September 14, 2022

Geoffrey Cain, Senior Fellow for Critical Emerging Technologies, Lincoln Network

Written Testimony Before the Homeland Security and Governmental Affairs Committee
Social Media's Impact on Homeland Security

Chairman Peters, Ranking Member Portman, and Members of the Committee:

It is an honor to be invited to testify here on social media's impact on national security. Today, I will talk about one of the greatest technological threats facing our homeland security and democracy: TikTok, the social media app owned by the Chinese parent company ByteDance.

TikTok is the fastest-growing social media app ever and is expected to hit 1.8 billion users by the end of this year. Known for its fun and digestible video snippets, the app is enormously popular among celebrities and Generation Z users. It goes to great lengths to appeal to the sensibilities of the American market by loudly proclaiming progressive, democratic, egalitarian values. It posts messages on social media supporting inclusivity, diversity, LGBTQ+ rights, and pro-life causes.

All this is a distraction from the reality behind TikTok's parent company in China, called ByteDance. As an investigative journalist in China and East Asia for thirteen years, I have been detained, harassed, and threatened for my reporting on Chinese technology companies. ByteDance and its subsidiary TikTok have sought to distract us from well-documented ties to the Chinese Communist Party.

In internal meetings, ByteDance's leaders have extolled communist party virtues, pledging their absolute loyalty to a totalitarian government. The celebrity and cat videos are a distraction. TikTok is a major threat to our national security and freedom of discourse. Its parent company has censored Uyghur refugees who have suffered under a genocide now being carried out in China's western region of Xinjiang, as well as other heinous crimes.

TikTok claims that, despite reporting to executives from a company in the People's Republic of China, called ByteDance, it keeps the data of American and global users on TikTok separate from ByteDance's business operations in China. There, the leaders of the Chinese Communist Party (CCP) have repeatedly declared their hostility to our democracy and way of life.

Today, I will show you how TikTok has orchestrated a campaign of distraction and deflection to mask the alarming truth. Americans face the grave and unprecedented threat of software in our pockets that contains powerful surveillance and data-gathering capabilities, owned by private companies that must nevertheless comply with the dictates of the CCP, which has signaled its ambitions to assert global jurisdiction over private companies everywhere as a condition for doing business in China. TikTok is a disaster waiting to happen for our homeland security and the privacy of our citizens.

TikTok's Troubled Emergence in America

TikTok's explosive growth in America has been a troubling story of conflicting statements, broken promises, hollow reassurances, and profiteering complacency. We have TikTok executives here

today. According to their internal guidelines, if you ask them about the influence of their Chinese parent company ByteDance over the American product TikTok, executives must deceptively tell you that ByteDance is a separate parent company and that you should talk to ByteDance instead. They will attempt to confuse you, claiming that TikTok takes a localized approach, hiring local moderators, implementing local policies, and showing local content.[1]

TikTok executives will not tell you the real story about their ties to the world's most sophisticated and dystopian police state. They will not tell you about a Beijing-based engineer known as the "Master Admin" who had, according to leaked audio from internal company meetings, "access to everything" on the app.[2] Their employer does not give them the authority to tell the full truth. A leaked, 53-page public relations document that TikTok executives call their "Master Messages" tells employees to "Downplay the parent company ByteDance, downplay the China association, downplay AI."[3] They won't tell you that they report to ByteDance, and that ByteDance reports to the CCP.

The relationship between TikTok and ByteDance has been a problem from the start. Eight years ago, in 2014, the Chinese arm of the major Silicon Valley venture capital firm Sequoia Capital invested in TikTok's parent company ByteDance in China with a $500 million valuation, paving the way for its expansion into America. Sequoia Capital's China arm has been building ties to China's party elite—for example, by later hiring the daughter of a member of the CCP's powerful Standing Committee.[4]

TikTok's fast expansion into the American market was only possible because China has rigged the market, offering ByteDance vast market protection in China while banning competing American social media apps Facebook, Instagram, Twitter, and Google. In 2016, ByteDance initiated a $1 billion purchase of a Chinese-based music streaming company called Music.ly, popular among American teenagers. Nine months later, ByteDance merged Music.ly with its own software, cementing TikTok as the American version of its Chinese app, Douyin.

