HEATHER SMITH
CIRCUIT CLERK
2024 JUN 25 AM 10:01
CLEBURNE COUNTY
HEBER SPRINGS, ARKANSAS

IN THE CIRCUIT COURT OF CLEBURNE COUNTY, ARKANSAS
CIVIL DIVISION

STATE OF ARKANSAS, *ex rel.*
TIM GRIFFIN, ATTORNEY GENERAL **PLAINTIFF**

v. **CASE NO. 12CV-24-149**

PDD HOLDINGS INC. F/K/A
PINDUODUO INC.; AND WHALECO INC.
D/B/A TEMU **DEFENDANTS**

COMPLAINT

I. INTRODUCTION

1. Defendants are the creators, marketers, and operators of Temu. Temu purports to be an online shopping platform, but it is dangerous malware, surreptitiously granting itself access to virtually all data on a user's cell phone.

2. Specifically, Temu is purposefully designed to gain unrestricted access to a user's phone operating system, including, but not limited to, a user's camera, specific location, contacts, text messages, documents, and other applications. Temu is designed to make this expansive access undetected, even by sophisticated users. Once installed, Temu can recompile itself and change properties, including overriding the data privacy settings users believe they have in place. Even users without the Temu app are subject to Temu's gross overreach if any of their information is on the phone of a Temu user. Temu monetizes this unauthorized collection of data by selling it to third parties, profiting at the direct expense of Arkansans' privacy rights.

3. The State of Arkansas, *ex rel.* Tim Griffin, Attorney General (the "State") brings this consumer protection action against PDD Holdings Inc. and WhaleCo Inc. ("Defendants") to redress and restrain violations of the Arkansas Deceptive Trade Practices Act ("ADTPA"), Ark. Code Ann. § 4-88-101, *et seq.* and the Arkansas Personal Information Protection Act ("PIPA"), Ark. Code Ann. § 4-110-101, *et seq.* The State seeks an order enjoining Defendants' conduct challenged herein, imposing civil penalties, and providing all other monetary and equitable relief to which the State is entitled.

4. In 2022, Defendants launched Temu, an online shopping platform, in the United States. The Temu mobile application and website (the "Temu platform," "Temu app," or "temu.com"), allow users to purchase low-cost goods manufactured in China.

5. Pinduoduo (the "Pinduoduo platform" or "Pinduoduo app") is an online shopping platform that was the precursor for the Temu platform. Nasdaq-listed Chinese company PDD Holdings Inc., which runs the Chinese e-commerce giant Pinduoduo Inc., owns Temu.

6. The Temu app is wildly popular throughout the United States, with usage driven both via word of mouth and by an aggressive multibillion dollar marketing campaign. This campaign recently made headlines for multiple advertisements that Temu aired during the 2024 Super Bowl, as well as additional advertisements that aired immediately following the game.[1] The advertisements "featured animated characters using the app to transform their lives to the tune of

[1] Erin Snodgrass, *Temu dropped tens of millions of dollars on its flurry of Super Bowl ads—and its big spending may pay off*, BUSINESS INSIDER (Feb. 12, 2024), https://www.businessinsider.com/temu-spends-millions-super-bowl-ads-effort-win-us-users-2024-2 (last accessed June 18, 2024).

a catchy jingle. The marketing campaign urged viewers...to 'shop like a billionaire' as the ad's avatars filled their homes with $10 toasters and $6 skateboards."[2]

7. In 2023, Temu was the most downloaded app in the United States,[3] with users spending almost twice the amount of time on its platform than on rival Amazon.[4]

8. But Temu is more than an e-commerce juggernaut. Within the last year, security experts and users have raised a host of security and privacy concerns about the Temu and the Pinduoduo apps.

9. In mid-2023, Apple suspended the Temu app from the Apple App Store for misrepresentations Temu made regarding the types of data Temu can access or collect from users, including how it collects and uses the data.[5] Google suspended the Pinduoduo app from its Google Play app store in March 2023 because it contained malware.[6]

10. Consequently, experts and technologists engaged in further, more granular investigations. Security researchers concluded that the Temu app "is purposefully and intentionally

---

[2] *Id.*

[3] Sarah Perez, *Temu was the most-downloaded iPhone app in the US in 2023*, TECHCRUNCH (Dec. 12, 2023), https://techcrunch.com/2023/12/12/temu-was-the-most-downloaded-iphone-app-in-the-u-s-in-2023/ (last accessed June 18, 2024).

[4] Jinshan Hong, *Shoppers Spend Almost Twice as Long on Temu App Than Key Rivals*, BLOOMBERG (Dec. 11, 2023), https://www.bloomberg.com/news/articles/2023-12-12/shoppers-spend-almost-twice-as-long-on-temu-app-than-rivals-like-amazon?sref=gni836kR (last accessed June 18, 2024).

[5] Clothilde Goujard, *Booming Chinese shopping app faces Western scrutiny over data security*, POLITICO (July 24, 2023), https://www.politico.eu/article/booming-chinese-shopping-app-temu-faces-western-scrutiny-over-data-security-2/ (last accessed June 18, 2024).

[6] Helen Davidson, *Addictive, absurdly cheap and controversial: the rise of China's Temu app*, THE GUARDIAN (Oct. 5, 2023), https://www.theguardian.com/world/2023/oct/06/addictive-absurdly-cheap-and-controversial-the-rise-of-chinas-temu-app (last accessed June 18, 2024).

loaded with tools to execute virulent and dangerous malware and spyware activities on user devices that have downloaded and installed the TEMU app."[7]

11. According to these experts, Temu collects a shocking amount of sensitive user data ("Personally Identifiable Information," or "PII") beyond what is necessary for an online shopping app. Some examples include users' granular location using the Global Positioning System ("GPS") and even biometric information such as users' fingerprints.

