Filed: 6/13/2023 10:36 AM
Clerk
Allen County, Indiana
ED

IN THE SUPERIOR COURT OF ALLEN COUNTY

INDIANA, *Plaintiff*, v. TIKTOK INC., TIKTOK PTE. LTD, BYTEDANCE INC., BYTEDANCE LTD., *Defendants.*	Cause No. 02D03-2212-PL-000401 **PUBLIC REDACTED**

FIRST AMENDED COMPLAINT

1. TikTok vacuums up reems of highly sensitive and personal information about Indiana consumers, including their interests, their locations, the types of phones they have, the apps on their phones, who their contacts are, the content they create, their facial features, their voice prints, and even "where your eyes are looking on your phone."[1] At the same time, TikTok deceives and misleads consumers about the risks the app poses to their data.

2. 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.

3. China's data and cybersecurity regimes do not protect consumers' privacy, rather, they ensure the government's control over their data. Thanks to a wave of recent national security, cybersecurity, and data security laws and regulations, in China, "[t]here will be no secrets. No

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

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."[2]

4. Nevertheless, TikTok obfuscates and misleadingly downplays the risk of the Chinese Government and Communist Party accessing and exploiting Indiana consumers' data.

5. 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.

6. But the highly sensitive data that TikTok collects from Indiana consumers is and has been accessible, in multiple ways, 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.

7. Further, current and recent versions of TikTok's privacy policy state that it may share data it collects with its parent company ByteDance or other affiliates, or certain entities, within its corporate group, many of whom are subject to Chinese law.

8. 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.

9. 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.

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

10. 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 and may have been shared with persons subject to Chinese laws.

11. TikTok's omission of China in its U.S. privacy policy, the link to which is and has been 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.

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

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

14. 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.

15. 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.

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

17. The Chinese Government and Communist Party have a demonstrated interest in "leveraging private sector data – including foreign data and that of firms like ByteDance – to grow

its stores and become the world's most data-rich power,"[3] and have shown the intent and willingness to investigate, surveil, harass, and intimidate individuals outside of China, including in Indiana.[4] Defendants themselves have admitted that employees in China and in the U.S. used TikTok user data to identify the physical locations of journalists who had published critical reports about the company.

18. TikTok's statements and omissions paint a false, deceptive, and misleading 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.[5]

19. 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.

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

21. 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.

22. 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.

23. The State of Indiana demands a jury trial.

---

[3] Rachel Lee, et al., *TikTok, ByteDance, and their ties to the Chinese Communist Party*, at 23, SENATE SELECT COMM. ON FOREIGN INTERFERENCE THROUGH SOCIAL MEDIA (Mar. 14, 2023).

[4] 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.

[5] *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 . . . .").

JURISDICTION AND VENUE

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

25. 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.*

26. 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."

27. 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."

28. 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).

29. 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).

30. Defendants operate a social media application and platform that they have purposefully directed to operate in the State of Indiana to Hoosiers within the applicable statute of limitations. In Indiana alone, the TikTok app "[redacted]." Defendants are actively serving content to and collecting data from at least [redacted] in Indiana. On

information and belief, millions of Hoosiers downloaded the TikTok app in Indiana and provided TikTok access to data associated with Indiana IP addresses.

31. As in other states, Defendants collect data from Indiana users, including location-based data, to directly serve content to users in Indiana. Moreover, the content that Defendants serve to those Indiana users is informed by those users' presence in or connection with Indiana. This location [redacted] In other words, Defendants serve Indiana-specific content to Hoosiers in Indiana.

32. In addition to the content that is informed by Indiana users' location in Indiana, Defendants also monetize their location by serving location-specific advertisements. "[redacted]"[9]

33. Upon information and belief, Defendants pay individuals located in the state of Indiana for content that those users, called "creators," post to TikTok.

34. Defendants have purposefully availed themselves of the benefit of transacting business in Indiana through the marketing, sale, and operation of a well-known social media and advertising network. In fact, Defendants are well-aware of their presence in Indiana and the

[redacted]

[7] *Id.*
[8] *Id.*
[9] *Id.*

financial rewards for operating within Indiana by serving Hoosiers content. [redacted] This Court has personal jurisdiction over Defendants under IND. R. TRIAL P. 4.4(A).

PARTIES

35. Plaintiff Indiana is the State of Indiana.

36. Defendant TikTok Inc. is a for-profit entity incorporated in the State of California, 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. has a valuation of at least $50-75 billion. TikTok Inc. made nearly $4 billion in revenue in 2021 and an estimated $10–12 billion in 2022.

37. Defendant TikTok Pte. Ltd is a related corporate entity, which is headquartered at 8 Marina View, #43–00, Asia Square Tower 1, Singapore 018960. This related corporate entity is nominally listed on the Apple App Store, Google Play Store, and Microsoft Store.

38. Defendant ByteDance Inc. is a for-profit entity incorporated in the State of Delaware. ByteDance is headquartered at 250 Bryant St, Mountain View, CA, 94041.