From the start, the acquisition was concerning. The *Financial Times* reported that ByteDance did not seek approval from the Committee on Foreign Investment in the United States (CFIUS), the government body that reviews foreign inflows into strategic and sensitive businesses in the U.S. According to the report, ByteDance executives believed they did not need to begin a CFIUS review because they were acquiring a Chinese company, not an American one.

This was a decision of questionable legality. Music.ly had an office in Los Angeles, placing this acquisition under the jurisdiction of CFIUS. CFIUS still has the authority to investigate and reverse the acquisition, which would force ByteDance to sell TikTok and terminate its American operations.

Other alarm bells sounded in the early days of TikTok in America. In 2018, ByteDance's and TikTok's founder and previous CEO, Zhang Yiming, wrote a letter promising Chinese regulators

---

[1] 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.

[2] Emily Baker-White, "Leaked Audio from 80 Internal TikTok Meetings Shows That U.S. User Data Has Been Repeatedly Access From China," *Buzzfeed*, June 17, 2022, https://www.buzzfeednews.com/article/emilybakerwhite/tiktok-tapes-us-user-data-china-bytedance-access.

[3] Chris Stokel-Walker, "Inside TikTok's Attempts to 'Downplay the China Association.'"

[4] Juro Osawa and Shai Oster, "Sequoia Capital's China Arm Employed Daughter of Politburo Member," *The Information,* September 9, 2022, https://www.theinformation.com/articles/sequoia-capitals-china-arm-employed-daughter-of-politburo-member.

that his company would follow "core socialist values," would introduce these "correct values into technology and products" and would ensure his products promoted the CCP's agenda. These "values," he wrote, included "strengthening the work of Party construction," "deepening cooperation with official Party media," and strengthening "content review" in line with these Party "values."[5]

ByteDance's public statements in China should be cause for alarm. American government employees, military personnel, and people in sensitive and strategic industries use TikTok. Because China has little separation between private business and the government's authoritarian ideology, ByteDance, like all Chinese companies, maintains an in-house Communist Party Committee mandated to enforce the political loyalty of employees in China. At a committee meeting in April 2018, ByteDance executives declared that their social media algorithm must be informed by the "correct political direction" and that content should "highlight socialist core values."

ByteDance engineers in China, not America, developed the algorithm that TikTok used in America. TikTok engineers employed in Mountain View, California reported to senior executives in China, where the company's Communist Party Committee set the course of ByteDance products.[6]

Researchers from the Citizen Lab, an internet research institute at the University of Toronto, found that the Chinese app Douyin and the American version TikTok use the same base code, but alter them for different markets.[7] Recent findings about the capabilities of TikTok code and data-gathering capabilities have been concerning. In August 2022, privacy researcher Felix Krause found that TikTok's browser contains code that can track users' keystrokes, including if they type in login information, passwords and credit card information. This is not a practice among major social media competitors. TikTok responded by claiming it uses this code for debugging and troubleshooting.[8]

We should take TikTok's claims with a grain of salt. Previously, in 2020, TikTok executives said they would end a similar feature that allowed TikTok to read users' Apple iOS clipboards, but never gave a clear date for the removal of the feature. Apple's clipboard allows users to save snippets of information on their phones which, for some users, could include sensitive military and government data, and could stay in TikTok's servers even if an iPhone user deletes it after a moment. Despite these promises to end the feature, an Apple software update later revealed TikTok was still snooping on the clipboard. It remains unclear if TikTok still has kept the feature, which it has not publicly clarified.[9]

TikTok and China's Human Rights Atrocities

---

[5] David Bandurski, "Tech Shame in the "New Era,"" China Media Project, April 11, 2018, https://chinamediaproject.org/2018/04/11/tech-shame-in-the-new-era/.

