UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS

EVELIA RODRIGUEZ; ERIKKA WILSON; AND A.N., A MINOR; on behalf of themselves and all others similarly situated,

Plaintiffs,

v.

BYTEDANCE, INC.; BEIJING DOUYIN INFORMATION SERVICE CO. LTD. F/K/A BEIJING BYTEDANCE TECHNOLOGY CO. LTD.; BYTEDANCE LTD.; BYTEDANCE PTE. LTD.; BEIJING BYTEDANCE TECHNOLOGY CO. LTD.; AND TIKTOK, INC. F/K/A MUSICAL.LY, INC.,

Defendants.

CASE NO. _____

CLASS ACTION

JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

TABLE OF CONTENTS

Page

Plaintiffs, individually and on behalf of all others similarly situated (the "Class"), bring this class action complaint by and through undersigned counsel, against Beijing Douyin Information Service Co. Ltd. f/k/a Beijing ByteDance Technology Co. Ltd. ("Beijing Douyin"); Beijing ByteDance Technology Co. Ltd.; ByteDance, Inc.; ByteDance Ltd.; ByteDance Pte. Ltd. ("ByteDance") and TikTok, Inc. f/k/a Musical.ly, Inc. ("TikTok, Inc.") (collectively, "Defendants").

I. INTRODUCTION

1. In 2020, Defendants launched a video editing application, CapCut ("the CapCut app"), in the United States. The app began as a clone of Jianying, a Chinese video-editing app that Defendants rolled out a year earlier in China.[1] The app allows users to create, edit and customize videos, which they may then post online on a number of different social media platforms such as Instagram, Facebook, YouTube, Linkedin, and TikTok, the social media platform run by Defendants. Among other things, the CapCut app allows users to edit videos with various templates, filters, visual effects, and music.

2. The CapCut app has become extremely popular; it is routinely among the top apps in rankings of weekly downloads in the United States and had more than 400 million downloads globally last year alone,[2] making it the fourth most frequently downloaded app in the world.[3] As a result, the CapCut app now has more than 200 million monthly active users and is experiencing

[1] https://www.wsj.com/articles/tiktoks-chinese-parent-has-another-wildly-popular-app-in-the-u-s-e14c41fc.

[2] *Id.*

[3] https://blog.apptopia.com/worldwide-and-us-download-leaders-2022.

exponential growth.[4] The CapCut app is one of the most popular apps for mobile devices in the United States and the world.

3. The CapCut app is "heavily promoted" by Defendant TikTok, Inc. on its social media platform, which has one of the largest user bases in the world.[5] The TikTok, Inc. social media platform allows users to post 60-second videos of activities such as dancing, lip-syncing, and stunts, including videos created using the CapCut app. The TikTok app, like the CapCut app, is among the most downloaded apps available.

4. Defendant ByteDance was founded in 2012, and has consistently operated in Beijing, China. ByteDance has created numerous apps employing technologies such as artificial intelligence and facial recognition. ByteDance and affiliated Defendants also own Defendant TikTok, Inc., which runs the highly popular TikTok app. As detailed further below, revelations recently made public by whistleblowers and others indicate that ByteDance exercises day-to-day control over Defendant TikTok, Inc., and participates extensively in its day-to-day operations.

5. ByteDance is a Chinese company with reported connections to the Chinese government (including a direct ownership interest by China state-owned entities). The company has recently become the subject of significant public scrutiny for its failure to protect the privacy of user data. Among other things, officials both inside and outside the United States government have recognized the significant national security risks posed by the apps marketed by ByteDance and its affiliates. For example, as early as 2020, several Senators wrote to the FTC asking the agency to initiate an investigation into privacy violations, stating: "[f]aced with compelling evidence

[4] https://www.wsj.com/articles/tiktoks-chinese-parent-has-another-wildly-popular-app-in-the-u-s-e14c41fc.

[5] *Id.*

that this wildly popular social media platform is blatantly flouting binding U.S. privacy rules, the FTC should move swiftly to launch an investigation and forcefully hold violators accountable for their conduct."[6]

6. Because of such data privacy concerns, U.S. military branches and several State governments have banned the use of the TikTok app on government-issued phones, and the State of Montana has banned downloading the app entirely.[7] The United States government is now considering a similar ban of the app across the United States, and the Justice Department is investigating the surveillance of American journalists by TikTok's Chinese owners.[8] In February 2023, Senators Richard Blumenthal and Jerry Moran signed a bipartisan letter asking the government to "swiftly conclude its investigation and impose strict structural restrictions" between TikTok's U.S. operations and its Chinese operations, including potentially separating the companies.[9] As this record shows, Defendants have a track record of failing to protect the privacy of the data of users of their apps and of violating their privacy rights.

7. This action seeks to ensure that the privacy of CapCut users is adequately protected. The CapCut app facilitates the collection of a wide range of private information from users, including their biometric information. However, as noted in a March 19, 2023 article in the

[6] https://www.reuters.com/article/us-tiktok-privacy-usa-children/u-s-senators-urge-probe-of-tiktok-on-childrens-privacy-idUSKBN2352YD.

[7] https://inc.com/jason-aten/the-department-of-defense-is-warning-people-not-to-use-tiktok-over-national-security-concerns.html.

[8] https://www.wsj.com/articles/tiktoks-chinese-parent-has-another-wildly-popular-app-in-the-u-s-e14c41fc.

[9] https://www.theguardian.com/technology/2023/mar/16/the-tiktok-wars-why-the-us-and-china-are-feuding-over-the-app.

Wall Street Journal, because CapCut is "a tool app, it has largely avoided regulatory scrutiny over its practice in handling user data."[10]

8. The privacy concerns with respect to the CapCut app are particularly significant. First, the CapCut app is ultimately owned by a China-based company, which has a legal obligation to share information with the Chinese government under binding Chinese law and which, in fact, is in business with China state-owned entities. Second, the app has been aggressively promoted by Defendant TikTok, Inc.

9. As a result, the app has rapidly grown in popularity among both users and non-users of the TikTok app alike, and Defendants have gained access to the private and personal information of millions of users of the app.

10. Defendants have used automated software, proprietary algorithms, artificial intelligence, facial recognition, and other technologies to commercially profit from Plaintiffs' and Class Members' identities, unique identifying information, biometric data and information, images, video and digital recordings, audio recordings, clipboard data, geolocation, names, e-mail addresses, passcodes, social media accounts, messaging services, telephone numbers, and other private, non-public, or confidential data and information, or meaningful combination thereof, as more fully set forth herein.

11. Defendants, through the CapCut app, collected, captured, obtained, stored and, upon information and belief, disclosed and otherwise disseminated Illinois resident CapCut users' biometric information in violation of the Illinois Biometric Information Privacy Act ("BIPA"), 740

[10] https://www.wsj.com/articles/tiktoks-chinese-parent-has-another-wildly-popular-app-in-the-u-s-e14c41fc.

ILCS § 14/1, *et seq.* Public policy in Illinois provides that, given the risks of unwanted data collection, Illinois citizens have the right to make decisions about the fate of their unique biometric identifiers and information. Defendants' actions violated those rights.

12. In addition, unknown to CapCut users, the CapCut app may be used to conduct clandestine surveillance of users by individuals located in China. Based on information and belief, the CapCut app has clandestinely collected vast quantities of private and personally identifiable user data and content accessible to individuals in China, which could be employed to identify, profile, and track the physical and digital location and activities of United States users now and in the future.

13. Defendants covertly collect and use CapCut users' highly sensitive and immutable biometric identifiers and information.

14. Defendants unjustly profit from the secret harvesting of a massive array of private and personally identifiable CapCut user data and content that they can use for targeted advertising, improvements to Defendants' artificial intelligence technologies, patent applications, and the development of consumer demand for, and use of, Defendants' other products. In addition, Defendants have collected fees from users for cloud storage service and for additional features and effects that are unavailable with the basic app.

15. Users' data may be utilized for various purposes, including tracking users by age, gender, location, operating system, and interest in order to attract marketing and ad sales. By collecting and filtering this user data, Defendants are able to utilize the data to, among other things, improve their sophisticated targeted ad and marketing platform that allows their clientele to target demographics with precision.

16. Users are further at risk because Defendants' conduct exposes CapCut user data to access by the Chinese government to assist that government. As a result of such concerns, CapCut has been banned in India along with other China-based video- editing apps.[11]

17. Defendants' conduct violates statutory, constitutional, and common law privacy, data, biometrics and consumer protections and should be enjoined.

II. PARTIES

A. Plaintiffs

18. **Plaintiff Evelia Rodriguez** is a citizen and resident of Oroville, California. On or about April 13, 2023, Ms. Rodriguez saw an ad on TikTok that showed a video with two pictures of two different people being combined into one image. She wanted to try it so she downloaded the CapCut app onto her mobile device. Ms. Rodriguez did not read any privacy policy or terms of use for the CapCut app, nor did she see any discernable hyperlinks to or warnings about these items.

19. While Ms. Rodriguez merely wanted to try out the CapCut app by combining two photos from the photo album on her device, the CapCut app gained access to all of the photos and videos on her device. Since that time, Ms. Rodriguez has used the CapCut app to create additional video content.

20. Ms. Rodriguez expected that CapCut would protect and secure her content against access by or disclosure to unauthorized parties. Ms. Rodriguez did not consent to any third parties accessing her content, user data, and highly sensitive biometric identifiers and information.

[11] https://www.wsj.com/articles/tiktoks-chinese-parent-has-another-wildly-popular-app-in-the-u-s-e14c41fc.

21. **Plaintiff Erikka Wilson** is a citizen and resident of Chicago, Illinois. Erikka downloaded the CapCut app around March 2023. Erikka uses the app to edit videos and images. Erikka does not recall ever reading a privacy policy or terms of use before using the CapCut app.

22. **Plaintiff A.N., a minor,** is a citizen and resident of Chicago, Illinois, who brings this suit by and through her mother and legal guardian, Erikka Wilson, who is, and at all relevant times was, an individual and resident of Chicago, Illinois.

23. A.N. uses the CapCut app to edit videos. She is 14 years old and will be in the ninth grade in the Fall, 2023. A.N. used the CapCut app during the seventh and eighth grades.

24. A.N. was able to use the CapCut app without setting up an account or reading a privacy policy or terms of use. A.N. was able to later create an account without obtaining any permission or authorization from a parent.

B. Defendants

1. Beijing Douyin Information Service Co. Ltd. f/k/a Beijing ByteDance Technology Co. Ltd.

25. Defendant Beijing Douyin Information Service Co. Ltd. f/k/a Beijing ByteDance Technology Co. Ltd. ("Beijing Douyin") is, and at all relevant times was, a privately held company headquartered in Beijing, China. Defendant Beijing Douyin is a subsidiary of Defendant ByteDance Ltd., which is also headquartered in Beijing, China. The Chinese government owns a 1% share of Defendant Beijing Douyin, which has been described as a "golden share" that allows the Chinese government to, among other things, exercise control over Beijing Douyin.[12] In China,

[12] https://www.businessinsider.in/stock-market/news/tiktok-parent-bytedance-has-special-stock-owned-by-chinas-government-heres-how-golden-shares-give-beijing-influence-over-the-social-media-giant-/articleshow/99094188.cms. *See also* https://www.wsj.com/articles/xi-jinpings-subtle-strategy-to-control-chinas-biggest-companies-ad001a63.

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."[13]

2. Beijing Douyin Information Service Co. Ltd. f/k/a Beijing ByteDance Technology Co. Ltd.

26. Defendant ByteDance Ltd. owns 100% of Douyin Group (HK) Ltd. f/k/a ByteDance (HK) Co., Ltd., which is headquartered in Hong Kong. Douyin Group (HK) Co., Ltd. in turn owns 99% of Beijing Douyin Information Service Co. Ltd. ("Beijing Douyin"), which is headquartered in Beijing, China. The remaining 1% is owned by China state-owned entities.

3. Beijing ByteDance Technology Co. Ltd.

27. Defendant Beijing ByteDance Technology Co. Ltd. ("Beijing ByteDance"), at all relevant times was, a privately held company headquartered in Beijing, China. Defendant Beijing ByteDance was a subsidiary of ByteDance Ltd., which was also headquartered in Beijing, China. In 2022, Beijing ByteDance was renamed Beijing Douyin Information Service Co. Ltd. ("Beijing Douyin").

4. ByteDance, Inc.

Defendant ByteDance, Inc. is, and at all relevant times was, a Delaware corporation with its principal place of business in Palo Alto, California. Defendant ByteDance, Inc. is, and at all relevant times was, a wholly owned subsidiary of Defendant ByteDance Ltd.

[13] U.S.-China Economic and Security Review Commission, 2021 Report to Congress, at 9 (Nov. 2021).

5. ByteDance Ltd.

28. Defendant ByteDance Ltd. is, and at all relevant times was, a Cayman Islands corporation headquartered in Beijing, China.

6. ByteDance Pte. Ltd.

29. Defendant ByteDance Pte. Ltd. is, and at all relevant times was, a Singapore private limited company headquartered in Singapore.

7. TikTok, Inc. f/k/a Musical.ly, Inc.

30. Defendant TikTok, Inc. f/k/a Musical.ly, Inc. ("TikTok, Inc.") is, and at all relevant times, was, a California corporation with its principal place of business in Culver City, California.[14] Defendant TikTok, Inc. also maintains offices in Palo Alto, California and Mountain View, California.[15] Defendant TikTok, Inc. is a wholly owned subsidiary of TikTok, LLC, which in turn is a wholly owned subsidiary of TikTok, Ltd., and TikTok, Ltd. – like Defendant ByteDance, Inc. – is a wholly owned subsidiary of Defendant ByteDance Ltd.

C. Defendants Operate As A Single Enterprise

31. Defendants do not function as separate and independent corporate entities. To the contrary, company insiders have acknowledged that Defendant TikTok is "tightly controlled" by Defendant ByteDance and its China-based affiliates.[16]

---

[14] https://www.cnbc.com/2019/10/14/tiktok-has-mountain-view-office-near-facebook-poaching-employees.html.

[15] https://www.washingtonpost.com/technologyD/2019/11/05/inside-tiktok-culture-clash-where-us-views-about-censorship-often-were-overridden-by-chinese-bosses/; https://www.cnbc.com/2019/10/14/tiktok-has-mountain-view-office-near-facebook-poaching-employees.html.

[16] https://www.cnbc.com/2021/06/25/tiktok-insiders-say-chinese-parent-bytedance-in-control.html.

32. At all relevant times, Defendants TikTok, Inc. and ByteDance, Inc. have shared offices in Silicon Valley and also have shared employees. U.S. and China-based employees of the Defendant family of companies perform work concerning the CapCut app that is at the center of the lawsuit.

33. At all relevant times, Defendant ByteDance has directed the operations of Defendants TikTok, Inc. and ByteDance, Inc. with respect to the CapCut app, and Defendants TikTok, Inc. and ByteDance, Inc. have reported to Defendant ByteDance and its China-based affiliates.

34. At all relevant times, Defendant ByteDance and its China-based affiliates have collected and analyzed data from the United States regarding the performance of various features of the CapCut app, and has worked with Defendants TikTok, Inc. and ByteDance, Inc. to address performance issues and promote the CapCut app. Additionally, at all relevant times, Defendant ByteDance, its China-based affiliates, and their engineers have done significant coding for the CapCut app and its many versions and updates.

