EXHIBIT 1

Redacted Version

FOR OFFICIAL USE ONLY

UNITED STATES DEPARTMENT OF COMMERCE
Office of Intelligence and Security
Deputy Assistant Secretary for Intelligence and Security
Washington, D.C. 20230

September 17, 2020

MEMORANDUM FOR THE SECRETARY

THROUGH: Rob Blair
Director
Office of Policy and Strategic Planning

FROM: John K. Costello
Deputy Assistant Secretary for Intelligence and Security
Office of Intelligence and Security

SUBJECT: Proposed Prohibited Transactions Related to TikTok Pursuant to Executive Order 13942

I. INTRODUCTION

On August 6, 2020, President Trump signed Executive Order ("EO") 13942, "Addressing the Threat Posed by TikTok, and Taking Additional Steps to Address the National Emergency With Respect to the Information and Communications Technology and Services Supply Chain" declaring that TikTok, a short video sharing application owned by the Chinese company ByteDance Ltd. ("ByteDance" or the "Company"), poses a threat to the national security, foreign policy, and economy of the United States. EO 13942 serves as an update to EO 13873, "Securing the Information and Communications Technology and Services Supply Chain." EO 13942 directs you to identify and prohibit transactions within 45 days. This memorandum serves to recommend a set of business-to-business transactions related to TikTok's operation in the United States that should be prohibited to address the national security threat posed by TikTok and to satisfy your obligation under the EO. The Department has carefully considered EO 13942 and other available information regarding TikTok's structure and operations. This includes consideration of publicly available reporting, classified or otherwise protected information, and information from parent company ByteDance.

The President concluded that TikTok, a messaging and social media application owned by ByteDance, a Chinese company, poses a threat to the national security, foreign policy, and economy of the United States. This memorandum contains an additional, unclassified threat analysis sufficient to demonstrate the national security risk that ByteDance and TikTok present to the United States. Assessments by the U.S. Intelligence Community ("USIC") and the Department of Homeland Security have reached concurrent and similar conclusions. Their assessments are included in Appendix A and B, respectively, and they contain classified, privileged, or otherwise protected information.

.

II. BACKGROUND

A. Background on ByteDance

ByteDance, headquartered in Beijing, was founded in 2012 by former Microsoft engineer and entrepreneur Zhang Yiming.[1] Specializing in artificial intelligence (AI) and machine-learning enabled content platforms, the Company's operations surpassed more than one billion users across its apps in June 2019, with many of those users residing outside of China. [2,3]

The Company's domestic products include Toutiao, a personalized news aggregator, and Douyin, a short video service, both of which are hugely popular inside China. ByteDance's international products include TikTok, the global version of Douyin, Helo, a social media platform focused on the Indian market, and BaBe (Baca Berita), Indonesia's leading news and content app.[4]

ByteDance successes have been attributed to its algorithm, which tailors content for users.[5,6] The Company has kept its algorithm mostly shrouded; however, Yiming has explained that it is powered through AI and machine learning. [7,8] This recommendation system has long been considered the Company's core asset and driving force behind the growing user base and advertiser revenue.[9]

The Company has made strategic investments in the AI and technology, media, and telecom ("TMT") sectors.[10,11,12,13] In relation to its Toutiao application, the Company's investments have been interpreted as wide sweeping ambitions of a company possessing the world's leading destination for online content.[14]

As of November 2019, ByteDance had over 60,000 employees and 15 research and development centers around the globe, potentially including ByteDance's Mountain View Location in California.[15][16] In April 2018, ByteDance announced that it would collaborate with the Berkeley Artificial Intelligence Research Lab at the University of California, Berkeley. The two parties stated that they were exploring

---

[1] https://www.aspi.org.au/report/mapping-more-chinas-tech-giants
[2] https://www.aspi.org.au/report/mapping-more-chinas-tech-giants
[3] https://www.cnn.com/2019/06/20/tech/tiktok-bytedance-users/index html
[4] https://chinatechmap.aspi.org.au/#/company/bytedance
[5] https://www.forbes.com/sites/bernardmarr/2018/12/05/ai-in-china-how-buzzfeed-rival-bytedance-uses-machine-learning-to-revolutionize-the-news/#37f1752840db
[6] https://www.ft.com/content/d7d1eff2-c307-11e8-95b1-d36dfef1b89a
[7] https://technode.com/2019/09/29/bytedance-testing-recommendation-algorithm-enterprise-service/
[8] https://digital.hbs.edu/platform-rctom/submission/bytedance-ai-application-secrete-sauce-behind-the-worlds-most-valuable-private-startup/
[9] https://technode.com/2018/01/12/toutiao-algorithm/
[10] https://www.fastcompany.com/company/bytedance
[11] https://cn.linkedin.com/in/fenghai
[12] https://www.spglobal.com/marketintelligence/en/news-insights/trending/-UcopxsTH0viBoRZyrj2KQ2
[13] https://pandaily.com/bytedance-invests-182-million-in-sports-community-platform/
[14] https://alltechasia.com/toutiaos-3-acquisitions-show-global-ambitions/
[15] https://www.reuters.com/article/us-bytedance-tiktok-exclusive/exclusive-tiktok-owner-bytedance-moves-to-shift-power-out-of-china-sources-idUSKBN2341VJ
[16] https://www.bytedance.com/en/

joint research projects and academic exchanges.[17] ByteDance has grown its portfolio of applications across 150 markets and 75 languages.[18] "In late 2018, a US$3 billion round of investment led by Japanese tech conglomerate Softbank Group valued the company at US$78 billion. Other major investors include the Chinese affiliate of U.S. venture capital firm Sequoia Capital, U.S. private equity investor KKR, Chinese investment firm Hillhouse Capital and corporate venture unit SIG Asia."[19] In May 2020, ByteDance was valued at around $100 billion.[20]

B. Background on the TikTok mobile application

TikTok, a short-form video app, is ByteDance's most successful international product.[21,22] TikTok users watch, create, and share 15-second videos shot on cellphones. The application generates revenue through in-app purchases and advertisements.[23] The app has a global audience that has grown to more than 700 million users in just a few years.[24,25] ByteDance achieved that meteoric growth, in part, by investing US$1 billion into ads on the social platforms of its Western rivals Facebook, Facebook-owned Instagram, and Snapchat.[26]

The TikTok app was launched in the United States in May 2017. In November 2017, ByteDance acquired Musical.ly, an American lip-syncing application, for $850 million and merged it with its TikTok app.[27] The company then formally merged and integrated Musical.ly and TikTok, rebranding Musical.ly as TikTok and discontinuing Musical.ly as a standalone app in 2018.[28] In the first quarter of 2018, TikTok was the most downloaded iPhone app worldwide, topping Facebook, YouTube and Instagram. According to mobile intelligence firm Sensor Tower in November 2019, TikTok passed 1.5 billion downloads worldwide on the App Store and Google Play.[29] TikTok's popularity is predominately amongst a younger audience. According to October 2019 reporting surrounding a leaked company document used to solicit advertisers, "the majority of TikTok users (69%) are from Generation Z (ages 16 to 24), while 25% are age 25 and older. Most users are also female (60%). In the U.S., TikTok has more than 30 million monthly active users who spend, on average, 46 minutes on the app per user per day. Globally, the number of monthly active users is 800 million."[30]

III. THE NATIONAL SECURITY, FOREIGN POLICY, AND ECONOMIC RISK TIKTOK POSES TO THE UNITED STATES

[17] https://www.prnewswire.com/news-releases/bytedance-partners-with-berkeley-artificial-intelligence-research-lab-to-foster-future-ai-innovators-and-entrepreneurs-300623346 html
[18] https://www.linkedin.com/company/bytedance
[19] https://www.aspi.org.au/report/mapping-more-chinas-tech-giants
[20] https://fortune.com/2020/08/05/microsoft-tiktok-sale-valuation-price-cost-worth-bytedance-deal/
[21] https://www.aspi.org.au/report/mapping-more-chinas-tech-giants
[22] https://digiday.com/media/everything-you-need-to-know-about-bytedance-the-company-behind-tiktok/
[23] https://www.investopedia.com/what-is-tiktok-4588933
[24] https://www.aspi.org.au/report/mapping-more-chinas-tech-giants
[25] https://digiday.com/media/everything-you-need-to-know-about-bytedance-the-company-behind-tiktok/
[26] https://www.aspistrategist.org.au/the-clocks-ticking-for-regulators-on-tiktok/
[27] https://www.ft.com/content/d7d1eff2-c307-11e8-95b1-d36dfef1b89a
[28] https://www.vox.com/culture/2018/12/10/18129126/tiktok-app-musically-meme-cringe
[29] https://www.cnet.com/news/tiktok-hits-1-5-billion-downloads-report-says/
[30] https://digiday.com/media/everything-you-need-to-know-about-bytedance-the-company-behind-tiktok/

For the reasons that follow, we believe that TikTok presents the following risk to the national security, foreign policy, and economy of the United States consistent with the President's determination in EO 13942.

