', TikTok, 18-Jan-2023, <https://web.archive.org/web/20230203101952/https://newsroom.tiktok.com/en-us/tiktoks-state-affiliated-media-policy>
- 47 '大数据下的网络舆情应对', Cyberspace Administration of China, 29-Dec-2016, https://web.archive.org/web/20220520173515/http://www.cac.gov.cn/2016-12/29/c_1120214456.htm
- '人工智能、大数据与对外传播的创新发展', International Communications via People's Daily, 18-Apr-2019, <https://web.archive.org/web/20220523174958/http://media.people.com.cn/n1/2019/0418/c40628-31037065-2.html>
- 'Evaluating the Utility of Global Data Collection by Chinese Firms for Targeted Propaganda', Jamestown, 30-Oct-2020, <https://web.archive.org/web/20220929152445/https://jamestown.org/program/evaluating-the-utility-of-global-data-collection-by-chinese-firms-for-targeted-propaganda/>
- 48 Lili Turner and Nirit Hinkis, 'Chinese state media's global influencer operation', Miburo, 31-1-2022, <https://miburo.substack.com/p/csm-influencer-ops-1>
- Nirit Hinkis and Lili Turner, 'Chinese state media's global influencer operation: Why it matters', Miburo, 10-Feb-2021, <https://miburo.substack.com/p/chinese-state-medias-global-influencer>
- Fergus Ryan, Audrey Fritz and Daria Impiombato, 'TikTok and WeChat: Curating and controlling global information flows', ASPI Policy Brief No. 37/2020, <https://ad-aspi.s3.ap-southeast-2.amazonaws.com/2020-09/TikTok%20and%20WeChat.pdf?VersionId=7BNJWaoHImPVE.6KKcBP1JRD5fRnAVTZ>
- Fergus Ryan, Daniella Cave and Vicky Xiuzhong Xu, 'Mapping more of China's technology giants: AI and surveillance,' ASPI Issues Paper No. 24/2019, <https://archive.md/wip/wP051>
- Albert Zhang, Jacob Wallis and Zoe Meers, 'Strange bedfellows on Xinjiang: The CCP, fringe media and US social media platforms,' ASPI, March 2021, http://web.archive.org/web/20221001172836/https://ad-aspi.s3.ap-southeast2.amazonaws.com/202103/Strange%20bedfellows.pdf?VersionId=mOh5mC5B_a08J6ntNwTC2q6GdjtWz4di
- Fergus Ryan, Ariel Bogle, Nathan Ruser, Albert Zhang and Daria Impiombato, 'Borrowing mouths to speak on Xinjiang,' ASPI Policy Brief No. 55/2021, <https://archive.md/yMRjM>
- Fergus Ryan, Daria Impiombato and Hsi-Ting Pai, 'Frontier influencers: The new face of China's propaganda,' ASPI Policy Brief No. 65/2022, <https://archive.md/MWUBv>
- Samantha Bradshaw, 'Influence operations and disinformation on social media,' Centre for International Governance Innovation, 23-Nov-2020, <https://archive.md/jMHuK>
- 49 Matthew Johnson, 'Safeguarding socialism: The origins, evolution, and expansion of China's total national security paradigm,' Sinopsis, 11-Jun-2020, <https://sinopsis.cz/en/johnson-safeguarding-socialism/>
- 50 Matthew Johnson, 'Safeguarding socialism: The origins, evolution, and expansion of China's total national security paradigm,' Sinopsis, 11-Jun-2020, <https://sinopsis.cz/en/johnson-safeguarding-socialism/>
- 51 John Fitzgerald, 'Beijing's Guoqing versus Australia's Way of Life', Inside Story, 27-Sept-2015, <https://insidestory.org.au/beijings-guoqing-versus-australias-way-of-life/>
- '中共中央关于加强党的执政能力建设的决定', Xinhua Net via 中央政府门户网站, 20-Aug-2008, <http://archive.today/zxuz6>
- 52 Matthew Johnson, 'Safeguarding socialism: The origins, evolution, and expansion of China's total national security paradigm,' Sinopsis, 11-Jun-2020, <https://sinopsis.cz/en/johnson-safeguarding-socialism/>
- 53 '习近平在中共中央政治局第三十次集体学习时强调: 加强和改进国际传播工作 展示真实立体全面的中国', People's Daily, 2-Jun-2021, <http://archive.today/E8T2y>

- 54 '中共中央关于全面深化改革若干重大问题的决定', Xinhua Net via 中央政府门户网站, 15-Nov-2013, <https://archive.ph/hs5gH>
- 55 '中共中央关于全面深化改革若干重大问题的决定', Xinhua Net via 中央政府门户网站, 15-Nov-2013, <https://archive.ph/hs5gH>
- 56 '习近平引领国际传播能力建设', CCTV via People's Daily, 14-Jun-2022, <http://archive.today/RYZkr>
- 57 '习近平: 讲好中国故事, 传播好中国声音', Qiushi, 2-Jun-2021, <http://archive.today/II79B>
- 58 '习近平: 讲好中国故事, 传播好中国声音', Qiushi, 2-Jun-2021, <http://archive.today/II79B>
- 59 '习近平在中央政治局第二十六次集体学习时强调 坚持系统思维构建大安全格局 为建设社会主义现代化国家提供坚强保障', Xinhua, 12-Dec-2020, <https://archive.vn/gQpAO>
- 60 'Profile (English-language): "Yuan Peng"', CICIR, <https://archive.vn/wip/qYiDo>
- 61 《国际战略与安全形势评估 2020/2021》卷首语, CICIR, 31-Dec-2020, <https://archive.vn/Xsnnq>
- 62 '港媒: 美国问题专家袁鹏 改名袁亦鲲出任国安部副部长', Lianhe Zaobao, 22-Feb-2023, <https://archive.md/CECOq>
- 63 '习近平: 讲好中国故事, 传播好中国声音', Qiushi, 2-Jun-2021, <http://archive.today/II79B>
- 64 'The party speaks for you: Foreign interference and the Chinese Communist Party's united front system', Australian Strategic Policy Institute, 9-Jun-2020, <https://www.aspi.org.au/report/party-speaks-you>
- 65 '让短视频平台展示好中国形象传播好中国声音', Xinhua, 6-Aug-2021, <http://archive.today/qk00A>
- 66 '让短视频平台展示好中国形象传播好中国声音', Xinhua, 6-Aug-2021, <http://archive.today/qk00A>
- 67 Paul Saba, 'On the Role of Agitation and Propaganda (Transcription)', Encyclopedia of Anti-Revisionism On-Line, originally published Dec-1978, <https://www.marxists.org/history/erol/ncm-8/rcp-agit-prop.htm>
- 'Talks at the Yen'an Forum on Literature and Art', Selected Works of Mao Tse-tung, 2-May-1942, https://www.marxists.org/reference/archive/mao/selected-works/volume-3/mswv3_08.htm
- '24. Correcting Mistaken Ideas', Quotations from Mao Tse Tung, 5-Mar-1949, <https://www.marxists.org/reference/archive/mao/works/red-book/ch24.htm>
- 70 'Analysis of the Classes in Chinese Society', Selected Works of Mao Tse-Tung, Mar-1926, https://web.archive.org/web/20230217043746/https://www.marxists.org/reference/archive/mao/selected-works/volume-1/mswv1_1.htm
- 71 'Document 9: A ChinaFile Translation', ChinaFile, 8-Nov-2013, <https://web.archive.org/web/20230217043230/https://www.chinafile.com/document-9-chinafile-translation>
- 72 Rogier Creemers, 'Xi Jinping's 19 August speech revealed? (Translation)', China Copyright and Media, 12-Nov-2013, <https://chinacopyrightandmedia.wordpress.com/2013/11/12/xi-jinpings-19-august-speech-revealed-translation/>
- 73 '网传习近平 8•19 讲话全文: 言论方面要敢抓敢管敢于亮剑', 中国数字时代 China Digital Times, 4-Nov-2013, <https://archive.vn/mtvA1>
- 74 Lily Kuo, 'Chinese journalists to be tested on loyalty to Xi Jinping', The Guardian, 20-Sep-2019, <https://www.theguardian.com/world/2019/sep/20/chinese-journalists-to-be-tested-on-loyalty-to-xi-jinping>
- 75 Willy Lam, 'Beijing Harnesses Big Data & AI to Perfect the Police State', The Jamestown Foundation, 21-Jul-2017, <https://jamestown.org/program/beijing-harnesses-big-data-ai-to-perfect-the-police-state/>
- 76 Liat Clark, 'China wants police installed in every internet company', Wired, 05-Aug-2015, <https://www.wired.co.uk/article/china-cyber-security-police-in-internet-headquarters>
- Liza Lin and Josh Chin, 'China's Tech Giants Have a Second Job: Helping Beijing Spy on Its People', The Wall Street Journal, 30-Nov-2017, <https://www.wsj.com/articles/chinas-tech-giants-have-a-second-job-helping-the-government-see-everything-1512056284>
- 77 John Garnaut, 'Hong Kong's outspoken media chiefs are facing growing intimidation', The Sydney Morning Herald, 30-May-2014, <https://www.smh.com.au/world/hong-kongs-outspoken-media-chiefs-are-facing-growing-intimidation-20140530-399ol.html>
- John Garnaut, 'Australia's China reset', The Monthly, Aug-2018, <https://www.themonthly.com.au/issue/2018/august/1533045600/john-garnaut/australia-s-china-reset#mtr>
- 79 'Asia-Pacific Absolute and autocratic control of information', Reporters Without Borders, <https://rsf.org/en/classement/2022/asia-pacific>
- 80 学而时习, '习近平: 讲好中国故事, 传播好中国声音', Qiushi, 2-Jun-2021, <http://archive.today/II79B>
- '习近平在中央政治局第三十次集体学习时强调: 加强和改进国际传播工作 展示真实立体全面的中国', People's Daily, 2-Jun-2021, <http://archive.today/E8T2y>
- 81 '中华人民共和国网络安全法', Xinhua, 7-Nov-2016, <https://archive.ph/lwrOs>
- 82 '科学大数据——国家大数据战略的基石', China Development Gateway, 7-Sep-2017, <https://archive.md/PkLNF>
- 83 '中华人民共和国国民经济和社会发展第十四个五年规划和 2035 年远景目标纲要' (transmitted March 12, 2021), Xinhua, March 13, 2022, <https://archive.ph/ZTF2U>

- ‘工业和信息化部关于印发大数据产业发展规划（2016 – 2020 年）的通知’, MIIT, December 18, 2016, <https://archive.ph/qa4Zx>
- 84 “十四五”大数据产业发展规划’, MIIT, November 2021, <https://archive.ph/hhRHt>
- 85 ‘中华人民共和国国家安全法（主席令第二十九号）’, 中央政府门户网站, 1-Jul-2015, <https://archive.md/xhfrx>
- 86 ‘中华人民共和国国家情报法’, 中国人大网, 12-Jun-2018, <https://archive.md/EvpjJ>
- 87 ‘中华人民共和国网络安全法’, CAC, 7-Nov-2016, <https://archive.ph/lwrOs>
- 88 ‘中华人民共和国数据安全法’, 中国人大网, 10-Jun-2021, <https://archive.md/IMQL0>
- 89 ‘中华人民共和国个人信息保护法’, 中国人大网, 20-Aug-2021, <https://archive.md/2cifD>
- Zach Dorfman, ‘Tech giants are giving China a vital edge in espionage,’ Foreign Policy, 23-Dec-2020, <https://foreignpolicy.com/2020/12/23/china-tech-giants-process-stolen-data-spy-agencies/>
- 90 Zach Dorfman, ‘Tech giants are giving China a vital edge in espionage,’ Foreign Policy, 23-Dec-2020, <https://foreignpolicy.com/2020/12/23/china-tech-giants-process-stolen-data-spy-agencies/>
- 91 ‘人工智能新赛场 – 中美对比’, CCID, May-2017, and 朱启超, 王婧凌, 李大光, ‘工智能叩开智能化战争大门’, PLA Daily, 23-Jan-2017, in Elsa B. Kania, ‘Battlefield Singularity: Artificial Intelligence, Military Revolution, and China’s Future Military Power,’ Center for New American Security, Nov-2017, <https://s3.us-east-1.amazonaws.com/files.cnas.org/hero/documents/Battlefield-Singularity-November-2017.pdf?mtime=20171129235805&focal=none>, p. 11
- 92 ‘Cyber Operations Enabling Expansive Digital Authoritarianism’, National Intelligence Council, 7-Apr-2020, <https://archive.md/lk3GK>
- 93 ‘中国人民解放军政治工作条例（节选）’, 十六大以来重要文献选编上 via China Reform Data, 5-Dec-2003, <https://archive.vn/xbKE6>
- 94 ‘中国人民解放军政治工作条例’, 《中央党内法规和规范性文件汇编》（1949 年 10 月—2016 年 12 月） via CCP Central Propaganda Department website, 9-Aug-2010, <https://archive.vn/zrrmu>
- 95 中国人民解放军军事科学院军事战略研究部, 《战略学》（2013 年版）, 军事科学出版社, 2013, p. 116. An English-language translation of the text is available from the China Aerospace Studies Institute, see Academy of Military Science Military Strategy Studies Department, *The Science of Military Strategy* (2013 Edition), Beijing: Military Science Press, 2013, <https://www.airuniversity.af.edu/CASI/Display/Article/2485204/plas-science-of-military-strategy-2013/>
- 96 中国人民解放军军事科学院军事战略研究部, 《战略学》（2013 年版）, 军事科学出版社, 2013, p. 116. See Academy of Military Science Military Strategy Studies Department, *The Science of Military Strategy* (2013 Edition), Beijing: Military Science Press, 2013, <https://www.airuniversity.af.edu/CASI/Display/Article/2485204/plas-science-of-military-strategy-2013/>
- 97 ‘习近平首次军队训词意义重大’, Study China via People’s Daily, 3-Jan-2016, <https://archive.vn/gNgJK>
- 98 陳津萍 和 張貽智, ‘軍改後中共「中央軍委政治工作部」組織與職能之研究’, 軍事社會科學專刊, Aug-2019: pp. 27-50
- 99 ‘李弼程, 胡华平, 熊尧, ‘网络舆情引导智能代理模型’, 国防科技, 2019, <https://archive.md/QdOcx>
- 100 Elsa B. Kania, ‘Battlefield Singularity: Artificial Intelligence, Military Revolution, and China’s Future Military Power,’ Center for New American Security, Nov-2017, <https://s3.us-east-1.amazonaws.com/files.cnas.org/hero/documents/Battlefield-Singularity-November-2017.pdf?mtime=20171129235805&focal=none>
- c.f. 刘全展, 李波, ‘大数据：信息化作战的制胜法宝’, PLA Daily, 15-Nov- 2015, in Elsa B. Kania, ‘Battlefield Singularity: Artificial Intelligence, Military Revolution, and China’s Future Military Power,’ Center for New American Security, Nov-2017, <https://s3.us-east-1.amazonaws.com/files.cnas.org/hero/documents/Battlefield-Singularity-November-2017.pdf?mtime=20171129235805&focal=none>, p. 27
- 101 ‘About ByteDance’, ByteDance, <https://web.archive.org/web/20191003163728/https://bytedance.com/en/about#leadership>
- Sam Byford, ‘How China’s ByteDance became the world’s most valuable startup’, The Verge, 30-Nov-2018, <https://archive.ph/EcHxq>
- 102 ‘海纳亚洲基金王琼：张一鸣在一张餐巾纸上画出了头条的产品原型’, ZTHC, 12-Jun-2022, <https://web.archive.org/web/20221117091553/https://m.zhongtoutu.com/h-nd-2913.html>
- 103 ‘风暴中的张一鸣：“创富神兽”让身家充满变数’, 21st Century Business Herald, 6-Aug-2020, <https://archive.ph/bsulN>
- 104 “饭否”归来 尚能饭否’, CYOL, 2-Dec-2010, <https://archive.ph/n0pvW>
- ‘作者介绍’, Chongzou, <https://archive.ph/NnQYB>
- 105 “饭否”归来 尚能饭否’, CYOL, 2-Dec-2010, <https://archive.ph/n0pvW>
- 106 ‘微博网站“饭否”关闭一年多后重新开放’, BBC, 30-Nov-2010, https://web.archive.org/web/20221209070202/https://www.bbc.com/zhongwen/simp/china/2010/11/101130_chi_na_fanfou_internet

- 107 '南开校友、今日头条创始人张一鸣在 2016 级新生开学典礼上的讲话', Nankai University, 19-Sep-2016, <https://web.archive.org/web/20221209053808/https://cs.nankai.edu.cn/info/1039/2356.htm>
- 108 '网络空间, 年轻创业者在这里逐梦', People's Daily, 18-Apr-2013, <https://archive.ph/llPyf>
- 109 '这个龙岩 80 后要怒砸 10 亿抢占下一个风口', Sina Fujian, <https://archive.ph/tbnsq>
- 110 '这个龙岩 80 后要怒砸 10 亿抢占下一个风口', Sina Fujian, <https://archive.ph/tbnsq>
- 111 "'饭否"归来 尚能饭否', CYOL, 2-Dec-2010, <https://archive.ph/n0pvW>
- '微博网站"饭否"关闭一年多后重新开放', BBC, 30-Nov-2010, https://web.archive.org/web/20221209070202/https://www.bbc.com/zhongwen/simp/china/2010/11/101130_china_fanfou_internet
- 112 '解码酷讯创业帮: 张一鸣这些 80 后老板们的"黄埔军校"', Economic Observer Network, 3-Sep-2016, <https://archive.ph/lqxue>
- 113 '海纳亚洲王琼自述: 为何投资今日头条?', Huxiu, 5-Apr-2016, <https://archive.ph/x1SMJ>
- 114 '这个龙岩 80 后要怒砸 10 亿抢占下一个风口', Sina Fujian, <https://archive.ph/tbnsq>
- 115 Yue Wang, 'Billionaire Zhang Yiming Steps Down As ByteDance Chairman', Forbes, 3-Nov-2021, <https://www.forbes.com/sites/ywang/2021/11/03/billionaire-zhang-yiming-steps-down-as-bytedance-chairman/?sh=57548d2e7016>
- 116 '36 氪独家 | 字节跳动搭建"直播大台", 张一鸣想在广告之外寻觅第二台"赚钱机器"', 36kr, 19-Mar-2019, <https://archive.ph/iL3OU>
- '从字节跳动"拆中台"寻找巨头中台演进的草蛇灰线', Jiemian, 11-Nov-2021, <https://archive.ph/ftPv6>
- 117 '张一鸣首谈字节跳动创业 7 年: 我们不是 APP 工厂, 是一个浪漫的公司', National Business Daily, 14-Mar-2019, <https://archive.ph/FMpPh>
- 118 'ByteDance CEO returns to the apartment where he first started the company', YouTube (ByteDance channel), 30-Jul-2020, https://www.youtube.com/watch?v=TIYPXpfA7_Q
- 119 '张一鸣的"上帝视角"', Pingwest, 15-Jun-2015, <https://web.archive.org/web/20221118014848/https://www.pingwest.com/a/51495>
- 120 '字节跳动二号人物登场', Jiemian via Sohu, 14-Mar-2020, <https://archive.ph/yWrXs>
- '张一鸣首谈字节跳动创业 7 年: 我们不是 APP 工厂, 是一个浪漫的公司', National Business Daily, 14-Mar-2019, <https://archive.ph/FMpPh>
- 121 '张一鸣退出字节跳动全球董事会, 梁汝波与八名核心高管走向前台', LatePost via WeChat, 2-Nov-2021, <https://web.archive.org/web/20211127192008/https://mp.weixin.qq.com/s/TkpV2ux3ibqj372c39cApg>
- '新加入视频功能的读图应用"图吧", 想借读图构建用户的兴趣图谱', 36kr, 28-Jun-2013, <https://archive.ph/ckyUU>
- 122 '海纳亚洲王琼自述: 为何投资今日头条?', Huxiu, 6-Apr-2016, <https://archive.ph/x1SMJ>
- Ryan Mac and Chang Che, 'TikTok's C.E.O. Navigates the Limits of His Power', New York Times, 16-Sep-2022, <https://web.archive.org/web/20221114134158/https://www.nytimes.com/2022/09/16/technology/tiktok-ceo-shou-zi-chew.html>
- Yunan Zhang and Juro Osawa, 'Tencent, Xiaomi Invested in TikTok's Parent, ByteDance', The Information, 20-Aug-2020, <https://www.theinformation.com/articles/tencent-xiaomi-invested-in-tiktoks-parent-bytedance?rc=zcbseh>
- 123 Murray Newlands, 'The Origin and Future Of America's Hottest New App: musical.ly', Forbes, 10-Jun-2016, <https://archive.ph/zTHL4>
- 124 'Petition for review, TikTok Inc. and ByteDance Ltd., Petitioners', The United States Court Of Appeals For The District Of Columbia Circuit, 10-Nov-2020, <https://web.archive.org/web/20210928143950/https://www.courthousenews.com/wp-content/uploads/2020/11/tiktok-cadc-petition.pdf>
- 125 '今日头条收购 Mus cal.ly: 海外野心与引信型公司宿命', Jiemian, 13-Nov-2017, <https://archive.ph/YZL3C>
- 'Mus cal.ly CEO 阳陆育: C 轮前投资方全部退出', Yicai, 13-Nov-2017, <https://archive.ph/Ma6QW>
- '微视努力撕掉抄袭标签 能否复制抖音增长轨迹?', Sina Tech via WeChat, 23-May-2018, <https://archive.ph/ELz6k>
- 'Petition for review, TikTok Inc. and ByteDance Ltd., Petitioners', The United States Court Of Appeals For The District Of Columbia Circuit, 10-Nov-2020, <https://web.archive.org/web/20210928143950/https://www.courthousenews.com/wp-content/uploads/2020/11/tiktok-cadc-petition.pdf>
- 126 '机会面前, 拼的是速度 | 21 读书', 21st Century Business Herald via China Fund, 23-Oct-2021, <https://archive.ph/GSj2X>
- 127 'Can pop music connect teens in China with the world? Musical.ly co-founder Louis Yang wants to find out', The China Project, 13-Sep-2017, <https://archive.ph/wQ9kU>