39. Defendant ByteDance Ltd. is a multinational internet technology holding company and is the parent company of TikTok Inc., TikTok Pte. Ltd., and ByteDance Inc. ByteDance Ltd. is headquartered in Room 503 5F, Building 2, 43 North Third Ring West Road, Beijing, 100086 China and registered in the Cayman Islands at C/O Vistra (Cayman) Limited, P. O. Box 31119, Grand Pavilion, Hibiscus Way, 802 West Bay Road, Grand Cayman, KY1 – 1205. ByteDance Ltd. is valued at more than $400 billion. ByteDance Ltd. reported $58 billion in revenue in 2021.

FACTUAL ALLEGATIONS

What TikTok Is

40. 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. TikTok was the most downloaded app globally in 2022.[10]

41. TikTok users register and create a profile 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.

42. According to TikTok's Privacy Policy, 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."[11] Prior versions of the policy noted that TikTok collected some GPS information from U.S. users, while the most recent version states that "current versions" of TikTok no longer do so.[12]

43. 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."[13]

---

[10] D. Curry, *Most Popular Apps (2023)*, BUSINESSOFAPPS (Feb. 28, 2023), https://bit.ly/3ZVgGen.
[11] *TikTok Privacy Policy*, TIKTOK (MAY 22, 2023), https://bit.ly/3kHRedg.
[12] *Id.*
[13] *Id.*

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

45. TikTok tracks Indiana consumers across their devices and across the internet. Specifically, when users log-in from multiple devices, TikTok can use their device ID or user ID 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."[14]

46. TikTok collects information from third-party websites like Cerebral, which admits to sending health information of its patients to TikTok.[15]

47. TikTok says that it "may link [users'] contact or account information with [their] activity on *and off* [the] Platform across all [their] devices, using [their] email or other log-in or device information . . . . to display advertisements on [the] Platform tailored to [users'] interests, preferences, and characteristics.[16]

48. TikTok also collects user content and associated metadata that users may never publish, and messages they compose but never send.

49. With users' permission, TikTok collects "information, including text, images, and videos, found in [their] device's clipboard," their phone's contacts, and other social network contacts.[17]

50. Older versions of TikTok collected GPS information from U.S. users and, if those users consented, their precise GPS location.

---

[14] *Id.*

[15] Emma Roth, *Cerebral admits to sharing patient data with Meta, TikTok, and Google*, THE VERGE (Mar. 11, 2023), https://bit.ly/3J4ZMEb.

[16] *Supra TikTok Privacy Policy*, https://bit.ly/3kHRedg (emphasis added).

[17] *Id.*

51. A report from privacy researcher Felix Krause found that TikTok can collect 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.[18] The code thus allows TikTok to capture additional highly personal information about consumers, including but not limited to passwords and credit card information.[19]

52. 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.[20] In 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."[21]

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

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

54. First, TikTok falsely states: "None of our data is subject to Chinese law,"[22] and fails to inform consumers in its Privacy Policy that their data is shared with entities and individuals in China.

---

[18] 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.

[19] *Id.*

[20] 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.

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

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

55. 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.

56. The combined purpose and effect of these statements and omissions 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. These statements and omissions are false, deceptive, and misleading.

57. Whether by the operation of law or the influence of the Chinese Government and Chinese Communist Party apparatus over TikTok's parent company, or both, any data or information accessed by Chinese citizens or persons within China is subject to Chinese law and is at risk of access and exploitation by the Government and/or Communist Party.

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

58. Data stored and accessible in China is subject to a starkly different set of restrictions, protections, and risks than is data stored and accessible only in the United States. The vulnerability of consumer data under the Chinese legal and regulatory regime is extreme and, where Chinese authorities may access Indiana consumers' data, poses material risk to their privacy and security.

59. 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.

60. 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."[23]

61. 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."[24]

62. The National Intelligence Law further requires 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."[25]

---

[23] 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 (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.

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

[25] NAT'L INTELLIGENCE LAW, art. 7; *see also id.* at art. 14 ("National intelligence work institutions lawfully carrying out intelligence efforts may request that relevant organs, organizations, and citizens provide necessary support, assistance, and cooperation.").

63. Article 16 provides that national security 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."[26]

64. Article 17 provides that these institutions "may . . . lawfully requisition, state organs', organizations' or individuals' transportation or communications tools, premises and buildings . . . ."[27]

65. 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."[28]

66. 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.[29]

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

---

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

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

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

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

68. "China's Cybersecurity Law lays the foundation for a cybersecurity review of network products and services, also known as the Cybersecurity Review Regime."[30] The law applies broadly to, among other persons, "network operators," which can encompass not only "telecommunications or internet service providers (ISPs)" but also "*anyone who uses [information communication and technology] systems*."[31] Article 28 requires these "network operators" to cooperate with national intelligence activities, as well as criminal investigations.[32]

69. 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."[33]

70. The Cybersecurity Law applies even more stringent requirements on organizations deemed "critical information infrastructure operators." 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."[34]

71. Since the law's enactment, authorities have issued regulations expanding its scope.[35]

---

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

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

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

[33] CYBERSECURITY LAW, art. 49.