[6] Fergus Ryan, Audrey Fritz, and Daria Impiombato, "TikTok and WeChat," Austrian Strategic Policy Institute, September 8, 2020, https://www.aspi.org.au/report/tiktok-wechat.

[7] Pellaeon Lin, "TikTok vs Douyin: A Security and Privacy Analysis," Citizen Lab, March 22, 2021, https://citizenlab.ca/2021/03/tiktok-vs-douyin-security-privacy-analysis/.

[8] Paul Mozur, Ryan Mac, and Chang Che, "TikTok Browser Can Track Users' Keystrokes, According to New Research," *The New York Times*, August 19, 2022, https://www.nytimes.com/2022/08/19/technology/tiktok-browser-tracking.html.

[9] Joel Thayer, "On TikTok, It's All Fun and Games Until China Wants Your Info," *The Verge,* July 21, 2022, https://www.theverge.com/2020/6/26/21304228/tiktok-security-ios-clipboard-access-ios14-beta-feature.

When TikTok began seeing explosive growth in America, I was deeply worried as a foreign correspondent and investigative journalist in Xinjiang, China, where I was researching my second book, *The Perfect Police State: An Undercover Odyssey Into China's Terrifying Surveillance Dystopia of the Future*. This is a region where an estimated 1.8 million people from the ethnic Uyghur, Kazakh and other predominately Muslim minority groups have been held in a network of some 300 concentration camps—the largest internment of ethnic minorities since the Holocaust. The people of Xinjiang live under a total surveillance dystopia seemingly crafted out of a science fiction novel, erected with the help of Chinese and American technology companies. They are watched by China's surveillance network, SkyNet, which is powered by novel technologies in artificial intelligence, facial recognition, voice recognition, and biometric data collection. In December 2017, I made my final visit to Xinjiang. Within three days, I was detained by police and asked to leave.

I believed that ByteDance's and TikTok's expansion into the U.S. was ominous for our democracy, and I began following the story carefully, interviewing TikTok employees, users, and former Chinese government officials about their operations. A Uyghur technology worker from the regional capital, Urumqi, who helped establish the government's surveillance systems in Xinjiang, told me, "Of course ByteDance can spy for the CCP, and they do it all the time. Every Chinese app submitted the government's orders to send them all the data of sensitive users like Uyghurs and different ethnic groups. Why would TikTok be any different? It doesn't matter if those companies are operating in America or not."

His concerns were appropriate. A former employee claimed that ByteDance had an active role in trying to suppress news about the Uyghur genocide, attempting to build an algorithm that would suppress Uyghur livestreams that could potentially spread news of atrocities on the Chinese app.[10] In November 2020, TikTok public policy executive Elizabeth Kanter, testifying before the British parliament, said, "There was [*sic*] some incidents where content was not allowed on the platform, specifically with regard to the Uyghur situation."

The Uyghur genocide—declared a "genocide" by the State Department in January 2021 because of the erasure of an entire group, including through the forced sterilization of women—is the culmination of China's fascistic propaganda about the racial and cultural superiority of the dominant Han Chinese ethnic group. TikTok policies, implemented until 2019, have reflected these censorial party practices that uphold the myths about strength, power and purity.[11] Internal memos leaked to *The Intercept*, an investigative news website, instructed TikTok moderators globally to suppress video posts created by users whom they deemed too poor, ugly, or disabled, as well as to censor users who harmed "national honor."

---

[10] Isobel Asher Hamilton, "ByteDance Tried to Build an Algorithm to Censor Uighur Livestreams on TikTok's Chinese Sister App, a Former Employee Has Claimed," *Insider*, February 19, 2021, https://www.businessinsider.com/bytedance-uighur-livestreams-douyin-censorship-2021-2.

[11] TikTok says it has changed many moderation and content policies since 2019. Its internal public relations guidance tells employees to say: "We're a platform that's nearly 3 years old and we're operating in the scale of other big players. We take this responsibility seriously. In the early days, we made mistakes with our moderation policies and we take responsibility for them." 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.