- 128 John Herrman, 'Who's Too Young for an App? Musical.ly Tests the Limits', New York Times, 16-Sep-2016, <https://web.archive.org/web/20221102192402/https://www.nytimes.com/2016/09/17/business/media/a-social-network-frequented-by-children-tests-the-limits-of-online-regulation.html>
- 129 'The most popular users on musical.ly', DW, 19-Oct-2016, <https://archive.ph/z4XFm>
- 129 '今日头条张一鸣: 短视频是内容创业的下一个风口', Sina, 20-Sep-2016, <https://web.archive.org/web/20221118040558/http://tech.sina.com.cn/i/2016-09-20/doc-ifxyqvy6859414.shtml>
- 130 Benita Zhang, '抖音内幕: 时间熔炉的诞生', Tencent News via Huxiu, 26-Oct-2020, <https://archive.ph/pgGxT>
- 131 '大事记', ByteDance, <https://web.archive.org/web/20230308045944/https://www.bytedance.com/zh/>
- '谁在管理 TikTok: 没有中心的网状组织、字节的全球化构想', LatePost via Laohu8, 7-Apr-2022, <https://archive.ph/yLV9W>
- 132 'TikTok 内幕: 张一鸣的巨浪征途', Jiemiao via Sina, 25-Apr-2022, <https://archive.ph/geqqt>
- '【爆料】Mus cal.ly 为何卖给了头条而不是出价更高的快手', iFeng, 10-Nov-2017, https://web.archive.org/web/20230308174817/https://tech.ifeng.com/a/20171110/44755384_0.shtml
- 'Musical.ly has lots of users, not much ad traction', Digiday, 5-Sep-2017, <https://archive.ph/giB5r>
- 'From Musers To Money: Inside Video App Musical.ly's Coming Of Age', Forbes, 11-May-2017, <https://archive.ph/NxiD0>
- 133 '大事记', ByteDance, <https://web.archive.org/web/20230308045944/https://www.bytedance.com/zh/>
- 'China's ByteDance buying lip-sync app Musical.ly for up to \$1 billion', Reuters, 10-Nov-2017, <https://www.reuters.com/article/us-musical-ly-m-a-bytedance-idUSKBN1DA0BN>
- '字节跳动收购的 musical.ly 正式并入 Tik Tok', Sina Tech, 2-Aug-2018, <https://archive.ph/Cmh5A>
- 134 'TikTok 内幕: 张一鸣的巨浪征途', Jiemiao via Sina, 25-Apr-2022, <https://archive.ph/geqqt>
- 135 '大事记', ByteDance, <https://web.archive.org/web/20230308045944/https://www.bytedance.com/zh/>
- Georgia Wells and Yang Jie, 'TikTok's Videos Are Goofy. Its Strategy to Dominate Social Media Is Serious.' The Wall Street Journal, 29-Jun-2019, <https://web.archive.org/web/20220930033958/https://www.wsj.com/articles/tiktoks-videos-are-goofy-its-strategy-to-dominate-social-media-is-serious-11561780861>
- 136 '沈南鹏: 王兴、张一鸣给我的启发和感受', China Businessman via FX361, 7-May-2021, <https://archive.ph/Th5E5>
- 137 '第二届中韩互联网圆桌会议', Xinhua, 2013, <https://archive.ph/hYgD0>
- 138 '首届世界互联网大会开幕 业界大佬齐聚乌镇', Yicai, 19-Nov-2014, <https://web.archive.org/web/20230101171859/https://www.yicai.com/news/4042409.html>
- 139 '鲁炜: 世界互联网大会实现了 3 个 C to C', Caixin, 19-Nov-2014, <https://archive.ph/dg7jL>
- '今日头条 CEO 张一鸣: 机器解放媒体人', Caixin, 19-Nov-2014, <https://archive.ph/q8rw8>
- 140 'China-US Internet Industry Forum opens in Washington DC', China Daily via gov.cn, 14-Dec-2014, <https://archive.ph/3lyph>
- 141 '互联网信息办公室主任鲁炜在美把库克贝索斯小扎见了个遍 #硅谷史上最美图片集不服来辩#', Huxiu, 7-Dec-2014, <https://archive.ph/0sr65>
- 142 'Chinese Internet regulator welcomed at Facebook campus', Reuters, 8-Dec-2014, <https://archive.ph/6Ku2C>
- '除了大合照, 中美论坛上大佬们还聊了什么?', China.org.cn, 24-Sep-2015, <https://archive.ph/vOM6j>
- '随习主席访美互联网公司除 BAT 还有哪些', Sina Finance, 22-Sep-2015, <https://archive.ph/fzghw>
- 143 '除了大合照, 中美论坛上大佬们还聊了什么?', China.org.cn, 24-Sep-2015, <https://archive.ph/vOM6j>
- 144 '专访张一鸣: 中国企业完全有能力在海外拓展', Global Times, 30-Sep-2015, <https://archive.ph/ruVnu>
- 145 'What's in a picture? The unspoken messages in Xi Jinping's group portrait with CEOs and senior executives during his first state visit to the US', SCMP, https://www.scmp.com/tech/leaders-founders/article/1861033/whats-picture-unspoken-messages-xi-jinpings-group-portrait?module=perpetual_scroll_0&pgtype=article&campaign=1861033
- 146 '第二届世界互联网大会', Huanqiu, <https://archive.ph/nxPHP>
- 147 '第二届世界互联网大会', Huanqiu, <https://archive.ph/nxPHP>
- 148 '中共中央宣传部原副部长鲁炜 涉嫌严重违纪接受组织审查', CCDI via gov.cn, 22-Nov-2017, <https://archive.ph/dmnzt>
- 149 '中央宣传部原副部长、中央网信办原主任鲁炜, 山东省政府原党组成员、副省长季缙绮严重违纪被开除党籍和公职', CCDI, 13-Dec-2018, https://web.archive.org/web/20221124050712/https://www.ccdi.gov.cn/toutiao/201802/t20180213_164223.html
- '中宣部原副部长鲁炜受贿 3200 万 判 14 年罚金 300 万', Xinhua via Sina, 26-Mar-2019, <https://archive.ph/7L1ZS>
- 'China's Former Top Internet Regulator Gets 14 Years for Corruption', WSJ, 26-Mar-2019, <https://archive.ph/2NM91>

- 150 “内涵段子”被永久关停, Xinhua, 10-Apr-2018,
https://web.archive.org/web/20220625025726/http://www.xinhuanet.com/politics/2018-04/10/c_129847557.htm
- 151 ‘端传媒 | 两千万日活的手机应用为何被突然斩杀?’, China Digital Times, 21-Apr-2018, <https://archive.md/tjF8b>
- 152 ‘争雄 BAT “头条帝国”何以崛起’, Caixin via Zhihu, 8-Feb-2020, <https://archive.ph/CFRLk>
- 153 ‘Complaint for injunctive and declaratory relief, TikTok Inc. and ByteDance Ltd.’, United States District Court, Central District of California Western Division, 24-Aug-2020,
<https://web.archive.org/web/20220416021500/https://s3.documentcloud.org/documents/7043165/TikTok-Trump-Complaint.pdf>
- 154 ‘中国共产党章程’, 12371.cn [Organisation Department], 22-Oct-2022,
<https://web.archive.org/web/20221126151852/http://www.12371.cn/2022/10/26/ART11666788342244946.shtml>
- 155 ‘小丫专访张一鸣: 我不是“新闻搬运工”’, CCTV, 27-Aug-2014,
<https://web.archive.org/web/20221115070825/http://jingji.cntv.cn/2014/08/27/ART11409120412396179.shtml>
- 156 ‘今日头条创始人回应低俗质疑: 从不主动 push 低俗内容’, Caijing via Sina, 14-Dec-2016,
<https://web.archive.org/web/20220708100249/http://tech.sina.com.cn/i/2016-12-14/doc-ifxyipt1331463.shtml>
- 157 ‘国家版权局对“今日头条”立案调查’, People’s Daily, 24-Jun-2014, <https://archive.ph/rR4mn>
- 158 ‘小丫专访张一鸣: 我不是“新闻搬运工”’, CCTV, 27-Aug-2014,
<https://web.archive.org/web/20221115070825/http://jingji.cntv.cn/2014/08/27/ART11409120412396179.shtml>
- 159 ‘国家版权局对“今日头条”立案调查’, People’s Daily, 24-Jun-2014, <https://archive.ph/rR4mn>
- 160 ‘国家版权局确认“今日头条”侵权: 积极整改是好现象’, People’s Daily, 16-Sep-2014, <https://archive.ph/1StWt>
- 161 Li Yuan, ‘China’s TikTok Blazes New Ground. That Could Doom It.’, New York Times, 5-Nov-2019,
<https://web.archive.org/web/20220930033958/https://www.nytimes.com/2019/11/05/business/tiktok-china-bytedance.html>
- 162 ‘今日头条创始人回应低俗质疑: 从不主动 push 低俗内容’, Caijing via Sina, 14-Dec-2016,
<https://web.archive.org/web/20220708100249/http://tech.sina.com.cn/i/2016-12-14/doc-ifxyipt1331463.shtml>
- 163 ‘北京网信办约谈今日头条、凤凰新闻手机客户端负责人 两家企业将暂停部分频道内容更新’, People’s Daily, 29-Dec-2017, <https://archive.ph/awbil>
- 164 ‘互联网不良内容的监管升级 微信微博今日头条纷纷自查’, Beijing News via China News, 12-Apr-2018,
<https://archive.ph/7DUhu>
- 165 ‘未成年怀孕成“网红”? 被央视点名的快手、火山小视频下架整改!’, National Business Daily, 6-Apr-2018,
<https://archive.ph/iuwhD>
- 166 ‘4 款 APP 被下架 今日头条暂停下载 3 周’, The Beijing News, 10-Apr-2018, <https://archive.ph/73Ddc>
- 167 ‘张一鸣宣布卸任字节跳动 CEO, 联合创始人梁汝波将接任’, The Paper, 20-May-2021, <https://archive.ph/fSp5h>
- 168 ‘字节跳动创始人张一鸣已卸任董事长 退出董事会--消息人士 (更新版)’, Reuters, 3-Nov-2021,
<https://www.reuters.com/article/bytedance-reshuffling-1103-wedn-idCNKBS2HO06L>
- 169 ‘北京网信办约谈今日头条、凤凰新闻手机客户端负责人 两家企业将暂停部分频道内容更新’, People’s Daily, 29-Dec-2017, <https://archive.ph/awbil>
- 170 ‘今日头条启动招聘 2000 名内容审核编辑: 党员优先’, The Paper, 3-Jan-2018,
https://web.archive.org/web/20221116013004/https://www.thepaper.cn/newsDetail_forward_1932733
- 171 ‘今日头条公布算法原理 称并非一切交给机器’, Leiphone, 12-Jan-2018,
<http://web.archive.org/web/20221122152458/https://www.leiphone.com/category/industrynews/cEc03ORUAeiwytnC.html>
- 172 ‘互联网不良内容的监管升级 微信微博今日头条纷纷自查’, Beijing News via China News, 12-Apr-2018,
<https://archive.ph/7DUhu>
- 173 ‘未成年怀孕成“网红”? 被央视点名的快手、火山小视频下架整改!’, National Business Daily, 6-Apr-2018,
<https://archive.ph/iuwhD>
- 174 ‘国家广播电视总局严肃处理“今日头条”“快手”传播有违社会道德节目等问题’, State Administration of Press, Publication, Radio, Film and Television of the PRC, 4-Apr-2018,
<https://web.archive.org/web/20200124192251/http://www.sapprft.gov.cn/sapprft/contents/6582/363639.shtml>
- 175 ‘“内涵段子”被永久关停 张一鸣发文致歉反思’, People’s Daily, 11-Apr-2018, <https://archive.ph/utuBC>
- 176 ‘致歉和反思’, Zhang Yiming via Toutiao, 11-Apr-2018, <https://archive.ph/wbVSM>
- 177 ‘全国“扫黄打非”办通报: “抖音”平台被行政处罚’, China News, 8-Jan-2021,
<https://web.archive.org/web/20220418033453/https://www.chinanews.com.cn/gn/2021/01-08/9381634.shtml>
- 178 ‘国家市场监督管理总局 行政处罚决定书’, SAMR, 12-Mar-2021, <https://archive.ph/7f0lo>
- 179 ‘市场监管总局、中央网信办、税务总局 联合召开互联网平台企业行政指导会’, SAMR, 13-Apr-2021,
<https://archive.ph/1VTwx>
- 180 ‘市场监管总局、中央网信办、税务总局 联合召开互联网平台企业行政指导会’, SAMR, 13-Apr-2021,
<https://archive.ph/1VTwx>

- '互联网平台企业向社会公开《依法合规经营承诺》（第一批）', SAMR, 14-Apr-2021, https://web.archive.org/web/20220413082741/https://www.samr.gov.cn/xw/zj/202104/t20210413_327811.html
- 'China Warns 34 Tech Firms to Curb Excess in Antitrust Review', Bloomberg, 13-Apr-2021, <https://web.archive.org/web/20220220232838/https://www.bloomberg.com/news/articles/2021-04-13/china-orders-34-tech-firms-to-curb-excesses-in-antitrust-review>
- '金融管理部门联合约谈部分从事金融业务的网络平台企业', State Administration of Foreign Exchange, 29-Apr-2021, <https://web.archive.org/web/20210515205240/https://www.safe.gov.cn/safe/2021/0429/18865.html>
- 'China Reins In Tech Giants' Finance Arms After Hobbling Ant', Bloomberg, 29-Apr-2021, <https://web.archive.org/web/20220407174002/https://www.bloomberg.com/news/articles/2021-04-29/china-orders-tencent-ByteDance-to-rectify-financial-operations>
- 'ByteDance Shelved IPO Intentions After Chinese Regulators Warned About Data Security', WSJ, 12-Jul-2021, <https://web.archive.org/web/20221206013550/https://www.wsj.com/articles/bytedance-shelvedipo-intentions-after-chinese-regulators-warned-about-data-security-11626078000>
- 'A Letter From Yiming', ByteDance, 19-May-2021, <https://web.archive.org/web/20220909193935/https://www.bytedance.com/en/news/60a526af053cc102d640c061>
- '张一鸣宣布卸任字节跳动 CEO，联合创始人梁汝波将接任', The Paper, 20-May-2021, <https://archive.ph/fSp5h>
- '国家互联网信息办公室、公安部加强对语音社交软件和涉深度伪造技术的互联网新技术新应用安全评估', CAC via Xinhua, 18-Mar-2021, <https://archive.ph/C5VRZ>
- 166 United States Court of Appeals for the District of Columbia Circuit, USCA CASE #20-1444 <https://web.archive.org/web/202208131115154/https://www.courthousenews.com/wp-content/uploads/2020/11/tiktok-cadc-petition.pdf>
- Vanessa Pappas, "Senate Hearing on Social Media and National Security", C-SPAN, 14-Sep-2022, <https://web.archive.org/web/20221109011249/https://www.c-span.org/video/?522807-1/senate-hearing-social-media-national-security&playEvent=>
- Parliament of Australia 'Select Committee on Foreign Interference through Social Media – 25/09/2020', Australian Parliament House Hansard, 25-Sep-2020, https://web.archive.org/web/20221125030444/https://www.aph.gov.au/Parliamentary_Business/Hansard/Hansard_Display?bid=committees%2Fcommsen%2F1a5e6393-fec4-4222-945b-859e3f8ebd17%2F&sid=0002
- 167 '迪士尼前高管加入字节跳动，TT 原总裁朱俊向其汇报', Beijing News via Sina, 19-May-2020, https://web.archive.org/web/20221210093341/https://k.sina.com.cn/article_1644114654_61ff32de02000zbnu.html
- 'ByteDance Names Kevin Mayer Chief Operating Officer', TikTok, 19-May-2020, <https://newsroom.tiktok.com/en-us/bytedance-names-kevin-mayer-chief-operating-officer>
- 168 '谁在管理 TikTok: 没有中心的网状组织、字节的全球化构想', LatePost via Laohu8, 7-Apr-2022, <https://archive.ph/yLV9W>
- 'TikTok Names CEO and COO', TikTok, 30-Apr-2021, <https://newsroom.tiktok.com/en-us/tiktok-names-ceo-and-coo>
- 169 'Chinese companies set up in Singapore to hedge against geopolitical risk', Financial Times, 30-Nov-2022, <https://www.ft.com/content/a0c11e3e-ab72-4b4b-a55c-557191e53938>
- 170 'Senate Hearing on Social Media and National Security', C-Span, 14-Sep-2022, <https://web.archive.org/web/20221109011249/https://www.c-span.org/video/?522807-1/senate-hearing-social-media-national-security&playEvent=>
- 171 'Billionaire ByteDance Founder Zhang Yiming Now Living Far From Home', The Information, 29-Sep-2022, <https://www.theinformation.com/articles/billionaire-bytedance-founder-zhang-yiming-now-living-far-from-home?rc=zcbseh>
- '知名律所合伙人高准担任字节跳动 CFO，或将操盘上市重任', Yicai, 25-Apr-2022, <https://archive.ph/PjSoB>
- 172 "'字节跳动"改名"抖音"了? 官方回应来了!', Nanfang Daily via Sohu, 9-May-2022, <https://archive.ph/1VhUy>
- 173 Letter from Shouzi Chew to U.S. Senators, Marsha Blackburn, U.S. Senator for Tennessee, 30-Jun-2022, <https://web.archive.org/web/20220702045206/https://www.blackburn.senate.gov/services/files/A5027CD8-73DE-4571-95B0-AA7064F707C1>
- 174 'TikTok's Owner ByteDance Quietly Changed Its China Unit's Name After U.S. Political Fears', The Information, 10-Aug-2022, <https://www.theinformation.com/articles/tiktoks-owner-bytedance-quietly-changed-its-china-units-name-after-u-s-political-fears?rc=zcbseh>
- 175 'Petition for review 2', Courthouse News Service, 10-Nov-2020, <https://web.archive.org/web/20210928143950/https://www.courthousenews.com/wp-content/uploads/2020/11/tiktok-cadc-petition.pdf>
- 176 'Petition for review 2', Courthouse News Service, 10-Nov-2020, <https://web.archive.org/web/20210928143950/https://www.courthousenews.com/wp-content/uploads/2020/11/tiktok-cadc-petition.pdf>