35. In addition, individuals in China working for ByteDance and its affiliates have exercised control over Defendant TikTok, Inc.: "Multiple TikTok sources, who spoke with *The Intercept* on the condition of anonymity . . , emphasized the primacy of ByteDance's Beijing HQ over the global TikTok operation, explaining that their ever-shifting decisions about what's censored and what's boosted are dictated by Chinese staff."[17]

[17] https://theintercept.com/2020/03/16/tiktok-app-moderators-users-discrimination/.

36. Defendant ByteDance made key strategy decisions for Defendants TikTok, Inc. and ByteDance, Inc., as well as for offices elsewhere in the world, and Defendants TikTok, Inc., ByteDance, Inc. and the other offices were charged with executing such decisions.

37. At all relevant times, and in connection with the matters alleged herein, each Defendant acted as an agent, servant, partner, joint venturer and/or alter ego of each of the other Defendants and acted in the course and proper scope of such agency, partnership, and relationship and/or in furtherance of such joint venture. Each Defendant acted with the knowledge and consent of the other Defendants and/or directed, authorized, affirmed, consented to, ratified, encouraged, approved, adopted and/or participated in the acts or transactions of the other Defendants.

38. At all relevant times, and in connection with the matters alleged herein, Defendants constitute a single enterprise with a unity of interest.

III. JURISDICTION AND VENUE

39. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1332(d) & 1367 because: (i) this is a class action in which the matter in controversy exceeds the sum of $5,000,000, exclusive of interest and costs; (ii) there are 100 or more class members; and (iii) some members of the class are citizens of states different from some Defendants, and also because more than one Defendant is a citizen or subject of a foreign state.

40. This Court has personal jurisdiction over Defendants because: (i) they transact business in the United States, including in this District; (ii) they have substantial aggregate contacts with the United States, including in this District; (iii) they engaged and are engaging in conduct that has and had a direct, substantial, reasonably foreseeable, and intended effect of causing injury

to persons throughout the United States, including in this District, and purposely availed themselves of the laws of the United States.

41. This Court further has personal jurisdiction with respect to the claims of the Illinois Subclass (defined below) because Defendants used and disseminated data derived directly from Illinois-based CapCut users and exposed residents of Illinois to ongoing privacy risks within Illinois based on the collection, capture, obtainment, disclosure, redisclosure and dissemination of their biometric identifiers and information. Furthermore, many of the images Defendants used for their unlawful collection, capture and obtainment of biometric identifiers and information were created in Illinois, uploaded from Illinois, and/or managed via Illinois-based user accounts, computers, and mobile devices. Because of the scope and magnitude of Defendants' conduct, Defendants knew that their collection, capture, obtainment, disclosure, redisclosure and dissemination of impacted individuals' biometric identifiers and information would injure Illinois residents and citizens. Defendants knew or had reason to know that collecting, capturing, obtaining, disclosing, redisclosing and disseminating Illinois citizens' and residents' biometric identifiers and information without providing the requisite notice or obtaining the requisite releases would deprive Illinois citizens and residents of their statutorily-protected privacy rights, neutralize Illinois citizens' and residents' ability to control access to their biometric identifiers and information via their Illinois-managed devices and exposed minors in Illinois to potential surveillance and other privacy harms as they went about their lives within the state.

42. Furthermore, through the CapCut app, Defendants actively collect information harvested from the Illinois-based devices of Illinois residents, including location information based on users' SIM card and/or IP address.

43. Defendants use this harvested information to provide users with location-based services directed toward Illinois.

44. Defendants deliberate gathering of Illinois users' personally identifiable information is intentionally targeted toward Illinois residents, including Plaintiffs and the Class, and constitutes purposeful activity directed at devices and individuals in Illinois.

45. Venue is proper under 28 U.S.C. § 1391(b)(2) because a substantial part of the acts or omissions giving rise to the claims alleged herein occurred in Illinois. Alternatively, venue is proper under 28 U.S.C. § 1391(b)(3) because this Court has personal jurisdiction over Defendants.

IV. BACKGROUND

A. Defendants Are Part of A China-Based Tech Conglomerate That Markets Multiple Products In The United States.

46. Defendant ByteDance is one of China's largest technology companies with an estimated valuation of $200 billion.[18] In the last year alone, the tech conglomerate achieved a gross operating profit of approximately $25 billion.[19] ByteDance's former CEO, Zhang Yiming, was honored by an organization affiliated with the Chinese Communist Party as one of its "100 outstanding private entrepreneurs."[20] The list is "something of a guide to who is in the good books of the Chinese authorities."[21]

[18] https://www.hurun.net/en-US/Info/Detail?num=HD7Q8RVHK6WE#totop.

[19] https://www.economist.com/business/2023/04/13/bytedance-tiktoks-chinese-parent-reports-a-record-profit.

[20] https://weekinchina.com/2018/11/loyalty-points.

[21] *Id.*

47. Defendant ByteDance makes a variety of video and news-aggregation apps.[22] It "regards its platforms as part of an artificial intelligence company powered by algorithms that 'learn' each user's interests and preferences through repeat interaction."[23] Defendant ByteDance has pursued a strategy of seeking growth in overseas markets, including specifically the United States.[24]

48. Defendant ByteDance has generated billions of dollars in annual revenue for its investors. Investors in Defendant ByteDance and its affiliates include Sequoia Capital China, Russian billionaire Yuri Milner, Japanese technology giant SoftBank, and large private-equity firms such as KKR, General Atlantic, and Hillhouse Capital Group.[25]

49. ByteDance has expanded its influence and revenue through a series of acquisitions of apps developed in China, growing to be a dominant force in the social media market. For example, in 2016, Defendant ByteDance launched an app called "Douyin" in China. The app allowed users to create videos of themselves and share the videos with friends. The Douyin app mimicked an existing app, Musical.ly, which was created in 2014.[26] In 2017, ByteDance introduced an English-language version of the Douyin app for use outside China under the name "TikTok."

---

[22] https://www.wsj.com/articles/tiktoks-videos-are-goofy-its-strategy-to-dominate-social-media-is-serious-11561780861.

[23] https://www.law360.com/articles/1213180/sens-want-tiktok-investigated -for-national-security-threats; https://www.cotton.senate.gov/?p=press_release&id=1239.

[24] https://www.wsj.com/articles/tiktoks-videos-are-goofy-its-strategy-to-dominate-social-media-is-serious-11561780861.

[25] https://www.wsj.com/articles/lip-syncing-app-musical-ly-is-acquired-for-as-much-as-1-billion-1510278123; https://www.reuters.com/article/us-tiktok-cfius-exclusive/exclusive-us-opens-national-security-investigation-into-tiktok-sources-idUSKBN1XB4IL.

[26] https://www.wsj.com/articles/tiktoks-videos-are-goofy-its-strategy-to-dominate-social-media-is-serious-11561780861.

ByteDance then acquired the Musical.ly app and merged all existing accounts and data into a single app under the "TikTok" name.[27]

50. The TikTok app has become "one of the world's fastest-growing social media platforms" with a massive American audience.[28] By November 2019, the TikTok app had been downloaded more than 1.3 billion times worldwide, with more than 120 million downloads in the United States alone.[29] The TikTok app dominates its top competitors such as Facebook and Instagram. TikTok recently reported that it has more than 150 million monthly active users in the United States, approaching half of the U.S. population.[30]

B. In 2020, ByteDance Began Marketing A New App In The United States Designed To Facilitate Video Editing, Which Could Be Used To Create Videos And Post Them On A Variety Of Social Media Apps.

51. The TikTok app provided only basic tools to create and edit videos that users then posted on the app. In an ongoing effort to expand its offerings and increase its revenue, ByteDance developed a separate app, CapCut, that had far more sophisticated tools that users could employ to create and edit videos, which could then be posted on TikTok as well as a range of other social media platforms, such as YouTube, Instagram, Linkedin, and Facebook. The CapCut app could be used both by TikTok users and individuals who never downloaded or used the TikTok app.

---

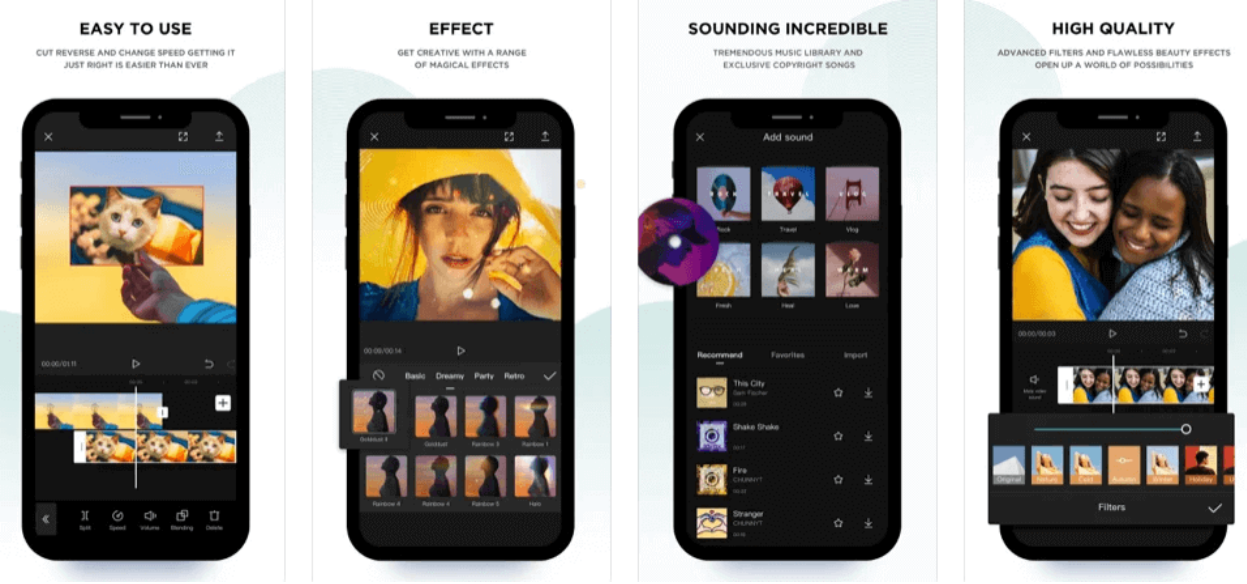
[27] http://culture.affinitymagazine.us/tik-tok-is-scamming-people-stealing-information/.

[28] https://www.washingtonpost.com/technology/2019/11/05/inside-tiktok-culture-clash-where-us-views-about-censorship-often-were-overridden-by-chinese-bosses/.

[29] *Id.*

[30] https://variety.com/2023/digital/asia/tiktok-150-million-us-monthly-users-government-ban-1235560251/.

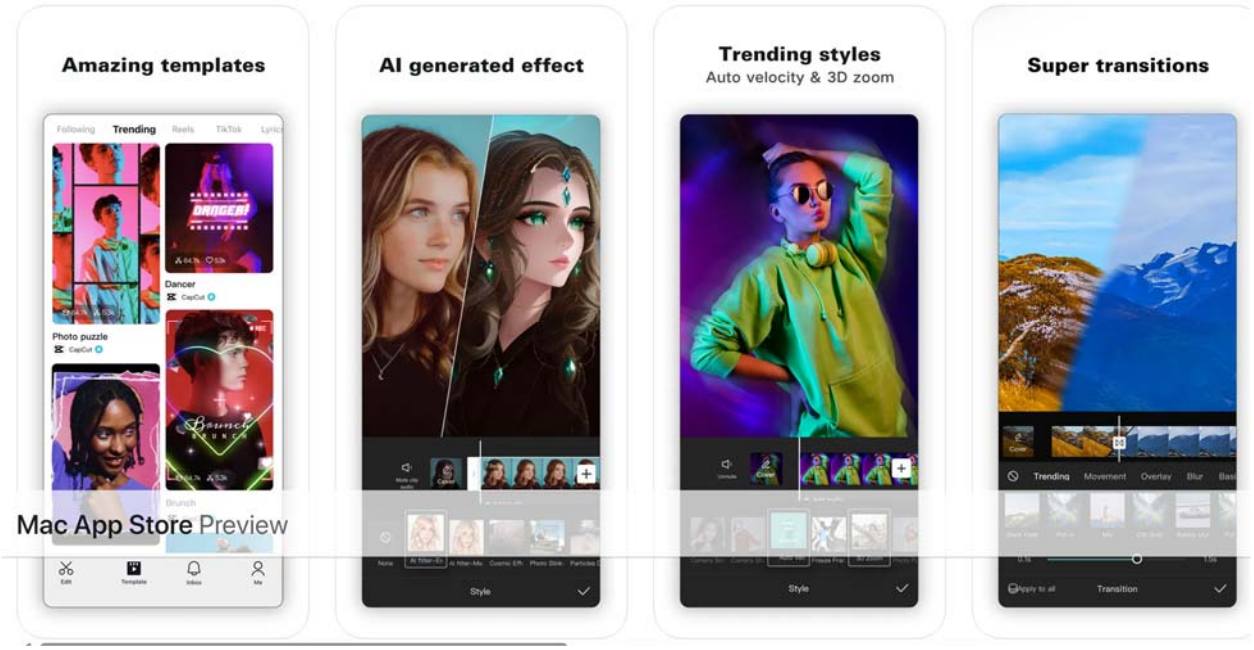
52. The CapCut app was launched in 2020 in the United States. The app allows users to edit videos with various templates, filters, visual effects and music to produce videos that look more professional and have a better chance of going viral on social media platforms.[31] Among other things, users may trim, cut, split or merge videos; change video speed; animate videos using various effects; highlight moments in videos using a freezing feature or slow motion; and add transition effects, music or sounds from a library containing millions of licensed songs.



53. The CapCut app is a highly advanced video editing app that exceeds the video editing capabilities available on TikTok; for example, the templates feature employs artificial intelligence to allow users to copy the editing style of existing videos.[32] Videos can be edited on almost any device imaginable using CapCut, including a user's PC (Mac & Windows), mobile phone (Android & iOS), or tablet.

[31] https://www.wsj.com/articles/tiktoks-chinese-parent-has-another-wildly-popular-app-in-the-u-s-e14c41fc.

[32] https://www.thespl.it/p/capcut-ai-unlocks-human-creativity.



54. Defendants charge users of the CapCut app for cloud storage service as well as for additional features and effects.[33] Users may obtain additional features and effects by paying for a monthly or yearly subscription to obtain premium features.[34] Likewise, CapCut charges a variable monthly fee to store videos on the cloud that is dependent on the amount of data that is being hosted.[35] In addition, as with the TikTok app, the CapCut app collects data from all users, which Defendants can then monetize in a variety of ways, resulting in significant profits.

55. Defendant ByteDance used a strategy to develop the CapCut app that is similar to the one it employed in developing TikTok, taking an app originally created and developed in China and then marketing it in the United States. In 2017, ByteDance launched the app in China

[33] https://www.wsj.com/articles/tiktoks-chinese-parent-has-another-wildly-popular-app-in-the-u-s-e14c41fc.

[34] https://www.thespl.it/p/capcut-ai-unlocks-human-creativity.

