



# The Tech Oversight Project.

## MEMORANDUM

To: Interested Parties

From: Sacha Haworth, Executive Director, Tech Oversight Project

Re: TikTok is a threat. So is the rest of Big Tech.

Date: March 20, 2023

---

**PURPOSE: *TikTok is a threat, and they are not the only Big Tech giant to blame.***

The dangers of TikTok are indisputable, and Congress' investigations into the platform are well warranted. From national security to children's safety online, many of the concerns about TikTok's role in our information ecosystem also mirror long-held concerns and dangers from other platforms. Companies like Google, Apple, Meta, Amazon, TikTok and their subsidiaries have force fed children dangerous and harmful content with predatory algorithms, aided U.S. adversaries and worked against U.S. national interests at home and abroad, and failed to protect users' personal data.

What's worse: Following the success of TikTok, many of these platforms redesigned their platforms and algorithms to perform like TikTok.

So while the House Energy and Commerce Committee prepares to question TikTok CEO Shou Zi Chew, Members of Congress cannot lose sight of the fact that their concerns are the same ones civil society organizations, NGOs, academics, and activists have drawn attention to for years in other prevalent tech platforms.

Right now, lawmakers are weighing the virtues of a TikTok ban in the United States versus a forced divestiture from Chinese Communist Party-connected parent company ByteDance. Regardless of which direction lawmakers choose, focusing solely on TikTok does not fully get at the heart of the practices every platform engages in to cause so much harm.

We believe Congress' task is three-fold:

1. *Hold TikTok and other companies (Google, Apple, Amazon, and Meta) accountable for undermining U.S. national interests and endangering our national security.*
2. *Hold TikTok and other companies (Google, Apple, Amazon, and Meta)*

*accountable for their business models that are centered on designing addictive platforms for young Americans that cause depression, anxiety, eating disorders, and suicides – all in the name of increasing screen time to sell ads.*

3. *Hold TikTok and other companies (Google, Apple, Amazon, and Meta) accountable for their massive surveillance infrastructure, data harvesting, and failures to protect our data.*

Below is a quick guide for lawmakers to learn more about why they need to hold all tech platforms accountable:

### **National Security-Related Concerns**

#### *TikTok*

- Former TikTok employees [confirmed that “boundaries between TikTok and ByteDance were so blurry as to be almost non-existent.”](#)
- A Forbes [review found](#) that 300 TikTok & ByteDance employees with employment history at Chinese state media outlets, including 15 that appeared to be employed concurrently.
- ByteDance [owns two of China's most popular apps](#), where Chinese state media entities run popular accounts and the apps comply with strict Chinese censorship laws.
- Per former employees, TikTok’s Owner ByteDance [used a news app](#) on millions of phones to push pro-China messages.
- In a September 2022 Senate hearing, TikTok’s COO [avoided saying whether ByteDance would keep U.S. user data from the Chinese government](#) or whether ByteDance may be influenced by China.
- As a Chinese company, ByteDance [was required to comply with Chinese law](#) which has no process for appealing or protesting requests for data collection.
- A former trust and safety employee with TikTok [shared with Congressional leaders](#) that the platform was lying about spying from the Chinese government.
- The whistleblower [told congressional investigators that Project Texas does not go far enough](#) and that a truly leak proof arrangement for Americans’ data would require a “complete re-engineering” of how TikTok is run.
- The [Department of Justice and the FBI are both investigating](#) TikTok for allegations that they spied on American journalists critical of the platform.

#### *Meta*

- Ad Trackers [estimated revenue](#) from Chinese advertisers have access to U.S. user data and the revenue they produce for Facebook may exceed \$5 billion annually, making it the second largest revenue source for Facebook after the U.S.
- The Chinese government, through state-run media entities, [was a major purchaser of Facebook ads](#), spending hundreds of thousands of dollars per quarter.
- Despite Facebook being banned to Chinese users by the CCP, [Chinese media outlets have](#) more than one billion followers on Facebook.

