Filed: 12/7/2022 2:24 PM
Clerk
Allen County, Indiana
BB

**IN THE SUPERIOR COURT OF ALLEN COUNTY**

| | |
|---|---|
| STATE OF INDIANA,<br><br>*Plaintiff*,<br><br>v.<br><br>TIKTOK INC.,<br><br>and,<br><br>BYTEDANCE LTD.,<br><br>*Defendants.* | Case No. _____ |

**COMPLAINT**

1. TikTok says its platform is all about spreading joy. But the more TikTok videos consumers view, and the more content that they create and share, the more TikTok learns about them—their interests, their locations, the types of phones they have, the apps on their phones, who their contacts are, their facial features, their voice prints, and even "where your eyes are looking on your phone."[1]

2. While TikTok vacuums up reams of this highly sensitive and personal information about Indiana consumers, it deceives and misleads them about the risks the app routinely poses to their data.

3. TikTok and its algorithm are owned by ByteDance Ltd., a Chinese company subject to Chinese law, including laws that mandate secret cooperation with China's intelligence activities.

4. The Chinese Government and Communist Party have a demonstrated interest in the kind of data that TikTok collects on its users, which they can use to spy on, blackmail, and coerce

[1] A. Thomas, *Cotton issues TikTok warning, cites national security concerns*, NORTHWEST ARKANSAS DEMOCRAT GAZETTE (Nov. 22, 2022), https://bit.ly/3H2o2qu.

those users, or to further develop China's artificial intelligence capabilities, or for any number of other purposes that serve China's national security and economic interests, at the expense of Indiana consumers.[2] China applies its laws as the Chinese Communist Party sees fit—whenever and wherever it sees fit—and there is no meaningful recourse for any individual or any company to refuse its demands.

5. China's data and cybersecurity regimes are not about privacy, they are about control. Thanks to a wave of recent national security, cybersecurity, and data security laws and regulations, in China, "[t]here will be no secrets. No VPNs. No private or encrypted messages. No anonymous online accounts. No trade secrets. No confidential data. Any and all data will be available and open to the Chinese government."[3]

6. TikTok tells Indiana consumers that their data is protected by comprehensive company protocols and practices, including rigid access controls managed by a U.S.-based security team. TikTok says it has never given the Chinese Government access to that data, and that it never would. TikTok says that none of this data is subject to Chinese law, and that Chinese law has nothing to do with TikTok. TikTok bends over backwards to downplay its Chinese parent company and the "China association."

7. Unlike every other major social media company, TikTok even fails to alert consumers when accounts affiliated with the Chinese Government and Communist Party are pushing controversial and divisive content on the platform.

---

[2] A. Thomas, *Cotton issues TikTok warning, cites national security concerns*, NORTHWEST ARKANSAS DEMOCRAT GAZETTE (Nov. 22, 2022), https://bit.ly/3H2o2qu.; M. Rubio and M. Gallagher, Op-Ed: *Ban TikTok in America*, THE WASH. POST (Nov. 10, 2022), https://wapo.st/3ugJyjq; MEM. FROM JOHN K. COSTELLO, DEPUTY ASSISTANT SEC'Y FOR INTEL. AND SEC., OFF. OF INTEL. AND SEC., THROUGH ROB BLAIR, DIRECTOR, OFF. OF POL'Y AND STRATEGIC PLANNING, TO THE SEC'Y, U.S. DEP'T OF COMMERCE, PROPOSED PROHIBITED TRANSACTIONS RELATED TO TIKTOK PURSUANT TO EXECUTIVE ORDER 13942, 2 (Sept. 17, 2020), https://bit.ly/3VJ1Vt9 ("Commerce Department Memorandum").

[3] The China Law Blog, *China Cybersecurity: No Place to Hide*, HARRIS BRICKEN (Oct. 11, 2020), https://bit.ly/3E2Gzkm.

8. TikTok's statements and omissions paint a picture for Indiana consumers that there is minimal risk of the Chinese Government and/or Communist Party, which controls the government, accessing and exploiting their data.[4] These statements are false, deceptive, and misleading.

9. The highly sensitive data that TikTok collects from Indiana consumers is accessible by individuals and entities subject to Chinese law and China's oppressive regime, including but not limited to laws requiring cooperation with China's national intelligence institutions and cybersecurity regulators. Chinese State and Communist Party officials have interpreted Chinese law as applying to any data in which China has a national intelligence or security interest, no matter where the data is located.

10. Further, TikTok's privacy policy states that it may share data it collects with its parent company ByteDance "or other affiliate of our corporate group,"[5] who are all subject to Chinese law.

11. TikTok has stored U.S. user data, including Indiana consumers' data, on servers owned and operated and/or hosted by Chinese companies subject to Chinese law.

12. TikTok also misleads Indiana consumers by failing to disclose specifically in its U.S privacy policy that its parent company ByteDance or certain other affiliates of its corporate group are located in China.

[4] *Chinese Communist Party*, BRITANNICA (Oct. 24, 2022), https://bit.ly/3haNejG; *see also* CONST. OF THE PEOPLE'S REPUBLIC OF CHINA pmbl. (Nov. 20, 2019), *available at* https://bit.ly/3FER8LD ("We the Chinese people of all ethnic groups will continue, under the leadership of the Communist Party of China and the guidance of Marxism-Leninism, Mao Zedong Thought, Deng Xiaoping Theory, the Theory of Three Represents, the Scientific Outlook on Development and Xi Jinping Thought on Socialism with Chinese Characteristics for a New Era, to uphold the people's democratic dictatorship . . . .").

[5] *TikTok Privacy Policy*, TIKTOK (June 2, 2021), https://bit.ly/3fsbUnd.

13. This omission is deceptive and misleading to Indiana consumers, who cannot know when they read and consent to the privacy policy the truth that their data may be shared with individuals and entities subject to Chinese laws.

14. TikTok's omission of China in its U.S. privacy policy, the link to which is included in TikTok's pages on the App Store and Google Play Store, is also deceptive and misleading to Indiana consumers, because it does not comply with Apple's or Google's requirements for application developers to be transparent with how and where users' data is used and accessed.

15. TikTok also misleads Indiana consumers about the level of influence and control exercised by its parent company, ByteDance, over TikTok and its operations.

16. TikTok claims its independence from ByteDance through various means, but evidence shows that ByteDance exercises significant influence and control over TikTok.

17. ByteDance's influence and control over TikTok is significant, because ByteDance cooperates closely with, and is influenced by, the Chinese Government and Chinese Communist Party.

18. Thus, in addition to denying the application of Chinese law to TikTok's U.S. user data, including Indiana consumers' data, TikTok also downplays the influence and pressure that the Chinese Communist Party may bring to bear on entities and individuals subject to Chinese law who have access to that data, further placing the data at risk.

19. TikTok thus routinely exposes Indiana consumers' data, without their knowledge, to access and exploitation by the Chinese Government and Communist Party.

20. The Chinese Government and Communist Party have demonstrated the intent and willingness to investigate, surveil, harass, and intimidate individuals outside of China, including

in Indiana.[6] Even TikTok's parent ByteDance has reportedly planned to use data gathered through TikTok to surveil Americans.

21. TikTok is a wolf in sheep's clothing. As long as TikTok is permitted to deceive and mislead Indiana consumers about the risks to their data, those consumers and their privacy are easy prey.

22. TikTok committed the acts alleged in this Complaint as part of a scheme, artifice, or device with intent to defraud or mislead, and therefore committed incurable deceptive acts.

23. At the very least, TikTok knew that its acts were deceptive, entitling the State to injunctive relief.

24. The State of Indiana seeks a permanent injunction to compel TikTok to cease its deceptive and misleading statements about the risk of access to and exploitation of consumers' data by the Chinese Government and/or Chinese Communist Party.

25. The State of Indiana further seeks civil penalties in light of TikTok Inc.'s unfair and deceptive conduct, which has harmed and continues to harm Indiana consumers.

26. The State of Indiana demands a jury trial.

## JURISDICTION AND VENUE

27. IND. CODE § 4-6-3-2 (2012) authorizes the Attorney General to bring actions on behalf of the State of Indiana.

28. IND. CODE § 24-5-0.5-4(c) (2020) empowers the Indiana Attorney General to "bring an action to enjoin a deceptive act" under Indiana's Deceptive Consumer Sales Act, *Id.* § 24-5-0.5, *et seq.*

[6] Compl., *United States v. Fan "Frank" Liu, et al.*, No. 22-MJ-257 (E.D.N.Y. Mar. 9, 2022), *available at* https://bit.ly/3ulEw5a.

29. IND. CODE § 24-5-0.5-4(g) further provides that where the "court finds any person has knowingly violated" the prohibition on deceptive acts, the Attorney General "may recover from the person on behalf of the state a civil penalty" of up to $5,000 "per violation."

30. IND. CODE § 24-5-0.5-8 also authorizes the Attorney General, through a petition brought under IND. CODE § 24-5-0.5-4(c), to seek a civil penalty against a person who commits an "incurable" deceptive act, of up to $500 "for each violation."

31. Accordingly, this Court has jurisdiction to hear this dispute and is further authorized to "order the supplier to pay to the state the reasonable costs of the attorney general's investigation and prosecution related to the action." IND. CODE § 24-5-0.5-4(c)(4).

32. The State of Indiana is a governmental organization and thus bears no requirement to give security for the payment of costs and damages for any party wrongfully enjoined. IND. R. CIV. P. 65(C).

**PARTIES**

33. Plaintiff Indiana is the State of Indiana.

34. Defendant TikTok Inc. is a for-profit entity incorporated in the State of Washington, which operates a social media application and platform known as "TikTok." TikTok Inc. is headquartered at 5800 Bristol Pkwy, Culver City, CA, 90230-6696. TikTok Inc. is valued at $50-75 billion. TikTok Inc. made nearly $4 billion in revenue in 2021.

35. Defendant ByteDance Ltd. is a multinational internet technology holding company and is the parent company of TikTok Inc. ByteDance Ltd. is headquartered at Room 503 5F, Building 2, 43 North Third Ring West Road, Beijing, 100086 China. ByteDance Ltd. is valued at more than $400 billion. ByteDance Ltd. reported $58 billion in revenue in 2021.

## FACTUAL ALLEGATIONS

### What TikTok Is

36. TikTok is a social media platform that centers on short videos created and uploaded by users and often set to music. TikTok is available as an application to download on smartphones and tablets, and most TikTok users interact with the platform through an application. Users can download the TikTok application from the Apple App Store, the Google Play Store, or the Microsoft Store.

37. TikTok users register and create a profile in order to access the platform. In doing so, TikTok users answer a few questions about themselves and provide some user information, including their birthdays and contact information.

38. When Indiana consumers use the TikTok platform, TikTok automatically collects their "IP address, geolocation-related data . . ., unique device identifiers, browsing and search history . . ., and Cookies."[7]

39. TikTok also collects other information about users' phones, including their "user agent, mobile carrier, time zone settings, identifiers for advertising purposes, model of [their] device, the device system, network type, device IDs, [their] screen resolution and operating system, app and file names and types, keystroke patterns or rhythms, battery state, audio settings and connected audio devices."[8]

40. TikTok also collects users' biometric information, including faceprints and voiceprints.

41. TikTok tracks Indiana consumers across their devices and across the internet. Specifically, when users "log-in from multiple devices, [TikTok] will be able to use [their] profile

[7] *TikTok Privacy Policy*, TIKTOK (June 2, 2021), https://bit.ly/3fsbUnd.
[8] *Id.*

information to identify [their] activity across devices. [TikTok] may also associate [them] with information collected from devices other than those [they] use to log-in to the Platform." Further, TikTok and its,

> service providers and business partners may link [users'] contact or account information with [their] activity on and off [the TikTok] Platform across all [their] devices, using [their] email or other log-in or device information. [TikTok's] service providers and business partners may use this information to display advertisements on [the TikTok] Platform and elsewhere online and across [their] devices tailored to [their] interests, preferences, and characteristics.[9]

42. If Indiana consumers consent, TikTok also collects their phone's contacts, precise GPS location, and information from other social media accounts or login services if users link them to TikTok or use them to sign up for TikTok.