A. Threat

1. The People's Republic of China ("PRC") presents a national security, foreign policy, and economic threat to the United States given its long-term effort to conduct espionage against the U.S. Government, corporations, and persons.

The threats flowing to the United States from PRC espionage activities are well-recognized. For example, according to the U.S. Intelligence Community's 2019 Worldwide Threat Assessment, the PRC presents a persistent cyber espionage threat and a growing threat to our core military and critical infrastructure systems. Additionally, according to Federal Bureau of Investigation ("FBI") Director Christopher Wray, PRC intelligence and economic espionage presents the greatest long-term threat to U.S. national security and economic security.[31] The PRC remains the most active strategic competitor responsible for cyber espionage against the U.S. Government ("USG") and U.S. corporations, allies, and persons. The USIC has assessed that Beijing will continue to authorize cyber espionage against key U.S. technology sectors when doing so addresses a significant national security or economic goal not achievable through other means. Additionally, the USIC remains concerned about the potential for PRC intelligence and security services ("PRCISS") to use Chinese information technology firms as routine and systemic espionage platforms against the United States and its allies.[32] The PRC's continued use of traditional espionage, [33,34,35] intellectual property theft of U.S. corporations, and theft of personally identifiable information ("PII") illustrate the PRC's intention to use bulk data collection for economic and national security activities that are hostile to the economic and national security interests of the United States.[36]

The FBI notes that it is the PRC's and the Chinese Communist Party's ("CCP") goal to introduce, understand, assimilate, and re-innovate foreign technology and knowledge to gain a technological edge. The PRC has demonstrated that it will achieve this goal by any means necessary, most notably through theft of foreign intellectual property.[37] The PRC Government has engaged in data collection on a massive scale across multiple domains as a means of generating information to enhance state security—and the political security of the CCP.[38] A report from Australian Think Tank Australian Strategic Policy Institute ("ASPI") describes the PRC Government's intent to use bulk data collection to support its efforts to shape, manage and control its global operating environment, and to generate cooperative and

---

[31] https://www.fbi.gov/news/speeches/the-threat-posed-by-the-chinese-government-and-the-chinese-communist-party-to-the-economic-and-national-security-of-the-united-states

[32] https://www.dni.gov/files/ODNI/documents/2019-ATA-SFR---SSCI.pdf, page 5

[33] https://www.justice.gov/opa/pr/former-cia-officer-arrested-and-charged-espionage

[34] https://www.justice.gov/opa/pr/northern-california-resident-charged-acting-illegal-agent

[35] https://www.justice.gov/opa/pr/former-intelligence-officer-convicted-attempted-espionage-sentenced-10-years-federal-prison

[36] See Appendix C for a list of Department of Justice cases that involve Chinese espionage.

[37] https://www.fbi.gov/file-repository/china-exec-summary-risk-to-corporate-america-2019.pdf/view

[38] https://www.aspi.org.au/report/engineering-global-consent-chinese-communist-partys-data-driven-power-expansion

coercive tools of domestic control.[39] The data collected and used by the PRC to these ends comes in many forms, including text, images, video, and audio. Large data sets can reveal patterns and trends in human behavior, providing a "pattern of life" that can be used to facilitate intelligence and surveillance targeting, particularly when aggregated with other data sets. Bulk data, like images and voice data, can also be used to train algorithms for facial and voice recognition. [40]

According to U.S. officials and analysts, the PRC is building massive databases of Americans' personal information. Evidence suggests that the PRC's pattern of targeting large-scale databases is a tactic used by the Chinese government to further its intelligence-gathering and to understand more about who to target for espionage, whether electronically or via human recruitment."[41] Once harvested, the data can be used to glean details about key government personnel and potential spy recruits, or to gain information useful for intelligence targeting and surveillance.[42,43]

Since 2012, more than 80% of the economic espionage cases brought by the Department of Justice's ("DOJ") National Security Division have implicated China and the frequency of cases continues to rise.[44,45] As reflected by recent DOJ indictments, the PRC continues demonstrated an intent and capability to collect vast quantities of sensitive data including corporate trade secrets related to U.S. military technology,[46] research related to COVID-19 vaccines, [47] and PII.[48,49,50] For example, in May of 2019, DOJ charged two Chinese nationals with conspiracy and intentional damage to a protected computer related to the hacking of Anthem, Inc. and stealing the sensitive personal data of approximately 78.8 million Americans in 2015.[51] January of 2020, DOJ charged four members of the People's Liberation Army, the armed forces of the PRC, with conspiracy, fraud and espionage related to the hacking into protected computers of Equifax Inc. and stealing the sensitive personal information of 145 million Americans in 2017.[52] In August of 2017, DOJ charged a Chinese national with conspiracy related to the Office of Personnel Management data breach, announced in 2015, where sensitive personal data of millions of current and former USG employees was stolen.[53] These are just a few of the numerous examples of the PRC's efforts to collect U.S. PII and sensitive personal data.

---

[39] https://s3-ap-southeast-2.amazonaws.com/ad-aspi/2019-10/Engineering%20global%20consent%20V2.pdf?eIvKpmwu2iVwZx4o1n8B5MAnncB75qbT

[40] http://webcache.googleusercontent.com/search?q=cache:HRPDTs985OIJ:https://www.technologyreview.com/2020/08/19/1006455/gtcom-samantha-hoffman-tiktok/&hl=en&gl=us&strip=1&vwsrc=0

[41] Rich Barger, Chief Intelligence Officer of ThreaetConnect, a Northern Virginia Cybersecurity Firm.

[42] https://www.washingtonpost.com/world/national-security/in-a-series-of-hacks-china-appears-to-building-a-database-on-americans/2015/06/05/d2af51fa-0ba3-11e5-95fd-d580f1c5d44e_story html

[43] See Appendix D for notable examples of Chinese government or government-affiliated groups targeting U.S. personally identifiable information.

[44] https://www.cnbc.com/2019/09/23/chinese-theft-of-trade-secrets-is-on-the-rise-us-doj-warns.html

[45] https://www.justice.gov/opa/information-about-department-justice-s-china-initiative-and-compilation-china-related

[46] https://www.justice.gov/opa/pr/two-chinese-hackers-working-ministry-state-security-charged-global-computer-intrusion

[47] https://www.justice.gov/opa/pr/two-chinese-hackers-working-ministry-state-security-charged-global-computer-intrusion

[48] https://www.justice.gov/opa/pr/member-sophisticated-china-based-hacking-group-indicted-series-computer-intrusions-including

[49] https://www.justice.gov/opa/pr/chinese-military-personnel-charged-computer-fraud-economic-espionage-and-wire-fraud-hacking

[50] https://www.cnn.com/2017/08/24/politics/fbi-arrests-chinese-national-in-opm-data-breach/index.html

[51] https://www.politico.com/story/2019/05/09/chinese-hackers-anthem-data-breach-1421341

[52] https://www.nytimes.com/2020/02/10/us/politics/equifax-hack-china html

[53]https://federalnewsnetwork.com/workforce/2017/08/fbi-arrest-may-be-first-linked-to-opm-hack/

2. The CCP exerts influence over private Chinese companies such as ByteDance and its employees through direct ties to personnel and corporate 'Party Committees.'

Corporate CCP Committees (*e.g.* Party Committees) are a mechanism through which Beijing expands its authority and supervision over nominally private or non-governmental organizations, creating different nuances of corporate governance with Chinese characteristics. [54] As of 2017, Party Committees existed in around 70 percent of 1.86 million private owned companies in China. [55,56,57] Party Committee is formed by a group of senior CCP members who are given a leadership position inside public and private companies operating in China. The 2012 Constitution of the Communist Party of China provides the legal framework for this activity. Within private enterprises, the Party Committee implements CCP's policies and operates through the Trade Union and the Communist Youth League Organization.