- 177 'Corporate Structure', ByteDance,
<https://web.archive.org/web/20210501000449/https://www.ByteDance.com/en/>
- 178 Written evidence submitted by TikTok (FL0022), UK House of Commons, Oct-2020,
<https://web.archive.org/web/20221101032109/http://committees.parliament.uk/writtenevidence/13247/pdf/>
'Corporate Structure', ByteDance,
<https://web.archive.org/web/20210501000449/https://www.ByteDance.com/en/>
- '張一鳴退任抖音名義股東', Hong Kong Economic Journal via Yahoo, 25-Jan-2023, <https://archive.ph/RYL0h>
- 179 '字节跳动香港公司更名为抖音集团, 概念股集体沸腾', Yicai, 9-May-2022, <https://archive.ph/NxFmn>
- '張一鳴退任抖音名義股東', Hong Kong Economic Journal via Yahoo, 25-Jan-2023, <https://archive.ph/RYL0h>
- 180 'Petition for review, TikTok Inc. and ByteDance Ltd., Petitioners', The United States Court Of Appeals For The District Of Columbia Circuit, 10-Nov-2020,
<https://web.archive.org/web/20210928143950/https://www.courthousenews.com/wp-content/uploads/2020/11/tiktok-cadc-petition.pdf>
'Corporate Structure', ByteDance,
<https://web.archive.org/web/20210501000449/https://www.ByteDance.com/en/>
Written evidence submitted by TikTok (FL0022), UK House of Commons,
<https://web.archive.org/web/20221101032109/http://committees.parliament.uk/writtenevidence/13247/pdf/>
'Corporate Structure', ByteDance,
<https://web.archive.org/web/20210501000449/https://www.ByteDance.com/en/>
- '張一鳴退任抖音名義股東', Hong Kong Economic Journal via Yahoo, 25-Jan-2023, <https://archive.ph/RYL0h>
- '字节跳动香港公司更名为抖音集团, 概念股集体沸腾', Yicai, 9-May-2022, <https://archive.ph/NxFmn>
- '抖音视界有限公司', Aiqicha Baidu, <https://archive.ph/E8QkD>
- '抖音有限公司', Aiqicha Baidu, <https://archive.ph/3xuZt>
- 181 'Petition for review, TikTok Inc. and ByteDance Ltd., Petitioners' 12, 26, The United States Court Of Appeals For The District Of Columbia Circuit, 10-Nov-2020,
<https://web.archive.org/web/20210928143950/https://www.courthousenews.com/wp-content/uploads/2020/11/tiktok-cadc-petition.pdf>
- 182 Cayman Islands General Registry, retrieved 4-Nov-2022, https://online.ciregistry.gov.ky/cos/faces/home?_adf.new-window-redirect=true
- 183 '字节跳动 CEO 梁汝波发内部信: 头条、西瓜等业务并入抖音', Sina, 2-Nov-2021, <https://archive.ph/AW4Yd>
- 184 '字节跳动 CEO 梁汝波发内部信: 头条、西瓜等业务并入抖音', Sina, 2-Nov-2021, <https://archive.ph/AW4Yd>
- 185 Letter from Shouzi Chew to U.S. Senators, Marsha Blackburn, U.S. Senator for Tennessee, 30-Jun-2022,
<https://web.archive.org/web/20220702045206/https://www.blackburn.senate.gov/services/files/A5027CD8-73DE-4571-95B0-AA7064F707C1>
'字节跳动 CEO 梁汝波发内部信: 头条、西瓜等业务并入抖音', Sina, 2-Nov-2021, <https://archive.ph/AW4Yd>
Cayman Islands General Registry, retrieved 4-Nov-2022, https://online.ciregistry.gov.ky/cos/faces/home?_adf.new-window-redirect=true
- 186 '北京甲艺丙科技有限公司', Aiqicha Baidu, <https://archive.ph/dyzQV>
'或赴港上市? 字节跳动成立抖音集团! 三位董事公布: 梁汝波领衔', NBD, 8-May-2022,
<https://web.archive.org/web/20221129141240/https://www.nbd.com.cn/articles/2022-05-08/2269021.html>
'梁汝波退出多家置业公司法定代表人', jrj.com, 30-Mar-2022, <https://archive.ph/p9sQG>
'北京微播视界科技有限公司', Baidu Aiqicha,
https://web.archive.org/web/20221018151516/https://aiqicha.baidu.com/company_detail_81699330266992
- 187 '梁汝波卸任杭州字节跳动科技公司职务', QCC via OfWeek, 17-Oct-2022, <https://archive.ph/koeAH>
'谁在管理 TikTok: 没有中心的网状组织、字节的全球化构想', LatePost via Laohu8, 7-Apr-2022,
<https://archive.ph/yLV9W>
'TikTok 内幕: 张一鸣的巨浪征途', Jiemian via Sina, 25-Apr-2022, <https://archive.ph/geqqt>
'抖音换帅: 张楠管国内、朱俊管国际, 分头迎战快手与 Facebook', LatePost via Tencent, 31-Oct-2019,
<http://web.archive.org/web/20221210092254/https://new.qq.com/omn/20191031/20191031A0KPLQ00.html>
- 188 '抖音有限公司', Tianyancha, <https://archive.ph/egkYD>
'抖音有限公司', Aiqicha Baidu, <https://archive.ph/3xuZt>
'厦门星辰启点科技有限公司', Baidu Aiqicha, <https://archive.ph/L2WJl>
'上海字跳网络技术有限公司', Tianyancha, <https://archive.ph/HMjBw>
'字节跳动组织调整: 集团 CFO、TikTok CEO 周受资将管理更多团队', LatePost via Laohu, 16-Jun-2021,
<https://archive.ph/5JKYN>
'字节跳动入股教育硬件品牌北京孔明科技', Huanqiu via Sohu, 27-Oct-2020, <https://archive.ph/uLDfr>
- 189 '抖音视界有限公司', Tianyancha, <https://archive.md/iQjpl>
'抖音视界有限公司', Aiqicha Baidu, <https://archive.ph/E8QkD>

- 190 張一鳴退任抖音名義股東', Hong Kong Economic Journal via Yahoo, 25-Jan-2023, <https://archive.ph/RYL0h>
- 191 '如何看待张一鸣退出抖音有限公司股东?', Zhihu, 22-Jan-2023, <https://archive.ph/B9dbJ>
- 192 TikTok 内幕: 张一鸣的巨浪征途', Jiemiao via Sina, 25-Apr-2022, <https://archive.ph/geqqt>
- '抖音视界有限公司', Tianyancha, <https://archive.md/iOjpl>
- '抖音视界有限公司', Aiqicha Baidu, <https://archive.ph/E8QkD>
- 張一鳴退任抖音名義股東', Hong Kong Economic Journal via Yahoo, 25-Jan-2023, <https://archive.ph/RYL0h>
- 193 '如何看待张一鸣退出抖音有限公司股东?', Zhihu, 22-Jan-2023, <https://archive.ph/B9dbJ>
- '谁在管理 TikTok: 没有中心的网状组织、字节的全球化构想', LatePost via Laohu8, 7-Apr-2022, <https://archive.ph/yLV9W>
- 194 Sam Biddle, Paulo Victor Ribeiro, Tatiana Dias, 'INVISIBLE CENSORSHIP: TikTok Told Moderators to Suppress Posts by "Ugly" People and the Poor to Attract New Users', The Intercept, 16-Mar-2020, <https://archive.ph/1n45R>
- Salvador Rodriguez, 'TikTok insiders say social media company is tightly controlled by Chinese parent ByteDance', CNBC, 25-Jun-2021, <https://web.archive.org/web/20221104203859/https://www.cnbc.com/2021/06/25/tiktok-insiders-say-chinese-parent-bytedance-in-control.html>
- Sylvia Varnham O'Regan, 'TikTok's \$4 Billion Advertising Machine Is Messy Behind the Scenes', The Information, 11-Aug-2022, <https://web.archive.org/web/20221114090438/https://www.theinformation.com/articles/tiktoks-4-billion-advertising-machine-is-messy-behind-the-scenes?rc=zcbseh>
- Emily Baker-White, 'TikTok Is Bleeding U.S. Execs Because China Is Still Calling The Shots, Ex-Employees Say', Forbes, 21-Sep-2022, <https://archive.ph/YQVm7>
- Emily Baker-White, 'TikTok Parent ByteDance Planned To Use TikTok To Monitor The Physical Location Of Specific American Citizens,' Forbes, 20-Oct-2022, <https://web.archive.org/web/https://www.forbes.com/sites/emilybaker-white/2022/10/20/tiktok-bytedance-surveillance-american-user-data/>
- Drew Harwell and Elizabeth Dwoskin, 'As Washington wavers on TikTok, Beijing exerts control', The Washington Post, 28-Oct-2022, <https://web.archive.org/web/20221101005158/https://www.washingtonpost.com/technology/interactive/2022/bytedance-tiktok-privacy-china/>
- Ryan Mac and Chang Che, 'TikTok's C.E.O. Navigates the Limits of His Power', New York Times, 16-Sep-2022, <https://web.archive.org/web/20221102210817/https://www.nytimes.com/2022/09/16/technology/tiktok-ceo-shou-zi-chew.html>
- 195 'TikTok Is Bleeding U.S. Execs Because China Is Still Calling The Shots, Ex-Employees Say', Forbes, 21-Sep-2022, <https://archive.ph/YQVm7>
- 196 '中华人民共和国国家安全法', gov.cn, 1-Jul-2015, https://web.archive.org/web/20221216184050/http://www.gov.cn/zhengce/2015-07/01/content_2893902.htm
- 197 '中华人民共和国国家情报法', National People's Congress of the PRC, 12-Jun-2018, <https://archive.ph/EvpjJ>
- 198 Raffaele Huang, 'TikTok's Efforts to Distance Itself From Chinese Parent Stumble Over Talent', WSJ, 16-Dec-2022, <https://archive.ph/RVsCa>
- Juro Osawa, Amir Efrati and Shai Oster, 'TikTok Still Has Key Software Developers in China Despite Effort to Move Offshore', The Information, 26-Aug-2021, <https://www.theinformation.com/articles/tiktok-still-has-key-software-developers-in-china-despite-effort-to-move-offshore?rc=zcbseh>
- Juro Osawa, Yunan Zhang and Amir Efrati, 'Breaking Off TikTok Will Be Hard to Do', The Information, 29-Jul-2020, <https://www.theinformation.com/articles/breaking-off-tiktok-will-be-hard-to-do?rc=zcbseh>
- Yingzhi Yang, Echo Wang and Alexandra Alper, 'Exclusive: TikTok owner ByteDance moves to shift power out of China – sources', Reuters, 28-May-2020, <https://web.archive.org/web/20221201022956/https://www.reuters.com/article/us-bytedance-tiktok-exclusive/exclusive-tiktok-owner-bytedance-moves-to-shift-power-out-of-china-sources-idUSKBN2341VJ>
- 199 '数据科学家-国际短视频-上海', ByteDance via LinkedIn, <https://web.archive.org/web/20230227050201/https://cn.linkedin.com/jobs/view/%E6%95%B0%E6%8D%AE%E7%A7%91%E5%AD%A6%E5%AE%B6-%E5%9B%BD%E9%99%85%E7%9F%AD%E8%A7%86%E9%A2%91-%E4%B8%8A%E6%B5%B7-at-%E5%AD%97%E8%8A%82%E8%B7%B3%E5%8A%A8-3362902087>
- 'Data Scientist/数据科学家', TikTok via LinkedIn, <https://web.archive.org/web/20230227050531/https://cn.linkedin.com/jobs/view/data-scientist-%E6%95%B0%E6%8D%AE%E7%A7%91%E5%AD%A6%E5%AE%B6-at-tiktok-3345866583>
- 200 '数据分析师-国际化短视频 (用户体验方向)', ByteDance, <https://archive.ph/njPBh>
- '出海大客户总监--北上广', ByteDance, <https://web.archive.org/web/20221031203410/https://jobs.bytedance.com/experienced/position/7020292300300863757/detail?recomId=0550f0ef-0f81-11ed-83ce-6c92bfa0d82e&sourceJobId=6777279603208620301>
- '服务端核心研发工程师-抖音服务架构-基础工程方向', ByteDance, <https://archive.ph/OUicS>

- 201 '推荐算法高级工程师 - 电商', ByteDance, <https://archive.ph/oXTbj>
'Tech Lead (Streaming Computing), Cloud Infrastructure', ByteDance, https://web.archive.org/web/20221114085637/https://jobs.bytedance.com/experienced/position/7035825062201100581/detail?use_ssr=1
'Tech Lead(Streaming Computing), Cloud Infrastructure', TikTok, <https://perma.cc/9NTN-53ED>
'Backend Software Engineer - TikTok (Livestreaming) – Singapore', ByteDance, <https://archive.ph/oHFHK>
'Backend Software Engineer - TikTok (Livestreaming) – Singapore', TikTok, <https://careers.tiktok.com/position/7094943341029280031/detail>
'Site Reliability Engineer, Recommendation Architecture', ByteDance, <https://archive.ph/Zvyan>
'Site Reliability Engineer, Recommendation Architecture', TikTok, <https://careers.tiktok.com/position/7057825736279623950/detail>
'Software Engineer - Recommendation Architecture', ByteDance, <https://archive.ph/L5qOZ>
- 202 We input "ByteDance" "TikTok" into the search field on LinkedIn, then selected *Filter by People*. The results included former employees of ByteDance or TikTok.
- 203 'Blake Chandlee', LinkedIn, <https://www.linkedin.com/in/blakechandlee/>
"ByteDance" "TikTok", LinkedIn, https://www.linkedin.com/search/results/people/?keywords=%22ByteDance%22%20%22TikTok%22&origin=GLOBAL_SEARCH_HEADER&sid=XJ~
- 204 Emily Baker-White, 'TikTok Is Bleeding U.S. Execs Because China Is Still Calling The Shots, Ex-Employees Say', Forbes, 21-Sep-2022, <https://web.archive.org/web/20221114090501/https://www.forbes.com/sites/emilybaker-white/2022/09/21/tiktok-bleeding-us-execs-china-control-bytedance/?sh=7332d8d89707>
'TikTok insiders say social media company is tightly controlled by Chinese parent ByteDance', CNBC, 25-Jun-2021, <https://web.archive.org/web/20230210063010/https://www.cnbc.com/2021/06/25/tiktok-insiders-say-chinese-parent-bytedance-in-control.html>
'TikTok's Spying Scandal and ChatGPT's Challenge to Google', New York Times, 6-Jan-2023, <https://archive.ph/1T57f>
- 205 'Tech Lead (DBA) , Cloud Infrastructure', ByteDance, <https://perma.cc/7W5G-VSVC>
- 206 'Tech Lead(DBA), Cloud Infrastructure', TikTok, <https://perma.cc/NNX8-YGLH>
Emily Baker-White, 'Leaked Audio From 80 Internal TikTok Meetings Shows That US User Data Has Been Repeatedly Accessed From China', BuzzFeed, 17-Jun-2022, <https://web.archive.org/web/20221113152059/https://www.buzzfeednews.com/article/emilybakerwhite/tiktok-tapes-us-user-data-china-bytedance-access>
- 207 '北京抖音信息服务有限公司', Baidu Aiqicha, <https://archive.ph/EXVxv>
- 208 '北京抖音信息服务有限公司', Baidu Aiqicha, <https://archive.ph/EXVxv>
- 209 '北京抖音信息服务有限公司', Baidu Aiqicha, <https://archive.ph/EXVxv>
'网投中文(北京)科技有限公司', Baidu Aiqicha, <https://archive.ph/q6Bj8>
'中网投(北京)科技有限公司', Baidu Aiqicha, <https://archive.ph/H5UzA>
'中国互联网投资基金管理有限公司', Baidu Aiqicha, <https://archive.ph/EFcs9>
'北京市文化投资发展集团资产管理有限公司', Baidu Aiqicha, <https://archive.ph/l8zAh>
'央视视频融媒体发展有限公司', Baidu Aiqicha, <https://archive.ph/KbeAY>
'公司简介', China Internet Investment Fund, <https://archive.ph/UxtPm>
- 210 Shou Zi Chew, Letter from TikTok CEO to US Senators, United States Senate, 30-Jun-2022, <https://web.archive.org/web/20220702045206/https://www.blackburn.senate.gov/services/files/A5027CD8-73DE-4571-95B0-AA7064F707C1>
- 211 '北京抖音信息服务有限公司', Baidu Aiqicha, <https://archive.ph/EXVxv>
'北京抖音信息服务有限公司', Baidu Aiqicha, <https://archive.ph/EXVxv>
'网投中文(北京)科技有限公司', Baidu Aiqicha, <https://archive.ph/q6Bj8>
'中网投(北京)科技有限公司', Baidu Aiqicha, <https://archive.ph/H5UzA>
'中国互联网投资基金管理有限公司', Baidu Aiqicha, <https://archive.ph/EFcs9>
'北京市文化投资发展集团资产管理有限公司', Baidu Aiqicha, <https://archive.ph/l8zAh>
'央视视频融媒体发展有限公司', Baidu Aiqicha, <https://archive.ph/KbeAY>
'公司简介', China Internet Investment Fund, <https://archive.ph/UxtPm>
- 212 Ryan McMorro, Qianer Liu and Cheng Leng, 'China moves to take 'golden shares' in Alibaba and Tencent units', Financial Times, 12-Jan-2023, <https://archive.md/PmxYE>
- 213 Ryan McMorro, Qianer Liu and Cheng Leng, 'China moves to take 'golden shares' in Alibaba and Tencent units', Financial Times, 12-Jan-2023, <https://archive.md/PmxYE>
- 214 Ryan McMorro, Qianer Liu and Cheng Leng, 'China moves to take 'golden shares' in Alibaba and Tencent units', Financial Times, 12-Jan-2023, <https://archive.md/PmxYE>

- 215 '爱党书记狂言砍网友的头 一张办公照把他出卖了', Aboluowang, 17-Jul-2012, <https://archive.md/yGthO>
- 216 "某官员 @爱我中华_情满神州 实名认证信息为...", @zuola via Twitter, 29-Jun-2012, <https://archive.md/zl8iv>
- 217 '人教社向河北省平山县小学生捐赠 2000 套《新编小学生字典》和 1000 套《中华传统美德格言》', Chinese Education Publishing & Media Group Ltd, 6-Jun-2012, <https://archive.md/1zi0F>
- 218 "某官员 @爱我中华_情满神州 实名认证信息为...", @zuola via Twitter, 29-Jun-2012, <https://archive.md/zl8iv>
- 218 '守好网络舆论阵地 助力美好淮南发展', Huainan Vanguard Network, 24-May-2019, <https://archive.ph/Lq0ja>
- '全国网信系统十九大精神宣讲团吉林省报告会综述', China Jilin via CAC, 20-Nov-2017, <https://archive.md/KS8Pz>
- '中央网信办党的十九大精神宣讲团走进中原网和郑州网信企业', Zhengzhou Evening News via Toutiao, 8-Nov-2017, <https://archive.md/uMfj5>
- '全国网信系统在豫首场宣讲报告会走进河南日报报业集团', Henan Mobile News, 9-Nov-2017, <https://archive.md/SCYmp>
- 219 "Are There TikTok Employees... Who Are Members Of The Chinese Communist Party?" Hawley Grills Exec', Forbes Breaking News via YouTube, 15-Sep-2022, <https://www.youtube.com/watch?v=meWM8d4Uz7Q>
- 220 '不忘初心 重温入党誓词', Study Times via People's Daily, <https://archive.ph/4AjRJ>
- 221 '【独家】党支部名单曝光 抖音何去何从', Epoch Times, 5-Aug-2020, <https://archive.ph/RVz3Z>
- 222 '【独家】党支部名单曝光 抖音何去何从', Epoch Times, 5-Aug-2020, <https://archive.ph/RVz3Z>
- 223 'New DOJ Filing: TikTok's Owner Is 'A Mouthpiece' Of Chinese Communist Party', NPR, 26-Sep-2020, <https://web.archive.org/web/20230114040919/https://www.npr.org/2020/09/26/917134452/new-doj-filing-tiktoks-owner-is-a-mouthpiece-of-chinese-communist-party>
- 'TikTok Downplays Chinese Communist Party Links in Australia Hearing', Bloomberg, 25-Sep-2020, <https://archive.ph/tVKA0>
- 224 '以党建为统领推动网络空间清朗', CAC, 16-Apr-2020, <https://archive.ph/S1SLL>
- 225 '以党建为统领推动网络空间清朗', CAC, 16-Apr-2020, <https://archive.ph/S1SLL>
- 226 'Constitution of the Communist Party of China', Xinhua, 24-Oct-2017, http://www.xinhuanet.com/english/download/Constitution_of_the_Communist_Party_of_China.pdf
- 227 'Constitution of the Communist Party of China', Xinhua, 24-Oct-2017, http://www.xinhuanet.com/english/download/Constitution_of_the_Communist_Party_of_China.pdf
- 228 '你是优秀健康记者吗？看看你是否符合这四个条件', Health Times, 29-Dec-2015, <https://web.archive.org/web/20221105041818/http://www.jksb.com.cn/index.php?m=special&c=index&a=show&d=388>
- '京华时报副总编辑张辅评：将群众路线进行到底', People's Daily via CCTV, 05-Sep-2011, <https://archive.ph/NA3Xo>
- '重磅 | 中国书协 第八届理事会 主席团名单', China Calligraphers Association, 4-Feb-2021, <https://archive.ph/vH6eq>
- '表彰 | 2022 年元旦春节两节期间“送万福进万家下基层公益活动”先进单位及个人', China Calligraphers Association via WeChat, 8-Apr-2022, <https://archive.ph/yWNA2>
- '（全国）教育书画协会少年分会第二次全国会员代表大会在京召开', CCTV via WeChat, 3-Jun-2021, <https://archive.ph/SQFdv>
- '送温暖发布会', All-China Federation of Trade Unions, 27-Dec-2018, <https://archive.ph/kyEMT>
- '送万福、进万家书法公益活动走进首都消防部队', NetEase, 2-Feb-2018, <https://archive.ph/Z0Ouj>
- '预祝上洋陈氏大宗祠 2 月 1 日庆典活动圆满举办', Hakka Anecdotes via WeChat, 31-Jan-2018, <https://archive.ph/197RJ>
- '市领导邓菊芳会见北京字节跳动科技有限公司副总裁陈志锋一行', Longyan UFWD via WeChat, 9-Oct-2019, <https://archive.ph/hvjXM>
- '集团领导到北京字节跳动科技有限公司洽谈合作', Fujian Media Group, 16-Mar-2019, <https://web.archive.org/web/20221116024217/http://www.fjrtv.net/folder2841/ly/report/2019-03-16/1879371.html>
- '中央统战部首度轮训新媒体从业人员，陈彤张一鸣邓飞等在列', The Paper, 19-May-2015, <https://archive.ph/3csmt>
- '政协第十一届福建省委员会增补委员名单', Fujian Daily via Southeastern Network, 16-Jan-2017, <https://archive.ph/p17S9>
- '政协第十二届福建省委员会委员名单', Southeastern Network, 21-Jan-2018, <https://archive.ph/xhd10>
- '今日头条将在福建龙岩建分公司？张一鸣说要支持家乡发展', Global Times, 19-Dec-2017, <https://archive.ph/F1BYo>
- '福建省海外联谊会第五届理事大会', Sina Fujian, <https://archive.ph/kZ8tN>
- '福建省新的社会阶层人士联谊会福州召开', Central United Front Work Department via Unity Network, 11-Oct-2017, <https://archive.ph/ZOplt>