43. A report from privacy researcher Felix Krause found that TikTok also collects copious amounts of information about users who visit third-party websites through TikTok's in-app browser. Specifically, his report finds that TikTok injects JavaScript into these third-party websites that allows TikTok to collect information about everything a user does on that website, including "every keystroke" entered.[10] The code thus allows TikTok to capture additional highly personal information about consumers, including but not limited to passwords and credit card information.[11]

44. TikTok has been caught on more than one occasion evading statutes and rules designed to protect users' data. In 2019 TikTok, formerly known as Musical.ly, settled Federal Trade Commission allegations that it violated the Children's Online Privacy Protection Act.[12] In

---

[9] *Id.*

[10] Felix Krause, *iOS Privacy: Announcing InAppBrowser.com - see what JavaScript commands get injected through an in-app browser*, FELIX KRAUSE (Aug. 18, 2022), https://bit.ly/3Uve3wJ.

[11] *Id.*

[12] Press Release, Fed. Trade Comm'n, Video Social Networking App Musical.ly Agrees to Settle FTC Allegations That it Violated Children's Privacy Law (Feb. 27, 2019), https://bit.ly/3BdNYeN.

2020, the *Wall Street Journal* reported that TikTok violated Google policies by collecting Android users' unique device identifiers to track them online "without allowing them to opt out."[13]

**TikTok Misleads Indiana Consumers about the Risk of the Chinese Government or Communist Party Accessing and Exploiting their Data**

45. TikTok misleads Indiana consumers about the risk of the Chinese Government, or Chinese Communist Party which controls the Government, accessing and exploiting their data.

46. First, in its public statements, TikTok falsely denies that U.S. user data, which includes Indiana consumers' data, is subject to Chinese law.

47. Second, TikTok downplays the influence and control exercised over it by its parent company, ByteDance, while ByteDance is significantly influenced by, and cooperates closely with, the Chinese Communist Party and Government.

48. The combined purpose and effect of these statements is to paint a picture for Indiana consumers that their data is not at risk of access and exploitation by the Chinese Government or Chinese Communist Party.

49. On the contrary, and by TikTok's own admission, although currently stored in the United States and Singapore, U.S. user data, including Indiana consumers' data, can be and is accessed by Chinese citizens, including individuals in China, working for a company based in China, and founded and led by Chinese citizens, all of whom are subject to Chinese law.

50. TikTok's privacy policy also permits TikTok to share U.S. user data, including Indiana consumers' data, with its parent company, ByteDance, or "other affiliate of our corporate group."[14] ByteDance and certain other affiliates of TikTok are located in China, and led by Chinese citizens located in China, all of whom are subject to Chinese law. Further, at least one of

[13] K. Poulsen and R. McMillan, *TikTok Tracked User Data Using Tactic Banned by Google*, WSJ (Aug. 11, 2020), https://on.wsj.com/3F5nVaR.

[14] *TikTok Privacy Policy*, TIKTOK (June 2, 2021), https://bit.ly/3fsbUnd.

those affiliates is partly owned by a Chinese State-owned enterprise, which grants the State significant influence over that entity.

51. Although TikTok states it is in the process of moving "protected" U.S. user data, which includes Indiana consumers' data, to an Oracle cloud in the United States, it is not clear what data will be deemed "protected," and TikTok still currently and for some years has stored that data on other systems in the U.S. and Singapore. At least until October 2020, some U.S. data was stored on servers owned and operated by ByteDance, a company subject to Chinese law, and pursuant to a contract with Alibaba, a company also subject to Chinese law.

52. Chinese law requires Chinese citizens, and individuals and entities in China to cooperate with national intelligence work undertaken by the Chinese Government and/or Chinese Communist Party, and grants regulators broad authority to access private networks, communication systems, and facilities to conduct invasive inspections and reviews.

53. TikTok's privacy policy applicable to U.S. users also fails to disclose to Indiana consumers that their data may be shared with entities and individuals in China who are subject to Chinese law.

54. TikTok's privacy policy previously informed consumers that the individuals and entities that it could share data with were located in China.

55. According to public reporting, TikTok eliminated any reference to China from its U.S. privacy policy sometime in 2019 or thereafter, even though the entities with which the policy stated it may share Indiana users' data did not change location.[15]

[15] D. Carroll, *Is TikTok a Chinese Cambridge Analytica data bomb waiting to explode?*, QUARTZ (May 7, 2019), https://bit.ly/3zDuAqO.

56. TikTok has updated its *European* privacy policy to clearly state that it permits individuals outside of Europe, including China, to access European user data.[16] TikTok has made no such update to its U.S privacy policy, which applies to Indiana consumers, explicitly informing them that their data is accessed by individuals and entities in China.

57. By omitting this reference to China, TikTok is painting a false picture for Indiana consumers that, although their data could once be shared with individuals and entities in China who are subject to Chinese law, that is no longer the case.

58. By omitting this reference to China, TikTok is also painting a false picture for Indiana consumers that it complies with Apple's and Google's requirements for application developers to be available on the App Store and the Google Play Store. Pursuant to those requirements, all application developers must provide consumers with complete and transparent information about how and where their data is accessed and used. TikTok's U.S. privacy policy does not.

59. Further, contrary to TikTok's public statements, TikTok's parent company ByteDance exerts significant influence and control over TikTok and its operations.

60. ByteDance is subject to significant influence by, and cooperates with, the Chinese Government and Chinese Communist Party.

61. Whether by the operation of law or the influence of the Chinese Government and Chinese Communist Party apparatus, or both, any data or information accessed by Chinese citizens or individuals or entities within China is subject to Chinese law and is at risk of access and exploitation by the Government and/or Communist Party.

[16] E. Fox, *Sharing an Update to Our Privacy Policy*, TIKTOK (Nov. 2, 2022), https://bit.ly/3uivRAs.

62. That risk is not speculative. It is based on straightforward readings of Chinese law, assessments by a bipartisan array of U.S. government officials and agencies, and analysis by experts familiar with, among other things, Chinese law and technology policy.

63. TikTok's public statements ignore or obfuscate this risk, misleading Indiana consumers about the ability of China's Government and Communist Party to access and exploit their sensitive personal information.

**Chinese Law Requires Chinese Nationals and Individuals and Entities in China to Cooperate with National Intelligence Activities and Grants the Chinese Government Broad Authority to Access Private Networks, Communications, and Facilities**

64. Chinese law requires Chinese citizens, and individuals and organizations or entities in China to cooperate with "national intelligence work" and grants Chinese Government and Communist Party officials broad, invasive authority to, among other things, access private networks, communications systems, and facilities to conduct inspections and reviews. These laws are broad, open-ended, and inscrutably applied. Moreover, there is no independent judiciary in China that operates outside the control of the Chinese Communist Party. Thus, there is no meaningful mechanism in China to resist these demands.

65. Laws including, but not limited to, the National Security Law, Cybersecurity Law, and National Intelligence Law are part of "an interrelated package of national security, cyberspace, and law enforcement legislation" that "are aimed at strengthening the legal basis for China's security activities and requiring Chinese and foreign citizens, enterprises, and organizations to cooperate with them."[17]

[17] M. Scot Tanner, *Beijing's New National Intelligence Law: From Defense to Offense*, LAWFARE (July 20, 2017), https://bit.ly/3fXfB4A (referring to laws addressing "Counterespionage (2014), National Security (2015), Counterterrorism (2015), Cybersecurity (2016), and Foreign NGO Management (2016), as well as the Ninth Amendment to the PRC Criminal Law (2015), the Management Methods for Lawyers and Law Firms (both 2016), and the pending draft Encryption Law and draft Standardization Law"); *see also* M. Haldane, *What China's new data laws are and their impact on Big Tech*, SOUTH CHINA MORNING POST (Sept. 1, 2021), https://bit.ly/3zM0jX3

66. China's National Security Law places "the responsibility and duty to safeguard national security" on all "*[c]itizens of the People's Republic of China*, all State bodies and armed forces, all political parties and people's organizations, *enterprises*, undertakings, organizations and all other social organizations."[18]

67. The National Intelligence Law expounds on this responsibility, requiring all organizations and Chinese citizens to "cooperate with national intelligence efforts," and permits national intelligence institutions to collect information, question organizations and individuals, and take control of facilities and "communication[ ] tools."[19]

68. Specifically, the National Intelligence Law provides that "[a]ll organizations and citizens shall support, assist, and cooperate with national intelligence efforts in accordance with law, and shall protect national intelligence work secrets they are aware of."[20]

69. Article 14 provides that "[n]ational intelligence work institutions lawfully carrying out intelligence efforts may request that relevant organs, organizations, and citizens provide necessary support, assistance, and cooperation."[21]

70. Article 16 provides that these institutions "may enter relevant restricted areas and venues; may learn from and question relevant institutions, organizations, and individuals; and may read or collect relevant files, materials or items."[22]

---

(describing later enacted Data Security Law and Personal Information Protection Law as being "built on the groundwork laid by the Cybersecurity Law"); W. Zheng, *Big data expert takes over as China's new cybersecurity chief*, SOUTH CHINA MORNING POST (Sept. 27, 2019), https://bit.ly/3t03fLR.

[18] NATIONAL SECURITY LAW OF THE PEOPLE'S REPUBLIC OF CHINA, art. 11, STANFORD (2015), https://stanford.io/3sScPjX (emphasis added).

[19] NATIONAL INTELLIGENCE LAW OF THE PEOPLE'S REPUBLIC OF CHINA, arts. 7, 17, STANFORD (2017) ("NAT'L INTELLIGENCE LAW"), https://stanford.io/3sScPjX.

[20] NAT'L INTELLIGENCE LAW, art. 7.

[21] NAT'L INTELLIGENCE LAW, art. 14.

[22] NAT'L INTELLIGENCE LAW, art. 16.

71. Article 17 provides that "[a]s necessary for their work, the staff of national intelligence work institutions may, in accordance with relevant national provisions, have priority use of, or lawfully requisition, state organs', organizations' or individuals' transportation or communications tools, premises and buildings . . . ."[23]

72. Against this backdrop are numerous laws and regulations designed to form a comprehensive cybersecurity regime. The "chief engineer at the [Ministry of Public Security's] Cybersecurity Bureau," Guo Qiquan, described the scheme as intended to "cover every district, every ministry, every business and other institution, basically covering the whole society. It will also cover all targets that need [cybersecurity] protection, including all networks, information systems, cloud platforms, the internet of things, control systems, big data and mobile internet."[24]

73. In the words of one firm with experience working in China, under this plan:

> No information contained on any server located within China will be exempted from this full coverage program. No communication from or to China will be exempted. There will be no secrets. No VPNs. No private or encrypted messages. No anonymous online accounts. No trade secrets. No confidential data. Any and all data will be available and open to the Chinese government.[25]

74. These laws and regulations include, but are not limited to, China's Cybersecurity Law and Data Security Law.

75. "China's Cybersecurity Law lays the foundation for a cybersecurity review of network products and services, also known as the Cybersecurity Review Regime."[26]

---

[23] NAT'L INTELLIGENCE LAW, art. 17.