According to press reporting, Party Committees have explicit roles even within foreign companies operating in the PRC, which has raised debates especially among the community of investors involved in joint ventures (JVs) with state-owned enterprises. Even if Chinese PRC Law regulates the establishment of Party Committees in foreign invested enterprises (both JVs and fully owned) without requiring governance roles for their members, recent trends in officials' attitudes — which are oriented toward the demand for more power — indicate accelerating interference by the CCP in corporate activities in the PRC. That suggests that these positions are not merely symbolic, but rather an eventual source of political pressure around the boardroom. [58]

ByteDance has significant and close ties to the CCP which could potentially be leveraged to further their agenda and exact pressure on ByteDance. In October of 2018, the All-China Federation of Industry and Commerce and the United Front Work Department of the Central Committee of the Communist Party of China published listed Mr. Zhang, as one of their "top 100 outstanding private entrepreneurs at the 40th anniversary of reform and opening up". According to press reporting in August 2020, the CCP has more than 130 committee members embedded at ByteDance's Beijing office in managerial positions.[59] This was a partial listing obtained by the press, and it remains unclear exactly how many of ByteDance's 60,000 employees across 230 global offices are Party or Committee members. It is also reported that TikTok has close CCP ties through its parent company, ByteDance, which employs over 130 CCP members as a part of an embedded CCP committee and many of whom

---

[54] https://www.chinabusinessreview.com/fact-sheet-communist-party-groups-in-foreign-companies-in-china/
[55] https://thediplomat.com/2019/12/politics-in-the-boardroom-the-role-of-chinese-communist-party-committees/
[56] https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwir3cKxo9DrAhUponIEHenaAIAQFjAAegQIAxAB&url=https%3A%2F%2Fwww.acga-asia.org%2Ffiles.php%3Faid%3D158%26id%3D1212&usg=AOvVaw0H3c8Zr4es4RXAJN2dMdA_, pg 42
[57] https://www.scmp.com/economy/china-economy/article/2174811/chinese-communist-party-needs-curtail-its-presence-private
[58] https://thediplomat.com/2019/12/politics-in-the-boardroom-the-role-of-chinese-communist-party-committees/
[59] https://www.theepochtimes.com/tiktoks-parent-company-employs-ccp-members-in-its-highest-ranks_3451561 html?ref=brief_News&utm_source=morningbrief&utm_medium=email&utm_campaign=mb&__sta=vhg.uosvpxsbnsmql.sjsqobf%7CJJT&__stm_medium=email&__stm_source=smartech

hold management positions.[60][61] There are bounty of examples of CCP activities within ByteDance that combined illustrate the part is deeply ingrained in the company. A few illustrative examples:

- According to September 2020 Chinese reporting, ByteDance established a party branch in in October 2014.[62] In April 2017, the Company then established a party committee consisting of party branches in the public affairs, technical support, and compliance operation department groups.[63,64,65] According to Chinese press reporting, Bytedance has more party members and party organizations and is more "red," insiders pointed out, as compared with other Internet companies.[66]

- In June 2018, the Bytedance Party Committee and the Party School of the Central Committee of the Communist Party of China jointly organized a theme party day event. Bytedance party member employees "faced the party flag, raised their right hand, clenched their fists, and reiterated their guarantee as a party member and vowed to never betray the party."[67,68,69]

- In March 2020, the Minister of Propaganda Department of the Fujian Provincial Party Committee visited the Bytedance factory in Fujian. During the visit, the minister told ByteDance that he hoped that the company would use its advantages in new media and new technologies to further spread and interpret "Xi Jinping Thought."[70,71,72,73]

In 2018, ByteDance drew the attention of PRC authorities which publicly shamed and reprimanded the company for its platforms' deviation from Party and State agendas. This resulted in a public atonement by the founder and CEO, Zhang Yiming, and an organizational restructuring. CCP infrastructure has been successfully built throughout ByteDance and its subsidiaries, where it can now leverage the access and power of the company's assets to further Party and State goals and objectives.[74,75,76,77,78]

According to Chinese press reporting in July 2020, a CCP event was held inside the corporate headquarters of ByteDance in Beijing's Haidian District, showing employees and CCP members holding

[60] https://www.thetimes.co.uk/article/video-app-linked-to-china-s-ruling-party-8c7j3ljlj
[61] https://www.theepochtimes.com/tiktoks-parent-company-employs-ccp-members-in-its-highest-ranks_3451561.html
[62] https://c.epochtimes.today/37385
[63] https://c.epochtimes.today/37385
[64] http://politics.people.com.cn/n1/2018/0615/c1001-30062480.html
[65] http://www.ce.cn/xwzx/gnsz/gdxw/201806/15/t20180615_29446989.shtml
[66] https://chinadigitaltimes net/chinese/2020/08/cdt导览党组织-中国互联网公司的标配
[67] https://c.epochtimes.today/37385
[68] http://politics.people.com.cn/n1/2018/0615/c1001-30062480.html
[69] http://www.ce.cn/xwzx/gnsz/gdxw/201806/15/t20180615_29446989.shtml
[70] https://c.epochtimes.today/37385
[71] http://politics.people.com.cn/n1/2018/0615/c1001-30062480.html
[72] http://www.ce.cn/xwzx/gnsz/gdxw/201806/15/t20180615_29446989.shtml
[73] https://archive.fo/fBKTa#selection-305.3-387.54
[74] https://chinamediaproject.org/2018/04/06/china-to-purge-online-video-services/
[75] http://www.sapprft.gov.cn/sapprft/contents/6582/363639.shtml
[76] https://foreignpolicy.com/2019/01/16/ByteDance-cant-outrun-beijings-shadow/
[77] https://www.wsj.com/articles/tiktok-looking-at-ways-to-shake-off-its-ties-to-china-11574073001
[78] https://edition.cnn.com/2018/11/02/tech/china-tech-communist-party/index html

a communist banner – making the close ties between the corporation and the CCP clear.[79] The event was held by the CCP branch of the Information and Communication Department and the Haidian District Overseas Chinese Federation and was titled, "Never forget the original intention, remember the mission, and promote the new era of Overseas Chinese Federation information communication work."[80]

There are a host of examples demonstrating the CCP's efforts to pressure on ByteDance. In April 2018, ByteDance received significant scrutiny and criticism by Chinese state-run media for alleged content violations on its Neihan Duanzi application. Neihan Duanzi was a popular parody and meme application hosted on Toutiao, or Jinri Toutiao, its news and information platform. This led to the PRC's top media regulator, the State Administration of Press, Publication, Radio, Film, and Television (SAPPRFT), to issue "rectification measures" against the company.[81] SAPPRFT deemed ByteDance to be in violation of public opinion, having violated "social morality," and demanded the permanent shut down of the Neihan Duanzi application, which circulated jokes, humorous videos, and memes, for having spread "vulgar" content.[82] SAPPRFT also compelled the company to draw inferences from this action for its other products.[83]

ByteDance founder and CEO Zhang Yiming issued a public apology letter in April 2018, in which he signaled his intent to correct his products to comply with State and Party directives, including the promotion of Party-controlled media.[84] He wrote that, "our product took the wrong path, and content appeared that was incommensurate with socialist core values." Yiming promised to "further deepen cooperation with authoritative [official party] media, elevating distribution of authoritative media content, ensuring that authoritative [official party] media voices are broadcast to strength."[85] Like all Chinese technology companies, ByteDance is reliant on government issued licenses to operate.[86] This letter provides deep insight into Yiming's personal intent to align with the PRC and CCP, the reciprocating effect for his company and products, as well as the inevitable rite of passage Chinese companies must make in order to exist within China's socialist market economy.[87] ByteDance complied by shutting Neihan Duanzi and announced the hiring of 2,000 moderators tasked with reviewing content with a preference on hiring candidates with a, "strong political sensitivity."[88]

3. PRC Law requires that companies subject to PRC Jurisdiction, such as ByteDance, assist with PRCISS intelligence and surveillance efforts.