12. Temu has "a complete arsenal of tools to exfiltrate virtually all the private data on a user's device and perform nearly any malign action upon command trigger from a remote server,"[8] gaining access—without permission or even notice—to "literally everything on [a user's device]."[9]

13. The Temu app's code is purposely designed to evade front-end security review and to change its own code once it has been downloaded to a user's phone. This allows the Temu app to exploit the user's PII and other data or to otherwise control the user's device, in unknown and unknowable ways.[10] As experts note, "[i]t is evident that great efforts were taken to intentionally hide the malicious intent and intrusiveness of the software."[11]

---

[7] *We believe PDD is a Dying Fraudulent Company and its Shopping App TEMU is Cleverly Hidden Spyware that Poses an Urgent Security Threat to U.S. National Interests*, GRIZZLY RESEARCH (Sept. 6, 2023), https://grizzlyreports.com/we-believe-pdd-is-a-dying-fraudulent-company-and-its-shopping-app-temu-is-cleverly-hidden-spyware-that-poses-an-urgent-security-threat-to-u-s-national-interests/ (last accessed June 18, 2024).

[8] *Id.*

[9] Kim Komando, *Get Temu, the popular shopping app, off your phone now*, KOMANDO.COM (Apr. 15, 2023), https://www.komando.com/kims-column/temu-security-concerns/883861/ (last accessed June 18, 2024).

[10] Grizzly Research, *supra* note 7.

[11] *Id.*

14. The ability to bypass phone security systems is dangerous because it potentially allows Temu to read a user's private messages, change the phone's settings, and track notifications.[12]

15. Following multiple reports showing the results of forensic review, some researchers labeled the Temu app as "the most dangerous malware/spyware package currently in widespread circulation."[13]

16. These privacy and security harms are compounded by the fact that Temu is owned by PDD Holdings Inc., a Chinese company that is subject to Chinese law, including laws that mandate secret cooperation with China's intelligence apparatus regardless of any data protection guarantees existing in the United States.

17. The sensitive PII that Temu collects from Arkansas residents is accessible by individuals and entities subject to Chinese law and beholden to China's regime, including but not limited to, laws requiring cooperation with China's national intelligence institutions and cybersecurity regulators. Chinese government officials have interpreted Chinese law as applying to any data in which China has a national intelligence or security interest, no matter where the data is located.

18. Such concerns regarding data security and privacy endemic to Temu and other Chinese-owned apps have led government entities to ban or restrict their use. For example, the State of Montana recently banned the Temu app, along with other popular apps that are "tied to

---

[12] Marvie Basilan, *After TikTok, Montana Bans WeChat, Temu And Telegram From Government Devices*, INTERNATIONAL BUSINESS TIMES (May 18, 2023), https://www.ibtimes.com/after-tiktok-montana-bans-wechat-temu-telegram-government- devices-3694060 (last accessed June 18, 2024).

[13] Grizzly Research, *supra* note 7.

foreign adversaries" such as TikTok, WeChat, and Telegram, from government devices due to the significant threats posed to users' security and privacy.[14] Likewise, Congress is currently investigating Defendants based on "concerns about Temu and the amount of data collected."[15]

19. Temu also sells thousands of items for children, including clothing, shoes, toys, games, and consumer electronics such as kids' tablets pre-loaded with educational apps.

20. The Consumer Protection Division of the Office of the Arkansas Attorney General is charged with, among other things, enforcing the ADTPA and the PIPA, and it represents and protects the state and the public as consumers. Ark. Code Ann. § 4-88-105(c).

21. The ADTPA prohibits deceptive and unconscionable business practices, and the PIPA requires that businesses protect data concerning Arkansas residents with reasonable security practices.

22. Accordingly, the State brings this action pursuant to the ADTPA and the PIPA and seeks preliminary and permanent injunctions preventing Defendants from acquiring, maintaining, and otherwise utilizing the PII of Arkansas residents, civil penalties, and all other available monetary and equitable relief allowed by law.

II. PARTIES

23. Plaintiff is the State of Arkansas, *ex rel.* Tim Griffin, Attorney General, who is authorized to enforce the ADTPA and the PIPA in this action pursuant to Ark. Code Ann. §§ 4-88-104, 4-88-113, and 4-110-108.

---

[14] Basilan, *supra* note 12.

[15] Letter from Cathy McMorris Rodgers and Gus M. Bilirakis, United States Congress Committee on Energy and Commerce, to Mr. Qin Sun, President of WhaleCo, Inc, d/b/a Temu and Pinduoduo, (Dec. 20, 2023), https://d1dth6e84htgma.cloudfront.net/CCP_Marketplace_Letter_to_WhaleCo_Inc_Temu_7f921e1a67.pdf (last accessed June 18, 2024).

24. Defendant PDD Holdings Inc. ("PDD Holdings") is a company that was founded in China in 2015 under the name Pinduoduo Inc. and is based in Dublin, Ireland. It owns and operates a portfolio of businesses and is listed on the Nasdaq stock exchange in the United States under the ticker symbol "PDD." Among other things, PDD Holdings owns and operates the Pinduoduo e-commerce platform that offers various consumer products. PDD Holdings also owns the company that operates the Temu online marketplace (WhaleCo, Inc., discussed *infra*). PDD Holdings was formerly known as Pinduoduo Inc., with headquarters in Shanghai, China. In February 2023, PDD Holdings moved its "principal executive offices" from Shanghai, China to Dublin, Ireland.[16] However, it continues to have significant operations in China, with multiple subsidiaries located within that country.

25. Defendant WhaleCo Inc. ("Temu") is, and at all relevant times was, a corporation incorporated in Delaware and headquartered in Boston, Massachusetts. Temu is an online marketplace that is ultimately operated by Defendant PDD Holdings.

26. Defendants do not function as separate and independent corporate entities. Defendant Temu is directly controlled by Defendant PDD Holdings.