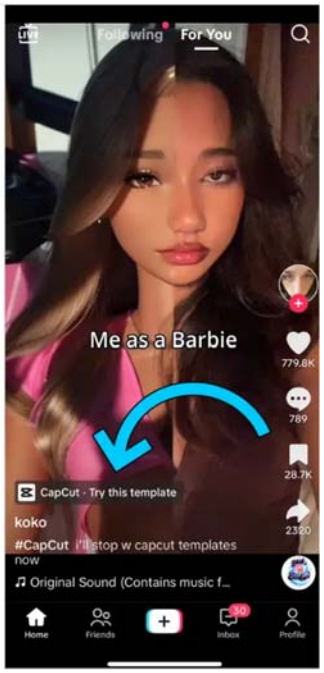
[35] https://productmint.com/how-does-capcut-make-money/#:~:text=CapCut%20Make%20Money%3F-,CapCut%20makes%20money%20by%20charging%20users%20for%20premium%20features.,a%20monthly%20or%20yearly%20subscription.

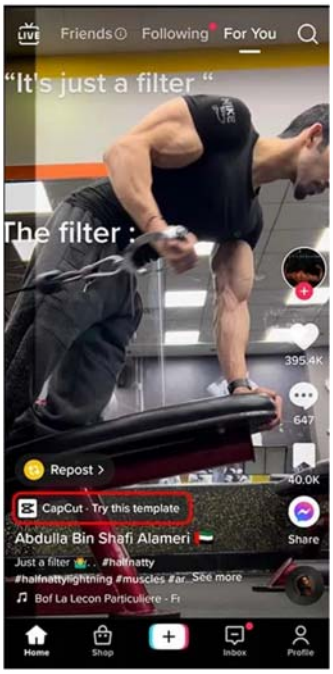
under the brand name Jianying. Jianying quickly rose to the top of the Chinese app charts. Meanwhile, ByteDance extended the app's functionality through, among other things, acquisitions of other Chinese-created technology. In 2018, for instance, ByteDance purchased the startup Shenzhen Lianmeng Technology for $300 million. Shenzhen Lianmeng Technology had previously developed the popular app Faceu, which topped China's free app charts in 2016 and 2017. ByteDance then integrated the firm's technology into Jianying. Once it became the de-facto leader in China, ByteDance sought to market the app in the United States.[36]

56. ByteDance had one significant advantage in marketing the CapCut app in the United States, that it did not possess when it introduced TikTok to the U.S. marketplace. When the CapCut app was introduced in the United States in 2020, ByteDance was already a leader in the technology space with a leading social media platform, TikTok. ByteDance utilized the popular TikTok app to heavily promote its new CapCut video editing app to users in the United States. For example, videos appearing on TikTok that are edited by CapCut direct viewers to the CapCut app, thereby increasing the number of users downloading the CapCut app.[37]

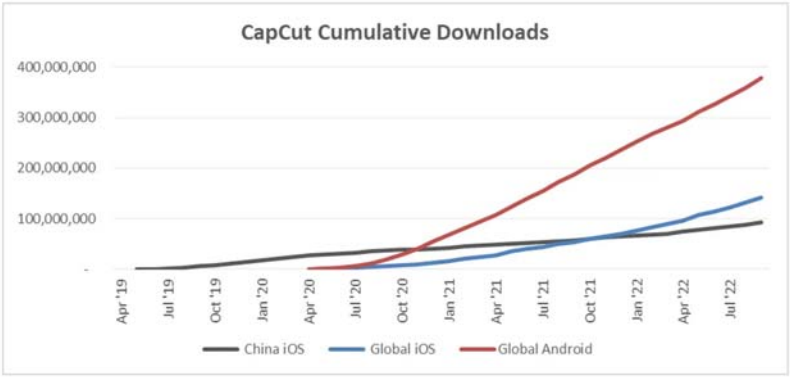
[36] https://productmint.com/how-does-capcut-make-money/#:~:text=CapCut%20Make%20Money%3F-,CapCut%20makes%20money%20by%20charging%20users%20for%20premium%20features.,a%20monthly%20or%20yearly%20subscription.

[37] https://www.wsj.com/articles/tiktoks-chinese-parent-has-another-wildly-popular-app-in-the-u-s-e14c41fc.

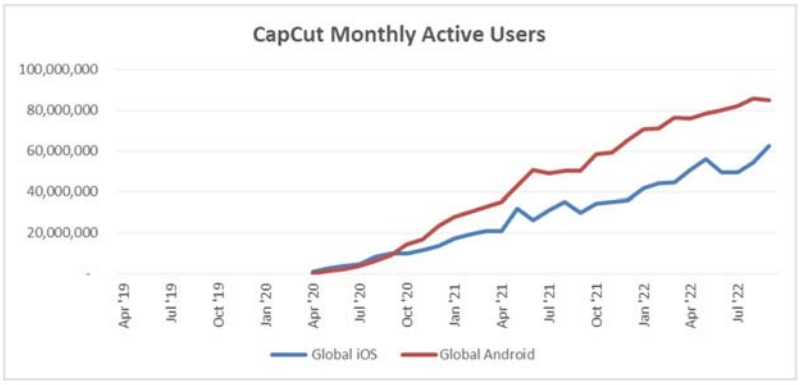




57. As a result of Defendants' heavy promotion of the CapCut app, it has become one of the most popular apps available in the United States, with more than 200 million monthly active users and global downloads of more than 400 million last year alone.[38]



[38] *Id.*



[39]

58. Conversely, the CapCut app has allowed Defendants to dramatically increase the number of videos uploaded to TikTok, and thus the amount of profits that Defendants receive through the TikTok app, because the CapCut app facilitates video creation and has features that make it easy for users to upload videos created or edited using CapCut directly to the TikTok app. As explained by one commentator, "Another important aspect to consider is that CapCut acts as a quasi-user acquisition channel for TikTok and thus ByteDance. By making it easier for people to edit videos, TikTok has even more members that will upload videos on its platform. And the more and better content is being produced, the more users TikTok will attract."[40]

59. The CapCut app has allowed Defendants to expand their data collection activities to new individuals who had not previously downloaded their apps, including the TikTok app. Many users of the CapCut app have never downloaded the TikTok app. Rather, they use the CapCut app to edit videos for their personal use or that they post on other companies' social media apps, such as Instagram, Facebook, YouTube or Linkedin.

---

[39] https://www.thespl.it/p/capcut-ai-unlocks-human-creativity.

[40] https://productmint.com/how-does-capcut-make-money/#:~:text=CapCut%20Make%20Money%3F-,CapCut%20makes%20money%20by%20charging%20users%20for%20premium%20features.,a%20monthly%20or%20yearly%20subscription.

60. Unbeknownst to CapCut users, data collected by the CapCut app may be shared with the TikTok app, thereby further maximizing Defendants' profits. Information derived from CapCut users may be used to deliver and evaluate tailored advertisements. In addition, CapCut user data may be shared with third party social network service providers. Unbeknownst to CapCut users, personal and private information may be collected from users even before they set up an account.[41]

61. Defendants have unlawfully accumulated private and personally identifiable data and content from CapCut users from which Defendants are unjustly profiting.

C. Defendants Have a History Of Unlawfully and Covertly Collecting Private And Personally Identifiable Data And Content From Users of Their Products.

62. Defendants have a history of violating the privacy rights of users of their apps. On November 15, 2020, for example, CBS News 60 Minutes published an investigative report on TikTok that raised significant concerns regarding the privacy of user data collected by the TikTok app. In the report, a former member of the U.S. intelligence community stated that "What makes TikTok particularly concerning is its relationship with the Chinese Communist Party in Beijing, the government of China. The Chinese have fused their government and their industry together so that they cooperate to achieve the ends of the state." As the report observed, the TikTok app collected a range of private user data, including "your name, your home address, your personal network, who you're friends with, your online viewing habits and a whole host of other pieces of information." In addition, "TikTok asks users for access to their cameras, microphones, photos, videos, and contacts. More obscure data, like 'keystroke patterns,' are collected from everyone

[41] https://www.nbcnews.com/politics/white-house/white-house-posts-video-created-using-app-owned-tiktoks-parent-company-rcna77333.

using the app." As Senator Josh Hawley noted in the report, the collection of this data was particularly concerning because of TikTok's ownership by ByteDance, "a Chinese parent company that has direct ties to the Chinese Communist Party." As he observed, "under Chinese law, TikTok, ByteDance, the parent, is required to share data with the Chinese Communist Party."

63. In June 2022, an article in *Buzzfeed News* further confirmed many of these concerns, citing leaked meeting audio from company employees demonstrating that China-based ByteDance has repeatedly accessed non-public data of U.S. TikTok users; as one insider observed, "Everything is seen in China"; Beijing-based engineers had "access to everything."[42] Defendants have since acknowledged that ByteDance engineers were involved in developing the algorithms used in TikTok and that China-based employees have had access to user data.[43] Separately, *Forbes* reported in October 2022 that Chinese executives used TikTok "to monitor the personal location of some specific American citizens," leading to an investigation by the U.S. government.[44]

64. In May 2023, Yintao Yu, former head of engineering for Defendant ByteDance's U.S. operations, publicly stated that the Chinese government maintained access to the company's U.S. user data. He alleged that the Chinese government could monitor ByteDance's work from its headquarters in Beijing and had provided the company with guidance on advancing "core communist values." "The Committee maintained supreme access to all the company data, even

[42] https://www.buzzfeednews.com/article/emilybakerwhite/tiktok-tapes-us-user-data-china-bytedance-access.

[43] https://www.blackburn.senate.gov/services/files/A5027CD8-73DE-4571-95B0-AA7064F707C1.

[44] https://www.forbes.com/sites/emilybaker-white/2022/10/20/tiktok-bytedance-surveillance-american-user-data/?sh=2a6a7f566c2d. *See also* https://www.nytimes.com/2022/12/22/technology/byte-dance-tik-tok-internal-investigation.html.

data stored in the United States."[45] According to Mr. Yu, "the Chinese Communist Party is able to access international and US data through a 'backdoor channel code' in TikTok."[46]

65. In November 2022, the Director of the FBI, Christopher Wray, testified before Congress that the FBI had significant "national security concerns" regarding the TikTok app, including "the possibility that the Chinese government could use it to control data collection on millions of users." As Director Wray observed, Chinese law essentially requires Chinese companies to "do whatever the government wants them to in terms of sharing information or serving as a tool of the Chinese government." "And so that's plenty of reason by itself to be extremely concerned."[47]

66. Based on such concerns, TikTok has been banned from government devices. The U.S. Army initially banned the app on government-owned devices based on concerns specific to Defendants and their close relationship to the Chinese government.[48] The U.S. Navy, Marines, Air Force and Coast Guard, as well as the Department of Defense and the Transportation Security Administration have likewise banned the TikTok app due to the risk that user data is being sent to China.[49] In taking such actions, the U.S. Department of Defense noted TikTok's "ability to convey

[45] https://thehill.com/policy/technology/4002792-former-executive-of-tiktok-parent-company-claims-china-maintained-access-to-us-data/.

[46] https://www.yahoo.com/lifestyle/tiktok-insider-says-chinese-government-093502126.html.

[47] https://www.npr.org/2022/11/17/1137155540/fbi-tiktok-national-security-concerns-china.

[48] https://www.businessinsider.com/us-government-agencies-have-banned-tiktok-app-2020-2.

[49] https://www.businessinsider.com/us-government-agencies-have-banned-tiktok-app-2020-2#1-the-navy-banned-tiktok-from-government-devices-1.

location, image and biometric data to its Chinese parent company, which is legally unable to refuse to share data with the Chinese Government."[50]

67. Expanding on these measures, United States Senators proposed a bill banning all federal employees from using the TikTok app on government issued phones because it "presents a major security risk."[51] Agreeing with this proposal, President Biden issued a directive in March 2023 ordering that the TikTok app be removed from all government devices.[52]

68. More than 30 state governments in the United States have followed federal authorities in banning the TikTok app from government devices, citing privacy concerns.[53] In addition, the State of Montana recently passed legislation that prohibits TikTok from operating within the State and bans downloads of the app within the State.[54]

69. Based on such national security and privacy concerns, Federal Communications Commissioner Brendan Carr has called on the federal government to completely ban the TikTok app in the United States. He also urged Apple and Google to remove it from their app stores,

---

[50] https://www.inc.com/jason-aten/the-department-of-defense-is-warning-people-not-to-use-tiktok-over-national-security-concerns.html.

[51] https://www.reuters.com/article/us-usa-china-tiktok/us-senators-seek-to-ban-federalemployees-from-using-tiktok-on-their-phones-idUSKBN20Z1E4.

[52] https://www.cbsnews.com/news/tiktok-banned-us-government-where-else-around-the-world/.

[53] https://news.yahoo.com/map-here-are-the-states-that-have-banned-tik-tok-on-government-devices-162434392.html#:~:text=TikTok%20is%20banned%20on%20state%20devices%20in%20more%20than%2030%20U.S.%20states.

[54] https://www.msn.com/en-us/news/us/montana-becomes-first-state-to-ban-tiktok-after-governor-signs-bill-into-law/ar-AA1bk7FP?ocid=msedgntp&cvid=a464877bbc2c43ab9af8bcae49e2718f&ei=11; https://apnews.com/article/tiktok-ban-montana-bytedance-a79eb96897d206dbe3ef3b188482d912.

citing its "pattern of surreptitious data practices."[55] As Mr. Carr observed, "All the data is available inside China. We're talking search and browsing history, keystroke patterns, biometrics, potentially including face prints and voice prints being available inside Beijing,"[56]

70. Likewise, Senator Marco Rubio and Representative Mike Gallagher recently introduced legislation to completely ban TikTok "and other social media companies that are effectively controlled by the CCP from operating in the United States."[57]

71. Such concerns regarding Defendants' violations of the privacy of users of their apps are not limited to the United States. Due to similar concerns, the TikTok app has been banned on devices used by staff of the European Parliament, European Commission and the EU Council as well as government devices in Canada and Taiwan.[58] In addition, India completely banned the TikTok app from devices in that country in 2020.[59]

72. As authorities have recognized, the privacy concerns are significant, given that Chinese companies have a legal obligation to cooperate with the Chinese government and provide the government with user data they collect. Thus, for example, Senator Hawley has noted: "all it takes is one knock on the door of their parent company, based in China, from a Communist Party

---

[55] https://techcrunch.com/2022/06/28/fcc-commissioner-writes-to-apple-and-google-about-removing-tiktok/#:~:text=An%20FCC%20Commissioner%2C%20Brendan%20Carr,users%27%20data%20up%20until%20January.

[56] https://www.skynews.com.au/world-news/global-affairs/culture-of-lawlessness-whistleblower-makes-explosive-claims-about-the-tiktoks-shocking-links-to-chinese-communist-party/news-story/1c5f2ef3dcbd1faca66318fa7eb524d2?amp.

[57] https://www.npr.org/2022/11/17/1137155540/fbi-tiktok-national-security-concerns-china; *see also* https://www.washingtonpost.com/opinions/2022/11/10/marco-rubio-ban-tiktok-america-china-mike-gallagher/.

[58] *Id.*

[59] *Id.*

official for that data to be transferred to the Chinese government's hands, whenever they need it."[60] As a former TikTok employee acknowledged (as reported in the *Wall Street Journal*): "We're a Chinese company … We answer to China."[61]

73. Indeed, China-based ByteDance exercises significant day-to-day control over operations in the United States of its affiliates. As a recent *Washington Post* story reported based on statements by former and current employees, China signs off on all major decisions regarding American operations including decisions regarding American users' data:

> 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.[62]

74. Other reports from former employees are in accord. For example, another recent report quoted employees as stating: "'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.'"[63]

---

[60] https://www.nbcnews.com/politics/congress/hawley-takes-aim-tiktok-china-congressional-hearing-n1076586.