Over the last several years, the PRC government has actively worked to increase its influence over all Chinese companies, and citizens, through new laws and regulations.[89] Of these laws, the 2017

---

[79] https://c m.163.com/news/a/EL1772BO05322C4C.html?fbclid=IwAR0tOOxaB0BYBVFOwxfQQ5Q6Vv8O5MvRFTdGLiIItnagv8KyQTZuz8cPmgA

[80] https://www.taiwannews.com.tw/en/news/3982027

[81] https://chinamediaproject.org/2018/04/06/china-to-purge-online-video-services/

[82] http://www.sapprft.gov.cn/sapprft/contents/6582/363639.shtml

[83] http://www.sapprft.gov.cn/sapprft/contents/6582/365922.shtml

[84] https://chinamediaproject.org/2018/04/11/tech-shame-in-the-new-era/

[85] https://foreignpolicy.com/2019/01/16/ByteDance-cant-outrun-beijings-shadow/

[86] https://www.wsj.com/articles/tiktok-looking-at-ways-to-shake-off-its-ties-to-china-11574073001

[87] https://chinamediaproject.org/2018/04/11/tech-shame-in-the-new-era/

[88] https://edition.cnn.com/2018/11/02/tech/china-tech-communist-party/index html

[89] See Appendix E for a description of 2015's National Security Law and 2017's Cybersecurity Law, which similarly compel companies and citizens to comply with government directives in furtherance of national security and intelligence objectives. It also contains a broader description of 2017's National Intelligence Law.

National Intelligence Law is the most explicit in its requirements for PRC companies and citizens in complying with and assisting in intelligence and national security objectives. The Intelligence Law obliges individuals, organizations, and institutions to assist Public Security and State Security officials in carrying out a wide array of intelligence work. Specifically, Article 7 of the 2017 National Intelligence Law provides that "[a]n organization or citizen shall support, assist in and cooperate in national intelligence work in accordance with the law and keep confidential the national intelligence work that it or he knows." Article 14 permits Chinese intelligence institutions to request citizens and organizations to provide necessary support, assistance, and cooperation. Furthermore, Article 17 allows Chinese intelligence agencies to take control of an organization's facilities, which includes communications equipment.

Though less explicit in their requirements, China has maintains other laws under which ByteDance also would be required to assist PRC state security and intelligence services. The PRC's National Cybersecurity Law, passed in 2017, requires network operators to store select data within China and allows Chinese authorities to conduct spot-checks on a company's network operations. Article 28 of China's Cybersecurity Law states, "Network operators shall provide technical support and assistance to public security organs and national security organs that are safeguarding national security and investigating criminal activities in accordance with the law." [90] The PRC's National Security Law, passed in 2015, states, "All citizens of the People's Republic of China....shall have the responsibility and obligation to maintain national security."[91] According to press reporting, "[the law] includes elements that define criticism of the government as a form of subversion. It is very vague in defining what kind of specific actions would constitute a citizen endangering state security." [92]

As the recently passed Hong Kong Security Law demonstrates, the PRC now seeks to apply its security laws beyond the borders of mainland China. Article 38 of the Hong Kong Security Law specifically states the law is applicable to every individual including those outside of or not from Hong Kong. Arguably, this would apply the Hong Kong Security Law to every person or company on earth regardless of whether or not they're in mainland China. Finally, Chinese companies that oppose requests from PRC intelligence or security services do not have adequate legal recourse to challenge such requests, given the PRC judiciary's lack of independence from the CCP. Though PRC law purportedly requires that courts exercise judicial power independently without outside interference, judges regularly received political guidance on pending cases, including instructions on how to rule, from both the government and the CCP, particularly in politically sensitive cases. [93]

4. ByteDance has complied with and assisted the PRC with its domestic surveillance, censorship, and propaganda efforts.

ByteDance's submission and compliance with Chinese law has rendered it a reliable, useful, and far reaching ear and mouthpiece for the Party and State. Since Zhang Yiming's public apology in April 2018, ByteDance's commitment to CCP directives has come to fruition in signed strategic agreements,

---

[93] See Dr. Christopher Ashely Ford, Assistant Sec'y of State for the U.S. Dep't of State Bureau of Int'l Security and Nonproliferation, Remarks at the Multilateral Action on Sensitive Techs. Conference (Sept. 11, 2019), https://www.state.gov/huawei-and-its-siblings-the-chinese-tech-giants-national-security-and-foreign-policy-implications/.

systemic censorship of content across its platforms, and the harvesting of user data. These events paved the way for the CCP to maintain regular access to and leverage ByteDance platforms. Through Douyin, ByteDance has actively assisted and complied with CCP domestic directives in surveillance, censorship, and propaganda efforts

As highlighted by news reporting after these events, there was a noticeable uptick in Chinese authorities' adoption of Douyin in their attempts to connect with a younger generation and ensure the communication of "core socialist values."[94] According to 2018 press reporting, there were more than 500 government agencies, Communist Party organizations, and official media Douyin accounts. According to the app, these government videos had been seen over 1.6 billion times as of June 2018.[95]

According to press reporting in May 2018, Douyin purged Peppa Pig, an animated children's series, from its platform after state-run media branded the imagery as a subversive symbol for the online counterculture after it became popular to use in memes and jokes.[96] State-run media wrote about those participating in the fad of making Peppa-related jokes, who "run counter to the mainstream value and are usually poorly education with no stable job. They are unruly slackers roaming around and the antithesis of the young generation the [Communist] party tries to cultivate."[97]

According to news reporting in 2019, most of ByteDance's activities in Xinjiang involve cooperation with Xinjiang authorities in Hotan, a part of Xinjiang that has been the target of some of the most severe repression. The city has seen an aggressive campaign of cemetery, mosque, and traditional housing demolition since November 2018, which continues today. In November 2019, the Beijing Radio and Television Bureau announced its "Xinjiang Aid" measures in Hotan to "propagate and showcase Hotan's new image"—after more than two years of mass detention and close surveillance of ethnic minorities there. These measures included guiding and helping local Xinjiang authorities and media outlets to use ByteDance's Toutiao and Douyin to broadcast a positive messaging campaign online.[98] A Tianjin Daily article reported in April 2020 that after listening to talks by representatives from ByteDance's Jinri Toutiao division, Hotan Propaganda Bureau official Zhou Nengwen said he was excited to use the Douyin platform to promote Hotan's products and image.[99]

On April 25, 2019, ByteDance signed a strategic cooperation agreement with the Ministry of Public Security's Press and Publicity Bureau in Beijing "aiming to give full play to the professional technology and platform advantages of Toutiao and Tiktok in big data analysis," strengthen the creation and production of "public security new media works," boost "network influence and online discourse power," and enhance "public security propaganda, guidance, influence, and credibility," among other aspects.[100]

---

[94] https://www.scmp.com/tech/china-tech/article/2150837/government-agencies-jump-short-video-bandwagon-ensure-chinese-youth

[95] https://www.scmp.com/tech/china-tech/article/2150837/government-agencies-jump-short-video-bandwagon-ensure-chinese-youth

[96] https://www.nytimes.com/interactive/2019/05/02/opinion/will-china-export-its-illiberal-innovation.html

[97] https://www.theguardian.com/world/2018/may/01/peppa-pig-banned-from-chinese-video-site

[98] https://web.archive.org/web/20191128000905/http://www nrta.gov.cn/art/2019/11/4/art_114_48597.html

[99] https://chinatechmap.aspi.org.au/#/company/ByteDance

[100] https://www.taiwannews.com.tw/en/news/3982027

5. ByteDance has censored or restricted TikTok content globally that is critical of or relevant to issues the CCP deems controversial.