27. At all relevant times, Defendant PDD Holdings directed the operations of Defendant Temu with respect to the Temu platform and app, and Defendant Temu has reported to Defendant PDD Holdings.

28. Moreover, employees from PDD Holdings worked on the Temu platform and app, including software engineers who previously developed the Pinduoduo app for PDD Holdings.

---

[16]Arjun Kharpal, *Tech giant PDD Holdings, parent of Pinduoduo and Temu, moves headquarters from China to Ireland*, CNBC (May 4, 2023), https://www.cnbc.com/2023/05/04/chinas-pdd-holdings-parent-of-temu-moves-headquarters-to-ireland.html (last accessed June 18, 2024).

29. Defendant PDD Holdings has made, and continues to make, key strategy decisions for Defendant Temu.

30. At all relevant times, and in connection with the matters alleged herein, each Defendant acted as an agent, servant, partner, joint venturer, or alter ego of the other Defendant, and each has acted in the course and proper scope of such agency, partnership, and relationship in furtherance of such joint venture. Each Defendant is liable under the ADTPA because it acted with the knowledge and consent of the other Defendants and directed, authorized, affirmed, consented to, ratified, encouraged, approved, adopted, and participated in the acts or transactions of the other Defendants. Ark. Code Ann. § 4-88-113(d)(1).

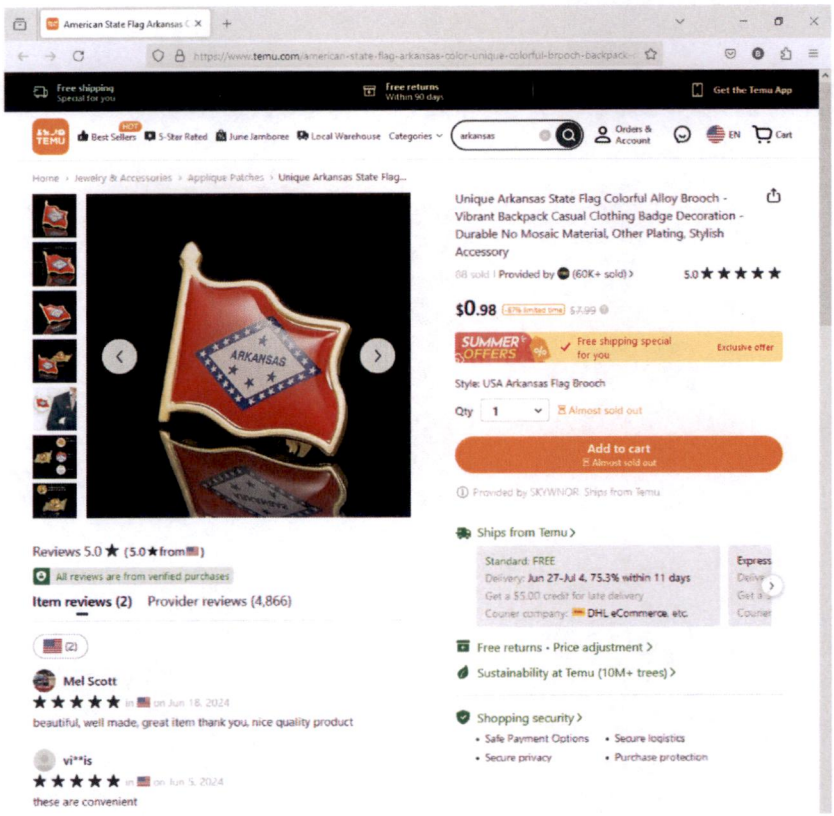
31. At all relevant times, and in connection with the matters alleged herein, Defendants constituted a single enterprise with a unity of interest. Notwithstanding this fact, and as detailed further below, each Defendant is also directly liable based on its own actions independent of any alter ego or single enterprise theory of liability.

III. JURISDICTION

32. This Court has jurisdiction over this action pursuant to Ark. Code Ann. §§ 4-88-104 and 16-4-101, as well as pursuant to the common law of the State of Arkansas.

33. Defendants have purposefully availed themselves of the privilege of doing business in the State of Arkansas. Defendants operate an e-commerce platform (the Temu app) that has been intentionally directed toward, marketed to, and downloaded by residents of the State of Arkansas. Defendants have engaged in myriad commercial transactions with Arkansas residents, taking payment from those residents in Arkansas-based commercial transactions and sending various products to Arkansas residents.

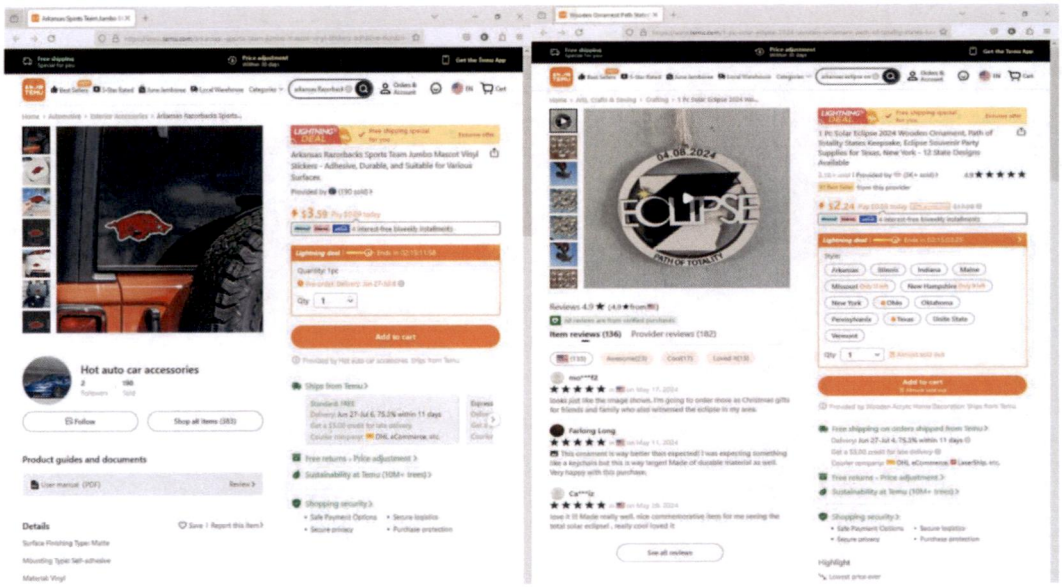
34. Moreover, the Temu app and platform offers dozens of products for sale specifically directed at Arkansas and Arkansans, including, but not limited to, Arkansas state flag lapel pins, [17] University of Arkansas Razorbacks vinyl car stickers, [18] and even keepsakes commemorating the total solar eclipse, [19] which passed directly through the State of Arkansas on April 8, 2024.