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

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

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

75. Nonetheless, ByteDance has attempted to obscure its ties to China and obscure the fact that user data is available to individuals in China, including the Chinese communist government. For example, it has been reported that TikTok eliminated any reference to China from its U.S. privacy policy sometime in 2019 or thereafter, even though the entities with which the policy stated it may share users' data did not change location.[64]

76. Indeed, TikTok documents demonstrate that TikTok's "messaging" strategy calls for company representatives to "Downplay the parent company ByteDance, downplay the China association, downplay AI."[65] Based on information and belief, Defendants' corporate strategy to downplay the association with China applies equally with respect to the CapCut app.

77. As a result of such allegations, the TikTok app was the subject of multiple class action lawsuits consolidated in a federal multidistrict litigation (MDL) proceeding, which Defendants recently settled for $92 million.[66]

D. Defendants Use The CapCut App To Continue And Expand Their Theft Of Users' Private And Personally Identifiable User Data And Content.

78. While it has received less scrutiny than the TikTok app, Defendants' CapCut app is no less of a threat to the privacy of its users.[67] CapCut is an app developed by TikTok's Chinese parent, ByteDance, that affords users powerful tools with which they can edit videos that may then be made public on a variety of social media platforms or remain private with the user. CapCut is a

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

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

[66] *In re TikTok, Inc. Consumer Privacy Litig.*, MDL 2948, No. No. 20-cv-4699 (N.D. Ill.).

[67] https://www.wsj.com/articles/tiktoks-chinese-parent-has-another-wildly-popular-app-in-the-u-s-e14c41fc.

separate and distinct app that provides tools to users that are not available on the TikTok app, and which can be used by individuals who never download or utilize the TikTok app. While the CapCut app contains a feature that allows users to post videos directly to TikTok,[68] videos created by CapCut may also be posted to other social media apps, such as YouTube, Instagram, Linkedin and Facebook.

79. Such videos are prominently featured on social media apps like TikTok and YouTube, which offer feeds of recommended videos that are selected based on each user's interests.

80. Such videos are an essential element of certain social media platforms' revenue models, which rely on targeted advertisements tied to such user-generated content. The greater the number of CapCut-generated videos that are uploaded to TikTok, for example, the greater the revenues received by Defendants from the TikTok app.

81. By prompting users to view videos with which they are more likely to engage (based on data they collect from users), TikTok and other social media platforms have increased their revenues at a significant pace.

82. The more user data social media platforms such as TikTok have at their disposal, the more efficiently and effectively they can deploy advertising and grow its profits. Thus, to the extent TikTok has access to data from CapCut users, it can grow its revenue and profits even more.

83. Unless publicly shared through the affirmative consent of a CapCut user, videos created using the CapCut app, which often include close-up views of faces and private acts unintended for public consumption, are inherently private, personal and sensitive.

[68] https://www.thespl.it/p/capcut-ai-unlocks-human-creativity.

84. Unbeknownst to users of the app, the CapCut app gains access to these private videos. Moreover, the app performs "pre-uploading" of content (videos, etc.), which sends the content to the platform even before the user clicks on "upload" or "post".

85. Likewise, unbeknownst to users, the CapCut app collects a broad array of private and personally identifiable data and content from which Defendants unjustly profit. The CapCut app collects a range of private and personal user data, including photos and videos, as well as location, gender and birthday.[69] CapCut collects personal data from its users to develop a data bank that can then be used for targeted advertising.[70]

86. Plaintiffs, the Class, and the Subclass have a reasonable expectation of privacy in the private and personally identifiable data and content on their devices.

87. From each device on which the CapCut app is installed, Defendants collect, among other items, the following user data and information:

a. username, password, age/birthday, email address, and profile image;

b. phone and social network contacts;

c. identifier and location information;

d. photos and videos and other user-generated content;

e. audio data;

f. product interaction and usage data;

g. crash data;

h. dump data;

[69] https://www.wsj.com/articles/tiktoks-chinese-parent-has-another-wildly-popular-app-in-the-u-s-e14c41fc.

[70] https://nerdschalk.com/who-made-capcut/.

i. performance data; and

j. diagnostics data.[71]

88. Defendants have built into the CapCut app the capacity to collect a range of private and personally identifiable information regarding users, including Mac address, SSID, BSSID, previously configured networks, IMEI information, device ID, IMSI information, phone number, voice mail number, MEID (Mobile Equipment Identifier), ICCID (Integrated Circuit Card Identifier), and SIM serial number.

89. In addition, Defendants have built into the CapCut app the capacity to collect fine-grained location information and location updates, access files on user devices and store them, and engage in offline data collection.

90. Collection of physical and digital location tracking data is highly invasive of CapCut users' privacy rights. "Location data is among the most sensitive personal information that a user can share with a company . . . Today, modern smartphones can reveal location data beyond a mere street address. The technology is sophisticated enough to identify on which floor of a building the device is located."[72] Over time, location data reveals private living patterns of CapCut users, including where they work, where they reside, where they go to school, and when they are at each of these locations. Location data, either standing alone, or combined with other information, exposes deeply private and personal information about CapCut users' health, religion, politics and intimate relationships.

---

[71] *Id.*

[72] https://www.law360.com/consumerprotection/articles/1221312/sens-prod-zuckerberg-why-keep-tracking-user-locations-.

91. Multiple experts have expressed concerns regarding CapCut's harvesting of users' personal data. For example, the Special Competitive Studies Project, a technology think tank funded by former Google CEO Eric Schmidt, lists CapCut as one of the Chinese apps that "pose similar challenges" to American security, "particularly with respect to data harvesting, data exploitation, and—possibly—covert influence."[73]

E. Defendants Are Violating The Illinois Biometric Information Privacy Act.

92. In 2008, Illinois enacted the Biometric Information Privacy Act ("BIPA"), 740 ILCS 14/1, et seq. to address the "very serious need [for] protections for the citizens of Illinois when it [comes to their] biometric information." Illinois House Transcript, 2008 Reg. Ses. No. 276. The Illinois Legislature recognized the importance of protecting the privacy of individuals' biometric data, finding that "[b]iometrics are unlike other unique identifiers that are used to access finances or other sensitive information." 740 ILCS 14/5(c). "For example, social security numbers, when compromised, can be changed. Biometrics, however, are biologically unique to the individual; therefore, once compromised, the individual has no recourse [and] is at heightened risk for identity theft ...." *Id.* As the Illinois Supreme Court has recognized, through the BIPA, "our General Assembly has codified that individuals possess a right to privacy in and control over their biometric identifiers and biometric information." *Rosenbach v. Six Flags Entm't Corp.*, 129 N.E.3d 1197, 1206 (Ill. 2019).

93. BIPA protects "biometric identifiers" and "biometric information." Biometric identifiers consist of "a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry." 740 ILCS 14/10. A "scan" under BIPA means to examine by observation or checking,

[73] https://scsp222.substack.com/p/tiktok-is-the-tip-of-the-iceberg.

or systematically in order to obtain data especially for display or storage. *In re Facebook Biometric Information Privacy Litigation*, No. 15-cv-03747-JD, 2018 WL 2197546, *3 (N.D. Cal. May 14, 2018). "Geometry" under BIPA is the relative arrangement of parts or elements. *Id.* Neither the term "scan" nor the term "geometry" require "actual or express measurements of spatial quantities like distance, depth, or angles." *Id.* Biometric information constitutes "any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual." 740 ILCS 14/10.

94. Defendants have unlawfully collected, possessed, stored, disseminated, used and profited from biometric identifiers (such as face geometry scans of CapCut users), and the biometric information derived therefrom, in multiple ways.

95. First, Defendants' BIPA and other biometrics-related violations are established by the functionality and code of the CapCut app itself, which includes scans of users' face geometry.

96. For example, the CapCut app uses an advanced video editor and camera face filters. Employing this technology, CapCut users edit their videos to, among other things, morph their face into another face; change the size, shape, height and width of their face; change particular features of their face (e.g., eyes, ears, nose, lips, mouth, cheeks), including the size and shape of such facial features; and so on. Users thereby create videos in which their faces and specific facial features take on a variety of dimensions and appearances. The CapCut app examines, detects and localizes the face and the arrangement of its various parts (e.g., the eyes, ears, nose, lips, mouth, cheeks) relative to the other parts, and then tracks the face and its various parts (and their relative arrangement) while in motion.

97. Second, Defendants' BIPA and other biometrics-related violations are further established by their ongoing work in China, which includes the application of facial recognition technology to CapCut users' videos by highly-trained engineers skilled in computer vision, convolutional neural network and machine learning.

98. Defendants' artificial intelligence work within China, which is closely tied to their United States operations, is among the most sophisticated in the world. "ByteDance has received accolades for being a top AI innovator from CBInsight who recognized the company on its 2018 AI 100 List as well as from Fast Company, who placed it on its most innovative companies list. In 2016, it founded its AI Lab, a research division led by Wei-Ying Ma, formerly of Microsoft Research Asia. The Lab's primary focus has been on developing innovative technologies to enhance ByteDance's content platforms."[74]

99. Defendants employ engineers in fields such as computer vision, convolutional neural network, and machine learning, all of which are used to generate the face geometry scans that Defendants derive from the videos of CapCut users. Defendants' China-based engineering team includes multiple researchers who perform work in these areas.

100. For example, Wei-Ying Ma served as a Beijing Douyin Vice President and led the AI Lab in Beijing since 2017. He is known for having developed an image retrieval system called NeTra, which is a tool for navigating very large image databases. Ma delivered a keynote speech at a Taipei Web Conference in which he acknowledged that Defendants use facial recognition technology and face geometry scans on their enormous and ever-growing database of face images

[74] https://www.forbes.com/sites/bernardmarr/2018/12/05/ai-in-china-how-buzzfeed-rival-bytedance-uses-machine-learning-to-revolutionize-the-news/?sh=16a0c3ed40db.

from user videos. During his speech, Ma used visual representations that show facial recognition and face geometry scans being performed on specific regions of face images, describing the "video understanding tasks" and analysis that are performed, and how they "convert this video into a structural representation."[75]

101. Defendant ByteDance processes and analyzes users' videos received from around the world at its facilities in China. *TechNode* reported that one of its vice presidents publicly told a gathering that ByteDance required more chips to continue uploading, processing and analyzing its vast database of videos accumulated from around the world. This vice president stated that "'Bytedance has the largest number of users in the world whose videos need to be analyzed and processed and uploaded, and we are purchasing a large number of chips.'"[76]

102. As the United States National Security Adviser noted, Defendants are "getting facial recognition" on millions of Americans as well as mapping their relationships, and then sending all of this "intimate data" back to China for processing through their apps.[77]

103. The potential applications and uses of this data are reflected in patent applications filed by Defendants' sister company ByteDance Network Technology Co., Ltd. The underlying technology in these patent applications involves age, race, and emotion detection through face images, including those derived from videos. The specific patent applications address such as facial image identification;[78] use of images and a facial recognition model to determine ethnic

[75] https://www.youtube.com/watch?v=2D29f4-J2mw (at 18:18 – 19:17).

[76] https://technode.com/2018/04/24/bytedance-jinri-toutiao-ai-chips/.

[77] https://www.forbes.com/sites/zakdoffman/2020/07/15/tiktok-trump-warning-facial-recognition-data-sends-china-ban/?sh=33766e422dea.

[78] Publication No. WO2020037963A1, https://patents.google.com/patent/WO2020037963A1/en.

information, race and age;[79] use of face and body images, and a facial recognition model, to determine age;[80] use of image and audio data sets to determine age;[81] use of face images extracted from videos to determine age;[82] facial expression recognition methods;[83] use of facial images extracted from videos to determine emotions;[84] and use of face images extracted from video segments to identify a face characteristic.[85]

104. ByteDance Network Technology Co., Ltd. has filed additional patent applications for a method for voice extraction involving voiceprints,[86] a voice recognition method,[87] and an age recognition method based on audio.[88] This is consistent with reporting that Defendant ByteDance "uses various AI technologies in its services [including] voice recognition ...."[89] During Wei-Ying

[79] Publication No. CN110046571A, available at https://patents.google.com/patent/CN110046571A/en.

[80] Publication No. CN109993150A, available at https://patents.google.com/patent/CN109993150A/zh.

[81] Publication No. CN110321863A, available at https://patents.google.com/patent/CN110321863A/en.

[82] Publication No. CN110163170A, available at https://patents.google.com/patent/CN110163170A/en; Publication No. CN110188660A, available at https://patents.google.com/patent/CN110188660A/en.

[83] Publication No. CN110097004A, available at https://patents.google.com/patent/CN110097004A/en.

[84] Publication No. CN110175565A, available at https://patents.google.com/patent/CN110175565A/en.

[85] Publication No. CN110163171A, available at https://patents.google.com/patent/CN110163171A/en.

[86] Publication No. CN110503961A, available at https://patents.google.com/patent/CN110503961A/en.

[87] Publication No. WO2019214628A1, available at https://patents.google.com/patent/WO2019214628A1/en.

[88] Publication No. CN110335626A, available at https://patents.google.com/patent/CN110335626A/en.

[89] https://medium.com/syncedreview/intel-and-bytedance-partner-on-ai-lab-b678036cbda4.

Ma's keynote speech at a Taipei Web Conference (above), he discussed the use of audio to identify speakers and published a slide during his speech entitled "Speaker Identification" that stated: "Detect identity, age, gender of speakers."[90]

105. As commentators have recognized, "TikTok's owner, Beijing-based ByteDance, is a hit app factory that has spent the last decade learning how to use artificial intelligence, machine learning, and facial recognition to figure out what people like and serve them endless streams of entertainment tailored to their interests and emotions."[91]

106. Finally, Defendants' BIPA and other biometrics-related violations are also established by Defendants' legal and political obligations to accumulate and share data, including biometric data, to assist the Chinese government in developing artificial intelligence and population surveillance and control technologies.

107. In 2017, the Chinese government released its Next Generation Artificial Intelligence Development Plan, in which it set 2030 as the temporal goal for becoming the world leader in artificial intelligence. To ensure achievement of its artificial intelligence goal, the Chinese government selected the five leading technology companies as "national champions" and assigned them particular areas of research and development within the artificial intelligence field. In exchange, these companies receive government support, including access to finance, preferential contract bidding and sometimes market share protection. The list of "national champions" has grown to at least 15 in recent years.[92]

---

[90] https://www.youtube.com/watch?v=2D29f4-J2mw (at 30:04).

[91] https://www.bloomberg.com/news/newsletters/2019-10-29/worries-that-tiktok-is-a-threat-to-national-security-have-merit.

[92] https://fortune.com/longform/tiktok-app-artificial-intelligence-addictive-bytedance-china/.

108. The United States government has recognized China's work in artificial intelligence as a potential threat to national security. Congress's National Security Commission on Artificial Intelligence, chaired by former Google CEO Eric Schmidt, published an interim report warning that China was outpacing the United States in artificial intelligence spending.[93]

109. The Chinese government's monitoring of, and control over, its own population are well known. Most notable is its pervasive use of artificial intelligence-enabled cameras to conduct video surveillance of its population.[94] As the South China Morning Post reported: "China's goal of becoming a global leader in artificial intelligence (AI) is nowhere more manifested than in how facial recognition technology has become a part of daily life in the world's second-largest economy. Facial recognition systems, which are biometric computer applications that automatically identify an individual from a database of digital images, are now being used extensively in areas such as public security, financial services, transport and retail across the country."[95] In fact, the Chinese government employs a variety of biometrics for population surveillance and control: "In addition to voice recognition, there are facial and pupil recognition, gathering of DNA samples—building the world's largest DNA database—and fingerprint scans."[96]

110. Artificial intelligence algorithms feed on data to learn and improve – thus, the more data the better the development of the algorithms driving the advance of the artificial

---

[93] *Id.*

[94] *Id.*

[95] https://www.scmp.com/tech/start-ups/article/2133234/meet-five-chinese-start-ups-pushing-facial-recognition-technology.