Other guidelines penalized users for posting about the 1989 Tiananmen Square massacre and the Uyghur genocide.[12] It called these posts "violations," even if the users who posted them were not based in China. The memo instructed moderators to be on the lookout for videos with an "abnormal body shape," "ugly facial looks," "dwarfism," an "obvious beer belly," "too many wrinkles," "eye disorders," "dilapidated housing," "slums, rural fields" and many other "low quality" traits.[13]

As these revelations came to light, TikTok scrambled to repair its image for the U.S. market. It claimed it was implementing stronger privacy and content moderation policies and made the odd claim that these policies were in place to prevent online bullying, even though the leaked internal documents made no mention of anti-bullying.

TikTok also said data was stored in America and on a backup server in Singapore, not in Beijing, where the parent company is based. In August 2020, the CFIUS issued a divestment order to ByteDance, ordering it to sell TikTok to an American company. The order went unenforced and was later reversed in June 2021. TikTok continues to operate freely in America, under China's control.

The Oracle Failure

After these controversies, TikTok announced in September 2020 that it had selected American technology giant Oracle as a "technology partner," restructuring its operations with Oracle bidding to purchase part of TikTok's U.S. operations. Oracle didn't purchase TikTok in the end (no one did). Instead, TikTok struck an agreement with Oracle to migrate Americans' data to Oracle servers in the U.S. It was trying to convince the U.S. government that the personal data of Americans would not end up in the hands of China's government.

This plan has already failed on many counts. In June 2022, the news website *Buzzfeed* published material from leaked audio files from 80 internal TikTok meetings. The leaks revealed that Chinese engineers had already been accessing the data of Americans from September 2021 to January 2022, which could then be easily stored on Chinese servers, even by accident. The leaks contradicted the sworn Congressional testimony of a TikTok executive in October 2021, who claimed inaccurately that a "world-renowned, U.S.-based security team" decides who will have access to Americans' data. TikTok employees said on the recordings that they had to work through China-based teams to figure out the flows of American data.[14]

Second, TikTok announced it would maintain backup storage of Americans' data on its own servers. This would erase the benefits of storing the data on Oracle cloud servers. Third, Oracle, despite being an American company, is a dubious data protection partner for TikTok; there is strong reason to doubt the private data of Americans will be completely safe with Oracle as well. Mara

---

[12] 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.

[13] Sam Biddle, Paulo Victor Ribeiro, Tatiana Dias, "Invisible Censorship," *The Intercept*, March 16, 2020, https://theintercept.com/2020/03/16/tiktok-app-moderators-users-discrimination/.

[14] Emily Baker-White, "Leaked Audio from 80 Internal TikTok Meetings Shows that U.S. User Data Has Been Repeatedly Access from China," *Buzzfeed*, June 17, 2022, https://www.buzzfeednews.com/article/emilybakerwhite/tiktok-tapes-us-user-data-china-bytedance-access.

Hvistendahl, a longtime China journalist at *The Intercept*, has documented Oracle's egregious conflicts of interest selling data analytics software to Chinese police authorities for mass surveillance.[15]

These conflicts of interest and split loyalties between China's hostile authoritarianism and America's homeland security run deep. Oracle has inappropriately advertised its software services for the U.S. Department of Defense to potential Chinese police and security clients. Oracle has offered China's Ministry of Public Security, the powerful, rights-abusing policing body, the data analytics software that undergirds China's *1984*-style surveillance dystopia and crimes against humanity. This includes marketing software directly to Chinese police authorities in Xinjiang, where they are carrying out genocide against the minority Uyghur population.[16]

TikTok's Shadowy Corporate Structure

Even if TikTok stores the data on Oracle's servers in America, Oracle's and TikTok's deep exposure to China makes that data susceptible to the vague, powerful data collection laws that give the Chinese government sweeping powers. If China demands this data—which would happen in secret, if it hasn't happened already—both TikTok in America and its parent company ByteDance in China will have few ways of resisting through legitimate court hearings and court appeals in China. The sad reality is that ByteDance's and TikTok's corporate structure makes them accountable to the authoritarian demands of the Communist Party.