[17] TEMU, *American State Flag Arkansas Color Unique Colorful Brooch*, TEMU, https://www.temu.com/american-state-flag-arkansas-color-unique-colorful-brooch-backpack-casual-clothing-badge-decoration-g-601099576454064.html (last accessed June 20, 2024).

[18] TEMU, *Arkansas Sports Team Jumbo Mascot Vinyl Stickers*, TEMU, https://www.temu.com/arkansas--sports-team-jumbo-mascot-vinyl-stickers-adhesive-durable-and-suitable-for-various-surfaces-g-601099593839578.html (last accessed June 20, 2024).

[19] TEMU, *Wooden Ornament Path States*, TEMU, https://www.temu.com/1-pc-solar-eclipse-2024-wooden-ornament-path-of-totality-states-keepsake-eclipse-souvenir-party-supplies-for-texas-new-york-12-state-designs-available-g-601099563636324.html (last accessed June 20, 2024).



35. These causes of action arise from or relate to Defendants' contacts with the State of Arkansas. Defendants are violating Arkansas residents' privacy rights by collecting more personal information from them than necessary during these Arkansas-based commercial transactions. Moreover, Defendants engage in deceptive and unconscionable trade practices to induce Arkansas residents to transact with Defendants.

36. This Court's exercise of personal jurisdiction is also reasonable. Defendants transact with countless Arkansas residents daily and ship an enormous number of products to the State of Arkansas. Defendants also substantially profit from the personal data that they improperly collect from Arkansas residents and product sales in the State of Arkansas.

37. Temu collects Arkansas sales tax from Arkansas residents who purchase items using the Temu app.

38. Venue is proper pursuant to Ark. Code Ann. §§ 4-88-104, 4-88-112, as well as pursuant to the common law of the State of Arkansas.

39. Plaintiff does not plead, expressly or implicitly, any cause of action or request any remedy that arises under federal law.

IV. FACTUAL ALLEGATIONS

A. Defendant PDD Holdings is a Chinese Online Retailer and Has Become One of the Largest E-Commerce Entities in the World Through Its Pinduoduo and Temu Apps.

40. Founded in 2015 by Chinese businessman, software engineer, and former Google employee, Colin Huang, PDD Holdings is one of China's largest companies, generating an estimated $383 billion in total value of goods sold before deductions in 2021.

41. Among other business activities, PDD Holdings operates Pinduoduo, an e-commerce app created in China that offers various consumer products.

42. Pinduoduo was developed to compete with Chinese online retailers Alibaba and JD.com by selling low-priced goods. The Pinduoduo app serves as a marketplace that recruits China-based suppliers to offer products and provides a range of low-cost products to consumers who visit its site. As described in Pinduoduo Inc.'s SEC filings, "[t]he platform pioneered an innovative 'team purchase' model. Buyers are encouraged to share product information on social networks, and invite their friends, family, and social contacts to form shopping teams to enjoy the more attractive prices available under the 'team purchase' option. Pinduoduo's buyer base helps attract merchants to the platform, while the scale of the platform's sales volume encourages merchants to offer more competitive prices and customized products and services to buyers, thus forming a virtuous cycle."[20]

[20] PDD HOLDINGS, FORM 20-F ANNUAL REPORT (2022).

43. While the Temu app has not yet introduced the "team purchase" feature in the United States, Temu does offer significant discounts to users who invite their friends to download the app,[21] thus incentivizing the proliferation of the app on social media platforms.

44. PDD Holdings operates a series of subsidiaries in China and has long maintained its corporate headquarters in Shanghai, China. However, following a growing chorus of geopolitical security and privacy concerns, and to obscure its connections to China, PDD Holdings recently disclosed that it was moving its "principal executive offices" to Dublin, Ireland. Nonetheless, the vast majority of PDD Holdings's business operations, including several subsidiaries, continue to be in China.

B. The Pinduoduo App is Considered Malware by an Overwhelming Number of Security Experts and Was Banned from Google's App Marketplace.

45. On March 21, 2023, Google suspended the Pinduoduo app from the Google Play Store after malware issues were found on the app.[22] Subsequently, independent security researchers were shocked at what they uncovered when they examined the app's source code and its behavior once installed on mobile devices. While many apps collect vast troves of user data, sometimes without explicit consent, these experts stated that Pinduoduo took violations of privacy and data security "to the next level."[23]

---

[21] *What is Temu*, NPR: PLANET MONEY (March 22, 2024), https://www.npr.org/transcripts/1197958526?ft=nprml&f=1197958526 (last accessed June 18, 2024).

[22] Baranjot Kaur & Abinaya Vijayaraghavan, *Google suspends China's Pinduoduo app on security concerns*, INSIDE RETAIL (March 24, 2023).

[23] Nectar Gan et al., *'I've never seen anything like this:' One of China's most popular apps has the ability to spy on its users, say experts*, CNN (Apr. 3, 2023), https://www.cnn.com/2023/04/02/tech/china-pinduoduo-malware-cybersecurity-analysis-intl-hnk/index.html (last accessed June 18, 2024).