[96] https://brandscovery.com/business/content-2254742-china-gathers-people-s-voices-new-identification-technology-drawing-concerns.

intelligence.[97] With better artificial intelligence comes more effective population surveillance and control.

111. To advance these interrelated goals, the Chinese government has worked with China-based technology companies to accumulate and share data. "Private [China-based] corporations and the [Chinese] Communist Party's security apparatus have grown together, discovering how the same data sets can both cater to consumers and help commissars calibrate repression. … Many [China-based] tech firms make a point of hiring the relatives of high party officials, and a vast state database of headshots might be shared with a private firm to train new facial recognition software, while the firm's trove of real-time user data might be offered to police, for a panoramic view of potential 'troublemakers.'"[98]

112. The lengths to which the Chinese government will go to obtain such data about ordinary Americans is further evidenced by large-scale hacking schemes, including one involving 145 million Americans whose data was held by Equifax,[99] and another involving 78 million Americans whose data was held by Anthem.[100] "The United States assessed that China was building a vast database of who worked with whom in national security jobs, where they traveled and what their health histories were, according to American officials. Over time, China can use the data sets to improve its artificial intelligence capabilities to the point where it can predict which Americans will be primed for future grooming and recruitment …."[101] "The hacks, security

[97] https://fortune.com/longform/tiktok-app-artificial-intelligence-addictive-bytedance-china/.

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

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

[100] https://www.nytimes.com/2019/05/09/technology/anthem-hack-indicted-breach.html.

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

researchers said, were an extension of China's evolving algorithmic surveillance system, which has greatly expanded over the past few years."[102]

113. However, where, as here, China-based technology companies, like Defendants, have surreptitiously amassed such data on their own, there is no need for the Chinese government to engage in hacking to obtain the data. Under Chinese law, the data is directly available to the government. That is because such China-based companies are required by law to secretly provide that data to the government upon demand:

> The message contained in each of China's state security laws passed since the beginning of 2014 is clear: everyone is responsible for the party-state's security. According to the CCP's definition of state security, the Party's political leadership is central. … And the party expects Chinese people and citizens to assist in collecting intelligence. The Intelligence Law states "any organization and citizen shall, in accordance with the law, support, provide assistance, and cooperate in national intelligence work, and guard the secrecy of any national intelligence work that they are aware of…" Not only is everyone required to participate in intelligence work when asked, but that participation must be kept secret.[103]

114. 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 and open-ended. 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

[102] https://www.nytimes.com/2019/05/09/technology/anthem-hack-indicted-breach.html.

[103] https://capx.co/britain-must-avoid-being-sucked-into-huaweis-moral-vacuum/. *See also* https://www.lawfareblog.com/beijings-new-national-intelligence-law-defense-offense.

basis for China's security activities and requiring Chinese and foreign citizens, enterprises, and organizations to cooperate with them."[104]

115. Defendant ByteDance, in particular, has a history of complying with the dictates of the Chinese government. In 2018, China's State Administration of Radio and Television, an arm of the Chinese Communist Party, ordered Defendant ByteDance to shut down one of its apps due to "vulgar" content. That prompted the CEO to publicly apologize. 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, elevating distribution of authoritative media content, [and] ensuring that authoritative [official Party] media voices are broadcast to strength."[105] His re-dedication to the Chinese Communist Party resulted in his being named one of the "100 outstanding private entrepreneurs" who were "chosen for being 'emblematic of the country's private economic development', while also being people who 'resolutely uphold the Party's leadership ….'"[106]

116. In a further show of allegiance to the Chinese government, Defendant ByteDance actively supports and participates in the spreading of Communist Party propaganda. It signed a strategic cooperation agreement with the Ministry of Public Security's Press and Publicity Bureau to promote the credibility of the police department, including within an area of China known for

[104] M. Scot Tanner, Beijing's New National Intelligence Law: From Defense to Offense, LAWFARE (July 20, 2017), https://bit.ly/3fXfB4A.

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

[106] https://capx.co/britain-must-avoid-being-sucked-into-huaweis-moral-vacuum/.

severe repression, demolition of mosques, and detention centers for ethnic minorities. Under that agreement, "all levels and divisions of police units from the Ministry of Public Security to county-level traffic police would have their own Douyin account to disseminate propaganda. The agreement also reportedly says ByteDance would increase its offline cooperation with the police department …."[107]

117. ByteDance further pledged to the Chinese government "'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."[108]

118. In addition, many of the employees of Defendant ByteDance and its affiliates are members of the Chinese Communist Party, which controls the Chinese government. 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.[109]

119. "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

[107] https://www.aspi.org.au/report/mapping-more-chinas-tech-giants.

[108] Mem. From John K. Costello, Dep. Ass. 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, 11 (Sept. 17, 2020), https://bit.ly/3VJ1Vt9 (quoting K. Everington, TikTok owners show true colors with communist flag, TAIWAN NEWS (Aug. 6, 2020), https://bit.ly/3H4QMP7)).

[109] *Id.* at 7–8.

department groups. According to Chinese press reporting, Bytedance has more party members and party organizations and is more 'red,' insiders pointed out, as compared with other Internet [C]ompanies."[110]

120. According to *Forbes*, "[t]hree hundred current employees at TikTok and its parent company ByteDance previously worked for Chinese state media publications, according to public employee LinkedIn profiles reviewed by Forbes. Twenty-three of these profiles appear to have been created by current ByteDance directors, who manage departments overseeing content partnerships, public affairs, corporate social responsibility and 'media cooperation.' Fifteen indicate that current ByteDance employees are also concurrently employed by Chinese state media entities."[111]

121. ByteDance has stated it makes "[h]iring decisions based purely on an individual's professional capability to do the job. For our China-market businesses, that includes people who have previously worked in government or state media positions in China."[112]

122. The insertion of such communist party members into private enterprises and the establishment of such party committees is a means by which the Chinese government and Chinese communist party issue direct control over nominally "private" companies. For example, the Commerce Department noted that internal Communist Party committees "are a mechanism through which Beijing expands its authority and supervision over nominally private or non-governmental organizations, creating different nuances of corporate governance with Chinese

[110] *Id.* at 8 (citing Chinese language news sources).

[111] 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.

[112] *Id.*

characteristics."[113] "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."[114]

123. 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."[115] For example, 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," specifically called for "further strengthen[ing] the Party's leadership of, and cohesive effect on, private economy practitioners."[116]

---

[113] Mem. From John K. Costello, Dep. Ass. 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, 7 (Sept. 17, 2020), https://bit.ly/3VJ1Vt9 (citing J. Laband, Fact Sheet: Communist Party Groups in Foreign Companies in China, CHINA BUSINESS REVIEW (May 31, 2018), https://bit.ly/3HmDbmH).

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

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

[116] *Id.*

124. The CapCut app's functionality and code, its application of facial recognition technology to CapCut user videos, patent applications for facial, voice, age, race/ethnicity and emotion recognition technologies, and Defendants' legal obligations and political ties to the Chinese government demonstrate the broad scope and implications of Defendants' BIPA and other biometrics violations.

F. Defendants Are Unjustly Profiting While Plaintiffs Suffer Harm.

125. Defendants possess user/device identifiers, biometric identifiers and information, private videos, and private video images sufficient to create a file of private and personally identifiable data and content for each CapCut user. Such files can be supplemented over time with additional private and personally identifiable user data and content, and all of this private and personally identifiable data and information has been, is, and will be used for economic and financial gain.

126. Defendants' unlawful possession and control over this data and information make tracking and profiling CapCut users, and targeting them with advertising, much more efficient, effective, and lucrative. Such private and personally identifiable data and content are used to analyze CapCut users' income, consumption habits, and preferences. Such information provides guidance as to what methods of advertising will be most effective on particular CapCut users, what products – including Defendants' own products – will be most attractive to particular CapCut users, and how much to spend on particular ads. Defendants unjustly have earned and continue to earn substantial profits and revenues from such targeted advertising and from generating increased demand for and use of Defendants' other products.

127. Defendants also unlawfully leverage the private and personally identifiable CapCut user data and content to improve their artificial intelligence technologies and file patent

applications, thereby unjustly increasing their past, present and future profits and revenues – and their market value.

128. Meanwhile, Plaintiffs, the Class and the Subclass have incurred, and continue to incur, harm as a result of the invasion of privacy stemming from Defendants' covert theft of their private and personally identifiable data and content – including their user/device identifiers, biometric identifiers and information, private videos and private video images.

129. Plaintiffs, the Class and the Subclass also have suffered and continue to suffer harm in the form of diminution of the value of their private and personally identifiable data and content as a result of Defendants' surreptitious and unlawful activities. Plaintiffs personal and private data has a significant commercial value. In 2018, California enacted the California Consumer Privacy Act ("CCPA") which recognizes the significant economic value of such consumer data. The act, among other things, permits businesses to purchase consumer information from consumers directly (Cal. Civ. Code § 1798.125(b)(1)) and permits business to assess and appraise consumer data with a monetary value (Cal. Civ. Code § 1798.125(a)(2)).

130. Plaintiffs and the Class have suffered benefit of the bargain damages, insofar as Defendants took more data than they were authorized to take and used that data for undisclosed and unauthorized purposes. Those benefit of the bargain damages include loss of control over property (their data) that has a marketable value. In addition, Plaintiffs and the Class assigned value to keeping their private data private, which was destroyed when Defendants inappropriately collected their data without adequate notice or authorization and used it for undisclosed purposes.

131. Finally, Plaintiffs, the Class, and the Subclass have incurred additional data usage and electricity costs that they would not have incurred but for Defendants' covert and unlawful actions.

G. Defendants Have Fraudulently Concealed Their Unlawful Conduct, Thereby Tolling Any Applicable Statutes of Limitations.

132. Each unauthorized collection of private data to Defendants is a separate "wrong" that triggers anew the relevant statute of limitations.

133. The applicable statutes of limitations are tolled as a result of Defendants' knowing and active concealment of their unlawful conduct alleged above – through, among other things, their obfuscation of the source code, misleading public statements, and hidden and ambiguous privacy policies and terms of use. Plaintiffs, the Class, and the Subclass were ignorant of the information essential to pursue their claims, without any fault or lack of diligence on their own part.

134. Also, at the time the action was filed, Defendants were under a duty to disclose the true character, quality, and nature of their activities to Plaintiffs, the Class and the Subclass. Defendants are therefore estopped from relying on any statute of limitations. Defendants' fraudulent concealment is common to the Class and the Subclass.

H. The Named Plaintiffs Have Been Injured By Defendants' Unlawful Conduct.

135. During the time that the CapCut app was installed on plaintiffs' devices, Defendants surreptitiously performed, among others, the following actions without notice to or the knowledge and consent of plaintiffs or, in the case of the minor plaintiffs, their legal guardians: (i) Defendants took plaintiffs' user/device identifiers and private videos from their devices; (ii) Defendants took plaintiffs' biometric identifiers and information (including face geometry scans)

from plaintiffs' device and/or videos; (iii) Defendants took plaintiffs' private and personally identifiable data and content from plaintiffs' devices; and (iv) Defendants made some or all such stolen data and content accessible to individuals in China – including individuals under the control of the Chinese government.

136. Defendants performed these acts for the purpose of secretly collecting plaintiffs' private and personally identifiable data and content – including their user/device identifiers, biometric identifiers and information, and private videos – and using such data and content to track, profile and target plaintiffs with advertisements. Further, Defendants have used plaintiffs' private and personally identifiable data and content for the purpose of developing their artificial intelligence capabilities and patenting commercially valuable technologies. Defendants and others now have access to private and personally identifiable data and content regarding plaintiffs that can be used for further commercial advantage and other harmful purposes. Defendants have profited, and will continue to profit, from these activities.

137. Meanwhile, plaintiffs have incurred harm as a result of Defendants' invasion of their privacy rights through their covert taking of plaintiffs' private and personally identifiable data and content – including their user/device identifiers, biometric identifiers and information, private videos and private video images. Plaintiffs also have suffered harm because Defendants' actions have diminished the value of their private and personally identifiable data and content. Moreover, plaintiffs have suffered injury to their devices. The battery, memory, CPU, and bandwidth of Plaintiffs' devices have been compromised, and as a result, the functioning of those devices has been impaired and slowed, due to Defendants' clandestine and unlawful activities.

Finally, Plaintiffs have incurred additional data usage and electricity costs that they and/or their guardians would not have incurred but for Defendants' covert and unlawful actions.

138. Neither Plaintiffs nor, in the case of the minor plaintiffs, their guardians, ever received notice that Defendants would collect, capture, receive, otherwise obtain, store, and/or use their biometric identifiers, face geometry scans, voiceprints or any of their other biometric information. Defendants never informed plaintiffs or their guardians of the specific purpose and length of time for which their biometric identifiers, face geometry scans, or any of their other biometric information would be collected, captured, received, otherwise obtained, stored, and/or used. Neither Plaintiffs nor, in the case of minors, their guardians, ever signed a written release authorizing Defendants to collect, capture, receive, otherwise obtain, store, and/or use their biometric identifiers, face geometry scans, voiceprints, or any of their other biometric information.

139. Based on counsel's investigation and analysis, CapCut deliberately designed its Terms of Service and Privacy Policy to decrease the likelihood that a user will receive, notice, or comprehend its terms and conditions or could provide meaningful, express consent to its conditions, in order to encourage users to sign up and not be deterred by accurate and truthful disclosures.

140. Plaintiffs did not know nor expect that Defendants would collect, store, and use their biometric identifiers and biometric information when they used the CapCut app.

141. Plaintiffs did not receive notice from Defendants (written or otherwise) that Defendants would collect, store, and/or use their biometric identifiers or biometric information. Plaintiffs did not receive notice from Defendants of the specific purpose and length of time that Defendants would collect, store, and/or use her biometric identifiers or biometric information.

Plaintiffs did not give authorization (written or otherwise) for Defendants to collect, store, and/or use her biometric identifiers or biometric information.

142. Plaintiffs were not aware of, nor do they recall seeing, a retention schedule setting out the guidelines for Defendants to permanently destroy biometric identifiers or biometric information.

I. Defendants' Privacy Policies And Terms of Use Do Not Constitute Notice of, Or Consent To, CapCut User Data Theft.

143. Defendants have adopted various privacy policies and terms of use for the CapCut app. Certain privacy policies purport to disclose that the CapCut app takes some (but not all) of the private and personally identifiable user data and content above.

144. Because the CapCut app begins taking private and personally identifiable user data – including user/device identifiers – immediately upon the completion of the download process, and before CapCut users are even presented with the option of signing-up for and creating an account, CapCut users have no notice of, and cannot consent to, the privacy policies and terms of use prior to such theft. In addition, Web users can browse to the CapCut site, and begin creating content without logging in or creating an account. CapCut users who have not signed up for an account have no notice of, and cannot consent to, the privacy policies and terms of use.