A series of leaked company documents and interviews by former employees has revealed TikTok to be exercising a CCP-aligned censorship campaign while harvesting a range of user data overseas. As expressed in 2020 press reporting, "TikTok's zealous data collection, use of Chinese infrastructure, and its parent company's close ties to the Chinese Communist Party make it a perfect tool for massive surveillance and data collection by the Chinese government."[101] The Washington Post reports TikTok claims that the U.S. application doesn't censor political content, or "take instructions from its parent company," and that no content moderators for U.S. TikTok are based in China. However, the same story notes that former employees disagree, stating that "moderators based in Beijing had the final call on whether flagged videos were approved."[102]

In September 2019, the Guardian published leaked documents detailing TikTok's guidelines for moderation, revealing systemic censorship and alleging the app is advancing China's foreign policy goals abroad.[103] The report identified that the guidelines divide banned material into two categories: violations and visible to self. Content marked as a "violation" results in a deletion from the site and can lead to the user being banned from the platform. Lesser infringements are marked as "visible to self," which leaves the content up on the site, but excludes its distribution through TikTok's algorithm.[104]

The report outlines how bans are designed to appear general purpose instead of specific exceptions. Banning criticism of China's socialist system falls under the company's general ban of "criticism/attack towards policies, social rules of any country, such as constitutional monarchy, monarchy, parliamentary system, separation of powers, socialism system, etc."[105] Another ban covers, "demonization or distortion of local or other countries' history such as May 1998 riots of Indonesia, Cambodian genocide, Tiananmen Square incidents."[106]

In response to the Guardian's 2019 reporting, TikTok stated that this guidance was no longer valid and responded: "In TikTok's early days we took a blunt approach to minimizing conflict on the platform, and our moderation guidelines allowed penalties to be given for things like content that promoted conflict, such as between religious sects or ethnic groups, spanning a number of regions around the world. As TikTok began to take off globally last year, we recognized that this was not the correct approach, and began working to empower local teams that have a nuanced understanding of each market. As we've grown, we've implemented this localized approach across everything from product, to team, to policy development." [107]

According to 2019 press reporting, during the Hong Kong protests, a search for "#hongkong" on Twitter revealed a vast visual patchwork of the city's unavoidable protests, including pro-China

---

[101] https://protonmail.com/blog/tiktok-privacy/?utm_campaign=ww-en-2a-generic-coms_soc-social_organic&utm_content=&utm_medium=soc&utm_source=twitter&utm_term=1595520917
[102] https://www.washingtonpost.com/technology/2019/11/05/inside-tiktok-culture-clash-where-us-views-about-censorship-often-were-overridden-by-chinese-bosses/
[103] https://www.theguardian.com/technology/2019/sep/25/revealed-how-tiktok-censors-videos-that-do-not-please-beijing
[104] https://www.theguardian.com/technology/2019/sep/25/revealed-how-tiktok-censors-videos-that-do-not-please-beijing
[105] https://www.theguardian.com/technology/2019/sep/25/revealed-how-tiktok-censors-videos-that-do-not-please-beijing
[106] https://www.theguardian.com/technology/2019/sep/25/revealed-how-tiktok-censors-videos-that-do-not-please-beijing
[107] https://www.theguardian.com/technology/2019/sep/25/revealed-how-tiktok-censors-videos-that-do-not-please-beijing

agitprop, sympathetic memes and imagery from the hundreds of thousands of pro-democracy marchers who have braved police crackdowns. But the same searches for Hong Kong on TikTok, reveal a remarkably different — and, for the PRC Government, more politically convenient — version of reality: playful selfies, food photos and singalongs, with barely a hint of unrest in sight.[108]

In November 2019, American teenager Feroza Aziz, 17, made a series of viral make-up tutorials on the app in which she calls upon viewers to research China's human rights abuses in Xinjiang and equates the situation to the Holocaust. Aziz claims her videos are being censored by TikTok and that her account was suspended after posting the videos. TikTok responded explaining that Aziz had broken the platform's rules on terrorism-related material, but did not explain in detail. One of her videos is intended to comically detail the derogatory comments she has received growing up Muslim. However, Aziz claims that after making a new account, she was immediately suspended after speaking out about the Uyghurs.[109] The case garnered widespread media attention, which led to TikTok to reverse its decision and reactivated Feroza's account.[110]

B. Vulnerability

1. The TikTok application collects vast amounts of sensitive personal information from users and this information is accessible to parent company ByteDance.

According to its privacy policy (b) (4) [redacted] TikTok collects a broad range of information from users.(b) [redacted] This includes: 1) registration information, such as age, username and password, language, and email or phone number; 2) profile information, such as name, social media account information, and profile image; 3) user-generated content, including comments, photographs, videos, and virtual item videos that you choose to upload or broadcast on the platform; 4) payment information, such as PayPal or other third-party payment information (where required for the purpose of payment); 5) phone and social network contacts (names and profiles); 6) opt-in choices and communication preferences; 7) information in correspondence users send to TikTok; and 8) information sent by users through surveys or participation in challenges, sweepstakes, or contests such as gender, age, likeness, and preferences. The application also collects data on how the application is used, including user behavior such as browsing and search history and technical and network details such as Internet protocol (IP) address, geolocation-related data, unique device identifiers, and cookies. TikTok also collects information from third parties, such as advertising and analytics partners.[112,113]

A number of independent technical analyses of the TikTok application have illustrated the large quantity of metadata collected from the application. Beyond what is considered personally identifiable

---

[108] https://www.washingtonpost.com/technology/2019/09/15/tiktoks-beijing-roots-fuel-censorship-suspicion-it-builds-huge-us-audience/

[109] https://www.theguardian.com/technology/2019/nov/27/tiktok-makeup-tutorial-conceals-call-to-action-on-chinas-treatment-of-uighurs

[110] https://www.smh.com.au/world/asia/tiktok-s-owner-is-helping-china-s-campaign-of-repression-in-xinjiang-report-finds-20191129-p53fcs html

(b) [redacted]

[112] Note that information provided by ByteDance in response to our administrative subpoena is entitled to business confidential treatment and should not be disclosed publicly.

[113] https://www.tiktok.com/legal/privacy-policy?lang=en

data, the TikTok application generates a large amount of technical and transactional data about its users including data such as tracking videos watched, and even how much of a video an individual watched and how many times.[114] TikTok videos are shared across other social media applications and the web via the TikTok website, and through third-party websites via direct embedding. This allows video to be served from TikTok systems, and for metadata on views and any linked user behavior to be captured and stored by the application. This behavior is similar to other major social media platforms, and some of the data – such as automatic scanning of clipboards – may relate to the application's attempt to detect automated bot and spam behavior.[115]

The privacy policy for U.S. TikTok users acknowledges that data can be shared with "parent, subsidiary, or other affiliate of our corporate group."[116] There is thus widespread concern that U.S.-based users' data could end up in China. TikTok has made public statements emphasizing that this is not a common practice, stating that its "goal is to minimize data access across regions so that, for example, employees in the Asia-Pacific (APAC)[sic] region, including China, would have very minimal access to user data from the European Union and United States."[117] Minimization does not, however, necessarily mean that there is no access. TikTok has issued stronger blanket denials, stating: "[w]e have never given any TikTok user data to the Chinese government, nor would we do so if asked."[118] TikTok also paid for an outside analysis, in which a team interviewed employees and examined the computer code to validate that the technical and organizational barriers between the U.S.-based TikTok operation and China were being maintained.[119]

Nevertheless, TikTok also states that it "may disclose your information to respond to subpoenas, court orders, legal process, law enforcement requests, legal claims, or government inquiries."[120] TikTok states that data is retained for as long as is needed to provide the service, or so long as there is a legitimate business interest, or in some circumstances for five years in accordance with legal obligations.[121] The company has published transparency reports highlighting the number of requests for personal information from governments around the world. China, however, is notably absent from this list.[122]

According to credible allegations, TikTok collected far more data in the past, including taking advantage of a loophole in the Android permission system to collect a device's MAC address, a permanent identifier of that device.[123] Independent security researchers have documented TikTok access to clipboard data, despite a past commitment to end this practice.[124] An Australian think tank has documented the evolving privacy practices of TikTok. They note TikTok's data collection has evolved

---

[114] https://www.washingtonpost.com/technology/2020/07/13/tiktok-privacy/
[115] A French researcher notes that "such practice is pretty standard," available at: *https://medium.com/@fs0c131y/tiktok-logs-logs-logs-e93e8162647a; See also*: https://medium.com/@fs0c131y/tiktok-what-is-an-app-log-da70193f875 and https://www.blackhillsinfosec.com/lets-talk-about-tiktok/
[116] https://www.tiktok.com/legal/privacy-policy?lang=en
[117] https://newsroom.tiktok.com/en-au/our-approach-to-security
[118] https://techcrunch.com/2020/08/12/tiktok-found-to-have-tracked-android-users-mac-addresses-until-late-last-year/
[119] https://www nytimes.com/2019/11/01/technology/tiktok-national-security-review.html
[120] https://www.tiktok.com/safety/resources/transparency-report?lang=en
[121] https://www.tiktok.com/legal/privacy-policy?lang=en
[122] https://www.tiktok.com/safety/resources/transparency-report?lang=en
[123] https://www.wsj.com/articles/tiktok-tracked-user-data-using-tactic-banned-by-google-11597176738
[124] https://arstechnica.com/gadgets/2020/06/tiktok-and-53-other-ios-apps-still-snoop-your-sensitive-clipboard-data/

as the platform matures, including collecting less location information.[125] The authors of the study acknowledge that what "TikTok is doing isn't fundamentally different" from similarly situated social media platforms,[126] yet the sheer amount of behavioral user data that is generated and collected allows a very detailed picture of an individual user to be created and potentially tracked across other digital contexts.