[34] CYBERSECURITY LAW, art. 35; *see also id.* at art. 37 ("Critical 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 informatization departments and the relevant departments of the State Council to conduct a security assessment").

[35] 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.

72. The 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.[36]

73. 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."[37]

74. 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."[38]

75. 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."[39] 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

[36] 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. Chinese authorities with the Cyberspace Administration of China (CAC) conducted a cybersecurity review of DiDi, a ride-hailing service in China, shortly after the company raised billions of dollars in a New York IPO. Although the law did not apply to DiDi at the time, officials prohibited new users from signing up with the app and eventually fined the company more than $1 billion.

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

[38] DATA SECURITY LAW, art. 24.

[39] 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 (emphasis added).

initially *collected* in China, to any foreign judicial or law enforcement agency without the prior approval of the relevant [Chinese Government] authorities."[40]

76. 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.[41] 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.

77. 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.

78. 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

[40] 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.

[41] *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).

force TikTok or ByteDance employees subject to Chinese law to hand over Indiana consumers' data in secret.

79. 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.

80. 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.

81. In sum, any Indiana consumer data that is 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.

82. Indiana consumers should know whether their data may be subject to these risks so that they can make informed decisions about whether to download and use TikTok, and what access permissions to grant the company. They do not, because TikTok deceives and misleads them.

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

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

84. TikTok states on its website: "None of our data is subject to Chinese law."[42]

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

85. 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."[43]

86. In response to questioning about the potential for the Chinese government to access U.S. user data, a common TikTok refrain has been to state that U.S. user data is stored in the United States and Singapore.[44] Now, it is to point to future plans to house U.S. data on an Oracle cloud in the United States and delete historical U.S. data from TikTok and ByteDance servers.[45]

87. 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[46] and access controls administered by a U.S.-based subsidiary.[47]

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

---

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

[44] *See* David Rubenstein, *Interview of TikTok CEO Shou Zi Chew*, YouTube (Mar. 3, 2022) at 13:09-13:55, https://bit.ly/3WRUJMr; Stone, *supra* note 43; *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.").

[45] *Written Testimony of Shou Chew*, U.S. HOUSE COMM. ON ENERGY AND COMMERCE (Mar. 23, 2023), https://bit.ly/3JNXNnd.

[46] *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.

[47] *Written Testimony of Shou Chew*, U.S. HOUSE COMM. ON ENERGY AND COMMERCE (Mar. 23, 2023), https://bit.ly/3JNXNnd.

[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),

89. Each of these statements is deceptive and misleading to Indiana consumers. 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]

90. Neither TikTok's data storage practices, nor its data security practices, negate the applicability of Chinese law to that data or to the persons 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.

91. 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.

92. 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.

93. Officials from across the political spectrum and branches of the government with knowledge and expertise in security matters have expressed alarm that because persons subject to Chinese law have access to U.S. user data, including ByteDance and its employees, if the Chinese

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.").

[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).

Government or Communist Party asked for U.S. user data, the company has no meaningful way to refuse.[50]

94. The Chinese Government and Communist Party can use access to TikTok's U.S. user data, including Indiana consumers' data, to undertake a variety of concerning activities, including conducting surveillance on U.S. citizens and residents.

95. In December 2022, ByteDance admitted that employees and leaders of its internal audit function in China and the U.S. had obtained TikTok user data of journalists, including an American reporter. The data included information about the journalists' locations. Statements from TikTok spokespersons confirmed that the internal audit employees had the power and authorization to access U.S. user data, calling the episode an "egregious abuse" of their authority. ByteDance's confirmation of the surveillance activity followed public denials that such monitoring occurred or was even possible.[51]

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

[51] 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; Baker-White, *Exclusive: TikTok Spied on Forbes Journalists*, FORBES (Dec. 22, 2022), https://bit.ly/3P7eL4e.

Contrary to TikTok's Assertions and Obfuscations, Indiana Consumer Data is Accessible in China and Subject to Chinese Law

96. 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.[52]

97. 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.[53]

98. In April 2020 TikTok said its "goal" was "to minimize data access across regions so that, for example, employees in the APAC region, including China, would have very minimal access to user data from the EU and US."[54]

99. 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."[55]

100. 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 situations where US employees had to turn to their colleagues in China to determine

[52] 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).

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

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

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

> 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.[56]

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.'"[57]

101. One former ByteDance executive even claims that Chinese authorities have their own access to that data via a "backdoor channel", and that ByteDance permits such access for fear of the Chinese government banning apps the company offers in China.[58] The executive alleges,

> ByteDance is similarly positioned to exploit nationalistic sentiments in other countries like the United States as well, since it collects data from its users in those countries – data which Mr. Yu observed it makes accessible to the CCP via a backdoor channel. Mr. Yu saw the backdoor channel in the code, which allows certain high level persons to access user data, no matter where the data is located, even if hosted by a U.S. company with servers located in the U.S. Chinese law requires the company to grant access to user data to the Chinese government. The company was aware that if the Chinese government's backdoor was removed from the international/U.S. version of the app, the Chinese government would, it feared, ban the company's valuable Chinese-version apps.