- 229 Michael Schuman, 'Why America Is Afraid Of TikTok', The Atlantic, 31-Jul-2020, <https://web.archive.org/web/20221102130912/https://www.theatlantic.com/international/archive/2020/07/tiktok-ban-china-america/614725/>
- 230 '政协第十一届福建省委员会增补委员名单', Fujian Daily via Southeastern Network, 16-Jan-2017, <https://archive.ph/p17S9>
'政协第十二届福建省委员会委员名单', Southeastern Network, 21-Jan-2018, <https://archive.ph/xhd1O>
'今日头条将在福建龙岩建分公司? 张一鸣说要支持家乡发展', Global Times, 19-Dec-2017, <https://archive.ph/F1BYo>
'福建省海外联谊会第五届理事大会', Sina Fujian, <https://archive.ph/kZ8tN>
'福建省新的社会阶层人士联谊会会在福州召开', Central United Front Work Department via Unity Network, 11-Oct-2017, <https://archive.ph/ZOplt>
'新闻聚焦 | 龙岩市首届文化旅游产业发展大会新闻发布会召开, 龙岩长汀向世界发出邀请, 欢迎您来做客……', Minxi Daily and Changting County Radio and Television Station via WeChat, 2-Apr-2019, <https://archive.md/gvQZv>
'新加坡华源会代表受邀出席第五届世界闽商大会', Hua Yuan Association via WeChat, 20-Jun-2016, <https://archive.md/42zRS>
- 231 '中央统战部首度轮训新媒体从业人员, 陈彤张一鸣邓飞等在列', The Paper, 19-May-2015, <https://archive.ph/3csmt>
- 232 '中央统战部首度轮训新媒体从业人员, 陈彤张一鸣邓飞等在列', The Paper, 19-May-2015, <https://archive.ph/3csmt>
- 233 '张辅评升任今日头条总编辑, 夏勇去职', Media Observer via Read01, 20-Feb-2017, <https://archive.ph/P6JTq>
'《红色气质》: 时长虽短“气质”不减', China Press and Publishing via Xinhua, 14-Jul-2016, <https://archive.ph/zX4UQ>
- 234 '字节跳动党委: 要把讲导向守责任放首位', The Paper via Sina, 29-Apr-2018, <https://archive.ph/EJNyo>
- 235 '北京抖音信息服务有限公司', Baidu Aiqicha, <https://archive.ph/EXVxv>
- 236 'The next chapter in our leadership', Sequoia Capital via Twitter, 5-Apr-2022, <https://archive.md/PVXV1>
- 237 '沈南鹏委员: 协同推进减碳和东西部协调发展', CPPCC, 8-Mar-2022, <https://web.archive.org/web/20221125161521/http://www.cppcc.gov.cn/zxww/2022/03/08/ART11646670339234351.shtml>
'Neil Shen', Center for China & Globalization, <https://archive.ph/394I5>
Alex Joske, 'The party speaks for you', Australian Strategic Policy Institute, 09-Jun-2020, <https://www.aspi.org.au/report/party-speaks-you>
- 238 '沈南鹏委员: 协同推进减碳和东西部协调发展', CPPCC, 8-Mar-2022, <https://web.archive.org/web/20221125161521/http://www.cppcc.gov.cn/zxww/2022/03/08/ART11646670339234351.shtml>
'Neil Shen', Center for China & Globalization, <https://archive.ph/394I5>
- 239 '创业投资基金专业委员会', AMAC, <https://archive.ph/wYufz>
'Forum Introduction', China Entrepreneurs Forum, <https://archive.ph/laNLW>
- 240 '中国人民政治协商会议第十四届全国委员会委员名单', CPPCC, 18-Jan-2023, <https://archive.md/RTB56>
Shai Oster and Juro Osawa, 'Sequoia Capital China Chief Leaves Beijing's Top Political Advisory Body', The Information, 20-Jan-2023, <https://www.theinformation.com/articles/sequoia-china-chief-leaves-beijings-top-political-advisory-body?rc=zcbseh>
'Form 6-K Report of Foreign Private Issuer Pursuant to Rule 13-a-16 or 15d-16 Under the Securities Exchange Act of 1934', Pinduoduo Inc. via US SEC, 29-Nov-2022, <https://archive.ph/vq6zj>
- 241 Juro Osawa and Shai Oster, 'Sequoia Capital's China Arm Employed Daughter of Politburo Member', The Information, 9-Sep-2022, <https://www.theinformation.com/articles/sequoia-capitals-china-arm-employed-daughter-of-politburo-member?rc=zcbseh>
- 242 'Report claims TikTok parent company ByteDance is working with China's Communist Party to spread propaganda on Xinjiang', Business Insider, Nov-2019, <https://web.archive.org/web/20191129091747/https://www.businessinsider.com/tiktok-parent-company-ByteDance-spreads-chinese-propaganda-report-2019-11>
- 243 '武警部队携手今日头条, 强强联合打造政务新媒体', Geek Park, 1-Dec-2017, <https://archive.ph/FfQt6>
'中华人民共和国人民武装警察法', Ministry of National Defence, 20-June-2020, https://web.archive.org/web/20220723031732/http://www.mod.gov.cn/regulatory/2020-06/20/content_4867004.htm
- 244 '武警部队携手今日头条, 强强联合打造政务新媒体', Geek Park, 1-Dec-2017, <https://archive.ph/FfQt6>
'中华人民共和国人民武装警察法', Ministry of National Defence, 20-June-2020, https://web.archive.org/web/20220723031732/http://www.mod.gov.cn/regulatory/2020-06/20/content_4867004.htm

- 245 '武警部队新媒体账号，集体入驻抖音啦！'，Affiliated Hospital of Logistics University of People's Armed Police Force via Sohu, 11-Apr-2019, <https://archive.ph/9Mulh>
- 246 Jichang Lulu and Filip Jirouš, 'Back to the Cheka: The Ministry of Public Security's political protection work', Sinopsis, 21-Feb-2022, <https://sinopsis.cz/wp-content/uploads/2022/02/mps1.pdf>
- 247 '武警部队携手今日头条，强强联合打造政务新媒体'，Geek Park, 1-Dec-2017, <https://archive.ph/FfQt6>
- 248 'Mapping more of China's tech giants: AI and surveillance', ASPI, Nov-2019, <https://www.aspi.org.au/report/mapping-more-chinas-tech-giants>
- 249 '重磅！公安部与抖音正式合作'，Southern Network, 26-Apr-2019, <https://archive.ph/TM7E5>
- 250 Mapping more of China's tech giants: AI and surveillance 18-20, ASPI, Nov-2019, <https://www.aspi.org.au/report/mapping-more-chinas-tech-giants>
- 251 '北京局开展广播电视和网络视听对口援疆工作'，National Radio and Television Administration, 4-Nov-2019, https://web.archive.org/web/20191126030214/http://www.nrta.gov.cn/art/2019/11/4/art_114_48597.html
- 'OHCHR Assessment of human rights concerns in the Xinjiang Uyghur Autonomous Region, People's Republic of China,' United Nations Office of the High Commission for Human Rights, 31-Aug-2022, <https://www.ohchr.org/sites/default/files/documents/countries/2022-08-31/22-08-31-final-assesment.pdf>
- Vicky Xiuzhong Xu, Daria Impiombato and Nathan Ruser, 'UN Uyghur report leaves no room for denial and no excuse for inaction,' The Strategist, 3-Sep-2022, https://www.aspistrategist.org.au/un-uyghur-report-leaves-no-room-for-denial-and-no-excuse-for-inaction/?utm_medium=email&utm_campaign=Daily%20The%20Strategist&utm_content=Daily%20The%20Strategist+CID_863221cf1139c8446269d7362ce45936&utm_source=CampaignMonitor&utm_term=UN%20Uyghur%20report%20leaves%20no%20room%20for%20denial%20and%20no%20excuse%20for%20inaction
- 252 '协会领导'，China Netcasting Services Association, <https://archive.ph/JWnJK>
- '中国网络视听节目服务协会第二届理事会常务理事名单'，China Netcasting Services Association, 17-Nov-2020, <https://archive.ph/RtNmF>
- '副会长单位'，China Netcasting Services Association, 1-Dec-2021, <https://archive.md/tHP6x>
- 253 '聂辰席'，China Netcasting Services Association, 27-Jun-2022, <https://archive.ph/42ovG>
- 254 '协会章程'，China Netcasting Services Association, <http://archive.today/bBS6W>
- '总局领导'，NRTA, <http://archive.today/Bbk2f>
- '协会简介'，China Netcasting Services Association, <https://archive.ph/tpDfh>
- '中宣部接管新闻出版电影 三大台合并'，Caixin, 21-Mar-2018, <https://archive.ph/enCea>
- 255 '《网络短视频平台管理规范》《网络短视频内容审核标准细则》发布'，People's Network, 10-Jan-2019, <https://archive.ph/UWgWc>
- '网络短视频内容审核标准细则（2021）'，China Netcasting Services Association, 16-Dec-2021, <https://archive.ph/C6jpS>
- 256 '领导成员'，Beijing Communication Industry Association, <https://archive.ph/vkXWt>
- 257 '协会章程'，Beijing Communication Industry Association, <https://archive.md/zD5MS>
- 258 '今天，人民日报成立的这个研究院不一般！'，People's Daily via WeChat, 19-Sep-2019, <https://archive.ph/nXtBv>
- 259 '今天，人民日报成立的这个研究院不一般！'，People's Daily via WeChat, 19-Sep-2019, <https://archive.ph/nXtBv>
- 260 '会员单位'，Internet Society of China, <https://web.archive.org/web/20230309001535/https://home.isc.org.cn/member-unit/index?kw=&level=3&p=4>
- 261 '中国互联网协会章程'，ISC, 25-Apr-2022, <https://perma.cc/U4E5-NWWH>
- 262 Emily Baker-White, 'LinkedIn Profiles Indicate 300 Current TikTok and ByteDance Employees Used To Work For Chinese State Media', Forbes, 11-Aug-2022, <https://www.forbes.com/sites/emilybaker-white/2022/08/10/bytedance-tiktok-china-state-media-propaganda/?sh=425dc8f4322f>
- 263 '国家网信办指导有关地方网信办依法查处违法违规网站平台及账号'，Xinhua, 5-Feb-2020, https://web.archive.org/web/20200806014435/http://www.xinhuanet.com/politics/2020-02/05/c_1125536088.htm
- 264 '字节跳动公司打造武汉疫情防控网络传播服务矩阵'，Wuhan CAC via WeChat, 24-Feb-2020, <https://web.archive.org/web/20221208164239/https://mp.weixin.qq.com/s?src=11×tamp=1670517314&ver=4214&signature=5ircLSQ5LGxcsX05pEvOJfgWiSVnzPKpsi7D8KGbteZluPEwxs%2ASQvWimYS1bTSDAmQ1ZA S%2AyHAVAm5vz8-aolt6FOGsnTS3PVvHIC1H0-M2NyyuTZdXJZvml2J3B03t&new=1>
- 265 '字节跳动公司打造武汉疫情防控网络传播服务矩阵'，Wuhan CAC via WeChat, 24-Feb-2020, <https://web.archive.org/web/20221208164239/https://mp.weixin.qq.com/s?src=11×tamp=1670517314&ver=4214&signature=5ircLSQ5LGxcsX05pEvOJfgWiSVnzPKpsi7D8KGbteZluPEwxs%2ASQvWimYS1bTSDAmQ1ZA S%2AyHAVAm5vz8-aolt6FOGsnTS3PVvHIC1H0-M2NyyuTZdXJZvml2J3B03t&new=1>
- 266 Liza Lin, 'China Clamps Down on Internet as It Seeks to Stamp Out Covid Protests', The Wall Street Journal, 1-Dec-2022, <https://web.archive.org/web/20221201143725/https://www.wsj.com/articles/china-clamps-down-on-internet-as-it-seeks-to-stamp-out-covid-protests-11669905228>

- 267 Liza Lin, 'China Clamps Down on Internet as It Seeks to Stamp Out Covid Protests', The Wall Street Journal, 1-Dec-2022, <https://web.archive.org/web/20221201143725/https://www.wsj.com/articles/china-clamps-down-on-internet-as-it-seeks-to-stamp-out-covid-protests-11669905228>
- 268 '习近平谈媒体融合发展金句：用主流价值导向驾驭“算法”', Qiushi, 16-Mar-2019, https://web.archive.org/web/20190323110922/http://www.qstheory.cn/2019-03/16/c_1124242581.htm
'加快推动媒体融合发展 构建全媒体传播格局', Qiushi, 15-Mar-2019, https://web.archive.org/web/20230309005056/http://www.qstheory.cn/dukan/qs/2019-03/15/c_1124239254.htm
- 269 '网络信息内容生态治理规定', CAC, 20-Dec-2019, https://web.archive.org/web/20221115143323/http://www.cac.gov.cn/2019-12/20/c_1578375159509309.htm
- 270 '互联网信息服务算法推荐管理规定', CAC, 4-Jan-2022, https://web.archive.org/web/20221118224204/http://www.cac.gov.cn/2022-01/04/c_1642894606364259.htm
- 271 Zhou Xin and Tracy Qu, 'TikTok's algorithm not for sale, ByteDance tells US: source', South China Morning Post, 13-Sep-2020, <https://web.archive.org/web/20200913160256/https://www.scmp.com/economy/china-economy/article/3101362/tiktoks-algorithm-not-sale-bytedance-tells-us-source>
'商务部 科技部公告 2020 年第 38 号 关于调整发布《中国禁止出口限制出口技术目录》的公告', Ministry of Commerce, 28-Aug-2020, <https://web.archive.org/web/20221031213250/http://www.mofcom.gov.cn/article/b/xxfb/202008/20200802996641.shtml>
'《中国禁止出口限制出口技术目录》调整内容', Ministry of Commerce, <https://web.archive.org/web/20220709223655/http://images.mofcom.gov.cn/fms/202008/20200828200911003.pdf>
- 272 '商务部 科技部公告 2020 年第 38 号 关于调整发布《中国禁止出口限制出口技术目录》的公告', Ministry of Commerce, 28-Aug-2020, <https://web.archive.org/web/20221031213250/http://www.mofcom.gov.cn/article/b/xxfb/202008/20200802996641.shtml>
'《中国禁止出口限制出口技术目录》调整内容', Ministry of Commerce, <https://web.archive.org/web/20220709223655/http://images.mofcom.gov.cn/fms/202008/20200828200911003.pdf>
- 273 'Planned TikTok deal entails China's approval under revised catalogue: expert', Xinhua, 30-Aug-2020, https://web.archive.org/web/20221030175546/http://www.xinhuanet.com/english/2020-08/30/c_139329598.htm
- 274 'Planned TikTok deal entails China's approval under revised catalogue: expert', Xinhua, 30-Aug-2020, https://web.archive.org/web/20221030175546/http://www.xinhuanet.com/english/2020-08/30/c_139329598.htm
- 275 字节跳动 via Today's Headlines, 30-Aug-2020, <https://archive.ph/XLz4u>
- 276 Zhou Xin and Tracy Qu, 'TikTok's algorithm not for sale, ByteDance tells US: source', South China Morning Post, 13-Sep-2020, <https://web.archive.org/web/20200913160256/https://www.scmp.com/economy/china-economy/article/3101362/tiktoks-algorithm-not-sale-bytedance-tells-us-source>
- 277 '国家互联网信息办公室、中华人民共和国工业和信息化部、中华人民共和国公安部、国家市场监督管理总局令 第 9 号:互联网信息服务算法推荐管理规定', Cyberspace Administration of China via Central People's Government of the People's Republic of China, 31-Dec-2021, <https://archive.ph/lAw2J>
- 278 '国家互联网信息办公室关于发布互联网信息服务算法备案信息的公告', Cyberspace Administration of China, 12-Aug-2022, <https://archive.ph/G8Xlx>
- 279 '抖音个性化推荐算法', CAC, https://web.archive.org/web/20221018203822/https://beian.cac.gov.cn/api/static/fileUpload/principalOrithm/additional/user_9b84b02a-0c7f-4bd4-81f2-5cad879ad4ab_96ed08c8-0ed8-4ab5-b04d-46cccf4c00ab.pdf
- 280 Will Knight, 'The Insanely Popular Chinese News App That You've Never Heard Of,' MIT Technology Review, 26-Jan-2017, <https://web.archive.org/web/20221122162904/https://www.technologyreview.com/2017/01/26/154363/the-insanely-popular-chinese-news-app-that-youve-never-heard-of/>
- 281 Alex Hern, 'Revealed: How TikTok censors videos that do not please Beijing,' The Guardian, 25-Sept-2019, <https://www.theguardian.com/technology/2019/sep/25/revealed-how-tiktok-censors-videos-that-do-not-please-beijing>
- Sam Biddle, Paulo Victor Ribeiro, Tatiana Dias, 'Invisible censorship: TikTok told moderators to suppress posts by “ugly” people and the poor to attract new users,' The Intercept, 16-Mar-2020, <https://theintercept.com/2020/03/16/tiktok-app-moderators-users-discrimination/>
- Markus Reuter and Chris Kover, 'Cheerfulness and censorship', netzpolitik.org, 23-Nov-2019, <https://web.archive.org/web/20230105104124/https://netzpolitik.org/2019/cheerfulness-and-censorship/>
- 282 '独家| 内部员工揭秘: TikTok 竟然这么审核内容', Pingwest, 14-Jun-2020, <https://archive.ph/RsUQX>
'The censor cannot hold: the pressure of controlling China's internet', France24, 6-Oct-2022, <http://web.archive.org/web/20221108193721/https://www.france24.com/en/live-news/20221006-the-censor-cannot-hold-the-pressure-of-controlling-china-s-internet>

- Markus Reuter and Chris Kover, 'Cheerfulness and censorship', netzpolitik.org, 23-Nov-2019, <https://web.archive.org/web/20220924071902/https://netzpolitik.org/2019/cheerfulness-and-censorship/>
- Shen Lu, 'I helped build ByteDance's vast censorship machine', Protocol, 18-Feb-2021, <https://web.archive.org/web/20221216031945/https://www.protocol.com/china/i-built-bytedance-censorship-machine>
- '前新浪微博内容审核员专访：中共如何打造网络“真理部”', VOA, 12-Aug-2020, <https://web.archive.org/web/20221209214136/https://www.voachinese.com/a/internet-censorship-20200812/5540475.html>
- 283 Alex Hern, 'Revealed: How TikTok censors videos that do not please Beijing,' The Guardian, 25-Sept-2019, <https://www.theguardian.com/technology/2019/sep/25/revealed-how-tiktok-censors-videos-that-do-not-please-beijing>
- 'Oral evidence: Forced labour in UK value chains, HC 810', Business, Energy and Industrial Strategy Committee, UK House of Commons, 5-Nov-2020, <https://archive.ph/i6vzE>
- Markus Reuter and Chris Kover, 'Cheerfulness and censorship', netzpolitik.org, 23-Nov-2019, <https://web.archive.org/web/20220924071902/https://netzpolitik.org/2019/cheerfulness-and-censorship/>
- 284 Sam Biddle, Paulo Victor Ribeiro, Tatiana Dias, 'INVISIBLE CENSORSHIP: TikTok Told Moderators to Suppress Posts by "Ugly" People and the Poor to Attract New Users', The Intercept, 16-Mar-2020, <https://archive.ph/1n45R>
- Abby Ohlheiser, 'Welcome to TikTok's endless cycle of censorship and mistakes', MIT Technology Review, 13-Jul-2021, <https://web.archive.org/web/20221119070904/https://www.technologyreview.com/2021/07/13/1028401/tiktok-censorship-mistakes-glitches-apologies-endless-cycle/>
- 285 Charlotte Colombo, 'TikTok has apologized for a 'significant error' after a video that suggested racial bias in its algorithm went viral', Insider, 8-Jul-2021, <https://archive.md/9jraE>
- Sam Shead, 'TikTok apologizes after being accused of censoring #BlackLivesMatter posts', CNBC, 2-Jun-2020, <https://web.archive.org/web/20230106130612/https://www.cnn.com/2020/06/02/tiktok-blacklivesmatter-censorship.html>
- Lily Kuo, 'TikTok sorry for blocking teenager who disguised Xinjiang video as make-up tutorial', The Guardian, 28-Nov-2019, <https://web.archive.org/web/20221224015107/https://www.theguardian.com/technology/2019/nov/28/tiktok-says-sorry-to-us-teenager-blocked-after-sharing-xinjiang-videos>
- Umberto Bacchi, 'TikTok apologises for censoring LGBT+ content', Reuters, 22-Sep-2020, <https://web.archive.org/web/20230107051422/https://www.reuters.com/article/britain-tech-lgbt-idUSL5N2GJ459>
- Eric Han, 'An update on recent content and account questions', TikTok, 28-Nov-2019, <https://web.archive.org/web/20221216024217/https://newsroom.tiktok.com/en-us/an-update-on-recent-content-and-account-questions>
- Vanessa Pappas, 'A message to our Black community', TikTok, 2-Jun-2020, <https://web.archive.org/web/20230107091339/https://newsroom.tiktok.com/en-us/a-message-to-our-black-community>
- Seth Melnick and Somar Musa, 'Hashtag view count display issue post-mortem', TikTok, 17-Jun-2020, <https://web.archive.org/web/20220925143948/https://newsroom.tiktok.com/en-us/hashtag-view-count-display-issue-post-mortem>
- 286 Shen Lu, 'I helped build ByteDance's vast censorship machine', Protocol, 18-Feb-2021, <https://web.archive.org/web/20221216031945/https://www.protocol.com/china/i-built-bytedance-censorship-machine>
- 287 '造谣“上海封城”，两人被上海警方立案侦查', CCTV, 23-Mar-2022, <https://archive.ph/MmKOz>
- 288 '2018 字节跳动企业社会责任报告', ByteDance, 2018, https://web.archive.org/web/20220130223125/https://if3-static.bytednsdoc.com/obj/eden-cn/uj_shpjpmmv_ljuhklafi/ljhwZthlaukjlkulzlp/csr/csr-2018.pdf
- 289 '2018 字节跳动企业社会责任报告', ByteDance, 2018, https://web.archive.org/web/20220130223125/https://if3-static.bytednsdoc.com/obj/eden-cn/uj_shpjpmmv_ljuhklafi/ljhwZthlaukjlkulzlp/csr/csr-2018.pdf
- 290 '2018 字节跳动企业社会责任报告', ByteDance, 2018, https://web.archive.org/web/20220130223125/https://if3-static.bytednsdoc.com/obj/eden-cn/uj_shpjpmmv_ljuhklafi/ljhwZthlaukjlkulzlp/csr/csr-2018.pdf
- 291 '中央网信办深入开展网络辟谣标签工作', China News, 29-Sep-2022, <https://web.archive.org/web/20221216004319/https://www.chinanews.com.cn/gn/2022/09-29/9863196.shtml>
- 292 '全国“扫黄打非”办公室召开网络有害信息和出版物特征值共享数据库系统例会', National Anti-Pornography and Anti-Illegal Publications Office, 30-Sep-2020, <https://archive.ph/CQfrZ>
- 293 '平台直播 白律白皮书' Self-regulatory Mechanism of Live Video Streaming Platforms, ByteDance, <https://web.archive.org/web/20230109045701/http://www.dlong.com/eWebEditor/uploadfile/201907100828538576693.pdf>
- 'THREAD: This seems really alarming so I did a little digging and found that apparently ByteDance...', @lzy_Niu via Twitter, 8-Jul-2020, https://web.archive.org/web/20211103183638/https://twitter.com/lzy_Niu/status/1280911594310991877