Finally, the infrastructure that underlies the TikTok application is not wholly separate from the Chinese application and the systems of ByteDance. Functionality including storage, internal management, and algorithms is still "partially shared across other ByteDance products."[127] Although similar to engineering projects in other global organizations, access can be granted based on need and efficiency requirements. One news report describes access granted to Chinese engineers to tackle problems in a U.S.-based system when their expertise was needed.[128] This implies that the data described above could well be accessible.

2. ***While ByteDance primarily stores U.S. TikTok user data in the United States and maintains a backup of U.S. user data*** (b) (4) ***, some user data was previously stored in China and there is evidence that some data is currently being transmitted to China.***

(b) (4)

[redacted]

[redacted] U.S. user data being stored outside of the United States presents significant risks in this case. (b) (4) is a Chinese company and, like ByteDance, is similarly beholden to PRC laws that require assistance in surveillance and intelligence operations. Additionally, any Chinese citizens with direct access to the data could be similarly compelled to assist PRCISS.

[125] https://s3-ap-southeast-2.amazonaws.com/ad-aspi/2020-09/PB37-TikTok%20and%20WeChat%20-%20Curating%20and%20controlling%20global%20information%20flows.pdf

[126] https://www.worldpoliticsreview.com/trend-lines/28974/how-much-of-a-threat-is-tiktok

[127] https://www reuters.com/article/us-usa-tiktok-cybersecurity-exclusive/exclusive-microsoft-faces-complex-technical-challenges-in-tiktok-carveout-idUSKCN256100

[128] https://www.theinformation.com/articles/breaking-off-tiktok-will-be-hard-to-do cited in ASPI report

(b) (4)

[redacted]

TikTok previously stored and processed U.S. user data within China before February 2019, making it subject to Chinese national security laws. According to 2019 press reporting, a ByteDance spokesperson explained that, "data from TikTok users who joined the service before February 2019 may have been processed in China. ByteDance has since reorganized its structure and operations to prevent user data from flowing into China."[131] Despite this claim, there are indications that some data from the TikTok app may be directly transmitted to China, bypassing ByteDance's leased or owned servers altogether in 2020, Cybersecurity firm Penetrum found that 37.70% of the IP addresses the TikTok Android package kit (APK) source code connects to are based in China. An APK installs and configures an application on a phone. The majority of these IP addresses are hosted by Alibaba.[132,133]

3. ***ByteDance stores some U.S. TikTok user data in U.S.-based servers leased by (b) (4) a state-owned entity (SOE) of the People's Republic of China.***

(b) (4)

Nevertheless, storing U.S. user data on servers owned and operated by (b) (4) introduces significant risks. (b) (4) is wholly owned and controlled by a single Chinese entity that is directly owned by the PRC Government. (b) (4) The Publicly-Traded

[131] https://qz.com/1613020/tiktok-might-be-a-chinese-cambridge-analytica-scale-privacy-threat/
[132] https://protonmail.com/blog/tiktok-privacy/
[133] https://penetrum.com/tiktok/Penetrum_TikTok_Security_Analysis_whitepaper.pdf, pg 2

(b) (4)

Company, through its controlling shareholder, (b) (4) ("the SOE"), (b) is majority-owned and controlled by the PRC Government. (b)

The Chinese Communist Party's influence in the SOE and the Publicly-Traded company, which indirectly own and control (b) (4) make (b) (4) vulnerable to exploitation by the Chinese Government. In the Federal Communications Commission's ("FCC") 2019 decision in *In Re: China Mobile,* the Commission was concerned about PRC laws[141] and certain practices that the PRC government could use to exploit, influence and control a state-owned enterprise.[142] Some of the concerns raised by the FCC in *In Re: China Mobile* about the Chinese government's ability to influence state-owned enterprises, and consequently their indirect subsidiaries, have already been realized when it comes to the SOE and the Publically-Traded Company.

For example, in *In Re: China Mobile,* the FCC noted an Office of the U.S. Trade Representative ("USTR") report, which stated that state-owned enterprises "are being pressured to amend their articles of association to ensure Communist Party representation on their boards of directors . . .and to ensure that they make important company decisions in consultation with internal Communist Party committees."[143] According to the Chinese government, the constitutional amendments were made to "define the status and role of Party organizations in State-owned enterprises."[144] State-owned enterprises would be required to form CCP organizations inside the enterprise to "focus their work on the operations of their enterprise," to "guarantee and oversee the implementation of the principles and policies of the Party and the state within their own enterprise" and "participate in making decisions on major issues in the enterprise."[145] According to the South China Morning Post, Xiao Yaqing, the director of SASAC, wrote: "Communist Party members at state enterprises form the 'most solid and

(b) (4)

[141] *China Mobile Order* at ¶ 17 ("Chinese law requires citizens and organizations, including state-owned enterprises, to cooperate, assist, and support Chinese intelligence efforts wherever they are in the world."); *see also*, National People's Congress of the People's Republic of China, National Intelligence Law, http://www.npc.gov.cn/npc/xinwen/2017-06/27/content_2024529 htm (June 27, 2017). For an unofficial English-language translation, *see, e.g.,* China Law Translate, National Intelligence Law of the P.R.C. (2017), https://www.chinalawtranslate.com/en/tag/national-intelligence-law/ (accessed May 29, 2019); *see also*, Murray Tanner, *Beijing's New National Intelligence Law: From Defense to Offense*, Lawfare (July, 20, 2017), https://www.lawfareblog.com/beijings-new-national-intelligence-law-defense-offense (citing laws on National Intelligence, Counterespionage, National Security, Counterterrorism, Cybersecurity, and Foreign NGO Management, amendments to PRC Criminal Law, Management Methods for Lawyers and Law Firms, and then-pending draft Encryption Law and draft Standardization Law); *see also*, Office of the Sec'y of Def. Ann. Rep. to Cong., *Military and Security Developments Involving the People's Republic of China 2019*, at 101 ("The 2017 *National Intelligence Law* requires Chinese companies, such as Huawei and ZTE, to support, provide assistance, and cooperate in China's national intelligence work, wherever they operate.").

[142] *China Mobile Order* at ¶ 18 (citing World Bank and USTR reports on Chinese state-owned enterprises demonstrating Chinese government exploitation, influence and control); *see also*, USTR, 2018 Report to Congress on China's WTO Compliance, at 13 (Feb. 2019).

[143] *China Mobile Order* at ¶ 18, n.60 (citing USTR 2018 Report to Congress on China's WTO Compliance); *see also* Ex. [116] at EB-2568, USTR, 2018 Report to Congress on China's WTO Compliance, at 13 (Feb. 2019).

[144] Full text of resolution on amendment to CPC Constitution, State Council of the People's Republic of China, http://english.gov.cn/news/top_news/2017/10/24/content_281475919837140.htm (Oct. 24, 2017).

[145] Constitution of the Communist Party of China, Revised and adopted at the 19th National Congress, Article 33, http://www.xinhuanet.com//english/download/Constitution_ of_ the_ Communist_Party _of_ China.pdf (Oct. 24, 2017).

reliable class foundation' for the Communist Party to rule the country."[146] This SOE, and through it, the Publically-Traded Company, Parent Entity, and (b) (4) are all controlled by the CCP. Therefore any data contained or managed by servers owned or controlled by (b) (4) including user data from U.S. TikTok users, may be directly accessible or within reach of the PRC government.

4. TikTok has been implicated in a number of information security and privacy incidents that raises significant concerns on the security and privacy of U.S. user data.