46. Researchers found that the app was programmed to bypass users' cell phone security in order to monitor activities on other apps, check notifications, read private messages, and change settings.[24] The researchers found code designed to achieve "privilege escalation," a type of cyberattack that exploits a vulnerable operating system to gain a higher level of access to data than is authorized.[25] It also could spy on competitors by tracking activity on other shopping apps and getting information from them.[26]

47. One security researcher described Pinduoduo as "the most dangerous malware" ever found among mainstream apps. [27]

48. Moreover, once the app was installed, the app was able to run in the background and prevent itself from being uninstalled.[28]

49. According to investigators, the Pinduoduo code allowed the app to access users' locations, contacts, calendars, notifications, and photo albums without their consent. Pinduoduo was also able to change system settings and access users' social network accounts and chats.[29]

50. According to one report by an IT security firm, "[c]ompany insiders said the exploits were utilized to spy on users and competitors, allegedly to boost sales. Pinduoduo

---

[24] *Id.*

[25] *Id.*

[26] *Id.*

[27] *Id.*

[28] *Id.*

[29] *Id.*

requested as many as 83 permissions, including access to biometrics, Bluetooth, and Wi-Fi network information."[30]

51. Analysts, including experts at Google, concluded that the Pinduoduo app was covertly collecting private and personal data from users without their knowledge and consent, including highly sensitive biometric data contained on users' devices. These functions were not accidental—they were intentionally built into the design of the app. "Pinduoduo's malware was not a fringe or circumstantial effort. PDD recruited and hired a team of 100 programmers to find and exploit OEM customizations of Android (installed on mainstream brands of low-priced smartphones), intending to exploit vulnerabilities audited less often than the mainline Android codebase (estimates of over 50 such vulnerabilities were targeted)."[31]

52. Moreover, even after Defendants made changes to the Pinduoduo app in response to the suspension by Google, it continued to violate users' privacy rights. For example, multiple security vendors continue to rate Pinduoduo as "malicious," as reported by the malware statistics service VirusTotal.com.

53. On March 5, 2023, Pinduoduo issued a new update of its app, version 6.50.0, which removed the exploits. Researchers who investigated the update said although the exploits were removed, the underlying code was still there and could be reactivated to carry-out attacks.[32]

---

[30] Nicholas Foisy, *Temu App Poses Potential Data Risk for Consumers*, COMPASS IT COMPLIANCE (June 30, 2023), https://www.compassitc.com/blog/temu-app-poses-potential-data-risk-for-consumers (last accessed June 18, 2024).

[31] Grizzly Research, *supra* note 7.

[32] Nectar Gan, *supra* note 21.

54. Two days after the update, Pinduoduo disbanded the team of engineers and product managers who had developed the exploits, according to a Pinduoduo source.[33] Thereafter, most of the members on this team were transferred to work at Temu.[34]

C. *In 2022, PDD Holdings Developed the Temu App, Which Is Modeled on Pinduoduo's Design and Code and Which Defendants Aggressively Market in the United States.*

55. In 2022, Defendants developed the Temu app to be a global version of the Pinduoduo platform, with the United States as its principal market.[35]

56. Defendants have heavily promoted the Temu app, including through television advertisements, large online ad campaigns, and sponsorships. Temu spends billions on marketing, at times more than companies such as Walmart.

57. As a result of Defendants' heavy promotion of the Temu app, it has experienced exponential growth. In 2023, Temu was the most downloaded app in the United States.[36] As a result, the market capitalization of Defendant PDD Holdings has swelled.[37]

58. The same software engineers and product managers who developed Pinduoduo and turned it into "the most dangerous malware" ever found among mainstream apps, were transitioned to working on the Temu app within a year of Temu's introduction into the marketplace.[38]

---

[33] *Id.*

[34] *Id.*

[35] PDD HOLDINGS, *supra* note 18.

[36] Perez, *supra* note 3.

[37] Grizzly Research, *supra* note 7.

[38] Nectar Gan, *supra* note 21.

59. Like the Pinduoduo app, the Temu app provides a marketplace for Chinese suppliers to offer their products. However, the Temu app also handles delivery, promotion, and after-sales services for merchants on its platform. Temu's network now includes more than 80,000 suppliers.[39]

60. Temu is responsible for tens of millions of shipments into the United States each year—including via purchases made, finalized, and received in Arkansas—through Temu's network of more than 80,000 China-based sellers participating in its online marketplace.[40]

D. Precisely Like the Pinduoduo App, Defendants' Temu App Presents a Host of Undisclosed Privacy and Security Risks.

61. Just like the Pinduoduo app, Temu is using the inducement of low-cost Chinese-made goods to lure users into unknowingly providing near-limitless access to their PII. Such acts are deceptive and unconscionable under Arkansas law.

62. Temu's conduct came to light following the removal of the Pinduoduo app from Google's Play Store due to the presence of malware that exploited vulnerabilities in users' phone operating systems and allowed the app not only to gain undetected access to virtually all data stored on the phones, but also to recompile itself and potentially change its properties *once installed*, in a manner designed to avoid detection.

63. Around that same time, Apple expressed similar concerns about the Temu app, concluding that the app did not comply with Apple's data privacy standards and that Temu was

---

[39] SELECT COMM. ON THE CHINESE COMMUNIST PARTY, FAST FASHION AND THE UYGHUR GENOCIDE: INTERIM FINDINGS 4 (June 22, 2023), https://selectcommitteeontheccp.house.gov/sites/evo-subsites/selectcommitteeontheccp.house.gov/files/evo-media-document/fast-fashion-and-the-uyghur-genocide-interim-findings.pdf (last accessed June 18, 2024).