102. TikTok's privacy policy also permits "certain entities within our corporate group" to access U.S. data.[59] Similarly, prior to March 21, 2023, TikTok's privacy policy stated it may share U.S. data with ByteDance or another affiliate.

103. ByteDance and other affiliates and corporate group entities are located in China, meaning that those entities and their employees are subject to Chinese law.[60]

---

[56] 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.

[57] *Id.*

[58] First Am. Compl., at ¶18-19, *Yu v. ByteDance, Inc., et al.*, No. CGC-23-606246 (Super. Ct. San Francisco Cnty. May 12, 2023).

[59] *TikTok Privacy Policy*, https://bit.ly/3kHRedg.

[60] *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:

104. One affiliate of TikTok, Beijing Douyin Information Service Limited, formerly known as Beijing Bytedance Technology Co. Ltd.,[61] is 1% owned by a Chinese state-owned enterprise. That enterprise, "Wangtou Zhongwen (Beijing) Technology, 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."[62] The state entity also sits on the board of Beijing Douyin Information Service Limited.

105. 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."[63]

106. TikTok states that employees of Beijing Douyin Information Service Limited "are restricted from U.S. user database access."[64] However, that statement does not address past behavior. And 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.[65]

107. 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).

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.").

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

[62] *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.

[63] 2021 Commission Report at 9.

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

[65] 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.

108. Beijing Douyin Information Service Limited is under common control with TikTok by ByteDance.

109. Because TikTok's parent company and certain of its affiliates are subject to Chinese law and Chinese Government and Communist Party influence, and TikTok's privacy policy permits TikTok to share data with them, TikTok's statements that Chinese law does not apply to that data are false and misleading.

110. 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 persons 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 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.

Contrary to TikTok's Claims, TikTok's Data Storage Practices Have Been, and Are, Inadequate to Protect U.S. User Data from Access and Exploitation by the Chinese Government and Communist Party

111. When questioned about whether the Chinese government may access U.S. user data, TikTok has often stated that U.S. user data, which includes Indiana consumers' data, is stored

in the U.S. and Singapore.[66] These statements suggest to consumers that TikTok's data storage practices are sufficient to protect their data, and that it is not touchable by Chinese authorities.

112. These statements are deceptive and misleading in multiple ways. First, 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.

113. 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*.[67]

114. 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."[68] Mr. Cloutier also declared that ByteDance had its "own security team monitoring the technical access environment" for those servers.[69]

115. 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.

---

[66] *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.

[67] 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).

[68] Cloutier Suppl. Decl. ¶ 8, Doc. 43-2, *TikTok Inc. v. Trump*, No. 20-cv-02658 (D.D.C. Oct. 14, 2020).

[69] *Id*.

116. Additionally, TikTok, at least as of October 2020, contracted with Alibaba cloud for its backup data storage in Singapore.[70]

117. 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]."[71]

118. 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 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.

119. 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.

120. In testimony before Congress, TikTok CEO Shou Zi Chew said: "American data has always been stored in Virginia and Singapore, in the past."[72] This statement is false, deceptive, and misleading.

121. 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,

---

[70] 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).

[71] Commerce Department Memorandum at 15; *see also* G. Roumeliotis *U.S. blocks MoneyGram sale to China's Ant Financial on national security concerns*, REUTERS (Jan. 2, 2018), https://reut rs/3WXp2RU (reporting that 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").

[72] *TikTok CEO Testifies at House Energy and Commerce Committee Hearing*, at 1:54:44, C-SPAN (Mar. 23, 2023), https://bit.ly/3oWQQdc.

"it is impossible to keep data that should not be stored in [China] from being retained in [China]-based servers."[73]

122. Any information stored or retained on servers in China is subject to Chinese law.

123. TikTok and ByteDance information stored on Chinese servers in China includes information associated with, and shared through, ByteDance's proprietary software called Lark.[74]

124. Private consumer data has been shared over Lark, including in groups accessed by employees based in China.

125. According to *The New York Times*, data shared over Lark has included U.S. driver's licenses, child sexual abuse material, photos, IP addresses, and other information.[75]

126. Employees have expressed concern about these sharing practices to executives and in internal reports as early as 2021, but, upon information and belief, neither TikTok nor ByteDance has ever disclosed them to consumers.[76]

127. According to *Forbes*, the sensitive personal and financial information of certain TikTok users called "creators," including social security numbers and tax information, also is stored in China.[77]

128. TikTok has not disclosed to its creators that their sensitive personal and financial information has been and is stored in China.

---

[73] 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.

[74] Sapna Maheshwari and Ryan Mac, *Driver's Licenses, Addresses, Photos: Inside How TikTok Shares User Data*, N.Y. TIMES (May 24, 2023), https://nyti.ms/43SIemu ("Lark data from TikTok was also stored on servers in China as of late last year").