[24] W. Zheng, *Big data expert takes over as China's new cybersecurity chief*, SOUTH CHINA MORNING POST (Sept. 27, 2019), https://bit.ly/3t03fLR.

[25] The China Law Blog, *China Cybersecurity: No Place to Hide*, HARRIS BRICKEN (Oct. 11, 2020), https://bit.ly/3E2Gzkm.

[26] CSIS Briefs, *How Chinese Cybersecurity Standards Impact Doing Business in China*, CENTER FOR STRATEGIC AND INTERNATIONAL STUDIES (Aug. 2, 2018), https://bit.ly/3DupnTq.

76. The Cybersecurity Law applies broadly to, among others, "network operators," which can encompass not only "telecommunications or internet service providers (ISPs)" but also "anyone who uses [information communication and technology] systems."[27]

77. Article 28 of China's Cybersecurity Law requires these "network operators" to cooperate with national intelligence activities, as well as criminal investigations. Specifically, Article 28 provides that, "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."[28]

78. Article 49 further provides that "network operators shall cooperate with cybersecurity and informatization departments and relevant departments in conducting implementation of supervision and inspections in accordance with the law."[29]

79. The Cybersecurity Law applies even more stringent requirements and oversight on organizations deemed "critical information infrastructure operators."

80. For example, Article 35 provides that "[c]ritical information infrastructure operators purchasing network products and services that might impact national security shall undergo a national security review organized by the State cybersecurity and informatization departments and relevant departments of the State Council."[30]

81. Article 37 further provides that:

> [c]ritical information infrastructure operators that gather or produce personal information or important data during operations within the mainland territory of the People's Republic of China, shall store it within mainland China. Where due to business requirements it is truly necessary to provide it outside the mainland, they shall follow the measures jointly formulated by the State cybersecurity and

[27] *Id.*

[28] CYBERSECURITY LAW OF THE PEOPLE'S REPUBLIC OF CHINA, art. 28, Stanford (2017) ("CYBERSECURITY LAW"), https://stanford.io/3T5wes8.

[29] CYBERSECURITY LAW, art. 49.

[30] CYBERSECURITY LAW, art. 35.

> informatization departments and the relevant departments of the State Council to conduct a security assessment; where laws and administrative regulations provide otherwise, follow those provisions.[31]

82. Since the law's enactment, authorities have issued regulations expanding its scope.[32]

83. Exactly what type of organization may be designated a "critical information infrastructure operator" is not always clear. However, authorities' use of the applicable procedures indicates that tech companies and platforms could be subject to an invasive cybersecurity review, and that authorities' power to require a company to take any action pursuant to a cybersecurity review—even if justified only after the fact—could have significant consequences for its business.[33]

84. For example, in July 2021, just a few days after the Chinese ride-hailing service Didi raised billions of dollars in a New York IPO, the Cyberspace Administration of China (CAC), a "merged party-state institution listed under the Central Committee of the Chinese Communist Party,"[34] initiated a cybersecurity review of Didi. The CAC further "suspended new user registrations during the review" and ordered the removal of the company's applications from app stores in China.[35] Although the law and related regulations did not explicitly apply to Didi in advance of the review, CAC published a list of proposed new rules applying the cybersecurity

---

[31] CYBERSECURITY LAW, art. 37.

[32] B. Guo and B. Li, *China Issued New Measures for Cybersecurity Review in 2022*, WHITE & CASE (Feb. 8, 2022), https://bit.ly/3E2fRs8; J. Gong and C. Yue, *China Updated its Cybersecurity Review Regime*, BIRD & BIRD (Jan. 13, 2022), https://bit.ly/3fyWRrI.

[33] A. Huld, *Critical Information Infrastructure in China – New Cybersecurity Regulations*, THE CHINA BRIEFING (Aug. 30, 2021), https://bit.ly/3T8SOjH; *supra*, B. Guo and B. Li, *China Issued New Measures for Cybersecurity Review in 2022*, https://bit.ly/3E2fRs8; *supra*, J. Gong and C. Yue, *China Updated its Cybersecurity Review Regime*, https://bit.ly/3fyWRrI; M. Shi, et al., *Forum: Unpacking the DiDi Decision,* DIGICHINA, STANFORD (July 22, 2022), https://stanford.io/3T4ZAqM

[34] J. Horsley, *Behind the Façade of China's Cyber Super-Regulator*, DIGICHINA, STANFORD (Aug. 8, 2022), https://stanford.io/3FPAOYy.

[35] *Id*.; *supra*, B. Guo and B. Li, *China Issued New Measures for Cybersecurity Review in 2022*, https://bit.ly/3E2fRs8.

review requirements to Didi *after* it began its review.[36] CAC eventually imposed a $1.2 billion fine on the company.[37]

85. The Data Security Law applies in China as well as to "data handling activities outside the mainland territory of the PRC [that] harm the national security, the public interest, or the lawful rights and interests of citizens or organizations of the PRC."[38]

86. Article 24 provides that "[t]he State is to establish a data security review system and conduct national security reviews for data handling activities that affect or may affect national security."[39]

87. Further, Article 31 applies "[t]he provisions of the Cybersecurity Law . . . to the outbound security management of important data collected or produced by critical information infrastructure operators operating within the mainland territory of the PRC."[40]

88. Under the Data Security law, even "a company holding data belonging to a US citizen stored on a Chinese server may not be able to legally hand over that data to the US government without proper approval."[41] More specifically, under Article 35, whether operating critical information infrastructure or not, companies "are prohibited from providing any data *stored* in China, regardless of the data's sensitivity level and whether or not the data was initially *collected* in China, to any foreign judicial or law enforcement agency without the prior approval of the relevant [Chinese Government] authorities."[42]

---

[36] J. Horsley, *Behind the Façade of China's Cyber Super-Regulator*, https://stanford.io/3FPAOYy.

[37] *Id*.

[38] DATA SECURITY LAW OF THE PEOPLE'S REPUBLIC OF CHINA, art. 2, DIGICHINA STANFORD (2021) ("DATA SECURITY LAW"), https://stanford.io/3U5iijm.

[39] DATA SECURITY LAW, art. 24.

[40] DATA SECURITY LAW, art. 31.

[41] M. Haldane, *What China's new data laws are and their impact on Big Tech*, SOUTH CHINA MORNING POST (Sept. 1, 2021), https://bit.ly/3zM0jX3.

[42] R. Junck et. al, *China's New Data Security and Personal Information Protection Laws: What they Mean for Multinational Companies*, SKADDEN, ARPS, SLATE, MEAGHER & FLOM (Nov. 3, 2021), https://bit.ly/3NBc20c (emphasis added); DATA SECURITY LAW, art. 35.

89. Experts across a variety of fields, including law, national security, and technology agree that Chinese laws require any individuals or entities in China or otherwise subject to Chinese law to cooperate with the Chinese Government and/or Communist Party, including China's intelligence and security services, and that there is no meaningful way to resist these requirements, or any pressure brought to bear by the Party.[43] TikTok and ByteDance leadership and employees who are Chinese citizens or who are located in China are no exception; they are subject to the oppressive Chinese regime, including to these laws and requirements.

90. China's legal system also does not uphold American principles of a "rule of law" or individual rights, but rather a "rule by the Party" and State and Party interests. The rule by the Chinese Communist Party extends as far as its interests do, including to other countries.

91. The Chinese Government and Communist Party have a history and practice of seeking to apply these laws and others extraterritorially. China can use these laws and others to force TikTok or ByteDance employees subject to Chinese law to hand over consumers' data in secret.

92. China has also established more than 100 covert police stations around the world, including in the United States, and used extra-legal means to target and place pressure on Chinese citizens located abroad.

---

[43] *See, e.g.*, K. Kitchen, *The Chinese Threat to Privacy*, AM. FOREIGN POLICY COUNCIL, Issue 30, at 23 (May 2021), https://bit.ly/3A0bDyX; W. Knight, *TikTok a Year After Trump's Ban: No Change, but New Threats*, WIRED (July 26, 2021), https://bit.ly/3FWu2QW, (quoting K. Frederick, Director of the Tech Policy Center at the Heritage Foundation); K. Frederick, et al, *Beyond TikTok: Preparing for Future Digital Threats*, WAR ON THE ROCKS (Aug. 20, 2020), https://bit.ly/3WFF3fg; J. Barnes, *White House Official Says Huawei Has Secret Back Door to Extract Data*, N.Y. TIMES (Feb. 11, 2020), https://nyti ms/3udZHpH (quoting former National Security Advisor Robert O'Brien); A. Kharpal, *Huawei says it would never hand data to China's government. Experts say it wouldn't have a choice*, CNBC (Mar. 4,2019), https://cnb.cx/3Gmno6T (quoting NYU Professor of Law Emeritus and Director of the U.S.-Asia Law Institute J. Cohen and M. Thorley, postdoctoral research fellow at the University of Exeter with experience building a business in China); F. Ryan, et al., *TikTok and WeChat: Curating and controlling global information flows*, AUSTRALIAN STRATEGIC POL'Y INST., 36 (Sept. 1, 2020), https://bit.ly/3hm26vq; D. Harwell and T. Romm, *Inside TikTok: A culture clash where U.S. views about censorship often were overridden by the Chinese bosses*, WASH. POST (Nov. 5, 2019), https://wapo.st/3WPMX5S (quoting Alex Stamos, Director of the Stanford Internet Observatory).

93. Further, Chinese law enforcement and intelligence services interpret Chinese law as applying to any data, wherever it is stored, if China has a national security interest in that data. Chinese authorities have forced even refugees from China to hand over data stored outside of China to Chinese authorities under such circumstances, citing Chinese law.

94. In sum, any data stored *or accessed* by individuals or entities subject to Chinese laws, as written and as interpreted and applied by Chinese Government and Communist Party officials, is not safe from access by the Chinese Government and/or Communist Party.

**TikTok Misleads Indiana Consumers about the Risk of the Chinese Government Accessing their Data by Claiming that U.S. User Data is Not Subject to Chinese Law**

95. TikTok claims that U.S. user data, which includes Indiana consumers' data, is not subject to Chinese law.

96. TikTok states on its website: "None of our data is subject to Chinese law."[44]

97. TikTok representatives have made the same or similar public statements in multiple other fora. For example, in a 2020 interview, TikTok's former Global Security Officer Roland Cloutier stated, "Neither TikTok data, nor use, occurs in China, so therefore [the Chinese government] does not have jurisdiction over the platform. It's pretty simple. The data doesn't even exist in China." When the interviewer asked, "So if I understand this 100% correctly, because TikTok user data is stored in the United States, none of that is subject to Chinese law, right?" Mr. Cloutier answered, "Correct."[45]

[44] *Statement on TikTok's content moderation and data security practices*, TIKTOK (Oct. 24, 2019), https://bit.ly/3hm2QRe.

[45] J. Stone, *TikTok's security boss makes his case. Carefully.*, CYBERSCOOP (Aug. 27, 2020), https://bit.ly/3WRU9OL.

98. In response to questioning about the potential for the Chinese government to access U.S. user data, a common TikTok refrain is to state that U.S. user data is stored in the United States and Singapore.[46]

99. In response to questioning about the potential for the Chinese government to access U.S. user data, TikTok also frequently refers to its data security practices, including its "rigorous access controls and a strict approval process overseen by [its] U.S.-based leadership team, including technologies like encryption and security monitoring to safeguard sensitive user data."[47]

100. TikTok also has repeatedly claimed it has not shared information with the Chinese government and would not do so if asked.[48]

101. Each of these statements is deceptive and misleading. Neither TikTok's data storage practices, nor its data security practices, negate the applicability of Chinese law to that data or to the individuals and entities who are subject to Chinese law and have access to that data, or the risk of access by the Chinese Government or Chinese Communist Party.