[40] *Id.*

misleading users regarding how it used users' data. According to Apple, "Temu misled people about how it uses their data. Temu's so-called privacy nutrition labels—descriptions about the types of data an app can access, how it does so and what it uses them for—did not accurately reflect its privacy policy…Temu also isn't letting users choose not to be tracked on the internet," an option that all apps in Apple's online marketplace are required to provide.[41]

64. Security experts have concluded that the Temu app is "even more 'malicious' than the suspended pinduoduo-6-49-0 app."[42]

65. Forensic analysis of the Temu app's code reveals that the scope of the data collected by Temu is virtually limitless, going well beyond the scope of the data that is needed to run an online shopping app.

66. In addition to Bluetooth and Wi-Fi access, "Temu gains full access to all your contacts, calendars, and photo albums, plus all your social media accounts, chats, and texts. In other words, literally everything on your phone…No shopping app needs this much control, especially one tied to Communist China."[43] As another commentator observed on the Montana ban, the Temu app is "dangerous," due to the fact that it "bypasses" phone security systems to read a user's private messages, make changes to the phone's settings, and track notifications.[44]

67. An extensive forensic investigation of the app, published by an analyst firm on September 6, 2023, went so far as to claim that Defendant PDD Holdings was a "fraudulent company" and that "its shopping app TEMU is cleverly hidden spyware that poses an urgent

---

[41] Goujard, *supra* note 5.

[42] Grizzly Research, *supra* note 7.

[43] Komando, *supra* note 9.

[44] Basilan, *supra* note 12.

security threat to United States national interests," asserting "smoking gun evidence" that the "widely downloaded shopping app TEMU is the most dangerous malware/spyware package currently in widespread circulation."[45]

68. Among the primary findings of the report were the following:

a. "The app has hidden functions that allow for extensive data exfiltration unbeknown to users, potentially giving bad actors full access to almost all data on customers' mobile devices."

b. "It is evident that great efforts were taken to intentionally hide the malicious intent and intrusiveness of the software."

c. "Contributing to the danger of mass data exfiltration is the fast uptake rate of the TEMU app: over 100 million app downloads in the last 9 months, all in the United States and Europe. TEMU is not offered in China."

d. "The TEMU app development team includes 100 engineers who built the Pinduoduo app, which earned a suspension from the Google Play Store."

e. "Pinduoduo app got reinstated by removing the 'bad parts,' some of which were identically utilized as components of the TEMU app, strongly indicating malicious intent."

f. "We strongly suspect that TEMU is already, or intends to, illegally sell stolen data from Western country customers to sustain a business model that is otherwise doomed for failure."[46]

---

[45] *Id.*

[46] *Id.*

69. Specifically, the analysis concluded that the Temu app contains malware, spyware, and other means to "plunder" user data.[47]

70. The analysis further found that the Temu app has the capability to hack users' phones and override data privacy settings that users have purposely set to prevent their data from being accessed.[48]

71. Technical analysis of the Temu app found "all the signs of red-flag concern," noting that "[t]he calls to outside device data and functions that violate users' privacy are far more aggressive than any well-known consumer shopping app."[49]

72. While the report identified a host of concerns, some of the primary concerns can be identified as follows:

1. Design and Programming that Intentionally Evade Scrutiny

a. Dynamic compilation using runtime.exec()

73. Compiling is the process of creating a computer executable from a human-readable code.

74. A cryptically named function in the source code of the Temu app calls for "package compile" using runtime.exec(). Per the report, "[t]his means **a new program is created by the app itself.**" (emphasis original).[50]

---

[47] *Id.*

[48] *Id.*

[49] *Id.*

[50] *Id.*

75. The executable created by this function is not visible to security scans before or during installation of the app, or even with elaborate penetration testing.

76. Instead, this code enables the app to change its behavior—and possibly its entire function—*on the user's phone*, without anyone being able to know, much less prevent such a change.[51]

77. The Temu app can pass all required tests for approval into Google's Play Store, "despite having an open door built in for an unbounded use of exploitative methods. The local compilation even allows the software to make use of other data on the device that itself could have been created dynamically and with information from TEMU's servers."[52]

b. Use of android.permission.INSTALL_PACKAGES

78. In computer science, a "package" is a specialized program or set of specialized programs and associated documentation designed to carry out a particular task.

79. The Temu app seeks to use what Google classifies as a "high risk or sensitive permission"[53] of "android.permission.INSTALL_PACKAGES."

80. This means that upon installation, the Temu app gains permission from the user's device to subsequently install any further program (or "package") that Temu wishes without the user's knowledge or control.

---

[51] *Id.*

[52] *Id.*

[53] GOOGLE, *Use of the REQUEST_INSTALL_PACKAGES permission*, GOOGLE: HELP CENTER, https://support.google.com/googleplay/android-developer/answer/12085295?hl=en#zippy=%2Cpermitted-uses-of-the-request-install-packages-permission%2Cinvalid-uses) (last accessed June 18, 2024).

81. Google—which controls the Android operating system upon which the Temu app is built—allows this request only for apps whose "core functionality" requires this feature.[54] There is no justifiable use for this feature on the Temu app, which purportedly is simply an e-commerce platform.

c. Omitting requested permissions from the Temu app manifest file

82. A manifest file is required for every Android app,[55] and *must* contain certain information, including the permissions that the app needs in order to access protected parts of the system or other apps.[56]

83. Many of the permissions that the Temu app seeks from a user's device (that is, many of the features or data storage repositories on a user's device that the Temu app seeks to access) are omitted from the "manifest file" of the app.

84. As Google explains on its webpage for Android developers, "Android apps must request permission to access sensitive user data, such as contacts and SMS, or certain system features, such as the camera and internet access. Each permission is identified by a unique label."[57]

85. Violating this requirement, Temu omits a host of permissions from its manifest file. Some examples of the highly-sensitive permissions that the Temu app seeks—but does not identify in its manifest file—include permission requests for CAMERA, RECORD_AUDIO,

---

[54] GOOGLE, *Permissions and APIs that Access Sensitive Information*, GOOGLE: POLICY CENTER, https://support.google.com/googleplay/android-developer/answer/9888170 (last accessed June 18, 2024).