[75] *Id.*

[76] *Id.*

[77] Alexandra S. Levine, *TikTok Creators' Financial Info, Social Security Numbers Have Been Stored In China*, FORBES (May 30, 2023), https://bit.ly/3NnqtGS.

129. TikTok claims a data storage arrangement with Oracle will resolve all "reasonable" concerns about the security of U.S. user data.[78] In June 2022, TikTok stated that "100% of US user traffic is now being routed to Oracle cloud infrastructure" in the United States.[79] Eventually, TikTok says it will delete protected U.S. user data from its own systems.[80]

130. But TikTok has not committed to ending access by persons subject to Chinese law to all U.S. user data, including Indiana consumers' data.[81] TikTok only began deleting legacy U.S. user data from its own systems in March 2023, and does not expect to complete that process until later this year.[82] As of October 2022, Oracle had "'absolutely no insight one way or the other' into who can access TikTok user data."[83] CEO Shou Zi Chew did not deny in a March 23, 2023 congressional hearing that U.S. data can still be accessed by employees in China and admitted engineers in China have access to "global data."[84]

131. TikTok's elaborate efforts to alter its data storage practices are a tacit admission that its prior, much-touted practices were inadequate to protect U.S. consumers' data.

132. No part of this arrangement with Oracle, at least as it currently stands, addresses the sharing of private U.S. consumer data over Lark – an internal platform that stores data in China.

133. No part of this arrangement with Oracle addresses the storage of certain U.S. TikTok users' sensitive financial and personal information in China.

---

[78] Drew Harwell and Elizabeth Dwoskin, *As Washington wavers on TikTok, Beijing exerts control*, WASH. POST (Oct. 30, 2022), https://wapo.st/43uHUuI.

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

[80] *Id.*

[81] *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.

[82] *Written Testimony of Shou Chew*, U.S. HOUSE COMM. ON ENERGY AND COMMERCE (Mar. 23, 2023), https://bit.ly/3JNXNnd.

[83] 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.

[84] *TikTok CEO Testifies at House Energy and Commerce Committee Hearing*, at 1:52:38, C-SPAN (Mar. 23, 2023), https://bit.ly/3oWQQdc.

134. For all of the above reasons, TikTok U.S. user data is subject to Chinese law, and it is at clear risk of access and exploitation by the Chinese government and Communist Party. TikTok's assertions to the contrary are false, deceptive, and misleading.

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

135. 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 . . . ."[85]

136. Until very recently, TikTok's U.S. privacy policy stated: "We may share all of the information we collect with a parent, subsidiary, or other affiliate of our corporate group."

137. Similarly, as of March 21, 2023, TikTok's U.S. privacy policy states: "As a global company, the Platform is supported by certain entities within our corporate group, which are given limited remote access to Information We Collect."[86]

138. 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. Other entities with whom TikTok may share your data as described herein may be located outside of the United States."[87]

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

140. However, the word "China" does not appear in the recent and current versions of TikTok's privacy policy applicable to U.S. users, including Indiana consumers.

---

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

[86] *TikTok Privacy Policy*, https://bit.ly/3kHRedg.

[87] *Id.*

141. 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.

142. 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.[88] 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. Before choosing to permit access to such sensitive information, Indiana consumers would certainly want—and they deserve— to know whether their data could be shared or accessed in such a way as to expose them to intrusive, unaccountable monitoring by a foreign government.

143. 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.

144. Although TikTok's latest updates to its U.S. privacy policy on March 21, 2023 and again on May 22, 2023 include a link to more information about TikTok's arrangement with Oracle, the policy still makes no mention of China.

145. 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.

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

146. 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.

147. 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.[89] 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."[90] 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."[91]

148. 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, collection, use, handling, and sharing of user data, . . . and limit[] the use of the data to the . . . purposes disclosed."[92]

---

[89] APPLE DEVELOPER LICENSE AGREEMENT, at 18 (June 6, 2022), *available at* https://apple.co/3H8JnP3.

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

[91] APP STORE REVIEW GUIDELINES § 5.1.2, APPLE (last updated Oct. 24, 2022), *available at* https://apple.co/3XSFIdO (emphasis added).

[92] USER DATA, GOOGLE (last visited Dec. 1, 2022), https://bit.ly/3FjuR5D. [93] C. Stokel-Walker, *Inside TikTok's Attempts to 'Downplay the China Association'*, GIZMODO (July 27, 2022), https://bit.ly/3EV8XnY.

149. 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.

150. 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."