- 294 '平台直播 白律白皮书' Self-regulatory Mechanism of Live Video Streaming Platforms', ByteDance, <http://web.archive.org/web/20230309042939/http://www.invest-data.com/eWebEditor/uploadfile/201907100828538576693.pdf>
'THREAD: This seems really alarming so I did a little digging and found that apparently ByteDance...', @Izzy_Niu via Twitter, 8-Jul-2020, https://web.archive.org/web/20211103183638/https://twitter.com/Izzy_Niu/status/1280911594310991877
- 295 '平台直播 白律白皮书' Self-regulatory Mechanism of Live Video Streaming Platforms', ByteDance, <http://web.archive.org/web/20230309042939/http://www.invest-data.com/eWebEditor/uploadfile/201907100828538576693.pdf>
'THREAD: This seems really alarming so I did a little digging and found that apparently ByteDance...', @Izzy_Niu via Twitter, 8-Jul-2020, https://web.archive.org/web/20211103183638/https://twitter.com/Izzy_Niu/status/1280911594310991877
- 296 '平台直播 白律白皮书' Self-regulatory Mechanism of Live Video Streaming Platforms', ByteDance, <http://web.archive.org/web/20230309042939/http://www.invest-data.com/eWebEditor/uploadfile/201907100828538576693.pdf>
'THREAD: This seems really alarming so I did a little digging and found that apparently ByteDance...', @Izzy_Niu via Twitter, 8-Jul-2020, https://web.archive.org/web/20211103183638/https://twitter.com/Izzy_Niu/status/1280911594310991877
- 297 '平台直播 白律白皮书' Self-regulatory Mechanism of Live Video Streaming Platforms', ByteDance, <http://web.archive.org/web/20230309042939/http://www.invest-data.com/eWebEditor/uploadfile/201907100828538576693.pdf>
'THREAD: This seems really alarming so I did a little digging and found that apparently ByteDance...', @Izzy_Niu via Twitter, 8-Jul-2020, https://web.archive.org/web/20211103183638/https://twitter.com/Izzy_Niu/status/1280911594310991877
- 298 Shen Lu, 'I helped build ByteDance's vast censorship machine', Protocol, 18-Feb-2021, <https://web.archive.org/web/20221216031945/https://www.protocol.com/china/i-built-bytedance-censorship-machine>
- 299 Shen Lu, 'I helped build ByteDance's vast censorship machine', Protocol, 18-Feb-2021, <https://web.archive.org/web/20221216031945/https://www.protocol.com/china/i-built-bytedance-censorship-machine>
- 300 Shen Lu, 'I helped build ByteDance's vast censorship machine', Protocol, 18-Feb-2021, <https://web.archive.org/web/20221216031945/https://www.protocol.com/china/i-built-bytedance-censorship-machine>
- 301 '字节跳动党委: 要把讲导向守责任放首位', The Paper via Sina, 29-Apr-2018, <https://archive.ph/EJNyo>
- 302 '2018 字节跳动企业社会责任报告', ByteDance, 2018, https://web.archive.org/web/20220130223125/https://lf3-static.bytednsdoc.com/obj/eden-cn/uj_shpjpmmv_ljuhklafi/ljhwZthlaukjlkulzlp/csr/csr-2018.pdf
- 303 '字节跳动两员工收钱将指定内容推上抖音热榜 自首获刑', Fanwubi, 30-Nov-2021, <https://web.archive.org/web/20221114002717/https://www.fanwubi.org/Item/200523.aspx>
- 304 '抖音回应员工受贿被判刑: 将严厉打击内部贪腐', Fanwubi, 13-Dec-2021, <https://archive.ph/WnOaw>
- 305 Emily Baker-White, 'TikTok's Secret 'Heating' Button Can Make Anyone Go Viral', Forbes, 20-Jan-2023, <https://web.archive.org/web/20230207023409/https://www.forbes.com/sites/emilybaker-white/2023/01/20/tiktoks-secret-heating-button-can-make-anyone-go-viral/?sh=11952ae6bfd4>
- 306 '字节跳动投资报告', ByteDance via Vzko, Sep-2022, <https://web.archive.org/web/20230309021933/https://www.vzko.com/document/20221019fdf26403c23542f51b8cd8d8.html?keyword=%E5%AD%97%E8%8A%82%E8%B7%B3%E5%8A%A8>
- 307 '字节跳动投资报告', ByteDance via Vzko, Sep-2022, <https://web.archive.org/web/20230309021933/https://www.vzko.com/document/20221019fdf26403c23542f51b8cd8d8.html?keyword=%E5%AD%97%E8%8A%82%E8%B7%B3%E5%8A%A8>
- 308 '字节跳动投资报告', ByteDance via Vzko, Sep-2022, <https://web.archive.org/web/20230309021933/https://www.vzko.com/document/20221019fdf26403c23542f51b8cd8d8.html?keyword=%E5%AD%97%E8%8A%82%E8%B7%B3%E5%8A%A8>
- 309 '网络短视频内容审核标准细则 (2021)', China Netcasting Services Association, 16-Dec-2021, <https://archive.ph/C6jpS>
- 310 "'抖音'服务协议", Douyin, 06-Jul-2022, <https://archive.ph/8zrEY>
- 311 "'抖音'服务协议", Douyin, 06-Jul-2022, <https://archive.ph/8zrEY>
- 312 '《网络短视频平台管理规范》《网络短视频内容审核标准细则》发布', People's Network, 10-Jan-2019, <https://archive.ph/UWgWc>
'网络短视频内容审核标准细则 (2021)', China Netcasting Services Association, 16-Dec-2021, <https://archive.ph/C6jpS>

- 313 '《网络短视频平台管理规范》《网络短视频内容审核标准细则》发布', People's Network, 10-Jan-2019, <https://archive.ph/UWgWc>
- '网络短视频内容审核标准细则 (2021)', China Netcasting Services Association, 16-Dec-2021, <https://archive.ph/C6jpS>
- 314 '今日头条启动招聘 2000 名内容审核编辑: 党员优先', The Paper, 3-Jan-2018, https://web.archive.org/web/20221116013004/https://www.thepaper.cn/newsDetail_forward_1932733
- 315 '2018 字节跳动企业社会责任报告', ByteDance, https://web.archive.org/web/20220130223125/https://lf3-static.bytednsdoc.com/obj/eden-cn/uj_shpjpmmv_ljuhklafi/ljhwZthlaukjlkulzlp/csr/csr-2018.pdf
- 316 Shen Lu, 'I helped build ByteDance's vast censorship machine', Protocol, 18-Feb-2021, <https://web.archive.org/web/20221216031945/https://www.protocol.com/china/i-built-bytedance-censorship-machine>
- 'The censor cannot hold: the pressure of controlling China's internet', France24, 6-Oct-2022, <http://web.archive.org/web/20221108193721/https://www.france24.com/en/live-news/20221006-the-censor-cannot-hold-the-pressure-of-controlling-china-s-internet>
- '前新浪微博内容审核员专访: 中共如何打造网络“真理部”', VOA, 12-Aug-2020, <https://web.archive.org/web/20221209214136/https://www.voachinese.com/a/internet-censorship-20200812/5540475.html>
- 317 'Exclusive: ByteDance censored anti-China content in Indonesia until mid-2020 - sources', Reuters, 13-Aug-2020, <https://archive.ph/YXigt>
- 318 'Exclusive: ByteDance censored anti-China content in Indonesia until mid-2020 - sources', Reuters, 13-Aug-2020, <https://archive.ph/YXigt>
- 319 'TikTok Owner ByteDance Used A News App On Millions Of Phones To Push Pro-China Messages, Ex-Employees Say', BuzzFeed, 26-Jul-2022, <https://web.archive.org/web/20221108220821/https://www.buzzfeednews.com/article/emilybakerwhite/tiktok-bytedance-topbuzz-pro-china-content>
- 320 'TikTok Owner ByteDance Used A News App On Millions Of Phones To Push Pro-China Messages, Ex-Employees Say', BuzzFeed, 26-Jul-2022, <https://web.archive.org/web/20221108220821/https://www.buzzfeednews.com/article/emilybakerwhite/tiktok-bytedance-topbuzz-pro-china-content>
- 321 'Chinese government asked TikTok for stealth propaganda account,' Bloomberg, 29-Jul-2022, <https://archive.ph/hyF2j>
- 322 '舆情负责人', ByteDance, <https://web.archive.org/web/20221220123928/https://jobs.bytedance.com/experienced/position/6760519636069910792/detail?recomId=a3f08a23-8062-11ed-84f1-fa163ef1500c&sourceJobId=6839512909916686599>
- '高级舆情分析师', ByteDance, <https://archive.ph/dg3K0>
- '舆情分析专家', ByteDance, <https://archive.ph/sa2Ys>
- '互联网信息摘要与机器写稿关键技术及应用', Wu Wen Jun AI Science & Technology Award, 25-Jan-2018, <https://web.archive.org/web/20221220193738/http://award.wuwenjunkejijiang.cn/wj/news.aspx?pkid=11590&tid=13535>
- 'Xiaojun Wan', GitHub, <https://archive.ph/gvs2N>
- 'Ad Targeting', TikTok, <https://ads.tiktok.com/help/article/ad-targeting?lang=en>
- 'Purchase Intent Targeting', TikTok, <https://ads.tiktok.com/help/article?aid=10014017>
- 323 '字节跳动两员工收钱将指定内容推上抖音热榜 自首获刑', Fanwubi, 30-Nov-2021, <https://web.archive.org/web/20221114002717/https://www.fanwubi.org/ltem/200523.aspx>
- Emily Baker-White, 'TikTok's Secret "Heating" Button Can Make Anyone Go Viral', Forbes, 20-Jan-2023, <https://web.archive.org/web/20230207023409/https://www.forbes.com/sites/emilybaker-white/2023/01/20/tiktoks-secret-heating-button-can-make-anyone-go-viral/?sh=11952ae6bfd4>
- 324 'TikTok 内幕: 张一鸣的巨浪征途', Jiemian via Sina, 25-Apr-2022, <https://archive.ph/geqqt>
- 325 '张一鸣荣获“中关村创新创业青年英豪” 称科技企业应承担更多责任', Economic Daily, 7-Dec-2017, https://web.archive.org/web/20221117171922/http://www.ce.cn/xwzx/kj/201712/07/t20171207_27160272.shtml
- 326 '张一鸣荣获“中关村创新创业青年英豪” 称科技企业应承担更多责任', Economic Daily, 7-Dec-2017, https://web.archive.org/web/20221117171922/http://www.ce.cn/xwzx/kj/201712/07/t20171207_27160272.shtml
- 327 '张一鸣荣获“中关村创新创业青年英豪” 称科技企业应承担更多责任', Economic Daily, 7-Dec-2017, https://web.archive.org/web/20221117171922/http://www.ce.cn/xwzx/kj/201712/07/t20171207_27160272.shtml
- 328 '张一鸣荣获“中关村创新创业青年英豪” 称科技企业应承担更多责任', Economic Daily, 7-Dec-2017, https://web.archive.org/web/20221117171922/http://www.ce.cn/xwzx/kj/201712/07/t20171207_27160272.shtml
- 329 “十四五”时期中关村东城园发展规划', Beijing Doncheng Government via NCSTI.gov, 11-Sep-2022, <https://archive.ph/cTQqq>

- 330 '北京字节跳动企业社会责任报告', ByteDance, 10-Mar-2021,
<https://web.archive.org/web/20230216075729/http://p3-bd-official.byteimg.com/obj/bytedance-cn/2021%E5%8C%97%E4%BA%AC%E5%AD%97%E8%8A%82%E8%B7%B3%E5%8A%A8%E4%BC%81%E4%B8%9A%E7%A4%BE%E4%BC%9A%E8%B4%A3%E4%BB%BB%E6%8A%A5%E5%91%8A.pdf>
- 331 '北京字节跳动企业社会责任报告', ByteDance, 10-Mar-2021,
<https://web.archive.org/web/20230216075729/http://p3-bd-official.byteimg.com/obj/bytedance-cn/2021%E5%8C%97%E4%BA%AC%E5%AD%97%E8%8A%82%E8%B7%B3%E5%8A%A8%E4%BC%81%E4%B8%9A%E7%A4%BE%E4%BC%9A%E8%B4%A3%E4%BB%BB%E6%8A%A5%E5%91%8A.pdf>
- 332 '北京成立智源人工智能研究院', People's Network, 14-Nov-2018, <https://archive.ph/RgMuO>
'Addition of Certain Entities to the Entity List', Industry and Security Bureau via Federal Register, 09-Oct-2019,
<https://archive.ph/HhyU6>
'Treasury Identifies Eight Chinese Tech Firms as Part of The Chinese Military-Industrial Complex', U.S. Department of the Treasury, 16-Dec-2021, <https://home.treasury.gov/news/press-releases/jy0538>
- 333 'Treasury Identifies Eight Chinese Tech Firms as Part of The Chinese Military-Industrial Complex', U.S. Department of the Treasury, 16-Dec-2021, <https://home.treasury.gov/news/press-releases/jy0538>
'Addition of Certain Entities to the Entity List', Industry and Security Bureau via Federal Register, 09-Oct-2019,
<https://archive.ph/HhyU6>
- 334 '新一代人工智能发展规划的通知', gov.cn, 20-Jul-2017,
https://web.archive.org/web/20221105172041/http://www.gov.cn/zhengce/content/2017-07/20/content_5211996.htm
- 335 '新一代人工智能发展规划的通知', gov.cn, 20-Jul-2017,
https://web.archive.org/web/20221105172041/http://www.gov.cn/zhengce/content/2017-07/20/content_5211996.htm
- 336 '新一代人工智能发展规划的通知', gov.cn, 20-Jul-2017,
https://web.archive.org/web/20221105172041/http://www.gov.cn/zhengce/content/2017-07/20/content_5211996.htm
- 337 China Defence Universities Tracker, Australian Strategic Policy Institute, last updated 05-2021,
<https://unitracker.aspi.org.au/>
- 338 'Huazhong University of Science and Technology', Australian Strategic Policy Institute, 18-Nov-2019,
<https://unitracker.aspi.org.au/universities/huazhong-university-of-science-and-technology/>
- 339 'Person Re-Identification With Hierarchical Discriminative Spatial Aggregation', IEEE, vol. 17, 26-Jan-2022,
<https://archive.ph/cl1p5>
- 340 'People's Public Security University of China', ASPI, 21-Nov-2019,
<https://unitracker.aspi.org.au/universities/peoples-public-security-university-of-china/>
- 341 'An Overview of Deepfake: The Sword of Damocles in AI 265', 2020 International Conference on Computer Vision, Image and Deep Learning (CVIDL), 10-Jul-2020, <https://archive.ph/VPnsN>
'面向中文文本分类的词级对抗样本生成方法', 信息安全,
https://web.archive.org/web/20221028092147/https://kns.cnki.net/kcms/detail/detail.aspx?dbcode=CJFD&dbname=CJFDLAST2020&filename=XXAQ202009004&uniplatform=NZKPT&v=sJjxsAJahrnTSFLRDzmdhGKRLZ_mtsFBsH-JG14_mFZodpZrOEw0iY-qPZZoPip8
- 342 'Tsinghua University', ASPI, 21-Nov-2019, <https://unitracker.aspi.org.au/universities/tsinghua-university/>
- 343 '清华大学、字节跳动 | Multimodal Entity Tagging with Multimodal Knowledge Base (基于多模态知识库的多模态实体标注)', BAAI.ac.cn, 4-Jan-2022, <https://archive.ph/a35OS>
'Subspace Attack: Exploiting Promising Subspaces for Query-Efficient Black-box Attacks', 33rd Conference on Neural Information Processing Systems (NeurIPS 2019),
<https://proceedings.neurips.cc/paper/2019/file/2cad8fa47bbef282badbb8de5374b894-Paper.pdf>
'字节 AI Lab 推出业界首个系统性大分子体系的量子计算模拟方法, 成果入选《Chemical Science》', BAAI, 25-Jul-2022, <https://archive.ph/sOfco>
- 344 'Peking University', ASPI, 20-Nov-2019, <https://unitracker.aspi.org.au/universities/peking-university/>
- 345 '北京大学-字节跳动数字人文开放实验室', Research Center for Digital Humanities of PKU,
<https://archive.ph/MQG3k>
'北大、字节跳动等联合 | Contextual Representation Learning beyond Masked Language Modeling (掩码语言建模之上的语境表征学习)', BAAI.ac.cn, 11-Apr-2022, <https://archive.ph/5lOmF>
'Unified Perceptual Parsing for Scene Understanding', 15th European Conference on Computer Vision,
<https://web.archive.org/web/20211204180726/https://people.csail.mit.edu/bzhou/publication/eccv18-segment.pdf>
'北大万小军 | 智能文本生成: 进展与挑战', China InfoCom Media Group, 16-Feb-2023, <https://archive.ph/sjvod>
- 346 'Person Re-Identification With Hierarchical Discriminative Spatial Aggregation', IEEE, vol. 17, 26-Jan-2022,
<https://archive.ph/cl1p5>
'面向中文文本分类的词级对抗样本生成方法', 信息安全,

- https://web.archive.org/web/20221028092147/https://kns.cnki.net/kcms/detail/detail.aspx?dbcode=CJFD&dbna me=CJFDLAST2020&filename=XXAQ202009004&uniplatform=NZKPT&v=sJjxsAJahrTSFLRDzmdGkRLZ_mtsf BsH-JG14_mFZodpZrOEw0iY-qPZZoPip8
- 347 'Subspace Attack: Exploiting Promising Subspaces for Query-Efficient Black-box Attacks', 33rd Conference on Neural Information Processing Systems (NeurIPS 2019), <https://proceedings.neurips.cc/paper/2019/file/2cad8fa47bbef282badbb8de5374b894-Paper.pdf>
- 348 'Addition of Certain Entities to the Entity List', Industry and Security Bureau via Federal Register, 09-Oct-2019, <https://archive.ph/HhyU6>
- 349 '立昂技术与字节跳动在数据中心业务方面有合作', Shanghai Securities News, 20-May-2022, <https://archive.ph/8v0HX>
- 350 'Addition of Certain Entities to the Entity List', Industry and Security Bureau via Federal Register, 09-Oct-2019, <https://archive.ph/HhyU6>
- 'Treasury Identifies Eight Chinese Tech Firms as Part of The Chinese Military-Industrial Complex', U.S. Department of the Treasury, 16-Dec-2021, <https://archive.ph/ljRn3>
- 351 'Can SenseTime become a Chinese AI champion?', Financial Times, 29-Sep-2021, <https://archive.ph/bBkcP>
- 352 'Face – Inspire your Beauty', Amazon, <https://archive.ph/JxjPE>
- 'FaceU – Inspire your Beauty', Google Play, https://play.google.com/store/apps/details?id=com.lemon.faceu.oversea&hl=en_GB&gl=US
- 353 'U.S. Blacklists More Chinese Tech Companies Over National Security Concerns', The New York Times, 21-Jun-2019, <https://archive.ph/jMQCu>
- 354 '2018 业务拆解', Dawning Information Industry via Zhongtai Securities, 21-Apr-2019, https://pdf.dfcfw.com/pdf/H3_AP201904221321136186_1.pdf
- 355 'Addition of Certain Entities to the Entity List', Industry and Security Bureau via Federal Register, 09-Oct-2019, <https://archive.ph/HhyU6>
- 356 "看见词曲计划"上线, 讯飞音乐联动抖音音乐, 为优秀词曲助力', Jiangxi TV via China Daily, 19-Nov-2021, <https://web.archive.org/web/20221127041448/https://cn.chinadaily.com.cn/a/202111/19/WS61973540a3107be4979f8ffe.html>
- '抖音联手讯飞智声 AI 黑科技让明星念出你名字送专属祝福', iFeng, 11-Feb-2018, <https://archive.ph/amsVF>
- 357 '智能语音, 让飞书更高效', iFlytek, <https://archive.ph/wVle8>
- 358 'Treasury Identifies Eight Chinese Tech Firms as Part of The Chinese Military-Industrial Complex', U.S. Department of the Treasury, 16-Dec-2021, <https://home.treasury.gov/news/press-releases/jy0538>
- 359 'Addition of Certain Entities to the Entity List', Industry and Security Bureau via Federal Register, 09-Oct-2019, <https://archive.ph/HhyU6>
- 360 'Unified Perceptual Parsing for Scene Understanding', 15th European Conference on Computer Vision, <https://web.archive.org/web/20211204180726/https://people.csail.mit.edu/bzhou/publication/eccv18-segment.pdf>
- 361 '我国将强化互联网安全管理着力 提升保护网民个人信息能力', Economic Daily via gov.cn, 5-Aug-2015, <https://archive.ph/xPtUz>
- 362 '字节跳动党委书记张辅评: 抖音打造“警务亲民”新模式', Guangming Online, 14-Sep-2018, <https://archive.ph/VRNBJ>
- 363 '字节跳动党委书记张辅评: 抖音打造“警务亲民”新模式', Guangming Online, 14-Sep-2018, <https://archive.ph/VRNBJ>
- 364 '字节跳动党委书记张辅评: 抖音打造“警务亲民”新模式', Guangming Online, 14-Sep-2018, <https://archive.ph/VRNBJ>
- 365 '画好网上网下同心圆, 全国公安新媒体矩阵入驻今日头条、抖音', China Daily, 25-Apr-2019, <https://web.archive.org/web/20221116024646/http://ex.chinadaily.com.cn/exchange/partners/82/rss/channel/cn/columns/sz8srm/stories/WS5cc15248a310e7f8b15790d3.html>
- '2019 字节跳动 (中国) 企业社会责任报告', ByteDance, 2019, https://web.archive.org/web/20220130223129/https://lf3-static.bytednsdoc.com/obj/eden-cn/uj_shpjpmmv_ljuhklafi/ljhwZthlaukjlkulzlp/csr/csr-2019.pdf
- 366 '抖音发布《2022 年反诈报告》平台诈骗投诉量同比下降 78.96%', China News, 23-May-2022, <https://archive.ph/Va0ed>
- 367 '抖音发布《2022 年反诈报告》平台诈骗投诉量同比下降 78.96%', China News, 23-May-2022, <https://archive.ph/Va0ed>
- 368 'Smart Asian women are the new targets of CCP global online repression', ASPI, 3-Jun-2022, <http://web.archive.org/web/20230102150718/https://www.aspistrategist.org.au/smart-asian-women-are-the-new-targets-of-ccp-global-online-repression/>
- 'Removing Coordinated Inauthentic Behavior From China and Russia', Meta, 27-Sep-2022, <https://web.archive.org/web/20221219215524/https://about.fb.com/news/2022/09/removing-coordinated-inauthentic-behavior-from-china-and-russia/>