[55] ANDROID, *App manifest overview*, ANDROID: DEVELOPERS GUIDES, https://developer.android.com/guide/topics/manifest/manifest-intro (last accessed June 18, 2024).

[56] *Id.*

[57] *Id.*

WRITE_EXTERNAL_STORAGE, INSTALL_PACKAGES, and ACCESS_FINE_LOCATION.[58]

d. Detecting "root" access on a device

86. The Temu app checks a user's device to see whether it has "root" access, which is the highest level of access on a device. With root access, the user *and the Temu app* can read, modify, and write not only user files, but all files on the device, including the programming of other apps and the device's operating system. Temu could theoretically control or even disable any device where the user has root access and Temu has file writing permissions without the user's knowledge or consent.[59]

87. Root access detection also serves another purpose: obfuscating Temu's code. Security researchers require root access to conduct thorough investigations and evaluations of an app's security. One purpose of an app trying to determine whether a device has root access is to determine whether the app is being used in a "testing" environment and therefore needs to hide its nefarious behaviors. [60]

---

[58] Grizzly Research, *supra* note 7.

[59] *Id.*

[60] INDUSFACE, *How to Implement Root Detection in Android Applications?*, https://www.indusface.com/learning/how-to-implement-root-detection-in-android-applications/#:~:text=Security%20researchers%20or%20pen%20testers,app%20and%20a%20remote%20server (last accessed June 18, 2024).

e. Searching for "debuggers"

88. Security researchers and security features on mobile devices may employ a "debugger," which is a tool or program that enables one to view running application code. This is a critical tool for identifying malware that might be hidden within an app.[61]

89. Temu's code includes a query Debug.isDebuggerConnected(), which would alert the Temu app if a debugger is engaged on a user's device. Analysts believe this is intended to obstruct or obscure analysis of the app and most likely to change app behavior if an analyst is inspecting it dynamically.[62]

f. Purposely obfuscatory information architecture

90. The files, folders, classes, and functions of the Temu app are also designed, named, and cross-referenced to each other in a highly complex way that is designed to hamper investigation of the malicious aspects of the app. Indeed, analysts have concluded that "it is practically impossible for a human to read the decompiled code, and we believe TEMU uses additional tools in the compiling process to create this obfuscation. The most outstanding indicator of TEMU's code obfuscation is the top-level view of the JAVA source codegri after decompiling." These practices are in contrast to other apps that are much more transparent.[63]

g. Hiding previous versions of the Temu app and its files

91. Defendants have sought to cover their tracks by removing from the public domain prior versions of files associated with the app and have deleted features of the app when necessary

---

[61] Srinivas, *Debugging for malware analysis*, INFOSEC (Aug. 14, 2019), https://www.infosecinstitute.com/resources/malware-analysis/debugging-for-malware-analysis/ (last accessed June 18, 2024).

[62] Grizzly Research, *supra* note 7.

[63] *Id.*

to avoid detection of their wrongdoing. Analysts have concluded that "TEMU is hiding something" because of features of the Temu app that were similar to those of the Pinduoduo app that were mysteriously deleted in May 2023 after Google suspended Pinduoduo for malicious spyware and prior versions of certain files associated with the app have been removed from Google's Play Store.[64]

92. As one technical report noted with respect to the latter issue, "Many websites archive APK's [*i.e.,* versions of an app] published in Google's Play Store. However, TEMU's app seems to have disappeared from many of these archives, in particular almost all with Google Page Rank 6 or higher that appear on the top of Google searches. The TEMU APKs are removed from all websites with U.S. jurisdiction, indicating that legal measures by TEMU could be behind the exclusion from the web archives. Inaccessibility of the APK files makes malware research more cumbersome."[65]

2. Excessive, Unjustifiable, and Hidden Collection of Users' PII

93. Much of Temu's efforts to hide its behavior are done in furtherance of accessing and controlling virtually all aspects of a user's device and surreptitiously acquiring sensitive PII.

a. Users' granular location data

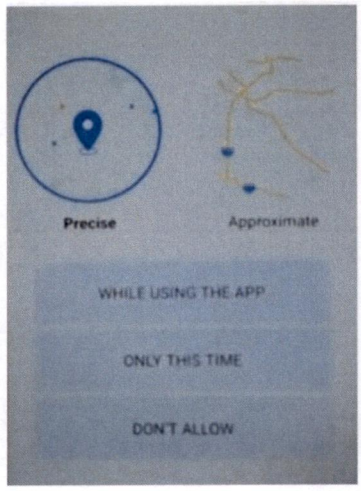
94. The Temu app gains access via permissions requests that it hides from its manifest file to user's "fine" location—that is, the app gets user's real-time GPS location within an accuracy of at least 10 feet.

95. In some instances, the app will purportedly seek permission to access the user's "precise" location versus "approximate" location (see the image below), but it does so by using

[64] Grizzly Research, *supra* note 7.

[65] *Id.*

what is referred to as a "dark pattern" or "nudge" to induce the user to give up his or her geolocation, with no explanation as to why the app needs this data.