- Facebook [set up a page for Chinese state media entity CCTV](#) to demonstrate promotion capabilities and attract more ad spending.
- Facebook [developed a censorship tool](#) in an attempt to court Chinese engagement.
- Facebook [declined to follow Twitter's lead in banning paid advertising](#) by state media entities in wake of Hong Kong protests.
- Facebook defended Chinese state media ads on Xinjiang as in compliance with company policies.
- A [study from the Center For Countering Digital Hate](#) found Chinese state media used Facebook to spread pro-Russian disinformation on Ukraine, including false narratives that NATO expansion is comparable to Hitler's control of Ukraine, that the U.S. is attempting to hide biolabs in Ukraine, and that the U.S. is using neo-Nazi organizations to suppress "rivals" in Ukraine.

### *Google*

- In an effort to court the Chinese market, [Google developed a censored version](#) of its platform for use in China and was forced to backtrack under pressure from human rights organizations.
- YouTube has [inconsistently enforced its labeling policy](#), allowing multiple Chinese state media channels to play videos without flagging content as state-sponsored.
- Chinese state media and local governments [paid YouTube influencers](#) to spread pro-China propaganda.
- YouTube [declined to take down pro-China influencer channels](#), claiming they weren't "linked to coordinated influence operations."
- Chinese state media [used Youtube to spread propaganda](#) related to Hong Kong protests.

### *Apple*

- Apple [reported \\$74 billion in annual sales](#) from China in September 2022, representing nearly 20% of the company's global sales.
- 155 of Apple's top 200 suppliers [are based in China](#).
- Amnesty International [recently stated](#) that "Apple has become a cog in the censorship machine, and that "if you look at the behavior of the Chinese government, you don't see any resistance from Apple."
- Apple [rolled out a China-specific software update](#) that limited the airdrop function that had been used by protesters to organize.
- Apple [provided customer data 96% of the time](#) when asked by the Chinese government.
- Apple [removed Taiwan flag emoji](#) from their keyboard for users in Hong Kong and Macau during pro-democracy protests in 2019.

### *Amazon*

- Amazon [made a heavy recruitment push](#) in early 2010s to attract Chinese sellers to its marketplace, including distribution of Chinese language tutorials and establishment of the "dragonboat" logistics system to connect Chinese goods with U.S. fulfillment centers.
- By the end of 2020, [nearly half of sellers in Amazon's top 10,000](#) were based in

China.

- The [vast majority of suppliers for Amazon-branded products](#), including Kindle and Echo devices, are based in China.
- Amazon [partnered with a Chinese state propaganda agency](#) to launch a China books portal in effort to grow support for Amazon in the country.
- Amazon [handed off cloud technology to Chinese companies](#) to continue operating AWS in China, allowing companies to monitor and take down content and collect customer information.
- Amazon [provides AWS services to Chinese surveillance company Hikvision](#), which is banned in the United States and has ties to the country's military.
- Amazon has [been accused by the USDA of aiding and abetting illegal imports](#) from China in violation of the Animal Health Protection Act and Plant Protection Act, which led to an outbreak of foot-and-mouth disease.
- Amazon's Twitch [spread disinformation regarding Ukraine](#) in the wake of Russia's invasion.

## **Harms to Children and Teens**

### *TikTok*

- Recently [unsealed documents](#) prove that TikTok parent ByteDance knew young people are more susceptible to being lured into trying dangerous stunts they view on the platform — known as viral challenges — because their ability to weigh risk isn't fully formed, which has led to death and suicide.
- [Researchers found](#) that TikTok's parent company ByteDance designed its Chinese equivalent app with design features similar to TikTok that "activate the reward centers of the brain" and "showed that areas involved in addiction were highly activated in those who watched personalized videos."
- [Leaked internal documents](#) show that TikTok's "ultimate goal" is adding daily active users by optimizing users' "retention" and "time spent" metrics – proving that their platform's business model is predicated on getting users addicted.
- [Reporting from the Wall Street Journal found that](#) "as a user's stream becomes more niche, they're more likely to encounter harmful content that is less vetted by moderators."
- A [non-profit study found](#) that TikTok may surface potentially harmful content related to suicide and eating disorders within minutes of them creating an account.
- A [Center for Countering Digital Hate study](#) found that upon starting new accounts for users aged 13 years old and pausing on content related to body image or mental health led users to be served pro-anorexia or suicide content within seconds.
- TikTok's parent ByteDance [harms U.S. children and teens by exposing them to harmful content and algorithms while protecting children in China](#) by requiring that users under the age of 14 register with Douyin's (TikTok's Chinese counterpart) heavily moderated "teen mode."
- In 2019, TikTok's predecessor Musical.ly [was fined \\$5.7 million by the Federal Trade Commission](#) for violating U.S. child privacy law.