TikTok has claimed that its operations fall outside Chinese legal jurisdiction, so we do not need to worry about the privacy of Americans' data. This trite and deceptive answer does not address the inherent contradiction in ByteDance's corporate structure that makes it prone to CCP data meddling and legal orders.

In November 2021, ByteDance's co-founder and new CEO, Liang Rubo, announced that TikTok would be separated into a standalone business unit, allegedly separate from the six main business units of TikTok.[17] The goal was to appeal to American government regulators who were concerned about the lack of separation between the American TikTok app and the other Chinese business affiliates under ByteDance. The restructuring, however, was in name only. It does not represent a spin-off of TikTok.

What we know as "TikTok," with its main American office in Los Angeles, is really part of a shell company incorporated in the Cayman Islands. According to the Cayman's corporate registry, the director in charge of the ByteDance shell company is Liang Rubo, who is also listed on ByteDance's website as the CEO of the ByteDance corporation in China. Because both the Cayman and Chinese companies have the same person in charge, it is difficult to take TikTok executives seriously when they argue that these are in fact separate companies divided by an impenetrable wall.[18] The Cayman

---

[15] Mara Hvistendahl, "How Oracle Sells Repression in China," *The Intercept*, February 18, 2021, https://theintercept.com/2021/02/18/oracle-china-police-surveillance/.

[16] Mara Hvistendahl, "How Oracle Sells Repression in China," *The Intercept*, February 18, 2021, https://theintercept.com/2021/02/18/oracle-china-police-surveillance/.

[17] Coco Feng, "ByteDance Carves Out TikTok as World's Most Valuable Technology Unicorn Finds Way to Satisfy U.S.-China Regulatory Demands," *South China Morning Post*, November 2, 2021, https://www.scmp.com/tech/article/3154537/bytedance-carve-out-tiktok-worlds-sole-hectocorn-splits-six-units-delineating.

[18] Brooks Barnes and Jack Nicas, "Disney's Head of Streaming Is New TikTok CEO," *The New York Times*, May 18, 2020, https://www.nytimes.com/2020/05/18/business/media/tiktok-ceo-kevin-mayer.html.

Islands are a notorious offshore tax and regulatory haven with little transparency, where Chinese kleptocrats evade American regulatory pressure.

The fuzzy corporate structure has troubling implications for Americans' private data. TikTok's privacy policy states: "We may share all of the information we collect with a parent, subsidiary, or other affiliate of our corporate group." TikTok does not clarify the definition of "our corporate group." Worded this way, TikTok executives have given themselves enormous latitude to share data with whomever they want within their parent ByteDance company, whether in China or the Cayman Islands shell company, despite promising to keep that data out of China's hands.

TikTok executives might decide to share data with ByteDance's key subsidiary in China, called Beijing ByteDance Technology. Here's the danger: the Chinese government owns a 1 percent stake in Beijing ByteDance Technology and has installed its own director on the subsidiary's board.[19] Yet under the privacy policy, TikTok might be contractually clear if American users brought a legal claim against the company for allowing their private data to end up in the hands of Chinese authorities, through Beijing ByteDance Technology.

The Vast Intrusions of Chinese Data Law

TikTok's claims that its America-based data is not subject to Chinese law reveals an egregious misrepresentation of the Chinese legal system. Increasingly, China is asserting global legal jurisdiction and is using this self-proclaimed authority to pressure American and other foreign companies with ties in China. China does not operate under the principle of rule of law, but rule by the Party. The Party has the sweeping authority to enforce a collection of vague laws that criminalize the refusal to hand over the data of anyone, often anywhere in the world, it deems a threat.

One regulation, put in force in January 2021, allows China's Commerce Ministry to tell international companies to choose between complying with the extraterritorial regulations of China or the U.S., including the various sanctions or export controls now in force under U.S. law. Chinese courts can then hold companies liable for complying with American restrictions on Chinese commerce unless the Commerce Ministry grants them a waiver.[20] If ByteDance were to treat TikTok as a separate business unit and submit to American government orders to, say, divest and sell TikTok, ByteDance might find itself in legal trouble in China, and pressured to hand over Americans' data in Chinese court.