151. 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 Further Misleads Indiana Consumers about the Risk of the Chinese Government Accessing their Data by Downplaying ByteDance's Control and the Heavy Influence of the Chinese Government and Communist Party

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

153. TikTok documents demonstrate that TikTok's "messaging" strategy calls for company representatives to "Downplay the parent company ByteDance, downplay the China association, downplay AI."[93]

154. Staying on message, in a public U.S. Senate hearing, then-CEO Vanessa Pappas admitted that "ByteDance is founded in China," but claimed "we do not have an official headquarters as a global company."[94]

155. TikTok's public statements also 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."[95]

"TikTok is led by its own global CEO, Shou Zi Chew, a Singaporean based in Singapore."[96]

"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."[97]

"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."[98]

---

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

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

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

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

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

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

156. TikTok asserts its independence from ByteDance control in its content moderation and data security practices.[99]

157. 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." TikTok also states that its "team" responsible for reviewing U.S. content "is led out of California," and further that "TikTok does not remove content based on sensitivities related to China."[100]

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

159. 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.[101] When asked whether anyone with access to TikTok's U.S. user data, which includes Indiana consumers' data, is a member of the Chinese Communist Party, Ms. Pappas said merely that TikTok could not attest to employees' political affiliations.[102]

160. 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

[99] June 2022 Letter to U.S. Senators at 3; *Statement on TikTok's content moderation and data security practices*, TIKTOK (Oct. 24, 2019), https://bit.ly/3hm2QRe.

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

[101] *Social Media's Impact on Homeland Security*, U.S. SENATE COMM. ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS, at 3:15:18 (Sept. 14, 2022) https://bit.ly/3P5kuWd; 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.

[102] *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.

that TikTok is an independent company and that the risk of consumers' data being accessed and exploited by the Chinese Government or the Chinese Communist Party is minimal to nonexistent.

161. These statements are deceptive and misleading. TikTok's parent company ByteDance owns and controls TikTok, and ByteDance is strongly connected to and influenced by the Chinese Government and Communist Party. This influence and control allows Chinese authorities to place significant pressure on these companies, which further places Indiana consumers' data at risk.

TikTok is Not an Independent American Company

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

163. 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.[103]

164. TikTok's algorithm still belongs to ByteDance, which declined to sell the technology to a U.S. company.[104]

165. ByteDance "plays a role in the hiring of key personnel at TikTok."[105]

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

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

[104] 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.

[105] 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)."

167. 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."[106]

168. 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."[107]

169. In April 2021, TikTok's current CEO, Shou Zi Chew, was named as CEO of TikTok while also serving as CFO of ByteDance Ltd.[108] He reports to the CEO of ByteDance.

170. 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.

171. 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."[109]

172. TikTok's Internal Audit team also reports to ByteDance's Internal Audit and Risk Control Department, led by an executive located in Beijing.[110]

---

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

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

[108] *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.

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

[110] 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.

173. ByteDance's Internal Audit and Risk Control Department investigates TikTok employees, including those located outside of China.[111] 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.[112] 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."[113]

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

175. 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.[114] Rather, they reported, major decisions related to TikTok are made by ByteDance founder Zhang Yiming and other ByteDance officials located in China.[115]

176. *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."[116]

---

[111] *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.

[112] 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.

[113] *Id*.

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

[115] *Id.*

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

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

178. 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.

179. At least some TikTok employees also have ByteDance e-mail addresses and can switch back and forth between the two based on the recipient of their communications.

180. 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.'"[117]

181. *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."[118]

182. 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 two companies are "blurry".[119] 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.

---

[117] 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.

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

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

183. 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.[120]

184. 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."[121]

185. TikTok employees in the United States regularly communicate with counterparts in China using ByteDance communication apps.[122]

186. Statements made by 24 former TikTok employees directly to an American journalist confirm that ByteDance is in full control of TikTok. Those statements include:[123]

> "'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."

The Chinese Government and Communist Party Exercise Significant Influence over ByteDance, and they Can Use it to Access TikTok Consumer Data

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

[121] *Id.*

[122] 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.

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

187. The Chinese Government and Chinese Communist Party have leverage over ByteDance. Because ByteDance controls TikTok, this influence further places Indiana consumers' TikTok data at risk of access and exploitation by Chinese authorities.

188. The Chinese Government and/or Communist Party have successfully forced ByteDance to alter certain business practices, and shutter one business altogether.

189. 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.'"[124] As a result of the action by the Chinese Government, ByteDance also hired thousands of moderators with qualifications including "'strong political sensitivity.'"[125]

190. 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 responsibility" and "[f]urther deepen cooperation with authoritative [official Party] media,

[124] Commerce Department Memorandum at 9.

[125] *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).

elevating distribution of authoritative media content, [and] ensuring that authoritative [official Party] media voices are broadcast to strength."[126]

191. 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."[127]

192. "Authoritative" Chinese State Media have posted content frequently on TikTok that is visible to Indiana consumers, although until January 2023, TikTok made no effort to alert consumers to that fact."[128]

193. In 2020, when TikTok reportedly was considering a purchase by a U.S. company, the Chinese government expanded its export control restrictions specifically to cover TikTok's algorithm.[129] As a result, ByteDance refused to sell, and retains control of TikTok.[130]