102. TikTok's assertions that it has not shared information with the Chinese government and would not do so if asked are also deceptive and misleading, because they do not negate the applicability of Chinese law to that data or to the individuals and entities who are subject to Chinese law and have access to that data, or the risk of access by the Chinese Government or Chinese Communist Party.

---

[46] *See* David Rubenstein, *Interview of TikTok CEO Shou Zi Chew*, YouTube (Mar. 3, 2022) at 13:09-13:55, https://bit.ly/3WRUJMr; *supra*, J. Stone, *TikTok's security boss makes his case. Carefully.*, https://bit.ly/3WRU9OL; *see also, e.g.*, *Statement on TikTok's content moderation and data security practices*, TIKTOK (Oct. 24, 2019), https://bit.ly/3hm2QRe ("We store all TikTok US user data in the United States, with backup redundancy in Singapore. Our data centers are located entirely outside of China, and none of our data is subject to Chinese law.").

[47] *See, e.g.*, S. Rodriguez, *TikTok insiders say social media company is tightly controlled by Chinese parent ByteDance*, CNBC (June 25, 2021), https://cnb.cx/3NYLiXS.

[48] *See Statement on the Administration's Executive Order*, TIKTOK (Aug. 7, 2020), https://bit.ly/3G5m2wZ; D. McCabe, *Lawmakers Grill TikTok Executive About Ties to China*, New York Times (Sept. 14, 2022), https://nyti.ms/3DP0kdW (quoting TikTok's "chief operating officer" Vanessa Pappas: "And we've also said under no circumstances would we give that data to China.").

103. As one expert told the *Washington Post*, the location of data *storage* is "'pretty much irrelevant.'" Rather, "'[t]he leverage the government has over the people who have access to that data, that's what's relevant.'"[49]

104. Chinese State and Communist Party officials also have interpreted Chinese law as applying to data no matter where it is located, if China has a national security or intelligence interest in that data.

105. There is very real and serious bipartisan concern across the U.S. government that the Chinese Government and/or Communist Party may access TikTok's U.S. user data. That includes Indiana consumers' data.

106. Officials from across the political spectrum and branches of the government with knowledge and expertise in security matters have expressed alarm that because individuals and entities subject to Chinese law have access to U.S. user data, including ByteDance and its employees, if the Chinese Government or Communist Party asked for U.S. user data, the company has no meaningful way to refuse.[50]

107. The Chinese Government and Communist Party can use access to U.S. user data, including Indiana consumers' data, to, among other things, help develop artificial intelligence technologies and assist China in its espionage efforts.[51]

---

[49] D. Harwell and T. Romm, *Inside TikTok: A culture clash where U.S. views about censorship often were overridden by the Chinese bosses*, WASH. POST (Nov. 5, 2019), https://wapo.st/3WPMX5S (quoting Alex Stamos, Director of the Stanford Internet Observatory).

[50] Letter from The Hons. Tom Cotton and Charles Schumer, U.S. Senate to J. Maguire, Acting Director of National Intelligence, Office of the Director of National Intelligence (Oct. 23, 2019), *available at* https://bit.ly/3DP1rdC; Commerce Department Memorandum at 2; Letter from Mark R. Warner, Chairman and Marco Rubio, Vice Chairman, U.S. Senate Select Comm. on Intel. to the Hon. Linda Khan, Chairwoman, Fed. Trade Comm'n (July 5, 2022), *available at* https://bit.ly/3WQB8fK; L. Feiner, *FBI is 'extremely concerned' about China's influence through TikTok on U.S. users*, CNBC (Nov. 15, 2022), https://cnb.cx/3Vk2nOw.

[51] Commerce Department Memorandum at 20.

108. The Chinese Government and Communist Party can also use access to TikTok's U.S. user data, including Indiana consumers' data, to conduct surveillance on U.S. citizens and residents. According to internal company documents described by *Forbes*, ByteDance has already planned to do so.[52] Reportedly, "in at least two cases," ByteDance's Internal Audit team, led by an executive in Beijing, "planned to collect TikTok data about the location of a U.S. citizen who had never had an employment relationship with the company" for surveillance purposes.[53]

109. Multiple U.S. government agencies have banned the use of TikTok on government devices over these very security concerns.[54]

110. These bipartisan concerns persist. As recently as November 2022, Senator Mark Warner (Democrat, Virginia) called TikTok "an enormous threat." He said, "[TikTok] is a massive collector of information, oftentimes of our children. They can visualize even down to your keystrokes. So, if you're a parent and you got a kid on TikTok, I would be very, very concerned."[55] Senator Tom Cotton (Republican, Arkansas) called the platform "one of the most massive surveillance programs ever, especially on America's young people."[56]

---

[52] E. Baker-White, *TikTok Parent ByteDance Planned to Use TikTok to Monitor the Physical Location of Specific American Citizens*, FORBES (Oct. 20, 2022), https://bit.ly/3UIRFR9.

[53] *Id*.

[54] M. Meisenzahl, *US government agencies are banning TikTok, the social media app teens are obsessed with, over cybersecurity fears—here's the full list*, BUSINESS INSIDER (Feb. 25, 2020), https://bit.ly/3G6nsaK.

[55] J. Mueller, *Warner: Parents should be 'very concerned' about TikTok*, THE HILL (Nov. 20, 2022), https://bit.ly/3FlQ4Mp.

[56] I. Fisher, *TikTok is a 'massive surveillance' tool for China, senators warn as Biden admin weighs proposal to spare app from U.S. ban*, FORTUNE (Nov. 20, 2022), https://bit.ly/3EOLIvs.

**TikTok's U.S. User Data, Including Indiana Consumers' Data, Is Accessible By, and May be Shared with, Individuals and Entities Subject to Chinese Law Requiring Cooperation with National Intelligence Institutions and Cybersecurity Regulators**

111. The bipartisan concerns about the risk to TikTok users' data are not speculative, because individuals and entities who are subject to Chinese law, including those working for ByteDance, may and do access TikTok's U.S. user data, including Indiana consumers' data.[57]

112. In litigation against the U.S. government, TikTok's former Global Chief Security Officer declared,

> TikTok relies on China-based ByteDance personnel for certain engineering functions that require them to access encrypted TikTok user data. According to our Data Access Approval Process, these China-based employees may access these encrypted data elements in decrypted form based on demonstrated need and only if they receive permission from our U.S.-based team.[58]

113. In April 2020 TikTok inferred that employees across the globe, "including [in] China" have "access to user data from the EU and US," stating that its "goal" was "to minimize" that access.[59]

114. In a June 2022 letter to multiple U.S. senators, TikTok acknowledged that "[e]mployees outside the U.S., including China-based employees, can have access to TikTok U.S. user data subject to a series of robust cybersecurity controls and authorization approval protocols overseen by our U.S.-based security team."[60]

115. According to audio recordings of internal TikTok meetings reported by *Buzzfeed*,

> engineers in China had access to US data between September 2021 and January 2022, at the very least. Despite a TikTok executive's sworn testimony in an October 2021 Senate hearing that a 'world-renowned, US-based security team' decides who gets access to this data, nine statements by eight different employees describe

[57] Letter from Shou Zi Chew, CEO, TikTok to the Hon. Marsha Blackburn, Roger Wicker, John Thune, Roy Blunt, Ted Cruz, Jerry Moran, Shelley Moore Capito, Cynthia Lummis, and Steve Daines, U.S. Senate (June 30, 2022), https://bit.ly/3hqccLL ("June 2022 Letter to U.S. Senators"); Cloutier Decl. ¶ 10, Doc. 15-2, *TikTok Inc. v. Trump*, No. 20-cv-02658 (D.D.C. Sept. 23, 2021).

[58] Cloutier Decl. ¶ 10, Doc. 15-2, *TikTok Inc. v. Trump*, No. 20-cv-02658 (D.D.C. Sept. 23, 2020).

[59] R. Cloutier, *Our approach to security*, TIKTOK (Apr. 28, 2020), https://bit.ly/3A3AlOM.

[60] June 2022 Letter to U.S. Senators at 3.

> situations where US employees had to turn to their colleagues in China to determine how US user data was flowing. US staff did not have permission or knowledge of how to access the data on their own, according to the tapes.[61]

Further, "a member of TikTok's Trust and Safety department in a September 2021 meeting" said, "'Everything is seen in China,'" and in another meeting another employee "referred to one Beijing-based engineer as a 'Master Admin' who 'has access to everything.'"[62]

116. TikTok has not committed to ending access by individuals or entities subject to Chinese law to U.S. user data, including Indiana consumers' data. For example, during a hearing of the U.S. Senate Committee on Homeland Security and Governmental Affairs, Senator Rob Portman asked Ms. Pappas: "Will TikTok commit to cutting off all data and data flows to China, China-based TikTok employees, ByteDance employees, or any other party in China that might have the capability to access information on US users?" Ms. Pappas did not make that commitment.[63]

117. In June 2022, TikTok stated that "100% of US user traffic is now being routed to Oracle cloud infrastructure" in the United States.[64] Eventually, TikTok "expect[s] to delete US users' protected data from our own systems and fully pivot to Oracle cloud services located in the US," though TikTok continues to use its own "U.S. and Singapore data centers for backup."[65]

118. TikTok CEO Shou Zi Chew claims this arrangement with Oracle will resolve all security concerns. But it is not clear what data will be deemed "protected" under this proposed

---

[61] E. Baker-White, *Leaked Audio From 80 Internal TikTok Meetings Shows that US User Data has been Repeatedly Accessed from China*, BUZZFEED NEWS (June 17, 2022), https://bit.ly/3u8Eb5N.

[62] *Id.*

[63] *Social Media's Impact on Homeland Security*, U.S. SENATE COMM. ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS, at 2:38:55 (Sept. 14, 2022), https://bit.ly/3P5kuWd; B. Fung, *TikTok won't commit to stopping US data flows to China*, CNN (Sept. 14, 2022) https://cnn.it/3G5beis; D. McCabe, *Lawmakers Grill TikTok Executive About Ties to China*, N.Y. TIMES (Sept. 14, 2022) https://nyti.ms/3DP0kdW.

[64] June 2022 Letter to U.S. Senators at 4.

[65] *Id.*

arrangement. Moreover, the CEO has not committed to limiting access to that data by all individuals and entities subject to Chinese law and the oppressive Chinese regime.

119. Additionally, according to Oracle, currently "Oracle is not providing anything 'other than our own security' for TikTok."[66] "'TikTok is running in the Oracle cloud, but . . . they have full control of everything they're doing,'" and Oracle has "'absolutely no insight one way or the other' into who can access TikTok user data."

120. In addition to TikTok's statements that some China-based employees may access unencrypted U.S. user data, which includes Indiana consumers' data, TikTok's privacy policy permits TikTok to share information with ByteDance "or other affiliate of our corporate group."[67]

121. ByteDance and any affiliates and their employees who are located in China or are Chinese citizens are subject to Chinese law and the oppressive Chinese regime, including but not limited to laws requiring cooperation with national intelligence institutions and cybersecurity regulators.[68]

122. Because ByteDance is subject to Chinese law, and TikTok's privacy policy expressly permits TikTok to share data with ByteDance, TikTok's statements that Chinese law does not apply to that data are false and misleading.