- 365 'How China Spreads Its Propaganda Version of Life in Xinjiang', New York Times, 22-Jun-2021, <https://web.archive.org/web/20221205103657/https://www.nytimes.com/interactive/2021/06/22/technology/xinjiang-uyghurs-china-propaganda.html>
- 'Removing Coordinated Inauthentic Behavior From China and Russia', Meta, 27-Sep-2022, <https://web.archive.org/web/20221219215524/https://about.fb.com/news/2022/09/removing-coordinated-inauthentic-behavior-from-china-and-russia/>
- 'Pro-PRC DRAGONBRIDGE Influence Campaign Leverages New TTPs to Aggressively Target U.S. Interests, Including Midterm Elections', Mandiant, 26-Oct-2022, <https://web.archive.org/web/20221217153852/https://www.mandiant.com/resources/blog/prc-dragonbridge-influence-elections>
- 'MAGA porn, hate for Trump: China-based accounts stoke division', Washington Post, 1-Nov-2022, <https://archive.ph/xlcnp>
- 366 'US warns about foreign efforts to sway American voters', AP News, 4-Oct-2022, <https://web.archive.org/web/20221119101144/https://apnews.com/article/2022-midterm-elections-russia-ukraine-campaigns-presidential-ea913f2b3b818651a9db1327adaa330a>
- 367 'Buying Influence: How China Manipulates Facebook and Twitter', NYT, 20-Dec-2021, <https://web.archive.org/web/20221130213118/https://www.nytimes.com/interactive/2021/12/20/technology/china-facebook-twitter-influence-manipulation.html>
- 368 Drew Harwell and Tony Romm, 'TikTok's Beijing roots fuel censorship suspicion as it builds a huge U.S. audience', Washington Post, 15-Sep-2019, <https://www.washingtonpost.com/technology/2019/09/15/tiktoks-beijing-roots-fuel-censorship-suspicion-it-builds-huge-us-audience/>
- 369 Drew Harwell and Tony Romm, 'TikTok's Beijing roots fuel censorship suspicion as it builds a huge U.S. audience', Washington Post, 15-Sep-2019, <https://www.washingtonpost.com/technology/2019/09/15/tiktoks-beijing-roots-fuel-censorship-suspicion-it-builds-huge-us-audience/>
- 370 Drew Harwell and Tony Romm, 'TikTok's Beijing roots fuel censorship suspicion as it builds a huge U.S. audience', Washington Post, 15-Sep-2019, <https://www.washingtonpost.com/technology/2019/09/15/tiktoks-beijing-roots-fuel-censorship-suspicion-it-builds-huge-us-audience/>
- 371 'TikTok: Ich habe China kritisiert, dann wurden meine Videos versteckt', Vice, 12-Dec-2019, <https://archive.ph/Yv5kG>
- 372 Fergus Ryan, Audrey Fritz and Daria Impiombato, 'TikTok and WeChat: Curating and controlling global information flows,' ASPI International Cyber Policy Centre Report No. 37/2020, <https://ad-aspi.s3.ap-southeast-2.amazonaws.com/2020-09/TikTok%20and%20WeChat.pdf?VersionId=7BNJWaoHImPVE.6KKcBP1JRD5fRnAVTZ>
- 373 Fergus Ryan, Audrey Fritz and Daria Impiombato, 'TikTok and WeChat: Curating and controlling global information flows,' ASPI International Cyber Policy Centre Report No. 37/2020, <https://ad-aspi.s3.ap-southeast-2.amazonaws.com/2020-09/TikTok%20and%20WeChat.pdf?VersionId=7BNJWaoHImPVE.6KKcBP1JRD5fRnAVTZ>
- 374 Fergus Ryan, Audrey Fritz and Daria Impiombato, 'TikTok and WeChat: Curating and controlling global information flows,' ASPI International Cyber Policy Centre Report No. 37/2020, <https://ad-aspi.s3.ap-southeast-2.amazonaws.com/2020-09/TikTok%20and%20WeChat.pdf?VersionId=7BNJWaoHImPVE.6KKcBP1JRD5fRnAVTZ>
- 375 'Election Integrity,' TikTok, <https://web.archive.org/web/20221221080501/https://www.tiktok.com/safety/en/election-integrity/>
- 376 'TikTok and Facebook fail to detect election disinformation in the US, while YouTube succeeds,' Global Witness, 21-Oct-2022, <https://web.archive.org/web/20221220033404/https://www.globalwitness.org/en/campaigns/digital-threats/tiktok-and-facebook-fail-detect-election-disinformation-us-while-youtube-succeeds/>
- 377 'TikTok and Facebook fail to detect election disinformation in the US, while YouTube succeeds,' Global Witness, 21-Oct-2022, <https://web.archive.org/web/20221220033404/https://www.globalwitness.org/en/campaigns/digital-threats/tiktok-and-facebook-fail-detect-election-disinformation-us-while-youtube-succeeds/>
- 378 Sarah Perez, 'Google exec suggests Instagram and TikTok are eating into Google's core products, Search and Maps', TechCrunch, 13-Jul-2022, <https://archive.md/Huq9H>
- 379 Kari Paul and Dan Milmo, 'Elon Musk completes Twitter takeover and 'fires top executives'', The Guardian, 28-Oct-2022, <https://www.theguardian.com/technology/2022/oct/27/elon-musk-completes-twitter-takeover>
- Sheila Dang, Paresh Dave and Hyunjoo Jin, 'After Elon Musk's ultimatum, Twitter employees start exiting', Reuters, 19-Nov-2022, <https://www.reuters.com/technology/after-elon-musks-ultimatum-twitter-employees-start-exiting-2022-11-18/>
- Sheila Dang, Paresh Dave and Hyunjoo Jin, 'Twitter lays off staff, Musk blames activists for ad revenue drop', Reuters, 5-Nov-2022, <https://www.reuters.com/technology/twitter-start-layoffs-friday-morning-internal-email-2022-11-04/>
- Kate Conger, Ryan Mac and Mike Isaac, 'Confusion and Frustration Reign as Elon Musk Cuts Half of Twitter's Staff', The New York Times, 4-Nov-2022, <https://www.nytimes.com/2022/11/04/technology/elon-musk-twitter-layoffs.html>

Ashley Belanger, 'Twitter lays off 5K contractors in surprise 2nd wave of cuts, more mods lost', Ars Technica, 15-Nov-2022, <https://arstechnica.com/tech-policy/2022/11/twitter-lays-off-5k-contractors-in-surprise-2nd-wave-of-cuts-more-mods-lost/>

Clare Duffy and Oliver Darcy, 'Twitter employees head for the exits after Elon Musk's 'extremely hardcore' work ultimatum', CNN, 18-Nov-2022, <https://edition.cnn.com/2022/11/17/tech/twitter-employees-ultimatum-deadline>

Kali Hays, 'Less than half of Twitter's remaining employees signed up to work for Elon Musk's 'hardcore' vision, leaving leaders scrambling to persuade people to stay', Business Insider, 18-Nov-2022, <https://www.businessinsider.com/twitter-elon-musk-half-working-2022-11>

Ryan Mac, Mike Isaac and Kellen Browning, 'Elon Musk's Twitter Teeters on the Edge After Another 1,200 Leave', The New York Times, 18-Nov-2022, <https://www.nytimes.com/2022/11/18/technology/elon-musk-twitter-workers-quit.html>

Kate Conger, Mike, Ryan Mac and Tiffany Hsu, 'Two Weeks of Chaos: Inside Elon Musk's Takeover of Twitter', The New York Times, 11-Nov-2022, <https://www.nytimes.com/2022/11/11/technology/elon-musk-twitter-takeover.html>

380 Thomas Perkins, 'TikTok Analysis', Internet 2.0, 4-Jul-2022, <https://internet2-0.com/wp-content/uploads/2022/08/TikTok-Technical-Analysis-17-Jul-2022.-Media-Release.pdf>

381 Thomas Perkins, 'TikTok Analysis', Internet 2.0, 4-Jul-2022, <https://internet2-0.com/wp-content/uploads/2022/08/TikTok-Technical-Analysis-17-Jul-2022.-Media-Release.pdf>

382 Thomas Perkins, 'TikTok Analysis', Internet 2.0, 4-Jul-2022, <https://internet2-0.com/wp-content/uploads/2022/08/TikTok-Technical-Analysis-17-Jul-2022.-Media-Release.pdf>

383 'Smart Asian women are the new targets of CCP global online repression', ASPI, 3-Jun-2022, <http://web.archive.org/web/20230102150718/https://www.aspistrategist.org.au/smart-asian-women-are-the-new-targets-of-ccp-global-online-repression/>

384 'TikTok Analysis', Internet 2.0, 4-Jul-2022, <https://internet2-0.com/wp-content/uploads/2022/08/TikTok-Technical-Analysis-17-Jul-2022.-Media-Release.pdf>

385 'Device Fingerprinting Techniques', Darkwave Technology 27-Sep-2013, <https://www.darkwavetech.com/index.php/device-fingerprint-blog/device-fingerprinting-techniques#:~:text=SDK-based%20device%20fingerprinting%20is%20the%20most%20powerful%20form,unique%20hardware%20based%20identifiers%20%28IMEI%2C%20MAC%20address%2C%20etc.%29>

386 'Manifest.permission', Android for Developers, <http://web.archive.org/web/20230217042729/https://developer.android.com/reference/android/Manifest.permission>

387 'EXCLUSIVE: TikTok Spied on Forbes Journalists', Forbes, 22-Dec-2022, <https://www.forbes.com/sites/emilybaker-white/2022/12/22/tiktok-tracks-forbes-journalists-bytedance/?sh=5aebf8af7da5>

'TikTok Parent ByteDance Planned to Use TikTok to Monitor The Physical Location Of Specific American Citizens', Forbes, 20-Oct-2022, <https://www.forbes.com/sites/emilybaker-white/2022/10/20/tiktok-bytedance-surveillance-american-user-data/?sh=436b90e36c2d>

'Leaked Audio From 80 Internal TikTok Meetings Shows That US User Data Has Been Repeatedly Accessed From China', BuzzFeed News, 18-Jun-2022, <https://www.buzzfeednews.com/article/emilybakerwhite/tiktok-tapes-us-user-data-china-bytedance-access>

388 'TikTok admits tracking FT journalists in leaks investigation', Financial Times, 23-Dec-2022, <https://www.ft.com/content/e873b98a-9623-45b3-b97c-444a2fde5874>

'EXCLUSIVE: TikTok Spied on Forbes Journalists', Forbes, 22-Dec-2022, <https://www.forbes.com/sites/emilybaker-white/2022/12/22/tiktok-tracks-forbes-journalists-bytedance/?sh=24c71c2e7da5>

389 'EXCLUSIVE: TikTok Spied on Forbes Journalists', Forbes, 22-Dec-2022, <https://www.forbes.com/sites/emilybaker-white/2022/12/22/tiktok-tracks-forbes-journalists-bytedance/?sh=24c71c2e7da5>

390 'Worldwide threats to the Homeland', House Homeland Security Committee, 15-Nov-2022, https://homeland.house.gov/activities/hearings/11/04/2022/worldwide-threats-to-the-homeland?utm_campaign=wp_the_cybersecurity_202&utm_medium=email&utm_source=newsletter&wpisrc=nl_cybersecurity202

391 'Fireside Chat with DNI Haines at the Reagan National Defense Forum', Office of the Director of National Intelligence, 12-Dec-2022, <https://web.archive.org/web/20221221203155/https://www.dni.gov/index.php/newsroom/news-articles/news-articles-2022/item/2346-fireside-chat-with-dni-haines-at-the-reagan-national-defense-forum>

392 'CIA Director Bill Burns on war in Ukraine, intelligence challenges posed by China', PBS, 16-Dec-2022, <https://web.archive.org/web/20221220084613/https://www.pbs.org/newshour/show/cia-director-bill-burns-on-war-in-ukraine-intelligence-challenges-posed-by-china>


- 393 'TikTok Seen Moving Toward U.S. Security Deal, but Hurdles Remain', NYT, 26-Sep-2022,
<https://web.archive.org/web/20221220031733/https://www.nytimes.com/2022/09/26/technology/tiktok-national-security-china.html>
- 'Exclusive: TikTok steps up efforts to clinch U.S. security deal', NYT, 23-Dec-2022,
<https://web.archive.org/web/20230103114037/https://www.reuters.com/technology/tiktok-steps-up-efforts-clinch-us-security-deal-2022-12-22/>
- 394 'TikTok Parent ByteDance Planned To Use TikTok To Monitor The Physical Location Of Specific American Citizens', Forbes, 20-Oct-2022, <https://www.forbes.com/sites/emilybaker-white/2022/10/20/tiktok-bytedance-surveillance-american-user-data/?sh=13bc42106c2d>
- 395 'TikTok Parent ByteDance Planned To Use TikTok To Monitor The Physical Location Of Specific American Citizens', Forbes, 20-Oct-2022, <https://www.forbes.com/sites/emilybaker-white/2022/10/20/tiktok-bytedance-surveillance-american-user-data/?sh=13bc42106c2d>
- 396 'Leaked Audio From 80 Internal TikTok Meetings Shows That US User Data Has Been Repeatedly Accessed From China', BuzzFeed, 18-Jun-2022,
<https://web.archive.org/web/20221220160321/https://www.buzzfeednews.com/article/emilybakerwhite/tiktok-tapes-us-user-data-china-bytedance-access>
- 397 'As Washington wavers on TikTok, Beijing exerts control', Washington Post, 28-Oct-2022,
<https://web.archive.org/web/20221101005158/https://www.washingtonpost.com/technology/interactive/2022/bytedance-tiktok-privacy-china/>
- 398 'Leaked Audio From 80 Internal TikTok Meetings Shows That US User Data Has Been Repeatedly Accessed From China', BuzzFeed, 18-Jun-2022,
<https://web.archive.org/web/20221220160321/https://www.buzzfeednews.com/article/emilybakerwhite/tiktok-tapes-us-user-data-china-bytedance-access>
- 399 'Privacy Policy', TikTok, 2-Dec-2022,
<https://web.archive.org/web/20221220210344/https://www.tiktok.com/legal/page/us/privacy-policy/en>
- 400 'Privacy Policy', TikTok, 2-Jun-2021, <https://archive.md/Zmb97>
- 401 "'Are There TikTok Employees... Who Are Members Of The Chinese Communist Party?" Hawley Grills Exec', Forbes Breaking News via YouTube, 15-Sep-2022, <https://www.youtube.com/watch?v=meWM8d4Uz7Q>
- 402 'Sharing an Update to our Privacy Policy, TikTok, 2-Nov-2022,
<https://web.archive.org/web/20221222004443/https://newsroom.tiktok.com/en-eu/sharing-an-update-to-our-privacy-policy>
- 403 'Portman Presses Meta Official on Policies Allowing Exploitation of Children', US Senate Committee on Home land Security & Governmental Affairs, 14-Sep-2022,
<https://web.archive.org/web/20221216222855/https://www.hsgac.senate.gov/media/minority-media/portman-presses-meta-official-on-policies-allowing-exploitation-of-children>
- 404 'Our approach to keeping U.S. data secure', TikTok, 6-Jul-2022,
<https://web.archive.org/web/20221216062057/https://newsroom.tiktok.com/en-us/our-approach-to-keeping-us-data-secure>
- 405 'Our approach to keeping U.S. data secure', TikTok, 6-Jul-2022,
<https://web.archive.org/web/20221216062057/https://newsroom.tiktok.com/en-us/our-approach-to-keeping-us-data-secure>
- 406 'Privacy Policy', TikTok, 2-Jun-2021,
<https://web.archive.org/web/20221220210344/https://www.tiktok.com/legal/page/us/privacy-policy/en>
- 407 'TikTok national-security deal roiled by internal strife', Politico, 16-Dec-2022,
<https://www.politico.com/news/2022/12/16/biden-administration-at-odds-over-forcing-tiktok-divestment-00074415>
- 408 'Lawmaker says sale of TikTok to US company could avoid outright ban', FT, 1-Jan-2023,
<https://archive.ph/eqQAH>
- 409 'Complaint for injunctive and declaratory relief, Case No. 2:20-cv-7672', United States District Court, Central District of California Western Division, 24-Aug-2020,
<https://web.archive.org/web/20211021140428/https://s3.documentcloud.org/documents/7043128/031133742970.pdf>
- 410 '外交部：支持 TikTok 等相关企业拿起法律武器维护正当权益', Xinhua, 24-Aug-2020,
https://web.archive.org/web/20210319224924/http://www.xinhuanet.com/world/2020-08/24/c_1126407522.htm
- 411 '新华国际时评：用法律武器向经济霸凌说“不”', Xinhua, 25-Aug-2020,
https://web.archive.org/web/20210319230159/http://www.xinhuanet.com/world/2020-08/25/c_1126409507.htm
- 412 'TikTok's algorithm not for sale, ByteDance tells US: source', SCMP, 13-Sep-2020,
<https://web.archive.org/web/20200913160256/https://www.scmp.com/economy/china-economy/article/3101362/tiktoks-algorithm-not-sale-bytedance-tells-us-source>
- '商务部 科技部公告 2020 年第 38 号 关于调整发布《中国禁止出口限制出口技术目录》的公告', Ministry of Commerce, PRC, 28-Aug-2020,

- <https://web.archive.org/web/20221031213250/http://www.mofcom.gov.cn/article/b/xxfb/202008/20200802996641.shtml>
- '《中国禁止出口限制出口技术目录》调整内容', Ministry of Commerce, PRC, <https://web.archive.org/web/20220709223655/http://images.mofcom.gov.cn/fms/202008/20200828200911003.pdf>
- 412 'Planned TikTok deal entails China's approval under revised catalogue: expert', Xinhua, 30-Aug-2020, https://web.archive.org/web/20221030175546/http://www.xinhuanet.com/english/2020-08/30/c_139329598.htm
- 413 '公司关注到商务部和科技部于 8 月 28 日, 联合公布《关于调整发布<中国禁止出口限制出口技术目录>的公告》, '公司将严格遵守《中华人民共和国技术进出口管理条例》和《中国禁止出口限制出口技术目录》, 处理关于技术出口的相关业务。', 字节跳动 via Today's Headlines, 30-Aug-2020, <https://archive.ph/XLz4u>
- 414 'Exclusive: China would rather see TikTok U.S. close than a forced sale', Reuters, 12-Sep-2020, <https://web.archive.org/web/20210802061955/https://www.reuters.com/article/us-china-bytedance-tiktok-exclusive/exclusive-china-would-rather-see-tiktok-u-s-close-than-a-forced-sale-idUSKBN2622L6>
- 415 'Chinese govt not an outsider in the TikTok deal', Global Times, 20-Sep-2020, <https://web.archive.org/web/20230109084253/https://www.globaltimes.cn/content/1201415.shtml>
- 'New TikTok deal shuns worst-case scenario: Global Times editorial', Global Times, 20-Sep-2020, <https://web.archive.org/web/20230109084259/https://www.globaltimes.cn/content/1201484.shtml>
- 'Say 'No!' to US robbery of TikTok: Global Times editorial', Global Times, 21-Sep-2020, <https://web.archive.org/web/20221111051931/https://www.globaltimes.cn/content/1201625.shtml>
- 'Chinese govt's involvement makes a difference in TikTok deal', Global Times, 21-Sep-2020, <https://web.archive.org/web/20221226025023/https://www.globaltimes.cn/content/1201503.shtml>
- 'TikTok extortion deal is unpalatable gambit: Global Times editorial', Global Times, 22-Sep-2020, <https://web.archive.org/web/20221205170929/https://www.globaltimes.cn/content/1201759.shtml>
- 'Chinese govt not an outsider in the TikTok deal', Global Times, 20-Sep-2020, <https://web.archive.org/web/20230109084253/https://www.globaltimes.cn/content/1201415.shtml>
- 'No disguising proposed TikTok deal is a dirty and underhanded trick: China Daily editorial', China Daily, 23-Sep-2020, <https://archive.md/xkpbQ>
- 'China to protect TikTok at "all cost"', Global Times, 26-Sep-2020, <https://web.archive.org/web/20221110152248/https://www.globaltimes.cn/content/1202146.shtml>
- 416 '认清"当代海盗"的真面目', People's Daily, 25-Sep-2020, <https://archive.ph/K9X6C>
- 'China to protect TikTok at "all cost"', Global Times, 26-Sep-2020, <https://web.archive.org/web/20221110152248/https://www.globaltimes.cn/content/1202146.shtml>
- 417 '【中国网评】巧取豪夺别国企业, 起底美式"规则和秩序"', China.com.cn via Xinhua, 4-Jan-2023, <https://archive.md/9Urx3>
- '美国又想强制 TikTok 出售业务, 专家: 美国刁难或进一步变本加厉', Global Times via Sina, 28-Dec-2022, <https://web.archive.org/web/20230109094150/https://finance.sina.com.cn/world/2022-12-28/doc-imxyetfn3616623.shtml>
- 'Relentless US crackdown on Chinese companies is doomed: experts', Global Times, 5-Dec-2022, <https://web.archive.org/web/20230109094209/https://www.globaltimes.cn/page/202212/1281136.shtml>
- 418 'Bipartisan support for new foreign interference laws', Parliamentary Joint Committee on Intelligence and Security, 7-Jun-2018, https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/Espionage/Interference/Media_Releases
- 'Statement by Chair and Deputy Chair, Parliamentary Joint Committee on Intelligence and Security, 8-Feb-2018, https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/Espionage/Interference/Media_Releases

This copy is for your personal, non-commercial use only. Distribution and use of this material are governed by our Subscriber Agreement and by copyright law. For non-personal use or to order multiple copies, please contact Dow Jones Reprints at 1-800-843-0008 or visit www.djreprints.com.