---

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

[127] 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)); *see also* E. Baker-White, *On TikTok, Chinese State Media Pushes Divisive Videos about U.S. Politicians*, FORBES (Dec. 1, 2022), https://bit.ly/3P0p4oM (discussing Chinese state media's use of TikTok and TikTok's failure to publicly label Chinese state-affiliated media until January 2023); *TikTok's state-affiliated media policy*, TIKTOK (Jan. 18, 2023), https://bit.ly/3MZzh4j; *TikTok rolls out its 'state-controlled media' label to 40 more countries*, TECHCRUNCH (Jan. 2023), https://tcrn.ch/3qzhPfh ("The Beijing-based video entertainment app is not being progressive with this implementation of the state-controlled media label. If anything, it's delayed. TikTok's peers have offered a similar system for labeling state-run media for years. For instance, YouTube in 2018 said it would begin to label state-funded broadcasters, and last year blocked Russian state-run channels from monetizing through ad dollars alongside Facebook. Meta had also been labeling state-controlled media since 2020 across its platform. And, prior to Elon Musk's takeover, Twitter's policy since 2020 had also been to label state-owned media.").

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

[129] 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.

[130] 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; *see also* J. Horsley, *Behind the Façade of China's Cyber Super-Regulator*,

194. The Chinese Communist Party is intertwined with ByteDance. 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]

195. "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 . . . as compared with other Internet [C]ompanies."[132]

196. A former ByteDance executive alleges that,

> It was known within the company that the CCP (the "Government") had a special office or unit in the company, which was sometimes referred to as the "Committee." While the Government office or Committee did not "work for" the company, it played a significant role. The Committee (1) guided how the company advanced core Communist values; and (2) regulated and monitored the company. For the Chinese version of the apps, the Committee possessed a "death switch" that could turn off the apps entirely.[133]

197. The executive further alleges that this,

> *Committee maintained supreme access to all the company data, even data stored in the United States*. Any engineer in Beijing could access U.S. user data located in the U.S. After receiving criticism about access from abroad, individual engineers in China were restricted from accessing U.S. user data, but the Committee continued to have access.[134]

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.

[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] First Am. Compl., at ¶27, *Yu v. ByteDance, Inc., et al.*, No. CGC-23-606246 (Super. Ct. San Francisco Cnty. May 12, 2023).

[134] *Id.* at ¶28 (emphasis added).

198. According to *Forbes*, "[t]hree hundred current employees at TikTok and its parent company ByteDance previously worked for Chinese state media publications," and at least fifteen of them still do.[135]

199. By downplaying ByteDance and the "China association," TikTok dismisses the significance of Communist Party influence on ByteDance and the risk that it poses to consumer data. But Party Committees "are a mechanism through which Beijing expands its authority and supervision over nominally private or non-governmental organizations."[136]

200. 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.[137]

201. 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."[138]

---

[135] 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.

[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; 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); *id.* (quoting F. Russo, *Politics in the Boardroom: The Role of Chinese Communist Party Committees*, THE DIPLOMAT (Dec. 24, 2019), https://bit.ly/3XOH6hN); *see also* 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.

[137] 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).

[138] 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.

202. 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 Private Economy in the New Era," also called for "further strengthen[ing] the Party's leadership of, and cohesive effect on, private economy practitioners."[139]

203. 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.[140]

204. 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.

205. TikTok wants Indiana consumers to believe that their data is safe. But Chinese authorities already have exercised leverage over and connection with ByteDance, and they can easily do so again to access TikTok user data, including data belonging to Indiana consumers.

206. Indiana consumers should have accurate information about risks posed to their data by ByteDance's control over TikTok, but Defendants deceptively muddy the waters and mislead Hoosiers about these risks.

Defendants Deceive Indiana Consumers through their Use of an In-App Browser

207. When a user clicks on a link from within the TikTok app, the user is directed to the selected web page through TikTok's in-app browser.

---

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

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

208. When the selected page opens in TikTok's browser, it appears to the average user that he or she exited the TikTok app to view the page. In reality, the user never left TikTok.

209. When any link is clicked, the normal TikTok display screen is immediately replaced with the linked webpage.

210. TikTok does not notify consumers at any point, before or after they click on a link within TikTok, that the link is opened using the in-app browser, and not the consumer's default browser on their phone.

211. When the TikTok in-app browser is open, no information identifying its belonging to TikTok is visible. Instead, TikTok displays the generic phrase "Web Browser" across the top of the screen.

212. When a user clicks on a link within TikTok, TikTok does not offer the user the option to open that link in their default browser, rather than in TikTok's in-app browser.

213. There is no readily discernable way to disable the in-app browser.

214. When a user selects a link from TikTok's in-app browser, whatever privacy controls the user set on their default browser do not apply.

215. A report from privacy researcher Felix Krause found that TikTok has the ability to collect 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.[141] The code thus allows TikTok to capture

[141] 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.

additional highly personal information about consumers, including but not limited to passwords, credit card information and health information.[142]

216. TikTok claims that it does "not collect keystroke or text inputs" entered by users on websites accessed through its in-app browser, but according to the researcher's report, it has the capability to do so. TikTok has also admitted to collecting some information about keystrokes, including patterns.[143] Additionally, the researcher reported that TikTok can collect other information about the user's interaction with the third-party website, such as links the user clicked on or anything copied to a user's clipboard, which could be highly sensitive information from any other source on a user's phone.