---

[66] E. Baker-White, *TikTok Parent ByteDance Planned to Use TikTok to Monitor the Physical Location of Specific American Citizens*, FORBES (Oct. 20, 2022), https://bit.ly/3UIRFR9.

[67] *TikTok Privacy Policy*, TIKTOK (June 2, 2021), https://bit.ly/3fsbUnd.

[68] *See, eg.*, *TikTok owner to 'strictly' obey China's tech takeover law*, BBC NEWS (Aug. 31, 2020), https://bbc.in/3UqgfX8; S. Hoffman, *The U.S. and China Data Fight is Only Getting Started*, FOREIGN POLICY (July 22, 2021), https://bit.ly/3UwxI00 ("The Chinese Communist Party has absolute power over China-based companies, which its laws—like the 2021 Data Security Law, 2015 National Security Law, 2016 Cybersecurity Law, or 2017 National Intelligence Law—have reinforced."); PATRICIA M. FIGLIOLA, CONG. RSCH. SERV., R46543, TIKTOK: TECHNOLOGY OVERVIEW AND ISSUES at Summary (Dec. 4, 2020), *available at* https://bit.ly/3G8YGGX ("ByteDance, like all technology companies doing business in China, is subject to Chinese laws that require companies operating in the country to turn over user data when asked by the government.").

123. Another affiliate of TikTok is Beijing Douyin Information Service Limited, formerly known as Beijing Bytedance Technology Co. Ltd., a China-based subsidiary of ByteDance.[69]

124. Beijing Douyin Information Service Limited is subject to Chinese law, as well as to direct control and influence by the Chinese Government/Communist Party by virtue of state ownership.

125. Beijing Douyin Information Service Limited is 1% owned by a Chinese state-owned enterprise, specifically "Wangtou Zhongwen (Beijing) Technology, which is owned by the China Internet Investment Fund (controlled by the Cyberspace Administration of China and the Ministry of Finance), China Media Group, and Beijing Municipality Cultural Investment Development Group."[70] The state entity also sits on the board of Beijing Douyin Information Service Limited.

126. In China, even a minority stake in a private company "makes any state-invested enterprise subject to Beijing's influence and control, no matter how small its investment," because "Chinese law already affords the state privileged status in the governance of any corporation for which it is a shareholder."[71]

127. TikTok states that employees of Beijing Douyin Information Service Limited "are restricted from U.S. user database access."[72]

[69] June 2022 Letter to U.S. Senators at 6.

[70] *Id.*; U.S.-CHINA ECONOMIC AND SECURITY REVIEW COMMISSION, 2021 REPORT TO CONGRESS, at 135-36, n. † (Nov. 2021) ("2021 Commission Report"), *available at* https://bit.ly/3gOwYFf.

[71] 2021 Commission Report at 9.

[72] June 2022 Letter to U.S. Senators at 6.

128. However, when questioned directly about whether Beijing Douyin Information Service Limited is an "affiliate" of TikTok with whom TikTok may share user data under its privacy policy, TikTok has not provided a clear answer.[73]

129. Indiana law addressing businesses and associations defines "affiliate" as "a person that directly, or indirectly through one (1) or more intermediaries, controls, is controlled by, or *is under common control with*, a specified person." IND. CODE § 23-1-43-1 (emphasis added).

130. Regardless then of whether TikTok affirmatively states that the term "affiliate" applies to Beijing Douyin Information Service Limited, with which it is under common control by ByteDance, for purposes of its privacy policy, a reasonable Indiana consumer would understand "affiliate of our corporate group" to include Beijing Douyin Information Service Limited.

131. Because Beijing Douyin Information Service Limited is subject to Chinese law, as well as to influence and control by the Chinese Government and Communist Party, to the extent TikTok's privacy policy permits TikTok to share U.S. user data, including Indiana consumers' data, with Beijing Douyin Information Service Limited, TikTok's statements that Chinese law does not apply to that data are false and misleading.

132. TikTok's assertions that U.S. user data are not subject to Chinese law are false, deceptive and misleading to Indiana consumers because they create the false impression that consumers' data is not at risk of access by the Chinese Government or Communist Party, when entities and individuals who do have access to that data, or with whom the data may be shared according to TikTok's privacy policy, are subject to Chinese laws, including but not limited to laws requiring cooperation with national intelligence institutions and cybersecurity regulators, and at least in one case are subject to direct influence and control by the Chinese Government and

[73] Press Release, Sen. Ted Cruz, Sen. Cruz to TikTok Official: 'You Have Dodged the Questions More Than Any Witness I Have Seen in My Nine Years Serving in the Senate,' (Oct. 26, 2021), https://bit.ly/3Un3yLL.

Communist Party. Further, Chinese State and Party officials have interpreted Chinese law as applying to any data in which it has a national intelligence or security interest, no matter where the data is located.

**TikTok's U.S. User Data Has been Stored on Servers Owned and Operated, and/or Hosted by Entities Subject to Chinese Law**

133. As noted above, when questioned about whether the Chinese government may access U.S. user data, TikTok often states that U.S. user data, which includes Indiana consumers' data, is stored in the U.S. and Singapore.[74]

134. These statements are deceptive and misleading because they do not disclose that U.S. user data, which includes Indiana consumers' data, is accessible to and may be shared with individuals and entities in China and otherwise subject to Chinese law. Further, Chinese State and Party officials have interpreted Chinese law as applying to any data in which it has a national intelligence or security interest, no matter where the data is located. TikTok's statements are also deceptive and misleading because they do not disclose that at least some of this data is or was, at least as of 2020, located on servers owned and operated by ByteDance or stored with Alibaba cloud—both Chinese companies subject to Chinese laws, including but not limited to laws requiring cooperation with national intelligence institutions and cybersecurity regulators.

135. Specifically, certain data centers used by TikTok in the United States to store U.S. user data, which includes Indiana consumers' data, at least as of October 2020, housed servers owned and operated by *ByteDance*.[75]

---

[74] *Statement on TikTok's content moderation and data security practices*, TIKTOK (Oct. 24, 2019), https://bit.ly/3hm2QRe; R. Zhong, *TikTok's Chief is on a Mission to Prove it's Not a Menace*, N.Y. TIMES (Nov. 18, 2019), https://nyti.ms/3WXmWl0; C. Porterfield, *U.S. Army Bans Soldiers from Using TikTok*, FORBES (Jan. 2, 2020), https://bit.ly/3WVOOGj.

[75] Commerce Department Memorandum at 16; Cloutier Suppl. Decl. ¶ 8, Doc. 43-2, *TikTok Inc. v. Trump*, No. 20-cv-02658 (D.D.C. Oct. 14, 2020).

136. In litigation, Mr. Cloutier declared that "ByteDance owns and operates all servers that are stored within the . . . facility" provided by CUA, China Unicom (Americas) Operations Ltd., a company "wholly owned and controlled by a single Chinese entity that is directly owned by the PRC Government."[76] Mr. Cloutier also declared that ByteDance had its "own security team monitoring the technical access environment" for those servers.[77]

137. ByteDance is subject to Chinese Law, including but not limited to laws requiring cooperation with national intelligence institutions and cybersecurity regulators. Chinese State and Party officials also have interpreted Chinese law as applying to any data in which it has a national intelligence or security interest, no matter where the data is located.

138. Additionally, TikTok, at least as of October 2020, contracted with Alibaba cloud for its backup data storage in Singapore.[78]

139. As the Commerce Department has noted, "Alibaba is a Chinese company and, like ByteDance, is similarly beholden to [Chinese] 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 [China's intelligence and security services]."[79]

140. In 2018, Alibaba was blocked by the U.S. from acquiring a U.S. money transfer company over national security concerns about "the safety of data that can be used to identify U.S. citizens."[80]

141. To state widely to consumers that the data is stored in data centers located in the United States and Singapore, but omit the identity of the owners, operators and/or hosts of the

[76] Cloutier Suppl. Decl. ¶ 8, Doc. 43-2, *TikTok Inc. v. Trump*, No. 20-cv-02658 (D.D.C. Oct. 14, 2020).
[77] *Id*.
[78] Commerce Department Memorandum at 15; Cloutier Suppl. Decl. ¶ 8, Doc. 43-2, *TikTok Inc. v. Trump*, No. 20-cv-02658 (D.D.C. Oct. 14, 2020).
[79] Commerce Department Memorandum at 15.
[80] G. Roumeliotis *U.S. blocks MoneyGram sale to China's Ant Financial on national security concerns*, REUTERS (Jan. 2, 2018), https://reut rs/3WXp2RU.

servers paints the false picture for Indiana consumers that their data is not at risk of access by the Chinese Government or Communist Party, when their data is stored on servers owned and operated and/or hosted by Chinese entities, who are subject to Chinese law, including but not limited to laws requiring cooperation with national intelligence institutions and cybersecurity regulators.

142. TikTok also misleads Indiana consumers about the storage of their data when it says that it does not store U.S. user data in China and that the data "does not exist" in China.

143. In reality, as shown by an internal document drafted by a member of ByteDance's Internal Audit team as reported by *Forbes*, even when using data centers located outside China, "it is impossible to keep data that should not be stored in [China] from being retained in [China]-based servers."[81]

144. Any information stored or retained on servers in China is subject to Chinese law, including but not limited to laws requiring cooperation with national intelligence institutions and cybersecurity regulators.

**TikTok's Privacy Policy is Misleading because it Does Not Disclose that User Data, which Includes Indiana Consumers' Data, May Be Shared with Individuals and Entities in China**

145. Public reporting shows that prior to sometime in 2019, TikTok's U.S. privacy policy stated: "We will also share your information with any member of our affiliate group, in China . . . ."[82]

146. TikTok's current U.S. privacy policy states: "We may share all of the information we collect with a parent, subsidiary, or other affiliate of our corporate group."[83]

[81] E. Baker-White, *TikTok Parent ByteDance Planned to Use TikTok to Monitor the Physical Location of Specific American Citizens*, FORBES (Oct. 20, 2022), https://bit.ly/3UIRFR9.

[82] D. Carroll, *Is TikTok a Chinese Cambridge Analytica data bomb waiting to explode?*, QUARTZ (May 7, 2019) https://bit.ly/3zDuAqO.

[83] *TikTok Privacy Policy*, TIKTOK (June 2, 2021), https://bit.ly/3fsbUnd.

147. TikTok's U.S. privacy policy further states: "TikTok may transmit your data to its servers or data centers outside of the United States for storage and/or processing. Third parties with whom TikTok may share your data as described herein may be located outside of the United States."[84]

148. Just as in 2019, TikTok's parent company, ByteDance, and other affiliates, are still located in China.

149. However, the word "China" no longer appears in TikTok's current privacy policy applicable to U.S. users, including Indiana consumers.

150. TikTok's current U.S. privacy policy does not alert Indiana consumers to the ability of TikTok to share their data with individuals or entities located in China, or for individuals or entities located in China to access that data.

151. TikTok has updated its *European* privacy policy to clearly state that it permits individuals located in a list of countries outside of Europe, specifically including China, to access European user data.[85] Disclosing the individual countries where user data may be accessed arms users with information they need to fully understand what laws and practices may apply to their data. Without that information, users are left totally in the dark about the consequences of agreeing to a privacy policy, and of consenting to specific data collection practices such as allowing TikTok to collect consumers' precise GPS location.

152. TikTok has made no such update to its U.S privacy policy, which applies to Indiana consumers, explicitly informing them that their data is accessed by and may be shared with individuals in China.

---

[84] *Id.*

[85] E. Fox, *Sharing an Update to Our Privacy Policy*, TIKTOK (Nov. 2, 2022), https://bit.ly/3uivRAs.