Another venue for harassment is the Data Security Law, passed in June 2021, giving China's government vast powers over the regulation and collection of "core data," a vague term that applies to any data that includes "national security, lifelines of the national economy, important aspects of people's lives, and the major public interest."[21] If any American TikTok data ends up on China-based servers, as the leaked audio files obtained by *BuzzFeed* show can easily happen, the CCP would have no trouble asserting the legal authority to obtain that data on "national security" grounds.

---

[19] Yingzhi Yang and Brenda Goh, "Beijing took stake and board seat in key ByteDance domestic entity this year," August 17, 2021, https://www.reuters.com/world/china/beijing-owns-stakes-bytedance-weibo-domestic-entities-records-show-2021-08-17/

[20] Amy Qin, "China's New Rules Could Hit U.S. Firms and Send a Message to Biden," Amy Qin, *The New York Times*, January 9, 2021, https://www.nytimes.com/2021/01/09/business/china-rules-trump-biden-sanctions.html.

[21] "Data Security Law of the People's Republic of China," June 10, 2021, http://www.npc.gov.cn/englishnpc/c23934/202112/1abd8829788946ecab270e469b13c39c.shtml

These laws only scratch the surface of China's broad and recent judicial expansion over the data of private citizens anywhere in the world. In June 2020, China passed the Hong Kong National Security Law, asserting extraterritorial jurisdiction over non-citizens of the People's Republic of China and Hong Kong, even if they live beyond China's borders, for collusion with "foreign forces."[22]

As of July 2022, China has charged at least 119 people under the law, which is usually targeted at political dissidents.[23] But the law's wording gives vast powers for the Chinese government to charge a person, anywhere in the world, including a TikTok or ByteDance executive traveling through Hong Kong, should that executive cooperate, for instance, with U.S. government requests to protect the data of American military personnel. TikTok closed its Hong Kong office in July 2020 and stopped offering the app in Hong Kong. This, however, does nothing to shield TikTok and its users from the ubiquitous and global territorial powers of the Hong Kong National Security Law.

Finally, two other sweeping laws, the 2015 National Security Law and the 2017 National Intelligence Law, assert similar government powers over private data in China and would apply to ByteDance and potentially its Caymans subsidiary TikTok.

The 2015 National Security Law states vaguely: "Citizens of the People's Republic of China, all state organs and armed forces, political parties and mass organization, enterprises, public institutions and other social organizations, all have the responsibility and obligations to preserve national security." This wording will compel ByteDance to fulfill any data obligation imposed by the Chinese government under the guise of "national security."[24]

The 2017 National Intelligence Law creates the obligation of "Chinese citizens to support national intelligence work," or face detention and possible criminal charges.[25] This law, of course, would apply to ByteDance and its executives in China, should Chinese intelligence agencies want to pressure them to hand over data on American government and military users gathered through TikTok.

Senators, I hope my testimony today will inform decisions you might be called upon to make about the TikTok threat. I hope that my summary of TikTok's connections to the CCP, data-gathering practices, broken promises, and pattern of deception has made a case to open a CFIUS review, once again. This review would potentially force ByteDance to sell TikTok to a more trustworthy company. It would be our best option moving forward. Thank you for having me.

---

[22] Human Rights Watch, "China: New Hong Kong Law a Roadmap for Repression," July 29, 2020, https://www.hrw.org/news/2020/07/29/china-new-hong-kong-law-roadmap-repression.

[23] Selina Cheng and Elliot Bentley, "How China's National Security Law Silences Hong Kong," July 1, 2022, https://www.wsj.com/articles/how-chinas-national-security-law-silences-hong-kong-11656673119.

[24] "National Security Law," July 1, 2015, https://www.chinalawtranslate.com/en/2015nsl/.

[25] Bonnie Girard, "The Real Danger of China's National Intelligence Law," February 23, 2019, https://thediplomat.com/2019/02/the-real-danger-of-chinas-national-intelligence-law/.