217. Just as TikTok does not alert users to the fact they are using an in-app browser at all, TikTok also does not alert users to its capabilities to collect sensitive information through the user's use of the in-app browser.

218. TikTok does not disclose its use of an in-app browser in its Privacy Policy or Terms of Service and does not inform consumers of data collection capabilities or practices associated specifically with the in-app browser.[144]

219. Because TikTok does not alert consumers to the fact that they remain in TikTok even though they are accessing another web page, those consumers do not know that when they access that page, TikTok's practices, policies and rules apply – not the choices the user has made regarding their default browser. TikTok gives users no meaningful choice to decide for themselves what kind of data they want exposed to TikTok through their web browsing activities.

---

[142] *Id.*

[143] Paul Mozur, et al., *TikTok Browser Can Track Users' Keystrokes, According to New Research*, N.Y. TIMES (Aug. 19, 2022), https://nyti ms/3lNQ54D.

[144] *TikTok Privacy Policy*, https://bit.ly/3kHRedg (the words "in-app browser" appear nowhere in the privacy policy); *Terms of Service*, TIKTOK (May 2023), https://bit.ly/3IF2H5k.

220. TikTok's use of an in-app browser, its failure to disclose its in-app browser when TikTok users click on links within TikTok, its failure to disclose its data collection capabilities and practices through its in-app browser, and its failure to provide a clear, readily apparent and easily accessible option to choose another browser, TikTok deceives Indiana consumers.

221. For all of the reasons set forth in this Complaint, TikTok also deceives Indiana consumers about the risk of data collected through TikTok's in-app browser being accessed and exploited by the Chinese Government and Communist Party.

CLAIMS

COUNT I

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

Data Security Misrepresentations

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

223. 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.*

224. 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).

225. 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.

226. Defendants knowingly deceived Indiana consumers, and continue to do so, because Chinese law reaches their data in all the ways described in this Complaint, and because if the Chinese Government or Communist Party want access to TikTok's U.S. user data, they can get it.

COUNT II

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

Misrepresentations about the Application of Chinese Law to Indiana Consumer Data

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

228. 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.*

229. 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).

230. 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), through its false, deceptive and misleading statements that U.S. user data, which includes Indiana consumers' data, is not subject to Chinese Law. In reality, 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.

231. 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.

COUNT III

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

TikTok's Privacy Policy is Deceptive and Misleading

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

233. 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.*

234. 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).

235. 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), because recent and current versions of its U.S. privacy policy have not alerted and do 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.

236. This is deceptive 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.

COUNT IV

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

TikTok Does Not Comply with App Developer Requirements

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

238. 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.*

239. 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).

240. 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), because recent and current versions of TikTok's U.S. privacy policy, which is accessible through its pages on the App Store and Google Play Store, have not alerted and do 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.

241. This is deceptive and misleading to Indiana consumers, who 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.

COUNT V

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

False, Deceptive, and Misleading Statements about the Influence and Control of the Chinese Government and Communist Party over Defendants

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

243. 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.*

244. 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).

245. 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), in its deliberate efforts to downplay ByteDance's control and influence over TikTok, and the Chinese Government and Communist Party's influence over ByteDance.

246. Defendants deceive and mislead Indiana consumers when they claim that TikTok is independent from ByteDance, when ByteDance's influence and direction over TikTok hiring, employees, and management shows that ByteDance exercises significant control over TikTok.

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

248. Defendants knowingly deceived Indiana consumers, and continue to do so, because Chinese authorities can exercise their leverage over and connection with ByteDance to access and exploit Indiana consumers' data.

249. 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.

250. 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).

251. 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.

COUNT VI

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

False, Deceptive, and Misleading Use of an In-App Browser

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

253. 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.*

254. 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).

255. 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), through TikTok's use of an in-app browser, their failure to notify consumers that TikTok uses an in-app browser, their

failure to inform consumers about the data collection capabilities and practices of the in-app browser, and their failure to offer consumers a clear, readily apparent and easily accessible option to use a different browser to access web pages from links within the TikTok app.

256. Defendants deceive Indiana consumers because they do not alert those consumers to the fact that clicking on a link from within TikTok will open the selected page from an in-app browser, and not from the user's chosen default browser.

257. Defendants deceive Indiana consumers by failing to inform them of the data collection capabilities and practices of the TikTok in-app browser, and by depriving them of the opportunity to exercise any meaningful choice to engage privacy controls for web browsing activities when they click on a link within the TikTok App.

258. Defendants deceive Indiana consumers by failing to offer them the clear choice to open a link in the TikTok app using their preferred browser.

259. Finally, for all the reasons stated in this complaint, Defendants deceive Indiana consumers about the risk of the Chinese Government or Communist Party accessing or exploiting their sensitive data, including any data collected through consumers' use of TikTok's in-app browser.

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: June 9, 2023

Respectfully submitted,

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