153. Removing the word "China" from these terms creates the deceptive and misleading impression that although Indiana consumers' data was once accessible in or could be shared with individuals in China subject to Chinese law, that is no longer the case.

154. TikTok also misleads and deceives Indiana consumers because in omitting the word "China" from its privacy policy, which is accessible through its pages on the App Store and the Google Play Store, TikTok fails to comply with Apple's and Google's requirements for application developers to appear on the App Store and Google Play Store.

155. Apple makes publicly available the terms and conditions with which all application developers must comply in order to be made available on the App Store, including its developer license agreement.[86] Apple requires application developers to "provide *clear and complete information to users* regarding Your collection, use and disclosure of user or device data in the App Description on the App Store" and "provide a privacy policy . . . explaining Your collection, use, disclosure, sharing, retention, and deletion of user or device data."[87] Application developers must also comply with the App Store Review Guidelines, which state that the developers "must provide access to information about how and *where* [user] data will be used" and that "[d]ata collected from apps may only be shared with third parties to improve the app or serve advertising." Further, "[d]ata collected for one purpose may not be repurposed without further consent unless otherwise explicitly permitted by law."[88]

156. Similarly, Google's Developer Policy Center requires application developers to, among other things, "be transparent in how you handle user data," "disclos[e your app's] access,

[86] APPLE DEVELOPER LICENSE AGREEMENT, at 18 (June 6, 2022), *available at* https://apple.co/3H8JnP3.
[87] *Id.* (emphasis added).
[88] APP STORE REVIEW GUIDELINES § 5.1.2, APPLE (last updated Oct. 24, 2022), *available at* https://apple.co/3XSFIdO (emphasis added).

collection, use, handling, and sharing of user data, . . . and limit[] the use of the data to the . . . purposes disclosed."[89]

157. TikTok's availability on the App Store and Google Play Store signals to Indiana consumers that TikTok complies with Apple's and Google's terms and policies for application developers. But, in its App Description on the App Store and the Google Play Store, TikTok links to its privacy policy, which makes no mention of TikTok's ability to share user data with individuals and entities in China or those individuals' and entities' access to that data, even though TikTok knows that the affiliates of its corporate group with which it says it may share data are located in China and subject to Chinese law.

158. By omitting this information from its U.S. privacy policy, TikTok is not being "transparent" about what it is doing with Indiana users' data. It is not providing "clear and complete information to users" about its "collection, use and disclosure of [their] user or device data," including but not limited to "how and where [their] data will be used."

159. TikTok deceives and misleads Indiana consumers who trust when they download the app from the App Store or the Google Play store that the app complies with all of Apple's and Google's requirements for application developers. The app does not comply with those requirements.

**TikTok Misleads Indiana Consumers about the Risk of the Chinese Government Accessing their Data by Downplaying the Control Exercised by its Parent Company in China, ByteDance, which is Significantly Influenced by, and Cooperates Closely with, the Chinese Government and Communist Party**

160. TikTok also misleads Indiana consumers about the risk of the Chinese Government's and/or Communist Party's access to their data by downplaying the significant

[89] USER DATA, GOOGLE (last visited Dec. 1, 2022), https://bit.ly/3FjuR5D.

influence and control that its parent company ByteDance has over TikTok. This is an intentional, strategic choice made by TikTok.

161. TikTok documents demonstrate that TikTok's "messaging" strategy calls for company representatives to "Downplay the parent company ByteDance, downplay the China association, downplay AI."[90]

162. In line with these internal "messaging" documents, TikTok and its representatives are in fact downplaying its parent company in China, ByteDance, and downplaying "the China association."

163. For example, in a public hearing before the U.S. Senate Committee on Homeland Security and Governmental Affairs, then-CEO Vanessa Pappas admitted that "ByteDance is founded in China," but claimed "we do not have an official headquarters as a global company."[91]

164. TikTok's public statements stress the independence of the company's leadership from ByteDance. Those statements include, but are not limited to:

> "TikTok's CEO has full autonomy for all decisions about TikTok's operations."[92]
>
> "TikTok is led by its own global CEO, Shou Zi Chew, a Singaporean based in Singapore."[93]
>
> "TikTok is led by an American CEO, with hundreds of employees and key leaders across safety, security, product, and public policy here in the U.S."[94]

---

[90] C. Stokel-Walker, *Inside TikTok's Attempts to 'Downplay the China Association'*, GIZMODO (July 27, 2022), https://bit.ly/3EV8XnY.

[91] D. McCabe, *Lawmakers Grill TikTok Executive About Ties to China*, N.Y. TIMES (Sept. 14, 2022), https://nyti.ms/3DP0kdW.

[92] E. Baker-White, *Inside Project Texas, TikTok's Big Answer to US Lawmakers' China Fears*, BUZZFEED (Mar. 10, 2022), https://bit.ly/3AU26tD.

[93] June 2022 Letter to U.S. Senators at 5.

[94] A. Kharpal, *U.S. is 'looking at' banning TikTok and Chinese social media apps, Pompeo says*, CNBC (July 7, 2020), https://cnb.cx/3Fc3XfL.

"Since May 2020, TikTok management has reported into the CEO based in the U.S., and now Singapore, who is responsible for all long-term and strategic day-to-day decisions for the business."[95]

165. TikTok also asserts its independence from ByteDance control in its content moderation and data security practices.

166. For example, TikTok states that access to U.S. user data, which includes Indiana consumers' data, is controlled by a "U.S. based security team."[96]

167. TikTok also states that its "team" responsible for reviewing content "pursuant to our U.S. policies" "is led out of California," and further that "TikTok does not remove content based on sensitivities related to China."[97]

168. Tik Tok also downplays "the China association" by dismissing Chinese Communist Party presence and influence within ByteDance as unimportant or irrelevant.

169. For example, when asked during a public Senate hearing whether TikTok or ByteDance employ members of the Chinese Communist Party, TikTok's Chief Operating Officer Vanessa Pappas did not directly answer the question, stating that no one who "makes a strategic decision at this platform" is a member of the Party.[98] When asked whether anyone with access to TikTok's U.S. user data, which includes Indiana consumers' data, is a member of the Chinese

[95] S. Rodriguez, *TikTok insiders say social media company is tightly controlled by Chinese parent ByteDance*, CNBC (June 25, 2021), https://cnb.cx/3NYLiXS.

[96] June 2022 Letter to U.S. Senators at 3.

[97] *Statement on TikTok's content moderation and data security practices*, TIKTOK (Oct. 24, 2019), https://bit.ly/3hm2QRe.

[98] Senate Hearing, https://bit.ly/3P5kuWd, at 3:15:18; E. Baker-White, *No TikTok Leaders have Ties to the Chinese Communist Party, COO Says in Heated Senate Hearing*, FORBES (Sept. 14, 2022), https://ibit.ly/BoEg.

Communist Party, Ms. Pappas said merely that TikTok could not attest to employees' political affiliations.[99]

170. TikTok's efforts to "downplay the parent company ByteDance" and "downplay the China association" are designed to, and have the effect of, painting a picture for Indiana consumers that the risk of their data being accessed and exploited by the Chinese Government or the Chinese Communist Party is minimal to nonexistent.

171. These statements are deceptive and misleading, because TikTok's parent company ByteDance owns and exercises significant control over TikTok, and because ByteDance has significant connections to, has been significantly influenced by, and cooperates with, the Chinese Government and Communist Party, placing U.S. user data, including Indiana consumers' data, at significant risk.

**ByteDance Exercises Significant Control over TikTok**

172. Contrary to its public statements, ByteDance exercises significant control over TikTok.

173. TikTok's algorithm was created by ByteDance and contains "some of the same underlying basic technology building blocks" as ByteDance's Chinese version of the app operating in China, known as Douyin.[100]

174. TikTok's algorithm still belongs to ByteDance, which declined to sell the technology to a U.S. company.[101]

---

[99] *Social Media's Impact on Homeland Security*, U.S. SENATE COMM. ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS, at 3:14:24 (Sept. 14, 2022), https://bit.ly/3P5kuWd; A. Smith, *GOP senator calls on Yellen to 'ensure' TikTok severs its connections to China*, NBC (Sept. 19, 2022), https://nbcnews.to/3ixsYJH.

[100] June 2022 Letter to U.S. Senators at 4.

[101] Z. Xin and T. Qu, *TikTok's algorithm not for sale, ByteDance tells US*, SOUTH CHINA MORNING POST (Sept. 13, 2020), https://bit.ly/3Uje9HQ.

175. ByteDance "plays a role in the hiring of key personnel at TikTok."[102]

176. High-level ByteDance employees have served in dual roles for ByteDance and for TikTok Inc., at least as recently as 2021.

177. In litigation, TikTok disclosed that the "Head of TikTok Inc.," Vanessa Pappas, was also "the interim head of the global TikTok business for ByteDance Ltd. ('ByteDance'), TikTok Inc.'s parent company."[103]

178. Similarly, TikTok's then-Global Chief Security Officer, Roland Cloutier, also had "responsibilities" working for both TikTok and its corporate parent, ByteDance. Specifically, those "responsibilities include[d] providing cyber risk and data security support for both TikTok Inc. and its corporate parent, ByteDance Ltd."[104]

179. In April 2021, TikTok's current CEO, Shou Zi Chew, was named as CEO of TikTok while also serving as CFO of ByteDance Ltd.[105]

180. The LinkedIn profiles of multiple other TikTok employees with a variety of responsibilities, from human resources to engineering, show they simultaneously exercise dual or additional roles at ByteDance.

181. According to *Buzzfeed*, as of March 2022, TikTok's U.S.-based personnel who will have access to TikTok data pursuant to its new arrangement with Oracle "report to middle managers in the United States, who report to a ByteDance executive in China."[106]

---

[102] June 2022 Letter to U.S. Senators at 5; *see also* D. Harwell and E. Dwoskin, *As Washington Wavers on TikTok, Beijing Exerts Control*, WASH. POST (Oct. 28, 2022), https://wapo.st/3VjMvLV (noting that managers in Beijing are "even the final decision-makers on human resources matters, such as whether an American employee can work remotely)."

[103] Pappas Decl. ¶ 1, Doc. 15-3, *TikTok Inc. v. Trump*, No. 20- cv-02658 (D.D.C. Sept. 23, 2020).

[104] Cloutier Decl. ¶ 1–2, Doc. 15-2, *TikTok Inc. v. Trump*, No. 20-cv-02658 (D.D.C. Sept. 23, 2020).

[105] *TikTok Names CEO and COO*, TIKTOK (Apr. 30, 2021), https://bit.ly/3OVyvWh; R. Mac and C. Che, *TikTok's CEO Navigates the Limits of His Power*, N.Y. TIMES (Sept. 16, 2020), https://nyti.ms/3OT6grk.

[106] E. Baker-White, *Inside Project Texas, TikTok's Big Answer to US Lawmakers' China Fears*, BUZZFEED NEWS (Mar. 11, 2022), https://ibit.ly/eqlB.

182. TikTok's Internal Audit team also reports to ByteDance's Internal Audit and Risk Control Department, led by an executive located in Beijing.[107]

183. ByteDance's Internal Audit and Risk Control Department investigates TikTok employees, including those located outside of China.[108] For example, according to *Forbes*, ByteDance's Internal Audit team conducted "multiple audits and investigations into [former Global Chief Security Officer Roland] Cloutier" for allegedly steering contracts to friends.[109] On information and belief, and according to current and former employees who reportedly spoke to *Forbes*, those investigations were "pretextual fishing expeditions designed to find a reason to push him out of the company."[110]

184. Public reporting demonstrates that multiple former TikTok employees have reported that ByteDance exercises significant control over TikTok's decision making and operations.