<https://www.wsj.com/articles/tiktok-algorithm-sex-drugs-minors-11631052944>

How TikTok Serves Up Sex and Drug Videos to Minors



BUSINESS

How TikTok Serves Up Sex and Drug Videos to Minors

The popular app can quickly drive young users into endless spools of adult content, including videos touting drug use and promoting pornography sites

By *Rob Barry* [Follow](#) , *Georgia Wells* [Follow](#) , *John West* [Follow](#) , *Joanna Stern* [Follow](#) and *Jason French*

Sept. 8, 2021 7:59 am ET

The account was one of dozens of automated accounts, or bots, created by The Wall Street Journal to understand what TikTok shows young users. These bots, registered as users aged 13 to 15, were turned loose to browse TikTok’s For You feed, the highly personalized, never-ending feed curated by the algorithm.

An analysis of the videos served to these accounts found that through its powerful algorithms, TikTok can quickly drive minors—among the biggest users of the app—into endless spools of content about sex and drugs.

TikTok served one account registered as a 13-year-old at least 569 videos about drug use, references to cocaine and meth addiction, and promotional videos for online sales of drug products and paraphernalia. Hundreds of similar videos appeared in the feeds of the Journal's other minor accounts.

TikTok also showed the Journal's teenage users more than 100 videos from accounts recommending paid pornography sites and sex shops. Thousands of others were from creators who labeled their content as for adults only.

Still others encouraged eating disorders and glorified alcohol, including depictions of drinking and driving and of drinking games.

The Journal shared with TikTok a sample of 974 videos about drugs, pornography and other adult content that were served to the minor accounts—including hundreds shown to single accounts in quick succession.

Of those, 169 were removed from the platform before the Journal shared them—whether by their creators or TikTok couldn't be determined. Another 255 were removed after being shared with the company, among them more than a dozen portraying adults as “caregivers” entering relationships with people pretending to be children, called “littles.”

The woman in the role-playing video said she wished TikTok did a better job of keeping adult content out of minors' feeds.

“I do have in my bio that is 18+ but I have no real way to police this,” she wrote in a message. “I do not agree with TikTok showing my content to someone so young.”

A spokeswoman declined to address the content of the individual videos, but said the majority didn't violate guidelines. She said TikTok removed some of the videos after the Journal's accounts viewed them, and restricted the distribution of other videos to stop the app from recommending them to other users, but declined to say how many.

The spokeswoman said the app doesn't differentiate between videos it serves to adults and minors but said that the platform is looking to create a tool that filters content for young users.

TikTok's terms of service say that users must be at least 13 years old, and that users under 18 need consent from their parents.

“Protecting minors is vitally important, and TikTok has taken industry-first steps to promote a safe and age-appropriate experience for teens,” the spokeswoman said in a statement. She noted that the app allows parents to manage screen time and privacy settings for their children's accounts.

The addiction machine

An earlier video investigation by the Journal found that TikTok only needs one important piece of information to figure out what a user wants: the amount of time you linger over a piece of content. Every second you hesitate or re-watch, the app tracks you.

Through that one powerful signal, TikTok can learn your most hidden interests and emotions, and drive users of any age deep into rabbit holes of content—in which feeds are heavily dominated by videos about a specific topic or theme. It's an experience that other social-media companies like YouTube have struggled to stop.

“All the problems we have seen on YouTube are due to engagement-based algorithms, and on TikTok it's exactly the same—but it's worse,” said Guillaume Chaslot, a former YouTube engineer who worked on that site's algorithm and is now an advocate for transparency in how companies use those tools. “TikTok's algorithm can learn much faster.”

The Journal assigned each of its 31 minor accounts a date of birth and an IP address. Most were also programmed with various interests, which were revealed to TikTok only through lingering on videos with related hashtags or images and through scrolling quickly past the others. Most didn't search for content and instead simply watched videos that appeared in their feed.

Here's how that can work:

The creator promoting the 420 friendly website didn't respond to questions about the video being shown to an account registered to a 13-year-old.

About a dozen of the Journal's 31 minor accounts ended up being dominated by a particular theme.

This can be especially problematic for young people, who may lack the capability to stop watching and don't have supportive adults around them, said David Anderson, a clinical psychologist at The Child Mind Institute, a nonprofit mental-health care provider for children.

He said those teens can experience a "perfect storm" in which social media normalizes and influences the way they view drugs or other topics.

Even when the Journal's accounts were programmed to express interest in multiple topics, TikTok sometimes zeroed in on single topics and served them hundreds of videos about one in close succession.

TikTok served one account, which had been programmed with a variety of interests, hundreds of Japanese film and television cartoons. In one streak of 150 videos, all but four featured Japanese animation—many with sexual themes.

The TikTok spokeswoman said the Journal's bots "in no way represents the behavior and viewing experience of a real person," in part because humans have diverse and changing interests. She added that the platform was "reviewing how to help prevent even highly unusual viewing habits from creating negative cycles, particularly for our younger users."

The spokeswoman said that when users encounter something they don't want to see, they can select "not interested" to see less of that content.

Dozens of the videos promoting paid pornography have since been deleted from the app.

In some cases, TikTok creators were clear about not wanting children to see their videos, labeling them (or their accounts) as for adults only. But the app served them anyway.

In one stretch of 200 videos, nearly 40% were labeled as being for adults only.

In all, at least 2,800 such videos were served to the Journal's minor accounts.

The proliferation of sexually charged content has stirred concerns inside TikTok. Videos directing people to OnlyFans were so abundant that in a meeting in the fall of 2020, the company's chief operating officer, Vanessa Pappas, asked employees to explain what the site was, according to a person familiar with the meeting.

After the meeting, TikTok at first decided to ban content directing users to OnlyFans, since employees argued much of the content on the site is pornographic, the person familiar with the decision said. The platform then decided to allow users to link to the site after other

employees pointed out that not everything on OnlyFans is X-rated, and that other social-media platforms allow links to the content.

The TikTok spokeswoman said that it prohibits nudity and sexual solicitation and removes accounts that redirect users to sexual content or services, including on OnlyFans.

A spokeswoman for OnlyFans said the site is strictly for people 18 years and older and declined to comment on TikTok accounts directing people to the site.

Policing

TikTok relies on a combination of algorithms and more than 10,000 people to police its huge and growing volume of content, according to former executives of the company.

The company said in a recent report that it removed 89 million videos in the second half of last year.

But it has been hard to keep up with the app's growth, the former executives said: TikTok now has about 100 million users in the U.S. consuming and producing videos, from about 25 million in 2019.

The company said that users upload tens of thousands of videos every minute.

To keep pace, moderators focus on the most popular content, leaving videos with lower view counts largely unreviewed, the former executives said.

In July, TikTok said that in the U.S. it would begin relying on its algorithms to both identify and remove certain types of videos that violate its rules in an effort to enforce its rules more quickly. Previously, TikTok's algorithms identified rule-breaking videos, but humans reviewed them before removal.

The company made the announcement after the Journal shared hundreds of examples of potentially rule-breaking content that the app had served its bots. TikTok said it has been experimenting with this new system over the past year.

TikTok's spokeswoman said that no algorithm will ever be completely accurate at policing content because of the amount of context that goes into understanding a video, particularly ones about drugs.

TikTok has also struggled to eradicate video posts promoting eating disorders.

Policing content has been complicated by the company's decisions in recent years to loosen some restrictions in the U.S., including around skin exposure and bikinis, according to several former executives and content moderators.

The result has been more sexualized videos on the platform, the people said.

The spokeswoman for TikTok said the company's policies evolve in response to industry norms and changing user behavior. She also said the company expects new and different content as TikTok's audience grows older and more diverse.

And that bot account registered for a teenage user that fell into the world of role-playing and other sexually oriented content?

—Kara Dapena, Joel Eastwood, Dave Cole, Maureen Linke and Siung Tjia contributed to this article.

Appeared in the September 9, 2021, print edition as 'TikTok Serves Up Sex and Drug Videos To Young Users'.

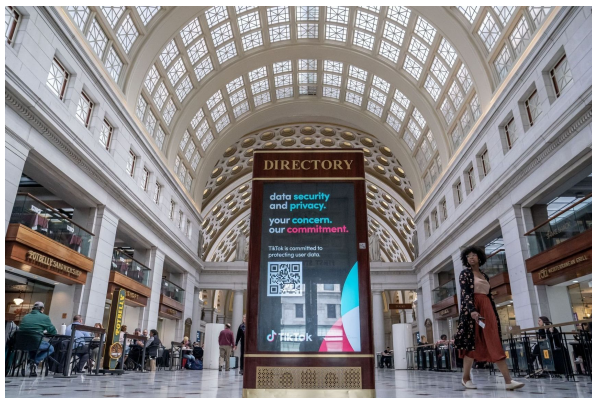
This copy is for your personal, non-commercial use only. Distribution and use of this material are governed by our Subscriber Agreement and by copyright law. For non-personal use or to order multiple copies, please contact Dow Jones Reprints at 1-800-843-0008 or visit www.djreprints.com.

<https://www.wsj.com/articles/china-says-it-opposes-a-forced-sale-of-tiktok-1a2ffc62>

BUSINESS

China Says It Opposes Forced Sale of TikTok

Biden administration demands that video app divest itself from its Chinese parent or face a U.S. ban



A TikTok advertisement at Union Station in Washington, D.C., addresses user security and privacy concerns.

PHOTO: NATHAN HOWARD/BLOOMBERG NEWS

By *Raffaele Huang* [Follow](#)

Updated March 23, 2023 9:09 am ET

SINGAPORE—China said it would strongly oppose any forced sale of TikTok, responding for the first time to a Biden administration demand that the short-video app divest itself from its Beijing-based parent ByteDance Ltd. or face a nationwide ban.

The comments came hours before TikTok Chief Executive Shou Zi Chew testifies Thursday at a congressional hearing over national-security concerns about user data. They put TikTok in the middle of geopolitical tensions between the U.S. and China that have largely centered around technology.

China's Commerce Ministry said Thursday that a sale or divestiture of TikTok would involve exporting technology and had to be approved by the Chinese government.

The reported efforts by the Biden administration would severely undermine global investors' confidence in the U.S., said Shu Jueting, a ministry spokeswoman.

"If the news is true, China will firmly oppose it," she said, referring to the forced sale.

The Biden administration has demanded that TikTok's Chinese owners sell their stakes, citing national-security concerns that Beijing could access U.S. users' data and influence the content that Americans consume.

Mr. Chew will be questioned Thursday over safety and security concerns about the Chinese-controlled platform that is popular in the U.S. He has said divesting the company from its Chinese owners doesn't offer any more protection than a multibillion-dollar plan TikTok has already proposed to ringfence U.S. user data.

ByteDance and TikTok didn't immediately respond to requests for comment after the ministry issued its stance. The companies have said they wouldn't share data with the Chinese government even if requested.

Beijing has increasingly signaled its desire to protect Chinese technology. It recently proposed to amend a

regulation restricting the export of Chinese-created content-recommendation algorithms, a secret sauce of TikTok's global success, which lawyers say is a reminder that Beijing has a hand to play in any deal.

TikTok has more than 150 million users in the U.S., its most lucrative market.

In 2020, when the Trump administration was pushing for a sale of TikTok's U.S. operations, China added algorithms to an export-control list. Any deals that involve transferring such technologies developed in China to a third party outside the country now require government approval.

ByteDance said at the time that it had applied for government approval for the preliminary agreement it reached with Oracle Corp. and Walmart Inc. to set up a new U.S. entity, TikTok Global. The idea eventually fell by the wayside, and China's official records show ByteDance has never received an approval for tech export.

TikTok's recommendation algorithm was initially developed from algorithms and artificial-intelligence models created by its parent, people familiar with the company have said, though the app's systems run on servers in Singapore and the U.S.

TikTok also shares a common algorithm architecture with ByteDance's China-focused video-sharing app Douyin, they said.

In recent exchanges with Beijing officials, ByteDance executives have understood that Beijing is very likely to block a sale or divestiture of TikTok's U.S. operations, even though the officials didn't explicitly say that, people familiar with the matter said Thursday. The authorities have encouraged ByteDance to firmly defend its interests, they said.

—Grace Zhu contributed to this article.

Write to Raffaele Huang at raffaele.huang@wsj.com

Corrections & Amplifications

Shu Jueting is a spokeswoman for China's Commerce Ministry. An earlier version of this article incorrectly spelled her name as Shu Yuting. (Corrected on March 23)



John Scott-Railton ✓
@jsrailton



Citizen Lab doesn't hand out Good Housekeeping seals of approval to apps.

And if we did, #TikTok wouldn't get one.

Their execs need to stop citing our research in their testimony as somehow exculpatory.

profdeibert ✓ @RonDeibert · 8h

My statement about #TikTok's continuing reference to @citizenlab research 📌

[Show this thread](#)

I am disappointed that TikTok executives continue citing the Citizen Lab's research in their statements to governments as somehow exculpatory.

I've called them out on this in the past, and it's unfortunate that I have to do it again.

Two years ago we analyzed the TikTok app. Our analysis was restricted to the application, and the kinds of data it collected. Broadly speaking, we found that it was similar to other social media apps: a vacuum cleaner of personal data. This is not a good thing.

We also highlighted additional concerns, including about latent functionality that could potentially be activated, and noted that TikTok contained some dormant code originally written for Douyin (TikTok's Chinese counterpart, also owned by ByteDance).

Our analysis was explicit about having no visibility into what happened to user data once it was collected and transmitted back to TikTok's servers. Although we had no way to determine whether or not it had happened, we even speculated about possible mechanisms through which the Chinese government might use unconventional techniques to obtain TikTok user data via pressure on ByteDance.

The conversation about potential privacy and national security concerns with TikTok should serve as a reminder that **most social media apps are unacceptably invasive-by-design, treat users as raw material for personal data surveillance, and fall short on transparency about their data sharing practices.** This is why comprehensive privacy legislation is desperately needed.

Ron Deibert, Director, the Citizen Lab, University of Toronto
March 22, 2023



11:10 PM · Mar 22, 2023 · 23.6K Views

36 Retweets 154 Likes 5 Bookmarks

I am disappointed that TikTok executives continue citing the Citizen Lab's research in their statements to governments as somehow exculpatory.

I've called them out on this in the past, and it's unfortunate that I have to do it again.

Two years ago we analyzed the TikTok app. Our analysis was restricted to the application, and the kinds of data it collected. Broadly speaking, we found that it was similar to other social media apps: a vacuum cleaner of personal data. This is not a good thing.

We also highlighted additional concerns, including about latent functionality that could potentially be activated, and noted that TikTok contained some dormant code originally written for Douyin (TikTok's Chinese counterpart, also owned by ByteDance).

Our analysis was explicit about having no visibility into what happened to user data once it was collected and transmitted back to TikTok's servers. Although we had no way to determine whether or not it had happened, we even speculated about possible mechanisms through which the Chinese government might use unconventional techniques to obtain TikTok user data via pressure on ByteDance.

The conversation about potential privacy and national security concerns with TikTok should serve as a reminder that **most social media apps are unacceptably invasive-by-design, treat users as raw material for personal data surveillance, and fall short on transparency about their data sharing practices.** This is why comprehensive privacy legislation is desperately needed.

Ron Deibert, Director, the Citizen Lab, University of Toronto
March 22, 2023



Crunch Time for TikTok and Americans' Freedom of Speech

March 22, 2023 / [Caitlin Vogus](#)

A nationwide ban on TikTok in the U.S. may violate the First Amendment and won't protect users

TikTok may be operating on borrowed time in the United States, as Congress and the White House increasingly target the social media app. Both the [House](#) and [Senate](#) have proposed a flurry of bills aimed squarely at TikTok, some of which would [ban the app entirely in the U.S.](#) Others would give the President or federal agencies the authority to restrict or ban foreign-owned information technology services like TikTok, or impose [transparency requirements](#) on services that store data in China. The White House has [demanded](#) that the Chinese company that owns TikTok, ByteDance, sell the app to divest it of Chinese ownership, and has threatened to ban TikTok in the U.S. if it does not. All of this follows laws passed in several states and Congress that [prohibit TikTok on government-issued devices](#).

Lawmakers and the Biden administration say these steps are needed because TikTok may give the Chinese government access to private information about the app's users and allow it to influence TikTok's content moderation. TikTok denies these claims and, in any case, asserts they can be addressed through structural mechanisms of [the sort it has proposed](#) to the Committee on Foreign Investment in the United States (CFIUS).

It's true that many social media platforms and other consumer-facing technologies, including TikTok, pose privacy concerns — and that governments, [including China](#), use social media for disinformation campaigns or to otherwise [try to influence public opinion](#). However, a nationwide ban on TikTok is not the answer to these concerns. Banning TikTok would undermine free expression in the United States and abroad, and it would not solve the problems the government believes TikTok creates.

A nationwide ban on TikTok would raise serious First Amendment concerns by directly restricting users' ability to speak and receive information. Americans — [especially younger Americans](#) — use TikTok to both spread and find information about many important topics, including [police brutality against Black people](#), [LGBTQ rights](#), [labor movements](#), [the experiences and rights of people with disabilities](#), [reproductive health](#), [campus safety](#), and [environmental policy and climate change](#). Some users participate in our democracy through TikTok, by hosting or viewing [voter registration campaigns](#) or subscribing to official accounts of [political candidates](#), [elected officials](#), or [government entities](#).

The Supreme Court has long recognized that the First Amendment protects not only the right to speak, but also the right to receive information – including the right to receive information from abroad. For example, in the 1960s, the Supreme Court [struck down](#) a federal law requiring the Postmaster General to detain “communist political propaganda” printed or prepared in a foreign country and mailed to the U.S., notify the addressee, and deliver the mail only upon request. Recognizing the likely deterrent effect of requiring an addressee to affirmatively request delivery of materials the government had labeled as communist propaganda, the Court held that the law violates the First Amendment. It explained that the government cannot “control the flow of ideas to the public,” including ideas (even propaganda) from abroad.

The Court has also held that prohibiting too much protected speech can [violate the First Amendment](#), especially if a law forecloses a unique and important means of communication. These First Amendment limits ensure that people can exercise other First Amendment rights of speech, press, and assembly and protect Americans’ participation in our democracy. For example, voters who are informed about political candidates and issues are better able to exercise their right to vote.

While other online services may remain available, a TikTok ban would foreclose users from speaking and receiving information through an important and distinct medium of expression. TikTok’s users choose to use the app to reach particular audiences, especially young people connecting with other young people, and because of its [distinctive capabilities for communication](#). Just as the Supreme Court has recognized that bans on [yard signs](#), [pamphlets](#), or [live entertainment](#) are not permitted under the First Amendment simply because other means of expression remain available, a ban on TikTok suppresses a unique medium of expression and suppresses too much speech.

Banning TikTok in the U.S. would also be what’s known as a “prior restraint” on speech, or a limit imposed on speech before it happens. A ban would prevent the millions of Americans who use TikTok from being able to speak through the app in the future and would prohibit new users from downloading the app. This “freeze” on TikTok users’ speech would come with [a heavy presumption against its constitutional validity](#). The Supreme Court has long recognized that [the chief purpose of the First Amendment is to prohibit prior restraints](#) and that prior restraints can be justified only by the most extraordinary circumstances. In the past, the Court has rejected even justifications based on national security interests, explaining that the First Amendment permits a prior restraint only when the government can demonstrate that [“disclosure . . . will surely result in direct, immediate, and irreparable damage to our Nation or its people.”](#)

Empowering the government to suppress TikTok nationwide may also mean giving it startling powers to censor, monitor, and screen other online services. While it is not clear how such a ban would be carried out as a technical matter, it could take the form of prohibiting app stores from carrying TikTok, potentially impinging on the First Amendment rights of app stores themselves (to make their own choices about what apps they host in their stores), as well as the rights of individuals to access communications apps. In addition, an app store prohibition may, ironically, [create](#)

[security risks](#) for American TikTok users by preventing them from downloading updates to the app that fix security vulnerabilities. Alternatively, a ban may require [internet service providers \(ISPs\) to engage in filtering](#) to block the service from American users, furthering concerns about prior restraints and potentially opening the door to other types of censorial filtering at the ISP level.