145. Moreover, even at the point at which CapCut users have the option to sign-up and create an account, Defendants do not provide such users actual notice of privacy policies or terms of use. Nor do Defendants present CapCut users with conspicuously located and designed hyperlinks to their privacy policies and terms of use, much less conspicuous warnings accompanying such hyperlinks. The CapCut app thus allows users to utilize the app without ever placing them on actual or constructive notice of the privacy policies and terms of use. This lack of

actual or constructive notice deprives CapCut users of the opportunity to accept or reject CapCut's privacy policies and terms of use, rendering such documents unenforceable.

146. Additionally, certain privacy policies and terms of use are ambiguous as to what conduct they purport to cover. Such privacy policies and terms of use are also substantively and procedurally unconscionable. The ambiguities render meaningless the purported disclosures and requirements in the remainder of these documents, and the substantive and procedural unconscionability render such documents unenforceable.

147. Moreover, even if CapCut users had knowingly accepted the terms of use (which they did not), the purported waiver of the right to seek public injunctive relief in a court of law is unenforceable under California law. *See, e.g., McGill v. Citibank*, 2 Cal. 5th 945 (2017); *Blair v. Rent-A-Center*, 928 F.3d 819 (9th Cir. 2019).

148. Any attempt to surreptitiously secure minor users' "consent" to CapCut's Terms of Use is unlawful and invalid.

149. Defendants do not make any attempt to secure the consent of parents or lawful guardians.

150. Defendants have not obtained consent from the parents or lawful guardians of minor Class Members for their accounts.

151. Defendants fail to make reasonable efforts to ensure that a parent or lawful guardian of minor Class Members receives direct notice of their practices regarding the collection, use, or disclosure of personal and biometric information.

152. Defendants do not at any point contact the parents or lawful guardians of minor Class Members to give them notice and do not even ask for contact information for the parents or lawful guardians of Class Members.

153. Thus, Defendants have no means of obtaining verifiable parental consent for minor class members, or the consent of any lawful guardian, before any collection, use, or disclosure of the personal information of minor Class Members.

154. Indeed, while Defendants recognize that individuals under age 13 should not be using the CapCut app at all and that the app is not suitable for such underage users, the app does not perform age verification to prevent underage users from using the app. Nor does it take steps necessary to ensure that minor users have obtained parental consent to use the app. Accordingly, Defendants have subjected underage users to a range of privacy violations unnecessarily because Defendants have failed to implement appropriate age verification measures that would prevent them from using the app.

155. Indeed, Defendants' failure to discourage underage use appears to be intentional. Among other things, as noted above, the TikTok app, which itself is heavily used by younger users, actively promotes use of the CapCut app, which is owned by the same corporate group. As the *Wall Street Journal* has observed, "through its powerful algorithms, TikTok can quickly drive minors—among the biggest users of the app—into endless spools of content about sex and drugs."[117] In fact, the FTC previously took action against TikTok for its failure to protect children, resulting in a settlement with the FTC and the imposition of a then-record civil COPPA penalty. Having lured large numbers of children to the TikTok platform through its powerful algorithms, including

[117] https://www.wsj.com/articles/tiktok-algorithm-sex-drugs-minors-11631052944.

children under the age of 13, Defendants then channeled those same underage users to the CapCut app through heavy promotion of the CapCut app on the TikTok platform.

156. In addition, the design of the CapCut app itself facilitates underage use. The CapCut app allows individuals to use the app without creating an account. As a result, underage users can use the app without reporting their age at all. Accordingly, Defendants not only fail to take adequate measures to discourage underage use, but they have taken active steps that encourage underage use in the way they have designed and promoted the CapCut app.

157. To the extent that Defendants attempt to claim that they obtained the minor Plaintiffs' consent, the minor Plaintiffs expressly disaffirm such consent.

V. CLASS ALLEGATIONS

158. Plaintiffs seek certification of the classes set forth herein pursuant to Federal Rule of Civil Procedure 23 ("Rule 23"). Specifically, Plaintiffs seek class certification of all claims for relief herein on behalf of a class and subclass defined as follows:

Nationwide Class: All persons who reside in the United States who used the CapCut app after it was launched in the United States.[118] Or, in the alternative:

Multi-State Consumer Protection Class: All persons who reside in California, Illinois, or any state with materially similar consumer protection laws[119] who used the CapCut app after it was launched in the United States.

[118] The CapCut app was launched in the United States in 2020.

[119] While discovery may alter the following, Plaintiffs assert that the other states with similar consumer fraud laws under the facts of this case include but are not limited to: Arkansas (Ark. Code § 4-88-101, et seq.); California (Cal. Bus. & Prof. C. §§ 17200 and 17500 et seq.); Colorado (Colo. Rev. Stat. § 6-1-101, et seq.); Connecticut (Conn. Gen. Stat. § 42-110, et seq.); Delaware (Del. Code tit. 6, § 2511, et seq.); District of Columbia (D.C. Code § 28-3901, et seq.); Florida

Illinois Subclass: All persons who reside in Illinois and used the CapCut app to create one or more videos after the app was launched in the United States.

159. Plaintiffs are the proposed class representatives for the Nationwide Class and the Multi-State Consumer Protection Class. Illinois Plaintiffs are the proposed class representatives for the Illinois Subclass.

160. Plaintiffs reserve the right to modify or refine the definitions of the Class and the Subclass.

161. Excluded from the Class and the Subclass are: (i) any judge or magistrate judge presiding over this action and members of their staff, as well as members of their families; (ii) Defendants, Defendants' predecessors, parents, successors, heirs, assigns, subsidiaries, and any entity in which any Defendant or its parents have a controlling interest, as well as Defendants' current or former employees, agents, officers, and directors; (iii) persons who properly execute and file a timely request for exclusion from the class; (iv) persons whose claims in this matter have been

(Fla. Stat. § 501.201, et seq.); Hawaii (Haw. Rev. Stat. § 480-1, et seq.); Idaho (Idaho Code § 48-601, et seq.); Illinois (815 ICLS § 505/1, et seq.); Maine (Me. Rev. Stat. tit. 5 § 205- A, et seq.); Massachusetts (Mass. Gen. Laws Ch. 93A, et seq.); Michigan (Mich. Comp. Laws § 445.901, et seq.); Minnesota (Minn. Stat. § 325F.67, et seq.); Missouri (Mo. Rev. Stat. § 407.010, et seq.); Montana (Mo. Code. § 30-14-101, et seq.); Nebraska (Neb. Rev. Stat. § 59 1601, et seq.); Nevada (Nev. Rev. Stat. § 598.0915, et seq,); New Hampshire (N.H. Rev. Stat. § 358-A:1, et seq.); New Jersey (N.J. Stat. § 56:8-1, et seq.); New Mexico (N.M. Stat. § 57-12-1, et seq.); New York (N.Y. Gen. Bus. Law § 349, et seq.); North Dakota (N.D. Cent. Code § 51-15- 01, et seq.); Oklahoma (Okla. Stat. tit. 15, § 751, et seq.); Oregon (Or. Rev. Stat. § 646.605, et seq.); Rhode Island (R.I. Gen. Laws § 6-13.1-1, et seq.); South Dakota (S.D. Code Laws § 37- 24-1, et seq.); Texas (Tex. Bus. & Com. Code § 17.41, et seq.); Virginia (VA Code § 59.1-196, et seq.); Vermont (Vt. Stat. tit. 9, § 2451, et seq.); Washington (Wash. Rev. Code § 19.86.010, et seq.); West Virginia (W. Va. Code § 46A-6- 101, et seq.); and Wisconsin (Wis. Stat. § 100.18, et seq.). *See Mullins v. Direct Digital, LLC*, No. 13-cv-1829, 2014 WL 5461903 (N.D. Ill. Sept. 30, 2014), aff'd, 795 F.3d 654 (7th Cir. 2015).

finally adjudicated on the merits or otherwise released; (v) counsel for Defendants; and (vi) the legal representatives, successors, and assigns of any such excluded persons.

162. **Ascertainability.** The proposed Class and Subclass are readily ascertainable because they are defined using objective criteria so as to allow Class and Subclass members to determine if they are part of the Class and/or one of the Subclass. Further, the Class and Subclass can be readily identified through records maintained by Defendants.

163. **Numerosity (Rule 23(a)(1)).** The Class and Subclass are so numerous that joinder of individual members herein is impracticable. The exact number of Class and Subclass members, as herein identified and described, is not known, but download figures indicate that the CapCut app was downloaded approximately 28 million times in the United States during the last year alone.[120]

164. **Commonality (Rule 23(a)(2)).** Common questions of fact and law exist for each cause of action and predominate over questions affecting only individual Class and Subclass members, including the following:

a) Whether Defendants engaged in the activities and practices referenced above;

b) Whether Defendants' activities and practices referenced above constitute a violation of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030;

c) Whether Defendants' activities and practices referenced above constitute a violation of the California Comprehensive Data Access and Fraud Act, Cal. Pen. C. § 502;

[120] https://www.wsj.com/articles/tiktoks-chinese-parent-has-another-wildly-popular-app-in-the-u-s-e14c41fc.

d) Whether Defendants' activities and practices referenced above constitute a violation of the Right to Privacy under the California Constitution;

e) Whether Defendants' activities and practices referenced above constitute an intrusion upon seclusion;

f) Whether Defendants' activities and practices referenced above constitute a violation of the California Unfair Competition Law, Bus. & Prof. C. §§ 17200 et seq.;

g) Whether Defendants' activities and practices referenced above constitute a violation of the California False Advertising Law, Bus. & Prof. C. §§ 17500 et seq.;

h) Whether Defendants' activities and practices referenced above constitute unjust enrichment concerning which restitution and/or disgorgement is warranted;

i) Whether Defendants' activities and practices referenced above constitute a violation of the Illinois Biometric Information Privacy Act, 740 ILCS 14/1, et seq.;

j) Whether Plaintiffs and members of the Class and Subclass sustained damages as a result of Defendants' activities and practices referenced above, and, if so, in what amount;

k) Whether Defendants profited from their activities and practices referenced above, and, if so, in what amount; and

l) What is the appropriate injunctive relief to ensure that Defendants no longer unlawfully: (i) take private and personally identifiable CapCut user data and content – including user/device identifiers, biometric identifiers and information, private videos and private video images, and video viewing histories; (ii) utilize private and personally identifiable CapCut user data and content to develop and patent commercially valuable artificial intelligence technologies; (iii) utilize private and personally identifiable CapCut user data

and content to create consumer demand for and use of Defendants' other products; (iv) give access to such private and personally identifiable CapCut user data and content to individuals in China and to third parties either in China or whose data is accessible from within China; (v) cause the diminution in value of CapCut users' private and personally identifiable data and content; (vi) cause injury and harm to CapCut users' devices; (vii) cause CapCut users to incur higher data usage and electricity charges; (viii) retain the unlawfully acquired private and personally identifiable data and content of CapCut users; and (ix) profile and target, based on the above activities, CapCut users with advertisements.

n) What is the appropriate injunctive relief to ensure that Defendants take reasonable measures to ensure that they and relevant third parties destroy unlawfully acquired private and personally identifiable CapCut user data and content in their possession, custody or control.

165. **Typicality (Rule 23(a)(3)).** Plaintiffs' claims are typical of the claims of members of the Class and Subclass because, among other things, Plaintiffs and members of the Class and Subclass sustained similar injuries as a result of Defendants' uniform wrongful conduct, and their legal claims all arise from the same events and wrongful conduct by Defendants.

166. **Adequacy (Rule 23(a)(4)).** Plaintiffs will fairly and adequately protect the interests of the Class and Subclass. Plaintiffs' interests do not conflict with the interests of the Class and Subclass members, and Plaintiffs have retained counsel experienced in complex class action and data privacy litigation to prosecute this case on behalf of the Class and Subclass.

167. **Predominance & Superiority (Rule 23(b)(3)).** In addition to satisfying the prerequisites of Rule 23(a), Plaintiffs satisfy the requirements for maintaining a class action under

Rule 23(b)(3). Common questions of law and fact predominate over any questions affecting only individual Class and Subclass members, and a class action is superior to individual litigation and all other available methods for the fair and efficient adjudication of this controversy. The amount of damages available to Plaintiffs is insufficient to make litigation addressing Defendants' conduct economically feasible in the absence of the class action procedure. Individualized litigation also presents a potential for inconsistent or contradictory judgments, and increases the delay and expense presented by the complex legal and factual issues of the case to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economy of scale, and comprehensive supervision by a single court.

168. **Final Declaratory or Injunctive Relief (Rule 23(b)(2)).** Plaintiffs also satisfy the requirements for maintaining a class action under Rule 23(b)(2). Defendants have acted or refused to act on grounds that apply generally to the Class and Subclass, making final declaratory and/or injunctive relief appropriate with respect to the Class and Subclass as a whole.

169. **Particular Issues (Rule 23(c)(4)).** Plaintiffs also satisfy the requirements for maintaining a class action under Rule 23(c)(4). Their claims consist of particular issues that are common to all Class and Subclass members and are capable of class-wide resolution that will significantly advance the litigation.

VI. APPLICABLE LAW

170. With the exception of BIPA, which applies exclusively to the claims of the Illinois Subclass, California's substantive laws apply to the statutory, constitutional and common law claims of every member of the Class, regardless of where in the United States the Class Member resides. California's substantive laws may be constitutionally applied to the claims of Plaintiffs and

the Class under the Due Process Clause, 14th Amendment §1, and the Full Faith and Credit Clause, Article IV, §1 of the U.S. Constitution. California has significant contacts, or significant aggregation of contacts, to the claims asserted by Plaintiffs and all Class Members, thereby creating state interests that ensure that the choice of California state law is not arbitrary or unfair.

171. Defendants' U.S. headquarters and principal places of business are located in California. Defendants also own property and conduct substantial business in California, and therefore California has an interest in regulating Defendants' conduct under its laws. Defendants' decision to reside in California and avail themselves of California's laws, and to engage in the challenged conduct from and emanating out of California, renders the application of California law to the claims herein constitutionally permissible.

172. California is also the state from which Defendants' alleged misconduct emanated. This conduct similarly injured and affected Plaintiffs and all other Class Members.

173. The application of California laws to the claims of the Class is also appropriate under California's choice of law rules because California has significant contacts to the claims of Plaintiffs and the proposed Class, and California has a greater interest in applying its laws here than any other interested state.

VII. CAUSES OF ACTION

FIRST CAUSE OF ACTION

VIOLATION OF THE COMPUTER FRAUD AND ABUSE ACT, 18 U.S.C. § 1030
(On Behalf of the Plaintiffs and the Class)

174. Plaintiffs repeat and incorporate by reference all preceding paragraphs as if fully set forth herein.

175. The Plaintiffs' and the Class's devices are, and at all relevant times have been, used for interstate communication and commerce, and are therefore "protected computers" under 18 U.S.C. § 1030(e)(2)(B).

176. Defendants have exceeded, and continue to exceed, authorized access to the Plaintiffs' and the Class's protected computers and obtained information thereby, in violation of 18 U.S.C. § 1030(a)(2), (a)(2)(C).

177. Defendants' conduct caused "loss to 1 or more persons during any 1-year period . . . aggregating at least $5,000 in value" under 18 U.S.C. § 1030(c)(4)(A)(i)(I), *inter alia*, because of the secret transmission of the Plaintiffs' and the Class's private and personally identifiable data and content – including user/device identifiers, biometric identifiers and information, and private videos and private video images never intended for public consumption.