185. According to the *New York Times*, twelve former TikTok and ByteDance employees and executives reported that TikTok's CEO, Shou Zi Chew, has "limited" decision making power.[111] Rather, they reported, major decisions related to TikTok are made by ByteDance founder Zhang Yiming and other ByteDance officials located in China.[112]

---

[107] E. Baker-White, *A China-Based ByteDance Team Investigated TikTok's Global Security Chief, Who Oversaw U.S. Data Concerns*, FORBES (Oct. 25, 2022), https://bit.ly/3uoxblj.

[108] *Id*.; E. Baker-White, *TikTok Parent ByteDance Planned to Use TikTok to Monitor the Physical Location of Specific American Citizens*, FORBES (Oct. 20, 2022), https://bit.ly/3UIRFR9.

[109] E. Baker-White, *A China-Based ByteDance Team Investigated TikTok's Global Security Chief, Who Oversaw U.S. Data Concerns*, FORBES (Oct. 25, 2022), https://bit.ly/3uoxblj.

[110] *Id*.

[111] R. Mac and C. Che, *TikTok's CEO Navigates the Limits of His Power*, N.Y. TIMES (Sept. 16, 2020), https://nyti.ms/3OT6grk.

[112] *Id.*

186. *Forbes* recently reported that "[a]t least five senior leaders hired to head departments at TikTok in the last two years have left the company after learning that they would not be able to significantly influence decision-making."[113]

187. *Forbes* further reported that senior leaders departed TikTok after learning they would be taking direction from ByteDance.

188. One former TikTok employee even reported to *Forbes* that their paycheck showed *ByteDance* as the drawer, not TikTok; another reported their tax returns listed *ByteDance* as their employer.

189. According to *Forbes*, even ByteDance's own Internal Audit team prepared a "risk assessment . . . in late 2021 [that] found that numerous senior employees felt 'that themselves and their teams are just 'figureheads' or 'powerless ombudsmen' who are 'functionally subject to the control of [China]-based teams.'"[114]

190. *Forbes* also reported that "[e]mployees who worked on product, engineering and strategy at TikTok into 2022—including those on teams handling sensitive U.S. user data—also told Forbes that they reported directly into ByteDance leadership in China, bypassing TikTok's executive suite."[115]

191. CNBC also reported that former TikTok employees described ByteDance as being "heavily involved" in decision making and operations at TikTok, and that boundaries between the

[113] E. Baker-White, *TikTok is Bleeding U.S. Execs Because China is Still Calling the Shots*, FORBES (Sept. 21, 2022), https://bit.ly/3XTSnNF.

[114] E. Baker-White, *A China-Based ByteDance Team Investigated TikTok's Global Security Chief, Who Oversaw U.S. Data Concerns*, FORBES (Oct. 25, 2022), https://bit.ly/3B3v5Lt.

[115] E. Baker-White, *TikTok is Bleeding U.S. Execs Because China is Still Calling the Shots*, FORBES (Sept. 21, 2022), https://bit.ly/3XTSnNF.

two companies are "blurry".[116] One employee reported working China's business hours in addition to U.S. business hours in order to be responsive to ByteDance employees working in China.

192. According to current and former employees who reportedly spoke with the *Washington Post*:

> China remains [TikTok's] central hub for pretty much everything . . . . Beijing managers sign off on major decisions involving U.S. operations, *including from the teams responsible for protecting Americans' data* and deciding which videos should be removed. They lead TikTok's design and engineering teams and oversee the software that U.S. employees use to chat with colleagues and manage their work. They're even the final decision-makers on human resources matters, such as whether an American employee can work remotely.[117]

193. According to the *Washington Post*, one employee "who works in U.S. content moderation" said, "As I get more senior at the company, I realize China has more control."[118]

194. TikTok employees in the United States regularly communicate with counterparts in China using ByteDance communication apps.[119]

195. Statements made by 24 former TikTok employees directly to an American journalist confirm that ByteDance is in full control of TikTok. Those statements include:[120]

> "'The Chinese execs, they're in control.' . . . 'The American execs are there to smile, look pretty, push away criticism. But ByteDance is still calling the shots behind the scenes.'"

> "TikTok is an American company on paper. It's a Chinese company underneath."

---

[116] S. Rodriguez, *TikTok insiders say social media company is tightly controlled by Chinese parent ByteDance*, CNBC (June 25, 2021), https://cnb.cx/3NYLiXS.

[117] D. Harwell and E. Dwoskin, *As Washington Wavers on TikTok, Beijing Exerts Control*, WASH. POST (Oct. 28, 2022), https://wapo.st/3VjMvLV (emphasis added).

[118] *Id.*

[119] A. Brown and D. Chmielewski, *The Inside Story of TikTok's Tumultuous Rise—and How it Defeated Trump*, FORBES (May 5, 2021), https://bit.ly/3XMUov8.

[120] G. Cain, *How China Got Our Kids Hooked on 'Digital Fentanyl'*, COMMON SENSE (Nov. 16, 2022), https://bit.ly/3VLbUhG.

**The Chinese Government and Communist Party Exercise Significant Influence over ByteDance**

196. The Chinese Government and Chinese Communist Party have exerted significant influence over ByteDance, and ByteDance cooperates closely with the Chinese Government and Chinese Communist Party.

197. The Chinese Government and/or Communist Party have influenced ByteDance's business decisions, including forcing the company to alter certain business practices, and shutter one business altogether.

198. In 2018, China's state media regulator, the State Administration of Press, Publication, Radio, Film and Television of the People's Republic of China, forced ByteDance to shut down one of its platforms for "having violated 'social morality.'"[121] As a result of the action by the Chinese Government, ByteDance also hired thousands of moderators with qualifications including "'strong political sensitivity.'"[122]

199. In response to the Chinese government's action, then CEO (and founder) of ByteDance Zhang Yiming issued a public apology, saying that ByteDance's "product took the wrong path" because "content appeared that was incommensurate with socialist core values." In this apology, Yiming traced "a deep-level cause of the recent problems in [ByteDance] [to]: "a weak [understanding and implementation of] 'the four consciousnesses' [of Xi Jinping]; deficiencies in education on the socialist core values; and deviation from public opinion guidance." He pledged, among other things, to "[s]trengthen the work of Party construction, carrying out education among our entire staff on the 'four consciousnesses,' socialist core values, [correct] guidance of public opinion, and laws and regulations, truly acting on the company's social

[121] Commerce Department Memorandum at 9.

[122] *Id.* at 9 (citing S. Pham, *Why China's Tech Giants are cozying up to the Communist Party*, CNN (Nov. 4, 2018), https://cnn.it/3OXvAfK).

responsibility" and "[f]urther deepen cooperation with authoritative [official Party] media, elevating distribution of authoritative media content, [and] ensuring that authoritative [official Party] media voices are broadcast to strength."[123]

200. ByteDance soon made good on Zhang Yiming's promise to cooperate further with "authoritative" media.

> 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."[124]

201. "Authoritative" Chinese State Media post content frequently on TikTok that is visible to Indiana consumers, though TikTok makes no effort to alert consumers to that fact.

202. Chinese State Media posts content on TikTok under several accounts managed by a "Washington D.C.-based outpost of the main Chinese Communist Party television news outlet, China Central Television."[125] That entity, MediaLinks TV LLC, reportedly is registered with the Department of Justice as a foreign agent. The accounts' profiles merely note that posts are "by MediaLinks TV LLC on behalf of CCTV" and state "More info at DOJ, D.C." Of course, the average Indiana consumer does not readily recognize "CCTV" as signifying Chinese State Media. Most consumers do not even see this meager disclosure, because is it only available on the accounts' profiles.

---

[123] D. Bandurski, *Tech Shame in the 'New Era*,' CHINA MEDIA PROJECT (Apr. 11, 2018), https://bit.ly/3Vidtnj.

[124] Commerce Department Memorandum at 11 (quoting K. Everington, *TikTok owners show true colors with communist flag*, TAIWAN NEWS (Aug. 6, 2020), https://bit.ly/3H4QMP7)).

[125] E. Baker-White, *On TikTok, Chinese State Media Pushes Divisive Videos about U.S. Politicians*, FORBES (Dec. 1, 2022), https://bit.ly/3P0p4oM.

203. One of these Chinese State Media accounts, @NewsTokss, regularly posts "divisive content," including about American politicians surrounding the 2022 midterm elections and controversial social issues, including the same ones pushed by "a China-based election influence operation."[126]

204. TikTok makes no effort to label these accounts and their content as controlled by Chinese State Media, even though every other major social media platform does.

205. The Chinese Government and Communist Party assert significant control over ByteDance's, and TikTok's, business decisions in other ways as well. In 2020, when TikTok reportedly was considering a purchase by a U.S. company, the Chinese government expanded its export control restrictions to cover TikTok's algorithm, making it much more difficult to complete the sale.[127] ByteDance subsequently refused to sell the technology, and TikTok remains in ByteDance's control.[128]

206. Like other technology companies in China, pursuant to regulations enacted by the Cyberspace Administration of China, "a merged party-state institution listed under the Central Committee of the Chinese Communist Party,"[129] ByteDance has shared details about its algorithm for Douyin—essentially the Chinese version of TikTok—with the internet regulator.[130]

---

[126] *Id.*

[127] P. Mozur, et al., *TikTok Deal Is Complicated By New Rules From China Over Tech Exports*, N.Y. TIMES (Aug. 29, 2020), https://nyti.ms/3XNyl7E.

[128] Z. Xin and T. Qu, *TikTok's algorithm not for sale, ByteDance tells US*, SOUTH CHINA MORNING POST (Sept. 13, 2020), https://bit.ly/3Uje9HQ.

[129] J. Horsley, *Behind the Façade of China's Cyber Super-Regulator*, DIGICHINA, STANFORD (Aug. 8, 2022), https://stanford.io/3FPAOYy; A. Liang, *Chinese internet giants hand algorithm data to government*, BBC NEWS (AUG. 16, 2022), https://bbc.in/3iwBsQZ.

[130] A. Kharpal, *Chinese Tech Giants Share Details of their Prized Algorithms with Top Regulator in Unprecedented Move*, CNBC (Aug. 15, 2022), https://cnb.cx/3Fl3yI4.

207. According to reporting cited by the Commerce Department, as of August 2020, at least 130 ByteDance employees, including "[m]any" in management positions, were members of the Chinese Communist Party.[131]

208. "According to September 2020 Chinese reporting, ByteDance established a party branch in October 2014. 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. 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 [C]ompanies."[132]

209. According to *Forbes*,

> [t]hree hundred current employees at TikTok and its parent company ByteDance previously worked for Chinese state media publications, according to public employee LinkedIn profiles reviewed by *Forbes*. Twenty-three of these profiles appear to have been created by current ByteDance directors, who manage departments overseeing content partnerships, public affairs, corporate social responsibility and 'media cooperation.' Fifteen indicate that current ByteDance employees are also concurrently employed by Chinese state media entities.[133]

210. ByteDance has stated it makes "[h]iring decisions based purely on an individual's professional capability to do the job. For our China-market businesses, that *includes people who have previously worked in government or state media positions in China*."[134]

211. By downplaying ByteDance and the "China association," TikTok ignores and dismisses the significance of Communist Party influence on ByteDance and the risk that it poses to consumer data. But the prevalence of the Party throughout private enterprise in China signifies

---

[131] Commerce Department Memorandum at 7–8 (citing N. Hao, *TikTok's Parent Company Employs Chinese Communist Party Members in its Highest Ranks*, THE EPOCH TIMES (Aug. 7, 2020), https://bit.ly/3OWXFnF).