## Meta

- Based on [recent reporting](#) and unsealed court records, Meta CEO Mark Zuckerberg was aware that Facebook and Instagram were designed to be addictive and detrimental to young people's mental health, particularly teen girls, but [lied to Congress under oath](#).
- In an effort to replicate the harmful TikTok platform and algorithm, Meta [recalibrated its product and algorithms](#) to emulate its platforms on TikTok and expand its base of young users despite knowing its products were already detrimental to youth mental health.
- Instagram had [planned to roll out an Instagram for Kids platform that was only shelved due to outcry](#) from parents and social media watchdog groups.
- Despite [leaked internal documents](#) laying out the problem that "thirty-two percent of teen girls said that when they felt bad about their bodies, Instagram made them feel worse," and adding that "teens blame Instagram for increases in the rate of anxiety and depression," Meta's senior leadership have done nothing to alter their platform or algorithm.

## Google

- In an effort to boost screen time on the platform, [YouTube redesigned their algorithm](#) to maximize views and increase profits from advertisers, which computer scientists criticized calling it an "addictive engine."
- After launching YouTube Kids, [consumer advocates filed a complaint with the FTC](#) noting that children were being served sexual content, advertising for alcohol, and promotion of unsafe behaviors.
- [Mental health experts warned](#) that YouTube is a growing source of anxiety and inappropriate sexual behavior among kids under the age of 13.
- Google and Youtube [violated children's privacy and settled a case](#) for a record \$170 million settlement brought by the FTC and New York Attorney General.
- In an effort to replicate the harmful TikTok platform and algorithm, [YouTube launched](#) YouTube Shorts as a TikTok clone.

## Apple

- A [2017 study found](#) that increased iPhone and smart phone usage led to increases in anxiety and depression among children and teens.
- Studies found that [increased iPhone usage was linked](#) to a doubling in the suicide rate among teenage girls.
- That [same study](#) "showed that those who spent more than five hours per day on electronic devices had almost twice the suicidal tendencies of those spent an hour or less per day."
- The [New York Times found](#) that Apple was cracking down on apps that fight iPhone addiction.

## Amazon

- [A recent report](#) shows that child predators are systematically using Amazon's Twitch to track and watch children.
- A [recent study from National Center on Sexual Exploitation](#) found that Amazon's Twitch was rife with sexual harassment, predatory grooming, child sexual abuse.

- Prominent [Twitch users campaigned](#) to have Amazon's Twitch remove gambling from their platform because it was leading to gambling addictions.
- [NBC News found](#) that Amazon's Wickr, an encrypted chat app, has "become a go-to destination for people to exchange images of child sexual abuse."
- Amazon was [under investigation by the FTC](#), which alleged that the voice-activated device collects and stores the transcripts of conversations the children have with it, along with information on what content the young users engage with on the device.

## **Massive Surveillance and Data Harvesting**

### *TikTok*

- A [cybersecurity firm review of TikTok](#) found data collection practices that were "overly intrusive" and suggested "the only reason this information has been gathered is for data harvesting."
- TikTok's [in-app browser includes code that can monitor keystrokes](#), user clicks on websites, making it possible for TikTok to capture sensitive information like credit card numbers and passwords.
- In a [September 2022 Senate hearing](#), TikTok's COO avoided saying whether ByteDance would keep U.S. user data from the Chinese government or whether ByteDance may be influenced by China.
- Internal TikTok meeting audio [revealed China-based ByteDance employees repeatedly accessed non-public data on U.S. tiktok users](#) despite the company's assurances on U.S.-based data storage.
- In 2019, TikTok's predecessor Musical.ly [was fined \\$5.7 million by the Federal Trade Commission](#) for violating U.S. child privacy law.