TikTok has previously faced charges that it illegally collected personal information from children. On February 27, 2019, the Federal Trade Commission (FTC) announced that TikTok agreed to pay $5.7 million to settle the violation of the Children's Online Privacy Protection Act (COPPA). "The operators of Musical.ly—now known as TikTok—knew many children were using the app but they still failed to seek parental consent before collecting names, email addresses, and other personal information from users under the age of 13."[147]

According to press reporting, in 2019, "a California college student accused popular video-sharing app TikTok in a class-action lawsuit of transferring private user data to servers in China, despite the company's assurances that it does not store personal data there. The lawsuit, filed in the U.S. District Court for the Northern District of California, alleges TikTok has surreptitiously "vacuumed up and transferred to servers in China vast quantities of private and personally-identifiable user data." The documents identify the plaintiff as Misty Hong, a college student and resident of Palo Alto, California, who downloaded the TikTok app in March or April 2019 but never created an account. Months later, Hong alleges to have discovered that TikTok had created an account for her without her knowledge and produced a dossier of private information about her, including biometric information gleaned from videos she created but never posted.

According to the filing, TikTok transferred user data to two servers in China - bugly.qq.com and umeng.com - as recently as April 2019, including information about the user's device and any websites the user had visited. Bugly is owned by Tencent, China's largest mobile software company, which also owns social network WeChat, while Umeng is part of Chinese e-commerce giant Alibaba Group. The lawsuit also claims that source code from Chinese tech giant Baidu is embedded within the TikTok app, as is code from Igexin, a Chinese advertising service, which security researchers discovered in 2017 was enabling developers to install spyware on a user's phone."[148]

TikTok has also been accused of evading privacy safeguards. A Wall Street Journal analysis from July 2020 uncovered that "TikTok skirted a privacy safeguard in Google's Android operating system to collect unique identifiers from millions of mobile devices, data that allows the app to track users online without allowing them to opt out."[149] The tactic, which experts in mobile-phone security said was concealed through an unusual added layer of encryption, appears to have violated Google policies

---

[146] Wendy Wu, *How the Communist Party controls China's state-owned industrial titans*, South China Morning Post, (June 17, 2017 9:01 AM) https://www.scmp.com/news/china/economy/article/2098755/how-communist-party-controls-chinas-state-owned-industrial-titans (last accessed June 29, 2020).

[147] https://www ftc.gov/news-events/press-releases/2019/02/video-social-networking-app-musically-agrees-settle-ftc

[148] https://www reuters.com/article/us-usa-tiktok-lawsuit/tiktok-accused-in-california-lawsuit-of-sending-user-data-to-china-idUSKBN1Y708Q

[149] https://search.proquest.com/docview/2432730526?rfr_id=info%3Axri%2Fsid%3Aprimo

limiting how apps track people and was not disclosed to TikTok users. TikTok ended the practice in November 2019, the Journal's testing showed.[150] This activity is not limited to Android users.

According to March 2020 press reporting, TikTok was identified as an app that can access any data a user copies to its clipboard on iPhones and iPads. Researchers explained that risk comes from the fact that iPhone or iPad app "can eavesdrop on a Mac." TikTok's logs clearly indicate that it is reading the content of the clipboard whenever it is opened, although researchers could not verify what TikTok is doing with the data it has read. "We can't say for sure what TikTok is doing with the data it has read."[151] ByteDance claimed that this problem was related to the use of an outdated Google advertising software development kit that was being replaced.[152]

Finally, according to July 2020 press reporting, engineers identified that on the beta version of Apple's iOS 14, which fixed the previous clipboard access issues, the TikTok app was caught again secretly accessing users' clipboards.[153] According to TikTok, the issue is "triggered by a feature designed to identify repetitive, spammy behavior," and it has "already submitted an updated version of the app to the App Store removing the anti-spam feature to eliminate any potential confusion."[154]

C. Consequence

1. Exploitation of TikTok user data imperils the privacy of U.S. citizens, the security of U.S. government personnel, and, at scale, directly threatens the economic security and national security of the United States.

One of the foremost national security risks presented by the TikTok mobile application in the United States is the possibility that the PRC government could, through lawful authority, extralegal influence (Communist Party) influence, or PRCISS, compel TikTok to provide systemic access to U.S. user's sensitive personal information. A number of press reports clearly indicate the PRC Government has already compelled TikTok to assist them for domestic surveillance, censorship, and propaganda action within China, and their compliance is indicative of how they are likely to respond to intelligence requests on U.S. users. Given the bounty of information TikTok could offer on foreign users, as well as the aforementioned cyber tactics employed by the PRC, the Department of Commerce assesses the PRC and PRCISS would not limit their use of TikTok to domestic concerns and would instead use it for foreign intelligence and surveillance.

ByteDance, as a company, and its subsidiaries are subject to PRC national security laws that require or compel the assistance of any Chinese citizen or entity in surveillance and intelligence operations. As ByteDance is subject to PRC jurisdiction, PRC laws can compel cooperation from ByteDance, regardless of whether ByteDance's subsidiaries are located outside the territory of the PRC.

---

[150] https://www.wsj.com/articles/tiktok-tracked-user-data-using-tactic-banned-by-google-11597176738?mod=searchresults&page=1&pos=3

[151] <https://www.forbes.com/sites/zakdoffman/2020/03/12/simple-apple-security-hack-if-you-have-tiktok-on-your-iphone-look-away-now/#7f1173741d61>

[152] https://www forbes.com/sites/zakdoffman/2020/06/26/warning-apple-suddenly-catches-tiktok-secretly-spying-on-millions-of-iphone-users/#3dce51f834ef

[153] https://www forbes.com/sites/zakdoffman/2020/07/01/anonymous-targets-tiktok-delete-this-chinese-spyware-now/

[154] https://www forbes.com/sites/zakdoffman/2020/06/26/warning-apple-suddenly-catches-tiktok-secretly-spying-on-millions-of-iphone-users/#642da5db34ef

Additionally, it is in ByteDance's best interest to maintain positive relations with the CCP as any perception that the company is 'disloyal' or not conducting its business with the best interest of the party could jeopardize its standing and business interests in China. This dynamic presents significant *extra-legal* pressure on ByteDance to comply with and actively assist in PRCISS intelligence collection and surveillance efforts.

Furthermore, ByteDance cannot account for surveillance that may be conducted on its operations without its explicit knowledge or awareness at a corporate level. Chinese intelligence services could compromise the (b) (4) servers themselves or intercept internet traffic coming to the server. Alternatively, PRCISS could compel the assistance of TikTok's engineering team or other personnel located in the PRC and involved in software development and engineering to directly compromise the app through routine app updates. PRCISS could also compel the assistance of any third-party companies with whom ByteDance contracts to service the TikTok application – including data management, software development, analytics, etc. These intelligence operations could ostensibly occur without ByteDance's express knowledge or awareness at a corporate level.

Given ByteDance's history of cooperation with PRC officials, the extensive amount of sensitive personal data collected by their apps both inside and outside of China, and their strong ties to the CCP and supporting its agenda, the TikTok app could expand the PRC's ability to conduct espionage on millions of U.S. persons. The PRC has stolen various types of sensitive data on millions of Americans to include health, financial, and other PII. Applications such as TikTok also collect other types of information, to include location data. The PRC could use combine these various types of data they possess and continue to collect in order to build dossier's on millions U.S. persons. Funneling all of these various types of information into their AI apparatus, could potentially create a platform to enhance the PRC's ability to identify espionage targets for counterintelligence purposes.

2. ***Exploitation of TikTok for censorship or propaganda for U.S.-based users directly threatens U.S. national security by surreptitiously influencing U.S. public opinion to those that align with Chinese government objectives.***

A critical, but secondary concern presented by TikTok is that the PRC government and the CCP can exert influence on ByteDance and, through the TikTok app, censor and shape content available to U.S. users in ways that can influence their opinions and views of China. The evidence included above raises significant concerns that the PRC government has significant leverage to exert pressure, actively or passively, on ByteDance to promote content that ensures a more positive view of China globally. Chinese companies, such as ByteDance, must comply with the China Internet Security Law as well as the CCP agenda since the party controls both the legal system and whether a company may function.[155] Reporting indicates that ByteDance employs more than 130 CCP members, to include senior positions within the company while reports claim that content moderators located in Beijing have censored anti-China content deemed to be critical of the PRC.[156] Even more contentious is the question around what TikTok promotes, recommends, and allows users to see. Users often take advantage of hash tags to help share content and create emerging communities. There are a number of examples of hash tags being blocked. In what TikTok described as a "glitch," a recently popular protest hash tag in the U.S.