[132] Commerce Department Memo at 8 (citing Chinese language news sources).

[133] E. Baker-White, *LinkedIn Profiles Indicate 300 Current TikTok and ByteDance Employees Used to Work for Chinese State Media—and Some Still Do*, FORBES (Aug. 11, 2022), https://bit.ly/3ijFf47.

[134] *Id.* (emphasis added).

its growing influence.[135] That growing presence and influence is a key feature of Chinese Government and Communist Party policy.[136]

212. For example, the Commerce Department noted that internal Communist 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."[137] Further:

> 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.[138]

213. According to the Center for Strategic and International Studies (CSIS), Chinese leaders have called for increasing the role of party committees in private enterprises, to "include giving a company's internal Party group control over the human resources decisions of the enterprise and allowing it to carry out company audits, including monitoring internal behavior."[139]

214. A September 15, 2020, Opinion issued by the General Office of the Central Committee of the Chinese Communist Party on "Strengthening the United Front Work of the

---

[135] S. Livingston, *The Chinese Communist Party Targets the Private Sector*, CSIS (Oct. 8, 2020), https://bit.ly/3uiMT1x; 2021 Commission Report (generally); S. Livingston, *The New Challenge of Communist Corporate Governance*, CSIS (Jan. 15, 2021), https://bit.ly/3gNPyNH.

[136] D. Wakabayashi, et al., *In Xi's China, the Business of Business is State-Controlled*, N.Y. TIMES (Oct. 17, 2020), https://nyti ms/3OVMICB; L. Wei, *China's Xi Ramps Up Control of Private Sector. 'We Have No Choice but to Follow the Party'*, WSJ (Dec.10, 2020), https://on.wsj.com/3P0YfAU.

[137] Commerce Department Memorandum at 7 (citing J. Laband, *Fact Sheet: Communist Party Groups in Foreign Companies in China*, CHINA BUSINESS REVIEW (May 31, 2018), https://bit.ly/3HmDbmH).

[138] Commerce Department Memo at 7 (quoting F. Russo, *Politics in the Boardroom: The Role of Chinese Communist Party Committees*, THE DIPLOMAT (Dec. 24, 2019), https://bit.ly/3XOH6hN).

[139] S. Livingston, *The Chinese Communist Party Targets the Private Sector*, CSIS (Oct. 8, 2020), https://bit.ly/3uiMT1x (citing Ye Qing, Vice Chairman of the All-China Federation of Industry and Commerce); S. Livingston, *The New Challenge of Communist Corporate Governance*, CSIS (Jan. 15, 2021), https://bit.ly/3gNPyNH.

Private Economy in the New Era," also called for "further strengthen[ing] the Party's leadership of, and cohesive effect on, private economy practitioners."[140]

215. There is growing evidence that these Communist Party goals are taking root, and that party committees are exerting greater influence over private enterprise in China.[141]

216. TikTok paints the picture of an independent U.S.-based company, with little to no risk of interference by its Chinese parent company or risk of access to its data by the Chinese Government or Communist Party. These efforts to downplay ByteDance's control and influence over TikTok, and thereby the significance of the Communist Party's influence over ByteDance, are deceptive and misleading.

217. ByteDance exercises significant control and influence over TikTok, and ByteDance in turn is under significant influence by, and cooperates closely with, the Chinese Government and Chinese Communist Party. This influence and cooperation provide the Chinese Government and Chinese Communist Party with clear leverage over, and the ability to exert pressure on, ByteDance, its leadership, and its employees. It has already done so, in multiple ways. There is no barrier, legal or otherwise, to the Chinese Government or Communist Party applying the same pressure on ByteDance to access U.S. user data, including Indiana consumers' data.

218. TikTok wants Indiana consumers to believe that their data is safe. But TikTok knows that if the Chinese Government or Communist Party want access to TikTok's U.S. user data, which includes Indiana consumers' data, they can get it.

[140] S. Livingston, *The Chinese Communist Party Targets the Private Sector*, CSIS (Oct. 8, 2020), https://bit.ly/3uiMT1x.

[141] S. Livingston, *The New Challenge of Communist Corporate Governance*, CSIS (Jan. 15, 2021), https://bit.ly/3gNPyNH.

## CLAIMS

## COUNT I

### Indiana Deceptive Consumer Sales Act, IND. CODE § 24-5-0.5, *et seq.*

### Data Security Misrepresentations

219. Plaintiff repeats and incorporates by reference each and every allegation contained in the preceding paragraphs as if fully set forth herein.

220. Indiana's Deceptive Consumer Sales Act provides that a "supplier may not commit an unfair, abusive, or deceptive act, omission, or practice in connection with a consumer transaction." IND. CODE § 24-5-0.5-3(a). The prohibited "act[s], omission[s], or practice[s]" "include[] both implicit and explicit misrepresentations." *Id.*

221. TikTok is a "supplier . . . who regularly engages in or solicits consumer transactions" in the state of Indiana, IND. CODE § 24-5-0.5-2(a)(3)(A), through the "sale . . . or other disposition of . . . a service, or an intangible" to "a person for purposes that are primarily personal, familial, charitable, agricultural, or household, or a solicitation to supply any of these things." *Id.* § 24-5-0.5-2(a)(1).

222. TikTok has and is engaged in "unfair, abusive, or deceptive act[s] . . . or practice[s] in connection with a consumer transaction," IND. CODE § 24-5-0.5-3(a), by deceiving and misleading Indiana consumers, namely individuals who download the TikTok application or who allow others to download the TikTok application, about the risk of the Chinese Government and Communist Party accessing and exploiting their data.

223. TikTok has and is engaged in "unfair, abusive, or deceptive act[s] . . . or practice[s] in connection with a consumer transaction," *id.*, through its false, deceptive and misleading statements that U.S. user data, which includes Indiana consumers' data, is not subject to Chinese

Law, when that data is accessible by and may be shared with individuals and entities who are subject to Chinese law and the oppressive Chinese regime, including but not limited to laws requiring cooperation with national intelligence institutions and cybersecurity regulators. Further, Chinese State and Communist Party officials have interpreted Chinese law as applying to any data in which China has a national intelligence or security interest, no matter where the data is located.

224. TikTok's statements that its U.S. user data, which includes Indiana consumers' data, is not subject to Chinese law are false, deceptive, and misleading. Through these statements, TikTok also paints a false, deceptive, and misleading picture for Indiana consumers that there is little to no risk of the Chinese Government or Chinese Communist Party, which controls the Government, accessing and exploiting their data.

225. TikTok has and is engaged in "unfair, abusive, or deceptive act[s] or practice[s] in connection with a consumer transaction," *id.*, because its U.S. privacy policy does not alert Indiana consumers to the fact that it may share their data with entities and individuals in China, who are subject to Chinese Law, including but not limited to laws requiring cooperation with national intelligence institutions and cybersecurity regulators.

226. TikTok knowingly misled and deceived Indiana consumers, and continues to do so, because any reasonably prudent person would know that because Chinese law reaches their data in all the ways described in this Complaint, if the Chinese Government or Chinese Communist Party want access to TikTok's U.S. user data, they can get it.

227. TikTok has and is engaged in "unfair, abusive, or deceptive act[s] . . . or practice[s] in connection with a consumer transaction," *id.*, because its U.S. privacy policy, which is accessible through its pages on the App Store and Google Play Store, does not alert Indiana consumers to the fact that it may share their data with entities and individuals in China, who are

subject to Chinese laws that expose their data to the Chinese government and Communist Party. Indiana consumers expect that any app appearing on the App Store or Google Play Store complies with the minimal requirements for application developers, including requirements to be transparent with users about how their data is accessed and used. TikTok's app does not.

228. TikTok has and is engaged in "unfair, abusive, or deceptive act[s] . . . or practice[s] in connection with a consumer transaction," *id.*, in its deliberate efforts to downplay ByteDance's control and influence over TikTok, and thereby the Chinese Government and Communist Party's influence over ByteDance.

229. TikTok deceives and misleads Indiana consumers when it claims that it is independent from ByteDance, when any reasonable person would understand that evidence of, among other things, ByteDance's influence and direction over TikTok hiring, employees, and management shows that ByteDance exercises significant control over TikTok.

230. TikTok's claims further deceive and mislead Indiana consumers because they obscure TikTok's "China association"—the influence that the Chinese Government and Communist Party have over ByteDance—and thus the risk that this influence poses to consumers' data through ByteDance's ownership and control of TikTok.

231. TikTok knowingly misled and deceived Indiana consumers, and continues to do so, because any reasonably prudent person with TikTok's knowledge would know that the influence and control ByteDance has over TikTok, and ByteDance's influence by and cooperation with the Chinese Government and Communist Party, means that if the Chinese Government or Chinese Communist Party want access to TikTok's U.S. user data, which includes Indiana consumers' data, they can get it.

232. The Attorney General is entitled to a permanent injunction prohibiting TikTok from continuing to make misrepresentations about the security of its data to Indiana consumers.

233. Indiana is entitled to a civil penalty not to exceed $5,000 for each violation of Indiana's Deceptive Consumer Sales Act, in accord with IND. CODE § 24-5-0.5-4(g).

234. TikTok committed the acts alleged in this Complaint as part of a scheme, artifice, or device with intent to defraud or mislead, and therefore committed incurable deceptive acts. Indiana is entitled to a civil penalty not to exceed $500 for each incurable deceptive act committed by TikTok. IND. CODE § 24-5-0.5-8.

**PRAYER FOR RELIEF**

WHEREFORE, Plaintiff prays for judgment against Defendants for each of the causes of action raised herein. Plaintiff respectfully requests that the Court enter judgment in its favor and that the Court:

A. Declare that TikTok's actions are unfair, abusive, and deceptive to Indiana consumers under IND. CODE § 24-5-0.5, *et seq*;

B. Permanently enjoin Defendants from continuing to treat Indiana consumers unfairly and deceptively in the ways described in these allegations;

C. Award Plaintiff a civil penalty of not more than five thousand dollars per each violation of Indiana's Deceptive Consumer Sales Act, in accord with IND. CODE § 24-5-0.5-4(g);

D. Award Plaintiff a civil penalty of not more than five hundred dollars for each violation of Indiana's Deceptive Consumer Sales Act prohibiting "incurable" deceptive acts and practices, in accord with IND. CODE § 24-5-0.5-4(g);

E. Award Plaintiff the costs incurred in pursuing this action, including reasonable attorneys' fees, reasonable and necessary costs of the suit, and prejudgment and post-judgment interest at the highest lawful rates;

F. Plaintiff demands a jury trial; and

G. Grant such other and further relief as this Court deems just and appropriate.

Date: December 7, 2022

Respectfully submitted,

/s/Scott L. Barnhart
Scott L. Barnhart (Attorney No. 25474-82)
Cory Voight (Attorney No. 23180-49)
Betsy M. DeNardi (Attorney No. 23856-71)
Office of Attorney General
Indiana Gov't Center South
302 West Washington St.
5th Floor
Indianapolis, IN 46204
Telephone: (317) 234-7132
Fax: (317) 233-7979

David H. Thompson*
Pete Patterson*
Brian W. Barnes*
Megan M. Wold*
John Tienken*
DeLisa L. Ragsdale*
COOPER & KIRK, PLLC
1523 New Hampshire Ave., N.W.
Washington, D.C. 20036
Tel: (202) 220-9600
Fax: (202) 220-9601

*Counsel for Plaintiff, State of Indiana*

*Applications for admission *pro hac vice* forthcoming