### *Meta*

- In 2011, Facebook [settled with the Federal Trade Commission](#) over allegations that it allowed private user information to be made public without warning.
- In 2013, a [Facebook bug exposed](#) the email addresses and phone numbers of six million users to anyone who had some connection to the user or knew at least one piece of their contact information.
- In 2014, Facebook [faced backlash for conducting a mood manipulation experiment](#) on more than 500,000 randomly selected users.
- In 2016, Trump consultant Cambridge Analytica [harvested private information from the Facebook profiles of more than 50 million users](#) without their permission in order to exploit huge parts of the American electorate.
- In 2018, Facebook [software bugs allowed the exposure](#) of personal information of nearly 50 million users.
- In 2019, the Federal Trade Commission [fined Facebook \\$5 billion dollars](#) over allegations that it violated a 2012 FTC order by being deceptive in how it protects consumer privacy and handles consumer data.
- In 2021, it came to light that Facebook [refused to notify more than 530 million users](#) whose personal data was stolen in a data breach sometime before August 2019.

## Google

- In 2019, Google and Youtube [violated children's privacy and settled a case](#) for a record \$170 million settlement brought by the FTC and New York Attorney General.
- Google [exposed the private data of hundreds of thousands of users](#) of the Google+ social network between 2015 and 2018, and did not disclose the glitch out of fears it could cause regulatory scrutiny.
- In 2022, the [Attorneys General of Texas, Washington, Indiana, and DC sued Google](#) alleging that it tracked users' locations after consumers believed they had disabled that feature.

## Apple

- According to a [report by independent researchers](#), Apple collects extremely detailed information on you with its own apps even when you turn off tracking – a direct contradiction of Apple's own description of how the privacy protection works.
- A [Washington Post investigation](#) into the iPhone's tracking protections found that they were “nowhere nearly as comprehensive as Apple's advertising might suggest.”
- In 2019, the [Wall Street Journal found](#) that 79 out of 80 of the iPhone apps they tested for tracking properties had an average of four trackers each.
- Apple has [known for years that apps on the app store were scamming iPhone users out of millions of dollars](#), yet failed to stop them from invading the app store.
- According to the [Washington Post](#), of the 1,000 highest-grossing apps on the App Store, nearly 2 percent are scams.
- A [review from Forbes](#) found that scam apps and fleeceware were rampant on the app store.
- In 2021, it was [found that some scam apps on Apple's app store made millions](#) of dollars and even stayed up on the marketplace for years.

## Amazon

- In June 2022, a [former Amazon employee was convicted for their role in the 2019 Capital One breach](#) that exposed the personal information of over 100 million people, including names, dates-of-birth, and social security numbers.
- Amazon's iRobot robot vacuums [captured sensitive pictures that were later leaked on social media](#) — including one of a woman sitting on the toilet.
- Amazon [employs thousands of workers around the world to listen to and transcribe audio captured by Amazon Alexa devices](#), while users may be unaware of the product's eavesdropping.
- Amazon [provides local police footage from users' Amazon's Ring product](#) without the owner's knowledge or consent.
- Amazon [was under investigation by the FTC](#), which alleged that the voice-activated device collects and stores the transcripts of conversations the children have with it, along with information on what content the young users engage with on the device.

**Conclusion:**

TikTok and its parent company ByteDance have endangered children and families, unnecessarily harvested our data, and threatened our national security through spying, data collection, and propaganda. Holding TikTok and China accountable are steps in the right direction, but doing so without holding other platforms accountable is simply not enough. Congress and the Biden Administration are right to be worried about TikTok and its enmeshed ties to the CCP. Lawmakers and regulators should use this week's hearing as an opportunity to re-engage with civil society organizations, NGOs, academics, and activists to squash all of Big Tech's harmful practices.

###