[155] https://www.wsj.com/articles/chinas-tech-giants-have-a-second-job-helping-the-government-see-everything-1512056284
[156] https://www reuters.com/article/usa-tiktok-indonesia-idINL4N2FF468

appeared to have no associated videos.[157] In 2019, the New York Times interviewed a former TikTok content moderator who claimed the company employed "shadow banning," which doesn't outright remove a video, but rather prevents it from being shared more widely on the platform's main video feed.[158] Other search terms around politically sensitive issues yield only innocuous results. The overall trend appears to be an attempt to avoid contentious, politically sensitive topics. Absent greater transparency, it is hard to understand the extent of interference in the growing venue of online discussion.[159] According to press reporting in 2019, TikTok provides no data about the videos it has removed from the app, and it shares no details about the artificial-intelligence tools that determine what viewers see.[160]

(b) (4) [redacted] former U.S. employees stated that the moderators based in China made the final decision of what content is allowed.[161]

TikTok's use of algorithms and machine learning capabilities are the what differentiates the app and has led to its popularity and widespread use. (b) (4) [redacted]

As a content sharing platform, TikTok plays a role in removing content and determining what videos users see. However, there is significant evidence that content on TikTok must be acceptable to the CCP. There are a few clear case studies of sensitive material being removed for political content, including an American teen who hid her message about Muslim persecution in western China in the guise of a make-up tutorial.[162] Also, due to its sophistication and capability, TikTok may offer an effective platform for the PRC to distribute pro-CCP propaganda and content to millions of U.S. users.

IV. RECOMMENDATION

[157] https://www refinery29.com/en-us/2020/05/9846670/tiktok-black-lives-matter-george-floyd-tag-blocked
[158] https://www.politico.com/magazine/story/2019/11/02/the-trouble-with-tiktok-229890
[159] ASPI July 2020 report
[160] https://webcache.googleusercontent.com/search?q=cache:Q1oqO6q2-5QJ:https://www.washingtonpost.com/technology/2019/11/05/inside-tiktok-culture-clash-where-us-views-about-censorship-often-were-overridden-by-chinese-bosses/+&cd=1&hl=en&ct=clnk&gl=us&client=firefox-b-1-d
[161] https://www.washingtonpost.com/technology/2019/11/05/inside-tiktok-culture-clash-where-us-views-about-censorship-often-were-overridden-by-chinese-bosses/
[162] https://www.bbc.com/news/technology-50559656

Barring a complete divestiture of ByteDance from the TikTok application, TikTok presents an immitigable risk to the national security, foreign policy, and economy of the United States. Appropriately addressing national security concerns through mitigation requires a baseline level of trust in the entity subject to the mitigation terms. Given that TikTok remains under ByteDance ownership, and that ByteDance remains under the control and influence of the PRC, there is no way to create such a baseline of trust that would allow for effective mitigation without a complete divestiture from ByteDance ownership.

The below prohibitions on certain business-to-business transactions deny access to and reduce the functionality of the TikTok mobile app within the land or maritime borders of the United States with the objective of preventing collection, transmission, and aggregation of U.S. user data by the TikTok app, ByteDance Ltd., and PRCISS. Note that these transactions do not directly prohibit the downloading or use of the TikTok app and are not directly targeted at users of the TikTok app. While these prohibitions may ultimately make the application less effective and may be challenging for U.S.-based TikTok users, they are necessary for the protection of U.S. national security.

We understand that there are on-going negotiations between ByteDance and the Committee on Foreign Investment in the United States ("CFIUS") regarding a potential divestiture of TikTok or a restructuring of its governance to attempt to mitigate national security risks presented by the ByteDance acquisition of Musical.ly. Further, we understand that under the EO signed on August 19, 2020, the President has established a deadline of November 12, 2020, for any deal or agreement to be reached.

In consideration of these negotiations, we recommend that the transactions identified herein be prohibited in a phased manner, with the prohibition for transaction one to become effective on September 20, 2020, and the prohibition for all other transactions become effective on November 12, 2020. Transaction 1 should be prohibited immediately as it directly limits the availability of the app to new users for download and thus limits the growth of U.S. user data at risk. Of the transactions listed below, this transaction would have the biggest impact in mitigating national security risks and is the most foundational to the functionality of the TikTok app in the United States. This should mitigate some national security risk immediately while allowing the USG the latitude to further evaluate the viability of national security mitigations in the context of CFIUS negotiations. To the extent the dates for the CFIUS process are extended, the dates for the secondary phase may also be extended.

In recommending a phased approach, we also considered the ability of all relevant parties, to include TikTok, to comply with the following prohibitions within a short timeframe. (b) (4) [redacted] Of course, feasibility of compliance should be balanced against national security need. Of the following transactions, transaction one allows for the greatest mitigation to national security while affecting the least number of parties and, in our estimation, being the easiest to implement.

Ultimately, a phased approach outlined above serves a number of purposes. It allows the U.S. government additional time to evaluate the effectiveness of and negotiate mitigations in the context of CFIUS, and reduces national security risk substantially – all the while allowing TikTok and other

relevant parties necessary time to prepare for compliance when the order comes into effect.

1. ***Any provision of services to distribute and maintain the TikTok mobile application, constituent code, or mobile application updates through an online mobile application store, or any online marketplace where mobile users may download or update applications for use on their mobile devices, accessible in the land or maritime borders of the United States and its territories;***

This prohibition would remove the TikTok app from U.S.-based mobile app stores, preventing mobile users from being able to download the app to their devices or receive updates. As scoped, this prohibition would only apply to app stores accessible in the United States, thus users would still be able to download the app while outside the United States. Additionally, the prohibition would not require the removal of the app from user devices, thus the app would remain on any device where the app has been downloaded prior to the order. However, these apps would no longer have the ability to be updated rendering them less effective and functional. This prohibit would limit availability of the app, but it alone would not prevent user data from being transmitted from user devices to TikTok data centers. Additional prohibitions below are necessary to minimize and reduce its use in the United States.

2. ***Any provision of internet hosting services enabling the functioning or optimization of the TikTok mobile application, within the land and maritime borders of the United States and its territories;***

Prohibition would prevent any ByteDance leased, owned, or operated server from being used to serve content or data to the TikTok app. User data could still be served by data centers, (b) (4) [redacted] operating outside of the United States. This would significantly reduce the functionality and usability of the app in the United States and prevent user data from being sent by way of routine use of the app.

3. ***Any provision of content delivery services enabling the functioning or optimization of the TikTok mobile application, within the land and maritime borders of the United States and its territories;***

ByteDance contracts with content delivery network ("CDN") providers[163] for the purposes of speeding delivery and optimizing service for users based in the United States. This prohibition would terminate those agreements and will likely further reduce functionality and usability of the app for users within the United States.

4. ***Any provision of directly contracted or arranged internet transit or peering services enabling the functioning or optimization of the TikTok application, within the land and maritime borders of the United States and its territories;***

[163] Content delivery services are service that copy, save, and deliver content, for a fee, from geographically dispersed servers to end-users for the purposes of enabling faster delivery of content.

Though ByteDance maintains (b) peering agreements[164] with companies for the purposes of speeding delivery and optimizing service for users based in the United States, this prohibition would ensure these services could not be retained in the future to enable to TikTok app or its functioning.

5. ***Any utilization of the TikTok mobile application's constituent code, functions, or services in the functioning of software or services developed and/or accessible within the land and maritime borders of the United States and its territories.***

This prohibition serves to prevent any potential circumvention of the aforementioned prohibitions, as it would prohibit any method by which TikTok code, functions, or services could be serviced in a separately named and sold mobile app to which the aforementioned provisions would not apply. Additionally, it prevents interoperability with third-party apps that utilize TikTok functions and services, thus reducing any U.S. user data that could be collected incidentally and made accessible to ByteDance.

We recommend that, consistent with your obligation under EO 13942, you prohibit these transactions effective September 20, 2020, though defer transactions 2 through 5 until November 12, 2020.

EXECUTIVE SECRETARIAT CLEARANCE:

_____ _____

Executive Secretariat Date

[164] Peering means a relationship between Internet service providers (ISP) where the parties directly interconnect to exchange Internet traffic, most often on a no-cost basis.

FOR OFFICIAL USE ONLY

Tracking Number: _____

DECISION FOR THE SECRETARY

Approval recommendation to prohibit transactions above in accordance with EO 13943.


_____ I approve the prohibitions outlined herein.

_____ I do not approve the prohibitions outlined herein.

_____ I approve as amended.

_____ I would like to discuss this issue.