178. Defendants' conduct also constitutes "a threat to public health or safety" under 18 U.S.C. § 1030(c)(4)(A)(i)(IV), due to the private and personally identifiable data and content of the Plaintiffs and the Class being made available to foreign actors, including foreign intelligence services, in locations without adequate legal privacy protections. That this threat is real and imminent is evidenced by the materials cited above.

179. Accordingly, the Plaintiffs and the Class are entitled to "maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief." 18 U.S.C. § 1030(g).

SECOND CAUSE OF ACTION

VIOLATION OF THE CALIFORNIA COMPREHENSIVE DATA ACCESS AND FRAUD ACT CAL. PEN. C. § 502
(On Behalf of the Plaintiffs and the Class)

180. Plaintiffs repeat and incorporate by reference all preceding paragraphs as if fully set forth herein.

181. Defendants' acts violate Cal. Pen. C. § 502(c)(1) because they have knowingly accessed, and continue to knowingly access, data and computers to wrongfully control or obtain data. The Plaintiffs' and the Class's private and personally identifiable data and content accessed by Defendants – including user/device identifiers, biometric identifiers and information, and private videos and private video images never intended for public consumption – far exceeds any reasonable use of the Plaintiffs' and the Class's data and content to operate the CapCut app. There is no justification for Defendants' surreptitious collection and transfer of the Plaintiffs' and the Class's private and personally identifiable data and content from their devices and their other social media accounts and allowing access to that information to individuals and third-party companies in China that are subject to Chinese law requiring the sharing of such data and content with the Chinese government.

182. Defendants' acts violate Cal. Pen. C. § 502(c)(2) because they have knowingly accessed and without permission taken, copied, and made use of data from a computer – and they continue to do so. Defendants did not obtain permission to take, copy, and make use of the Plaintiffs' and the Class's private and personally identifiable data and content – including user/device identifiers, biometric identifiers and information, and private videos and private video images never intended for public consumption – from their devices – and provide access to

individuals and companies that are subject to Chinese law requiring the sharing of such data and content with the Chinese government.

183. Accordingly, the Plaintiffs and the Class are entitled to compensatory damages, including "any expenditure reasonably and necessarily incurred by the owner or lessee to verify that a computer system, computer network, computer program, or data was or was not altered, damaged, or deleted by the access," injunctive relief, and attorneys' fees. Cal. Pen. C. § 502(e)(1), (2).

THIRD CAUSE OF ACTION

VIOLATION OF THE RIGHT OF PRIVACY UNDER THE CALIFORNIA CONSTITUTION
(On Behalf of the Plaintiffs and the Class)

184. Plaintiffs repeat and incorporate by reference all preceding paragraphs as if fully set forth herein.

185. Plaintiffs and the Class hold, and at all relevant times held, a legally protected privacy interest in their private and personally identifiable data and content – including user/device identifiers, biometric identifiers and information, and private videos and private video images never intended for public consumption – on their devices and in their other social media accounts.

186. There is a reasonable expectation of privacy concerning Plaintiffs' and the Class's data and content under the circumstances present.

187. The reasonableness of Plaintiffs' and the Class's expectation of privacy is supported by the undisclosed, hidden, and non-intuitive nature of Defendants' accessing private and personally identifiable data and content – including user/device identifiers, biometric identifiers

and information, and private videos and private video images never intended for public consumption – from Plaintiffs' and the Class's devices and other social media accounts.

188. Defendants' conduct constitutes and, at all relevant times, constituted a serious invasion of privacy, as Defendants either did not disclose at all, or failed to make an effective disclosure, that they would take and make use of – and allow individuals and companies based in China to take and make use of – Plaintiffs' and the Class's private and personally identifiable data and content. Defendants intentionally invaded Plaintiffs' and the Class's privacy interests by intentionally designing the CapCut app, including all associated code, to surreptitiously obtain, improperly gain knowledge of, review, and retain their private and personally identifiable data and content. These intrusions are highly offensive to a reasonable person, as evidenced by substantial research, literature, and governmental enforcement and investigative efforts to protect consumer privacy against surreptitious technological intrusions. The offensiveness of Defendants' intrusion is heightened by Defendants' making Plaintiffs' and the Class's private and personally identifiable data and content available to third parties, including foreign governmental entities whose interests are opposed to those of United States citizens. The intentionality of Defendants' conduct, and the steps they have taken to disguise and deny it, also demonstrate the highly offensive nature of their conduct. Further, Defendants' conduct targeted Plaintiffs' and the Class's devices, which contain Plaintiffs' and the Class's private and personally identifiable data and content.

189. Plaintiffs and the Class were harmed by, and continue to suffer harm as a result of, the intrusion as detailed throughout this Complaint.

190. Defendants' conduct was a substantial factor in causing the harm suffered by Plaintiffs and the Class.

191. Plaintiffs and the Class seek nominal and punitive damages as a result of Defendants' actions. Punitive damages are warranted because Defendants' malicious, oppressive, and willful actions were calculated to injure the Plaintiffs and the Class, and were made in conscious disregard of their rights. Punitive damages are also warranted to deter Defendants from engaging in future misconduct.

192. Plaintiffs and the Class seek injunctive relief to rectify Defendants' actions, including but not limited to requiring Defendants (a) to stop taking more private and personally identifiable data and content of Plaintiffs and the Class from their devices and their other social media accounts than is reasonably necessary to operate the CapCut app; (b) to make clear disclosures of Plaintiffs' and the Class's private and personally identifiable data and content that is reasonably necessary to operate the CapCut app; (c) to obtain Plaintiffs' and the Class's consent to the taking of their private and personally identifiable data and content; (d) to stop providing access to the Plaintiffs' private and personally identifiable data and content to individuals in China or transferring such data to servers or companies whose data is accessible from within China; and (e) to recall and destroy Plaintiffs' and the Class's private and personally identifiable data and content already taken in contravention of Plaintiffs' and the Class's right to privacy under the California Constitution.

193. The Plaintiffs and the Class seek restitution and disgorgement for Defendants' violation of their privacy rights. A person acting in conscious disregard of the rights of another is required to disgorge all profit because disgorgement both benefits the injured parties and deters the perpetrator from committing the same unlawful actions again. Disgorgement is available for conduct that constitutes "conscious interference with a claimant's legally protected interests,"

including tortious conduct or conduct that violates another duty or prohibition. Restatement (3rd) of Restitution and Unjust Enrichment, §§ 40, 44.

FOURTH CAUSE OF ACTION

INTRUSION UPON SECLUSION
(On Behalf of the Plaintiffs and the Class)

194. Plaintiffs repeat and incorporate by reference all preceding paragraphs as if fully set forth herein.

195. "One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person." Restatement (2nd) of Torts § 652B.

196. The Plaintiffs and the Class have, and at all relevant times had, a reasonable expectation of privacy in their devices and their social media accounts, and their private affairs include their past, present and future activity on their devices and their other media accounts.

197. The reasonableness of the Plaintiffs' and the Class's expectations of privacy is supported by the undisclosed, hidden, and non-intuitive nature of Defendants' taking of private and personally identifiable data and content from the Plaintiffs' and the Class's devices and social media accounts.

198. Defendants intentionally intruded upon the Plaintiffs' and the Class's solitude, seclusion, and private affairs – and continue to do so – by intentionally designing the CapCut app, including all associated code, to surreptitiously obtain, improperly gain knowledge of, review, and retain the Plaintiffs' and the Class's private and personally identifiable data and content –

including user/device identifiers, biometric identifiers and information, and private videos and private video images never intended for public consumption.

199. These intrusions are highly offensive to a reasonable person, as evidenced by substantial research, literature, and governmental enforcement and investigative efforts to protect consumer privacy against surreptitious technological intrusions. The offensiveness of Defendants' intrusion is heightened by Defendants' making the Plaintiffs' and the Class's private and personally identifiable data and content available to third parties, including foreign governmental entities whose interests are opposed to those of United States citizens. The intentionality of Defendants' conduct, and the steps they have taken to disguise and deny it, also demonstrate the highly offensive nature of their conduct. Further, Defendants' conduct targeted the Plaintiffs' and the Class's devices, which the United States Supreme Court has characterized as almost a feature of human anatomy, and which contain the Plaintiffs' and the Class's private and personally identifiable data and content.

200. The Plaintiffs and the Class were harmed by, and continue to suffer harm as a result of, the intrusion as detailed throughout this Complaint.

201. Defendants' conduct was a substantial factor in causing the harm suffered by the Plaintiffs and the Class.

202. The Plaintiffs and the Class seek nominal and punitive damages as a result of Defendants' actions. Punitive damages are warranted because Defendants' malicious, oppressive, and willful actions were calculated to injure the Plaintiffs and the Class, and were made in conscious disregard of their rights. Punitive damages are also warranted to deter Defendants from engaging in future misconduct.

203. The Plaintiffs and the Class seek injunctive relief to rectify Defendants' actions, including but not limited to requiring Defendants (a) to stop taking more private and personally identifiable data and content from the Plaintiffs' and the Class's devices and other social media accounts than is reasonably necessary to operate the CapCut app; (b) to make clear disclosures of the Plaintiffs' and the Class's private and personally identifiable data and content that is reasonably necessary to operate the CapCut app; (c) to obtain the Plaintiffs' and the Class's consent to the taking of such private and personally identifiable data and content; (d) to stop providing access to the Plaintiffs' and the Class's private and personally identifiable data and content to individuals in China or transferring such data to servers or companies whose data is accessible from within China; and (e) to recall and destroy the Plaintiffs' and the Class's private and personally identifiable data and content already taken in contravention of the Plaintiffs' and the Class's privacy rights.

204. Plaintiffs and the Class seek restitution and disgorgement for Defendants' intrusion upon seclusion. A person acting in conscious disregard of the rights of another is required to disgorge all profit because disgorgement both benefits the injured parties and deters the perpetrator from committing the same unlawful actions again. Disgorgement is available for conduct that constitutes "conscious interference with a claimant's legally protected interests," including tortious conduct or conduct that violates another duty or prohibition. Restatement (3rd) of Restitution and Unjust Enrichment, §§ 40, 44.

FIFTH CAUSE OF ACTION

VIOLATION OF THE CALIFORNIA UNFAIR COMPETITION LAW, BUS. & PROF. C. §§ 17200 *et seq.* (On Behalf of the Plaintiffs and the Class)

205. Plaintiffs repeat and incorporate by reference all preceding paragraphs as if fully set forth herein.

206. The Unfair Competition Law, California Business & Professions Code §§ 17200, et seq. (the "UCL"), prohibits any "unlawful," "unfair," or "fraudulent" business act or practice, which can include false or misleading advertising.

207. Defendants violated, and continue to violate, the "unlawful" prong of the UCL through violation of statutes, constitutional provisions, and common law, as alleged herein.

208. Defendants violated, and continue to violate, the "unfair" prong of the UCL because they accessed private and personally identifiable data and content – including user/device identifiers, biometric identifiers and information, and private videos and private video images never intended for public consumption – from the Plaintiffs' and the Class's devices and other social media accounts under circumstances in which the Plaintiffs and the Class would have no reason to know that such data and content was being taken.

209. Plaintiffs and the Class had no reason to know because (i) there was no disclosure of Defendants' collection and transfer of the Plaintiffs' and the Class's biometric identifiers and information, and private videos and private video images not intended for public consumption; (ii) there was no disclosure that Defendants had embedded source code within the CapCut app that makes Plaintiffs' and the Class's private and personally identifiable data and content accessible to third-party companies and individuals based in China where such companies and individuals are subject to Chinese law requiring the sharing of such data and content with the Chinese

government; and (iii) there was no effective disclosure of the wide range of private and personally identifiable data and content that Defendants took from the Plaintiffs' and the Class's devices. Defendants violated, and continue to violate, the "fraudulent" prong of the UCL because (i) Defendants made it appear that the Plaintiffs' private and personally identifiable data and content would not be collected and transferred unless the Plaintiffs and the Class chose to do so, but in fact Defendants collected and transferred such data and content without notice or consent; (ii) Defendants made it appear that the Plaintiffs' and the Class's private and personally identifiable data and content would not be provided to individuals or companies that are subject to Chinese law requiring the sharing of such data and content with the Chinese government; and (iii) Defendants have intentionally refrained from disclosing the uses to which the Plaintiffs' and the Class's private and personally identifiable data and content has been put, while simultaneously providing misleading reassurances about Defendants' data collection and use practices. The Plaintiffs and the Class were misled by Defendants' concealment, and had no reason to believe that Defendants had taken the private and personally identifiable data and content that they had taken or used it in the manner they did.

210. In addition, Defendants fail to adequately disclose that users' data will be accessible to individuals in China, and ultimately accessible by the Chinese communist government. To the contrary, Defendants assured Plaintiffs and the Class of the privacy of their data, while under Chinese law the Chinese government has an absolute right to access users' data.

211. Defendants' conduct is particularly egregious because these violations extend to underage users whom Defendants acknowledge should not be using the platform. Indeed, through their promotion on TikTok and other avenues, Defendants have encouraged underage use.

Moreover, they have failed to incorporate appropriate age verification and other measures in the CapCut app necessary to prevent underage use and have incorporated features in the design of the CapCut app that actually facilitate underage use.

212. Plaintiffs and the Class have been harmed and have suffered economic injury as a result of Defendants' UCL violations. First, Plaintiffs and the Class have suffered harm in the form of diminution of the value of their private and personally identifiable data and content. Second, they have suffered harm to their devices. The battery, memory, CPU and bandwidth of such devices have been compromised, and as a result the functioning of such devices has been impaired and slowed. Third, they have incurred additional data usage and electricity costs that they would not otherwise have incurred. Fourth, they have suffered harm as a result of the invasion of privacy stemming from Defendants' covert theft of their private and personally identifiable data and content – including user/device identifiers, biometric identifiers and information, and private videos and private video images.

213. Defendants, as a result of their conduct, have been able to reap unjust profits and revenues in violation of the UCL. This includes Defendants' profits and revenues from their targeted advertising, improvements to their artificial intelligence technologies, their patent applications, fees Defendants charged Plaintiffs for additional services and storage, and the increased consumer demand for and use of Defendants' other products. Plaintiffs and the Class seek restitution and disgorgement of these unjust profits and revenues.

214. Unless restrained and enjoined, Defendants will continue to misrepresent their private and personally identifiable data and content collection and use practices, and will not recall

and destroy Plaintiffs' and the Class's wrongfully collected private and personally identifiable data and content. Accordingly, injunctive relief is appropriate.

SIXTH CAUSE OF ACTION

VIOLATION OF THE CALIFORNIA FALSE ADVERTISING LAW, BUS. & PROF. C. §§ 17500 *et seq.* (On Behalf of the Plaintiffs and the Class)

215. Plaintiffs repeat and incorporate by reference all preceding paragraphs as if fully set forth herein.

216. California's False Advertising Law (the "FAL") – Cal. Bus. & Prof. Code §§ 17500, et seq. – prohibits "any statement" that is "untrue or misleading" and made "with the intent directly or indirectly to dispose of" property or services.

217. Defendants' advertising is, and at all relevant times was, highly misleading. Defendants do not disclose at all, or do not meaningfully disclose, the private and personally identifiable data and content – including user/device identifiers, biometric identifiers and information, and private videos and private video images never intended for public consumption – that they have collected and transferred from the Plaintiffs' and the Class's devices and other social media accounts. Nor do Defendants disclose that the Plaintiffs' and the Class's private and personally identifiable data and content has been made available to foreign government entities.