Not only would a TikTok ban suppress the speech of Americans, but it would also provide other countries with a justification for banning online services that facilitate free expression in their countries. While a ban on an entire online speech service would be novel in the United States, other countries have unfortunately already adopted this approach to silence criticism and dissent. Turkey, for example, has repeatedly blocked social media sites such as [YouTube](#) and [Twitter](#), citing national security concerns. Most recently, [Turkey sparked outrage after constraining access to Twitter and TikTok](#) following devastating earthquakes in that country and [arresting scores of people for “sharing provocative posts.”](#) A ban on TikTok in the U.S. would embolden governments worldwide — authoritarian and democratic alike — to impose their own restrictions on social media services in the name of privacy and national security. As a result, billions of people worldwide may lose access to the online services that provide easy to use, freely available outlets for their speech.

In addition to potentially violating the First Amendment and undermining free expression worldwide, a TikTok ban would not necessarily help protect Americans’ privacy. Even if banning TikTok would remove the Chinese government’s ability to collect data on Americans directly from the app, there are other avenues it could use to obtain this data. [Private data brokers routinely sell data to American law enforcement and intelligence agencies](#) and face no legal barrier to [selling data from other social media apps to the Chinese government or its proxies](#) – or other foreign governments or potentially hostile actors. If Congress is serious about addressing risks to Americans’ privacy, it could accomplish far more by focusing its efforts on passing comprehensive privacy legislation like the [American Data Privacy and Protection Act](#).

Concerns that the Chinese government could put a thumb on TikTok’s content moderation decisions to spread disinformation and propaganda are also not appropriately addressed by a ban. Even if the Chinese government — or any foreign country — uses TikTok or other social media in this way, the First Amendment prohibits the government from banning a service because it disagrees with the viewpoints expressed on it. Instead, counterspeech, both in the form of investigations that reveal disinformation campaigns and speech responding to and debunking disinformation, are the better way to respond to this concern while preserving free expression.

It is also important that any action that the government takes against TikTok or any other online service that facilitates speech on the basis of national security be done transparently, with sufficient information made available to the public so Americans can judge for themselves whether the government’s action is necessary. Not only should the government be required to give a public explanation of its actions “if practicable” (as [one proposed bill states](#)), but there should be a strong presumption that the government

must make the reasons for a ban or other restriction, and evidence supporting those reasons, publicly available. The government should not be able to keep its justification secret on the basis of nebulous or unjustified national security or law enforcement interests. The government's reasons for taking action against a speech intermediary like TikTok would also be at the heart of a court's consideration of a First Amendment challenge to those actions, since courts apply a high level of scrutiny to government restrictions on speech based on content or viewpoint.

In the midst of these debates over legislation to ban TikTok, the company has been negotiating a national security agreement with the Committee on Foreign Investment in the United States (CFIUS). [According to reports](#) by those briefed on TikTok's proposal, nicknamed Project Texas, TikTok would create a new subsidiary based entirely in the United States that would control access to U.S. users' data and content moderation decisions. The U.S. entity would be controlled by an independent board of directors selected by TikTok but approved by CFIUS, and the board would also report to CFIUS. Data from U.S. users would be hosted in the United States by Oracle, which would also oversee TikTok's content moderation and recommendation algorithm in the U.S., and report potential risks to the government, "which will then have the authority to inspect the issue in more detail."

[Some have criticized Project Texas as not doing enough to protect Americans from Chinese spying and influence](#), and CFIUS has not, to date, approved the plan. It has negotiated with TikTok since 2019 and can reject the plan and order divestiture. If it becomes the basis for resolution of the concerns that prompted the CFIUS review, Project Texas may raise First Amendment problems of its own, particularly if it empowers the government to oversee and overrule a private online service's [editorial decisions](#) about what content to host, bar, recommend, or deprioritize.

However, given the serious negative impacts of an outright ban on freedom of expression and the fact that it will not solve the privacy concerns that Congress claims motivate these bills, the government should consider other paths. If the government does not believe Project Texas sufficiently protects Americans' interests, it should explain the basis for its objections and why no other mitigation measures can adequately address the risk. Suppressing speech should be used only as an absolute last resort, in response to a government interest of the highest importance. The U.S. government should not undermine online free speech with an ill-conceived ban that sets a dangerous precedent for the U.S. and countries around the world.

Dear Member of Congress,

We, the undersigned organizations, write to express our concern about federal legislation and proposals that seek to impose a wholesale ban on TikTok in the United States. If passed by Congress and enacted into law, a nationwide ban on TikTok would have serious ramifications for free expression in the digital sphere, infringing on Americans' First Amendment rights and setting a potent and worrying precedent in a time of increased censorship of internet users around the world. A ban on TikTok by means of executive action would have a similar impact.

We recognize the grave concerns that TikTok and other social media platforms pose for the privacy of individual users. We are also aware and we recognize that U.S. government officials have cited serious concerns with respect to the threat that TikTok may pose to U.S. national security. ByteDance's prevarication in response to repeated queries about its handling of American users' data is unacceptable. But solutions short of a full-scale ban can address these vulnerabilities without resorting to an ill-advised, blanket approach that would impair free speech and set a troubling precedent that could curtail free expression worldwide.

The rise of apps like TikTok poses novel challenges to the digital commons. Nearly 150 million Americans use TikTok¹ to connect, and to create and share content. Whether they use the app to live stream, promote a small business, share their creative work, connect with family, or find information on how to vote, their speech is protected by the First Amendment. The Supreme Court has long recognized that the First Amendment encompasses the right to receive information, irrespective of its source, free from government interference.² If the government were to intervene to ban TikTok entirely, it would impair the rights of citizens to communicate in a manner of their choosing, giving rise to significant First Amendment concerns.

The Supreme Court has recognized that the digital realm is currently "one of the most important places to exchange views."³ People in the U.S. have a constitutional right to speak via the internet, and to do so on the platform of their choosing. For citizens, and particularly the tens of millions of young Americans who use TikTok, to witness a popular social media platform summarily shut down by the government will raise serious questions in the minds of a rising generation about the sanctity of free speech in our system of governance. Moreover, the enforcement of such a ban could force major changes in the operation of the internet in the United States, including potential requirements on service platforms to police and censor the traffic of users, or even a national firewall to prevent users from downloading TikTok from sources across our borders.

¹ TikTok [@tiktok], *Our CEO, Shou Chew, shares a special message on behalf of ...* [TikTok video], <https://www.tiktok.com/@tiktok/video/7212953186724842795>, March 21, 2023.

² *Stanley v. Georgia*, 394 U.S. 557, 564 (1969) ("It is now well established that the Constitution protects the right to receive information and ideas."); *Red Lion Broadcasting Co., Inc v. FCC* 395 U.S. 367, 390 (1969) ("It is the right of the public to receive suitable access to social, political, esthetic, moral, and other ideas and experiences ...").

³ *Reno v. ACLU*, 521 U. S. 844, 870 (1997).

In addition to the implications of a ban on domestic free expression, a legislative ban on TikTok in the U.S. would set an alarming global precedent, lending legitimacy to authoritarian regimes in shutting down and excluding services they disfavor. Major American digital platforms have been banned or severely restricted by governments, including the Chinese Communist Party,⁴ Pakistan,⁵ and Uganda,⁶ among others,⁷ seeking to silence dissent and opposition and obstruct the open flow of communication and information. When Nigeria banned Twitter for seven months in June 2021, the U.S. condemned the ban, reiterating its support for “the fundamental human right of free expression and access to information as a pillar of democracy in Nigeria.” Last year, the U.S. similarly denounced “Russia’s shuttering of independent media and technology platforms,”⁸ and when mass protests erupted in Iran after the killing of Mahsa Amini, the U.S. government strongly condemned the actions of the Iranian regime and called on the Iranian authorities to refrain from the “blocking or filtering of services.”⁹ In 2018, the Department of the Treasury’s Office of Foreign Assets Control designated individuals responsible for the blocking of social media applications in Iran as “engaging in censorship activities that prohibit, limit, or penalize the exercise of freedom of expression or assembly by citizens of Iran.” If the U.S. were to now put its statutory imprimatur on wholesale banning as a means of redressing its security concerns about digital platforms, other governments will follow suit, insisting that their own security concerns are equally pressing. A ban on TikTok would sorely undermine U.S. credibility as a defender of digital freedom, and invite copycat measures that could lead to severe constriction of expression worldwide.

Measures short of an outright ban may address potential security concerns raised in relation to TikTok. A proposal by Senators Blumenthal and Moran to expedite the investigation by the Committee on Foreign Investment in the United States (CFIUS) into TikTok could yield a plan that would mitigate security risks without denying users access to the platform.¹⁰ A comprehensive consumer privacy bill would limit data commodification, thereby dramatically increasing users’ security online. A robust privacy bill could address concerns not just at TikTok but across the multiple social media platforms—current and future—that have proven to be

⁴Eglé Juodytė, *Which websites and apps are blocked in China?*, <https://nordvpn.com/blog/blocked-sites-china/> (noting blocked sites include Western media sources, social media applications, and search engines), January 3, 2023.

⁵Abid Hussain, *Wikipedia ban in Pakistan over alleged blasphemous content lifted*, <https://www.aljazeera.com/news/2023/2/7/wikipedia-ban-in-pakistan-over-alleged-blasphemous-content-lifted>, February 7, 2023.

⁶Arthur Arnold Wadero, *Facebook to remain shut as govt talks with tech giant stall*, <https://www.monitor.co.ug/uganda/news/national/facebook-to-remain-shut-as-govt-talks-with-tech-giant-stall-3912172>, August 12, 2022.

⁷Martin Armstrong, *Where Social Media is Suppressed*, <https://www.statista.com/chart/23804/countries-blocking-social-media/>, January 17, 2022.

⁸*Statement by NSC Spokesperson Emily Horne on Russian Disinformation and Efforts to Undermine Free Press*, <https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/05/statement-by-nsc-spokesperson-emily-horne-on-russian-disinformation-and-efforts-to-undermine-free-press/>, March 5, 2022.

⁹*Joint Statement on Internet Shutdowns in Iran*, <https://www.state.gov/joint-statement-on-internet-shutdowns-in-iran/>, October 20, 2022.

¹⁰Letter from Senators Richard Blumenthal and Jerry Moran to Secretary of the Treasury Janet Yellen (February 16, 2023), <https://www.blumenthal.senate.gov/imo/media/doc/20230216cfiustiktok.pdf>.

vulnerable to intrusion by the CCP and other foreign governments.¹¹ It could also mitigate concerns not just of foreign data mining but also hacking, ransomware and other security vulnerabilities.

Current legislative and administrative proposals to ban TikTok risk violating First Amendment rights, and setting a dangerous global precedent for the restriction of speech. More effective, rights-respecting solutions are available and provide a viable alternative to meet the serious concerns raised by TikTok.

Sincerely,

PEN America
Access Now
Advocacy For Principled Action In Government
American Civil Liberties Union
Authors Guild
Center for Democracy & Technology
Fight for the Future
Free Press Action
Knight First Amendment Institute at Columbia University
National Coalition Against Censorship
New America's Open Technology Institute
Organization for Identity & Cultural Development
Public Knowledge
Surveillance Technology Oversight Project
Tully Center for Free Speech
Woodhull Freedom Foundation

¹¹Twitter, *Disclosing state-linked information operations we've removed*, https://blog.twitter.com/en_us/topics/company/2021/disclosing-state-linked-information-operations-we-ve-removed, December 2, 2021; Twitter Safety, *Disclosing networks of state-linked information operations we've removed*, https://blog.twitter.com/en_us/topics/company/2020/information-operations-june-2020, June 12, 2020; Ben Nimmo and David Agranovich, *Removing Coordinated Inauthentic Behavior From China and Russia*, <https://about.fb.com/news/2022/09/removing-coordinated-inauthentic-behavior-from-china-and-russia/>, September 27, 2022; Taylor Hatmaker, *Former Twitter employee found guilty of spying for Saudi Arabia*, <https://techcrunch.com/2022/08/09/twitter-spy-convicted-saudi-arabia/>, August 9, 2022.

The Government Hasn't Justified a TikTok Ban

By Adam Schwartz and David Greene
March 16, 2023

Freedom of speech and association include the right to choose one's communication technologies. Politicians shouldn't be able to tell you what to say, where to say it, or who to say it to. So we are troubled by growing demands in the United States for restrictions on TikTok, a technology that many people have chosen to exchange information with others around the world. Before taking such a drastic step, the government must come forward with specific evidence showing, at the very least, a real problem and a narrowly tailored solution. So far, the government hasn't done so.

Nearly all social media platforms and other online businesses collect a lot of personal data from their users. TikTok raises special concerns, given the surveillance and censorship practices of its home country, China. Still, the best solution to these problems is not to single-out one business or country for a ban. Rather, we must enact comprehensive consumer data privacy legislation. By reducing the massive stores of personal data collected by all businesses, TikTok included, we will reduce opportunities for all governments, China included, to buy or steal this data.

Many people choose TikTok

TikTok is a social media platform that hosts [short videos](#). It is owned by [ByteDance](#), a company headquartered in China. It has [100 million](#) monthly users in the United States, and [a billion](#) worldwide. According to Pew, [67%](#) of U.S. teenagers use Tiktok, and [10%](#) of U.S. adults regularly get news there. Many users choose TikTok over its competitors because of its unique content recommendation system; to such users, social media platforms are not fungible.

TikTok videos address topics "[as diverse as human thought](#)." [Political satirists](#) mock politicians. [Political candidates](#) connect with voters. [Activists](#) promote social justice. Many users create and enjoy entertainment like [dance videos](#).

Problems with TikTok bans

If the government banned TikTok, it would undermine the free speech and association of millions of users. It would also intrude on TikTok's interest in disseminating its users' videos—just as bookstores have a right to [sell books written by others](#), and newspapers have a right to [publish someone else's opinion](#).

In a First Amendment challenge, courts would apply at least "intermediate scrutiny" to a TikTok ban and, depending upon the government's intentions and the ban's language, might apply "strict scrutiny." Either way, the government would have to prove that its ban is "[narrowly tailored](#)" to national security or other concerns. At the very least, the government "must demonstrate that the recited harms are [real, not merely conjectural](#)." It also must show a "[close fit](#)" between the ban and the government's goals, and that it did not "burden substantially more speech than is necessary." So far, the government has not publicly presented any specific information showing it can meet this high bar.

Any TikTok ban must also contend with a federal statute that protects the free flow of information in and out of the United States: the [Berman Amendments](#). In 1977, Congress enacted the International Emergency Economic Powers Act ([IEEPA](#)), which limited presidential power to restrict trade with foreign nations. In 1988 and 1994, Congress amended IEEPA to further limit presidential power. Most importantly, the President cannot "regulate

or prohibit, directly or [indirectly](#),” either “any...personal communication, which does not involve a transfer of anything of value,” or the import or export of “any information or informational materials.” Banning TikTok would be an indirect way of prohibiting information from crossing borders. Rep. Berman explained:

“The fact that we disapprove of the government of a particular country ought not to inhibit our dialog with the people who suffer under those governments...We are [strongest and most influential](#) when we embody the freedoms to which others aspire.”

A TikTok ban would cause further harms. It would undermine information security if, for example, legacy TikTok users could not receive [updates to patch vulnerabilities](#). A ban would [further entrench](#) the social media market share of a [small number of massive companies](#). One of these companies, Meta, [paid a consulting firm](#) to orchestrate a nationwide campaign seeking to turn the public against TikTok. After India banned TikTok in 2020, following a border dispute with China, many Indian users [shifted](#) to Instagram Reels and YouTube Shorts. Finally, a ban would undermine our moral authority to criticize censorship abroad.

The 2020 TikTok ban

In 2020, former President Trump issued [Executive Orders](#) banning TikTok and [WeChat](#), another Chinese-based communications platform. EFF filed two [amicus briefs](#) in support of challenges to these bans, and published [three blog posts](#) criticizing them.

A federal magistrate judge granted a [preliminary injunction](#) against the WeChat ban, based on the plaintiff’s likelihood of success on their First Amendment claim. The court reasoned that the government had presented “scant little evidence,” and that the ban “burden[ed] substantially more speech than is necessary.”

In 2021, President Biden [revoked](#) these bans.

The DATA Act

This year, Rep. McCaul (R-TX) filed the federal “[DATA Act](#)” ([H.R. 1153](#)). A House committee [approved](#) it on a party-line vote.

The bill requires executive officials to ban U.S. persons from engaging in “any transaction” with someone who “may transfer” certain personal data to any foreign person that is “subject to the influence of China,” or to that nation’s jurisdiction, direct or indirect control, or ownership. The bill also requires a ban on property transactions by any foreign person that operates a connected software application that is “subject to the influence of China,” and that “may be facilitating or contributing” to China’s surveillance or censorship. The President would have to sanction TikTok if it met either criterion.

It is doubtful this ban could survive First Amendment review, as the government has disclosed no specific information that shows narrow tailoring. Moreover, key terms are unconstitutionally vague, as the ACLU explained in its [opposition letter](#).

The bill would weaken the Berman Amendments: that safeguard would no longer apply to the import or export of personal data. But many communication technologies, not just TikTok, move personal data across national borders. And many nations, not just China, threaten user privacy. While the current panic concerns one app based in one country, this weakening of the Berman Amendments will have much broader consequences.

The Restrict Act

Also this year, Sen. Warner (D-VA) and Sen. Thune (R-SD), along with ten other Senators, filed the federal “[RESTRICT Act](#).” The White House [endorsed](#) it. It would authorize the executive branch to block “transactions” and “holdings” of “foreign adversaries” that involve “information and communication technology” and create “undue or unacceptable risk” to national security and more.

Two differences between the bills bear emphasis. First, while the DATA Act requires executive actions, the RESTRICT Act authorizes them following a review process. Second, while the DATA Act applies only to China, the

RESTRICT Act applies to six “foreign adversaries” (China, Cuba, Iran, North Korea, Russia, and Venezuela), and can be expanded to other countries.

The RESTRICT Act sets the stage for a TikTok ban. But the government has publicly disclosed no specific information that shows narrow tailoring. Worse, three provisions of the bill make such transparency less likely. First, the executive branch need not publicly explain a ban if doing so is not “practicable” and “consistent with ... national security and law enforcement interests.” Second, any lawsuit challenging a ban would be constrained in scope and the amount of discovery. Third, while Congress can override the designation or de-designation of a “foreign adversary,” it has no other role.

Coercing ByteDance to sell TikTok

The Biden administration has demanded that ByteDance [sell TikTok](#) or face a possible U.S. ban, according to the company. But the fundamental question remains: can the government show that banning TikTok is narrowly tailored? If not, the government cannot use the threat of unlawful censorship as the cudgel to coerce a business to sell its property.

The context here is review by the Committee on Foreign Investment in the United States ([CFIUS](#)) of ByteDance’s ownership of TikTok. The CFIUS is a federal entity that reviews, and in the name of national security can [block](#), certain acquisitions of U.S. businesses by foreign entities. In 2017, ByteDance [bought](#) TikTok (then called Musical.ly), and in 2019, CFIUS began [investigating](#) the purchase.

In response, TikTok has committed to a plan called “[Project Texas](#).” The company would spend \$1.5 billion on systems, overseen by CFIUS, to block data flow from TikTok to ByteDance and Chinese officials. Whether a TikTok ban is narrowly tailored would turn, in part, on whether Project Texas could address the government’s concerns without the extraordinary step of banning a communications platform.

Excluding TikTok from government-owned Wi-Fi

Some public universities and colleges have [excluded TikTok from their Wi-Fi systems](#).

This is disappointing. Students use TikTok to gather information from, and express themselves to, audiences around the world. Professors use it as a [teaching tool](#), for example, in classes on media and culture. [College-based news media](#) write stories about TikTok and use that platform to disseminate their stories. Restrictions on each pose First Amendment problems.

These exclusions will often be ineffective, because TikTok users can switch their devices from Wi-Fi to cellular. This further reduces the ability of a ban to withstand First Amendment scrutiny. Moreover, universities are teaching students the wrong lesson concerning how to make fact-based decisions about how to disseminate knowledge.

Excluding TikTok from government-owned devices

More than half of U.S. states have [excluded TikTok from government-owned devices](#) provided to government employees. Some state [bills](#) would do the same.

Government officials may be at greater risk of espionage than members of the general public, so there may be heightened concerns about the installation of TikTok on government devices. Also, government has greater prerogatives to manage its own assets and workplaces than those in the private sector. Still, infosec policies targeting just one technology or nation are probably not the best way to protect the government’s employees and programs.

The real solution: consumer data privacy legislation

There are legitimate data privacy concerns about all social media platforms, including but not limited to TikTok. They all harvest and monetize our personal data and incentivize other online businesses to do the same. The result is that detailed information about us is widely available to purchasers, thieves, and government subpoenas.

[That's why EFF supports comprehensive consumer data privacy legislation.](#)

Consider [location data brokers](#), for example. Our phone apps collect detailed records of our physical movements, without our knowledge or genuine consent. The app developers sell it to data brokers, who in turn sell it to anyone who will pay for it. An [anti-gay group](#) bought it to identify gay priests. An [election denier](#) bought it to try to prove voting fraud. One broker sold data on who had visited [reproductive health facilities](#).

If China wanted to buy this data, it could probably find a way to do so. Banning TikTok from operating here probably would not stop China from acquiring the location data of people here. The better approach is to limit how *all* businesses here collect personal data. This would reduce the supply of data that any adversary might obtain.