218. Reasonable consumers, like the Plaintiffs and the Class, are – and at all relevant times were – likely to be misled by Defendants' misrepresentations. Reasonable consumers lack the means to verify Defendants' representations concerning their data and content collection and use practices, or to understand the fact or significance of Defendants' data and content collection and use practices.

219. Plaintiffs and the Class have been harmed and have suffered economic injury as a result of Defendants' misrepresentations. First, they have suffered harm in the form of diminution of the value of their private and personally identifiable data and content. Second, they have suffered harm to their devices. The battery, memory, CPU and bandwidth of such devices have been compromised, and as a result the functioning of such devices has been impaired and slowed. Third, they have incurred additional data usage and electricity costs that they would not otherwise have incurred. Fourth, they have suffered harm as a result of the invasion of privacy stemming from Defendants' accessing their private and personally identifiable data and content – including user/device identifiers, biometric identifiers and information, and private videos and private video images never intended for public consumption.

220. Defendants, as a result of their misrepresentations, have been able to reap unjust profits and revenues. This includes Defendants' profits and revenues from their targeted advertising, improvements to their artificial intelligence technologies, their patent applications, their fees and service charges, and the increased consumer demand for and use of Defendants' other products and services. Plaintiffs and the Class seek restitution and disgorgement of these unjust profits and revenues.

221. Unless restrained and enjoined, Defendants will continue to misrepresent their private and personally identifiable data and content collection and use practices, and will not recall and destroy Plaintiffs' and the Class's wrongfully collected private and personally identifiable data and content. Accordingly, injunctive relief is appropriate.

SEVENTH CAUSE OF ACTION

RESTITUTION / UNJUST ENRICHMENT
(On Behalf of the Plaintiffs and the Class)

222. Plaintiffs repeat and incorporate by reference all preceding paragraphs as if fully set forth herein.

223. Plaintiffs and the Class have conferred substantial benefits on Defendants by downloading and using the CapCut app. These include the Defendants' accessing the Plaintiffs' and the Class's private and personally identifiable data and content – including user/device identifiers, biometric identifiers and information, and private videos and private video images never intended for public consumption. Such benefits also include the revenues and profits resulting from Defendants' collection and use of such data and content for Defendants' targeted-advertising, improvements to their artificial intelligence technologies, their patent applications, fees Defendants charged Plaintiffs for additional services and storage, and the increased consumer demand for and use of Defendants' other products.

224. Defendants have knowingly and willingly accepted and enjoyed these benefits.

225. Defendants either knew or should have known that the benefits rendered by the Plaintiffs and the Class were given with the expectation that Defendants would not take and use the Plaintiffs' and the Class's private and personally identifiable data and content that Defendants have taken and used without permission. For Defendants to retain the aforementioned benefits under these circumstances is inequitable.

226. Through deliberate violation of the Plaintiffs' and the Class's privacy interests, and statutory and constitutional rights, Defendants each reaped benefits that resulted in each Defendant wrongfully receiving profits.

227. Equity requires disgorgement of Defendants' ill-gotten gains. Defendants will be unjustly enriched unless they are ordered to disgorge those profits for the benefit of the Plaintiffs and the Class.

228. As a direct and proximate result of Defendants' wrongful conduct and unjust enrichment, the Plaintiffs and the Class are entitled to restitution from Defendants and institution of a constructive trust disgorging all profits, benefits, and other compensation obtained by Defendants through this inequitable conduct.

EIGHTH CAUSE OF ACTION

VIOLATION OF ILLINOIS'S BIOMETRIC INFORMATION PRIVACY ACT, 740 ILCS 14/1, *et seq.* (On Behalf of the Plaintiffs and the Class)

229. Plaintiffs repeat and incorporate by reference all preceding paragraphs as if fully set forth herein.

230. BIPA makes it unlawful for any private entity to, among other things, "collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifiers or biometric information, unless it first: (1) informs the subject . . . in writing that a biometric identifier or biometric information is being collected or stored; (2) informs the subject . . . in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used; and (3) receives a written release executed by the subject of the biometric identifier or biometric information or the subject's legally authorized representative." 740 ILCS 14/15(b).

231. At all relevant times, the Illinois Plaintiffs were residents of Illinois and each is a "person" and/or a "customer" within the meaning of BIPA. 740 ILCS 14/15(b). The minor Illinois

Plaintiffs' legal guardians are their "legally authorized representative[s]" within the meaning of BIPA, and served in such capacity at all times relevant to this action. *Id.*

232. Each Defendant is, and at all relevant times was, a "corporation, limited liability company, association, or other group, however organized," and thus is, and at all relevant times was, a "private entity" under the BIPA. 740 ILCS 14/10.

233. The Illinois Plaintiffs and the Illinois Subclass had their "biometric identifiers," including their face geometry scans, as well as their "biometric information" collected, captured, received, or otherwise obtained by Defendants as a result of the Illinois Plaintiffs' and the Illinois Subclass's use of the CapCut app. 740 ILCS 14/10.

234. At all relevant times, Defendants systematically and surreptitiously collected, captured, received or otherwise obtained the Illinois Plaintiffs' and the Illinois Subclass's "biometric identifiers" and "biometric information" without first obtaining signed written releases, as required by 740 ILCS 14/15(b)(3), from any of them or their "legally authorized representatives."

235. In fact, Defendants failed to properly inform the Illinois Plaintiffs and the Illinois Subclass, or any of their parents, legal guardians, or other "legally authorized representatives," in writing (or in any other way) that the Illinois Plaintiffs' and the Illinois Subclass's "biometric identifiers" and "biometric information" were being "collected or stored" by Defendants. Nor did Defendants inform the Illinois Plaintiffs and the Illinois Subclass, or any of their parents, legal guardians, or other "legally authorized representatives," in writing of the specific purpose and length of term for which the Illinois Plaintiffs' and the Illinois Subclass's "biometric identifiers" and "biometric information" were being "collected, stored and used" as required by 740 ILCS 14/15(b)(1)-(2).

236. BIPA also makes it unlawful for a private entity "in possession of a biometric identifier or biometric information" to "sell, lease, trade, or otherwise profit from a person's or a customer's biometric identifier or biometric information." 740 ILCS 14/15(c).

237. Defendants are, and at all relevant times were, "in possession of" the Illinois Plaintiffs' and the Illinois Subclass's "biometric identifiers," including but not limited to their face geometry scans, and "biometric information." Defendants profited from such "biometric identifiers" and "biometric information" by using them for targeted advertising, improvements to Defendants' artificial intelligence technologies, Defendants' patent applications, and the generation of increased demand for and use of Defendants' other products. 740 ILCS 14/15(c).

238. Finally, BIPA prohibits private entities "in possession of a biometric identifier or biometric information" from "disclos[ing], redisclos[ing], or otherwise disseminat[ing] a person's or a customer's biometric identifier or biometric information unless" any one of four enumerated conditions are met. 740 ILCS 14/15(d)(1)-(4). None of such conditions are met here.

239. Defendants disclose, redisclose and disseminate, and at all relevant times disclosed, redisclosed and disseminated, the Illinois Plaintiffs' and the Illinois Subclass's "biometric identifiers," including but not limited to their face geometry scans, and "biometric information" without the consent of any of them or their "legally authorized representatives." 740 ILCS 14/15(d)(1). Moreover, the disclosures and redisclosures did not "complete[] a financial transaction requested or authorized by" the Illinois Plaintiffs, the Illinois Subclass or any of their legally authorized representatives. 740 ILCS 14/15(d)(2). Nor are, or at any relevant times were, the disclosures and redisclosures "required by State or federal law or municipal ordinance." 740 ILCS

14/15(d)(3). Finally, at no point in time were the disclosures ever "required pursuant to a valid warrant or subpoena issued by a court of competent jurisdiction." 740 ILCS 14/15(d)(4).

240. BIPA mandates that a private entity "in possession of biometric identifiers or biometric information" "develop a written policy, made available to the public, establishing a retention schedule and guidelines for permanently destroying biometric identifiers and biometric information when the initial purpose for collecting or obtaining such identifiers or information has been satisfied or within 3 years of the individual's last interaction with the private entity, whichever occurs first." 740 ILCS 14/15(a). But Defendants do not publicly provide any written policy establishing any retention schedule or guidelines for permanently destroying the Illinois Plaintiffs' and the Illinois Subclass's "biometric identifiers" and "biometric information." 740 ILCS 14/15(a).

241. BIPA also commands private entities "in possession of a biometric identifier or biometric information" to: (1) store, transmit, and protect from disclosure all biometric identifiers and biometric information using the reasonable standard of care within the private entity's industry; and (2) store, transmit, and protect from disclosure all biometric identifiers and biometric information in a manner that is the same as or more protective than the manner in which the private entity stores, transmits and protects other confidential and sensitive information. 740 ILCS 14/15(e). Based on the facts alleged herein, including Defendants' lack of an adequate public written policy, their failure to inform CapCut users that Defendants obtain such users' "biometric identifiers" and "biometric information," their failure to obtain written consent to collect or otherwise obtain CapCut users' "biometric identifiers" and "biometric information,"

and their unauthorized dissemination of CapCut users' "biometric identifiers" and "biometric information," Defendants have violated this provision too.

242. Defendants recklessly or intentionally violated each of BIPA's requirements and infringed the Illinois Plaintiffs' and the Illinois Subclass's rights to keep their immutable and uniquely identifying biometric identifiers and biometric information private. As individuals subjected to each of Defendants' BIPA violations above, the Illinois Plaintiffs and the Illinois Subclass are and have been aggrieved. 740 ILCS 14/20.

243. On behalf of themselves and the Illinois Subclass, the Illinois Plaintiffs seek: (1) injunctive and equitable relief as is necessary to protect the interests of the Illinois Plaintiffs and the Illinois Subclass by requiring Defendants to comply with BIPA's requirements; (2) $1,000.00 or actual damages, whichever is greater, for each negligent violation of BIPA by Defendants; (3) $5,000.00 or actual damages, whichever is greater, for each intentional or reckless violation of BIPA by Defendants; and (4) reasonable attorneys' fees and costs, including expert witness fees and other litigation expenses. 740 ILCS 14/20(1)-(4).

NINTH CAUSE OF ACTION

VIOLATION OF STATE CONSUMER PROTECTION STATUTES
(On Behalf of the Plaintiffs and the Multi-State Consumer Protection Class)

244. Plaintiffs repeat and incorporate by reference all preceding paragraphs as if fully set forth herein.

245. In the alternative to a nationwide class, Plaintiffs bring this action individually and on behalf of the Multi-State Consumer Protection Class.

246. Plaintiffs and Class members have been injured as a result of Defendants' violations of the state consumer protection statutes listed above in defining the Multi-State Consumer

Protection Class, which also provide a basis for redress to Plaintiffs and Class members based on Defendants' fraudulent, deceptive, unfair and unconscionable acts, practices and conduct.

247. Defendants' conduct as alleged herein violates the consumer protection, unfair trade practices and deceptive acts statutes of each of the jurisdictions encompassing the Multi-State Consumer Protection Class.

248. Defendants committed unfair and deceptive acts by surreptitiously accessing, collecting, storing, and/or disclosing Plaintiffs' and the Class's private information and data.

249. Defendants violated the Multi-State Consumer Protection Class states' unfair and deceptive acts and practices laws by engaging in these unfair or deceptive acts or practices.

250. Plaintiffs and the Class were injured and have suffered damages as a direct and proximate result of Defendants' unfair acts and practices.

251. Plaintiffs and the other Multi-State Consumer Protection Class Members' injuries were proximately caused by Defendant's unfair and deceptive business practices.

252. As a result of Defendants' violations, Defendants have been unjustly enriched.

253. Pursuant to the aforementioned states' unfair and deceptive practices laws, Plaintiffs and Class members are entitled to recover compensatory damages, restitution, punitive and special damages including but not limited to treble damages, reasonable attorneys' fees and costs and other injunctive or declaratory relief as deemed appropriate or permitted pursuant to the relevant law.

REQUEST FOR RELIEF

WHEREFORE, Plaintiffs respectfully request relief against Defendants as set forth below:

A. Entry of an order certifying the proposed class and subclass pursuant to Federal Rule of Civil Procedure 23;

B. Entry of an order appointing Plaintiffs as representatives of the class and subclass;

C. Entry of an order appointing Plaintiffs' counsel as co-lead counsel for the class and subclass;

D. Entry of an order for injunctive and declaratory relief as described herein, including but not limited to:

i. enjoining Defendants, their affiliates, associates, officers, employees and agents from transmitting CapCut user data and content to China or to other locations or facilities where such CapCut user data and content is accessible from within China;

ii. enjoining Defendants, their affiliates, associates, officers, employees and agents from taking CapCut users' private draft videos (including any frames, digital images or other content from such videos) and biometric identifiers and information without advance notice to, and the prior written consent of, such CapCut users or their legally authorized representatives (and, for the Illinois Subclass, without being in compliance with BIPA);

iii. enjoining Defendants, their affiliates, associates, officers, employees and agents from taking physical/digital location tracking data, device ID data, personally identifiable data and any other CapCut user data and content except that for which appropriate notice and consent is provided and which Defendants can show to be reasonably necessary for the lawful operation of the CapCut app within the United States;

iv. mandating that Defendants, their affiliates, associates, officers, employees and agents recall and destroy the CapCut user data and content already taken in violation of law;

v. mandating that Defendants, their affiliates, associates, officers, employees and agents remove from the CapCut app all software development kits based in China or whose data is otherwise accessible from within China;

vi. mandating that Defendants, their affiliates, associates, officers, employees and agents implement protocols to ensure that no CapCut user data and content is transmitted to, or otherwise accessible from within, China;

vii. mandating that Defendants, their affiliates, associates, officers, employees and agents hire third-party monitors for a period of at least three years to ensure that all of the above steps have been taken; and

viii. mandating that Defendants, their affiliates, associates, officers, employees and agents provide written verifications on a quarterly basis to the court and counsel for the Plaintiffs in the form of a declaration under oath that the above steps have been satisfied.

E. Entry of judgment in favor of each class and subclass member for damages suffered as a result of the conduct alleged herein, including compensatory, statutory, and punitive damages, restitution, and disgorgement, to include interest and prejudgment interest;

F. Award Plaintiffs reasonable attorneys' fees and costs; and

G. Grant such other and further legal and equitable relief as the court deems just and equitable.

DEMAND FOR JURY TRIAL

Plaintiffs hereby demand a jury trial for all claims so triable.

Dated this 28th day of July, 2023

Respectfully submitted,

HAGENS BERMAN SOBOL SHAPIRO LLP

By */s/ Steve W. Berman*
Steve W. Berman

1301 Second Avenue, Suite 2000
Seattle, WA 98101
Telephone: (206) 623-7292
Facsimile: (206) 623-0594
steve@hbsslaw.com

Jeannie Evans
HAGENS BERMAN SOBOL SHAPIRO LLP
455 N. Cityfront Plaza Dr., Suite 2410
Chicago, IL 60611
Telephone: (708) 628-4962
Facsimile: (708) 628-4952
jeannie@hbsslaw.com

Douglas G. Smith
AURELIUS LAW GROUP LLC
77 West Wacker Drive, Suite 4500
Chicago, IL 60601
Telephone: (312) 451-6708
dsmith@aureliuslawgroup.com

Attorneys for Plaintiffs and the Class