96. Moreover, these requests mislead users. The above prompt is provided when a user attempts to upload a photo to the Temu app. A reasonable consumer would assume that the location permission is confined to the use of photo uploads. The permission, however, extends to any time the user engages with the Temu app. This lack of clarity, coupled with the misleading default to the most privacy-invasive setting, harms users and robs them of their location privacy.

b. Microphone and camera access

97. Two permissions that Temu sneaks into its app without disclosing them in the manifest file are requests for CAMERA and RECORD_AUDIO.[66] These permissions grant the app access to all the audio and visual recording and storage functions of a user's device.

c. Additional sensitive PII

98. The Temu app accesses users' system logs, which is "the device's secret diary, with all its missteps and mishaps detailed. TEMU's code references the log files' address and options

[66] *Id.*

for shell commands. The only reason to introduce such strings into the proprietary code is to gather the log data to observe the user's active usage of their device. In accordance with this, TEMU's app requests a list of running processes using getRunningAppProcesses(), which together with the log files seems to make the app investigate the overall devices' activities quite thoroughly." [67]

99. This collection of data enables Temu to track user actions with other apps running on the user's device. This can be profoundly revealing and invasive, given that many of the apps we use daily involve our travel, health, religious practices, dating habits, friend groups, purchases, banking, and myriad other critical—and private—data points about who we are, what we do, and what we think.

100. Beyond these data points, Temu collects a host of other, discrete PII generated by the user's device, which are universally recognized as individually-identifying pieces of information that can be—and routinely are—used to track, monitor, and profile individuals. Two examples include a user's MAC address (a unique identifier tied to a user's phone)[68] and a user's Android Advertising ID (via the permission, "com.google.android.gms.permission.AD_ID"), which is a unique identifier used to track an individual's activity over time and across the various apps or websites he or she uses or visits.

101. In sum, Temu not only seeks a breathtaking array of sensitive data—well beyond what would be necessary or even justifiable for a shopping app—but it does so in a way that is purposely secretive and intentionally designed to avoid detection.

---

[67] *Id.*

[68] *Id.*

102. Analysis also found "a stack of software functions that are completely inappropriate to and dangerous in this type of software."[69]

103. Temu is particularly malicious because much of the data collection occurs as soon as the app is downloaded. Temu contains "a complete arsenal of tools to exfiltrate virtually all the private data on a user's device and perform nearly any malign action upon command trigger from a remote server."[70]

104. In addition to these concerns, other investigators examining Temu reported that older versions of the Temu app had a patching capability through a home-built framework known as "Manwe," which is an unpacking and patching tool that was also found in the malicious versions of Pinduoduo. Manwe could enable PDD Holdings to patch the app on the device rather than through the Apple App Store or Google Play Store. This is against app store policies, as it could enable the developer to push unauthorized code via updates to user devices.

105. Authorities in other countries have also raised alarms after examining the Temu app. For example, in the United Kingdom, "law enforcement authorities have issued a stark warning about this online marketplace. They have uncovered evidence of the app harvesting customer data and expressed concerns that this data may find its way into Chinese hands."[71]

106. In addition to the unauthorized collection of their data, users may suffer additional injuries. Indeed, as analysts have noted, regardless of whether users authorized the initial collection of such data by Defendants, Temu users may be subjected to additional injuries, including the

---

[69] *Id.*

[70] *Id.*

[71] Naveen Goud, *China Temu App caused data privacy concerns in United Kingdom*, CYBERSECURITY INSIDERS, https://www.cybersecurity-insiders.com/china-temu-app-caused-data-privacy-concerns-in-united-kingdom/ (last accessed June 18, 2024).

provision or sale of their data to unauthorized third parties or the use of their data in ways that users did not authorize by Defendants themselves.

107. Individuals who are not Temu users and have never signed up for the platform may also be adversely impacted. Unbeknownst to them, non-users who engage in electronic communications with Temu users, such as through email or text messages, may have their private communications subject to harvesting by Defendants who have broad access to Temu users' devices. In addition, individuals who never signed up for Temu but who have stored information on a Temu user's device may also have their data subject to unauthorized harvesting by Defendants.

3. Temu's Data Collection and App Design Belie the Platform and App's Privacy Policy

108. Despite these revelations, Defendants have recently declared, "At Temu, we prioritize the protection of privacy and are transparent about our data practices."[72]

109. This statement is demonstrably false. Indeed, Temu's Privacy Policy contains multiple misrepresentations that would prevent the reader from understanding the full scope of its privacy-invasive conduct.

110. For example, under the section titled "What Information Do We Collect?" the Privacy Policy lists "Information collected automatically," and states that Defendant collects "**Device Data:** We collect certain information about the device you use to access the Service, such as device model, operating system information, language settings, unique identifiers (including identifiers used for advertising purposes)." Temu acquires a significantly greater—and much more

[72] Temu, *Privacy Policy*, TEMU, https://www.temu.com/privacy-and-cookie-policy.html (last accessed June 20, 2024).

personal—array of data from a user's device, including but not limited to the user's (1) contacts, (2) calendars, (3) photo albums, (4) social media accounts, (5) chats, and (6) texts.

111. Similarly, Temu also seeks permissions to access the camera and microphone on a user's device. These permissions grant the app access to all the audio and visual recording and storage functions of a user's device.

112. Temu determines whether a user's device has "root" access. If the device has root access, Temu can read, modify, and write not only user files, but all files on the device, including the programming of other apps and the device's operating system.

113. Temu can also identify the other apps running on a user's device and track a user's actions on those apps.

114. Each of these functions occur automatically, and each extract highly sensitive PII from an individual's device. None of this functionality is described in the Privacy Policy.

115. Additionally, in the same section of Temu's Privacy Policy, the reader is informed that Defendant *only* collects "approximate" location data. Specifically, the Policy states: "**Location Data:** We collect your approximate location data (e.g. IP address)."

116. This is false. As explained herein, the Temu app contains code that seeks permission to access the user's GPS location immediately upon installation, and Temu's interface misleadingly prompts users into authorizing the acquisition of granular, GPS location data in perpetuity if they attempt to upload photos to the app.

4. Temu Subjects User Data to Misappropriation by Chinese Authorities

117. The data privacy violations documented with the Temu app are particularly concerning, not only because they subject user data to unauthorized collection and potential sale to

third parties, but also because Temu's parent company is required by Chinese law to provide use data to the Chinese government upon request.

118. As a technical analysis of the Temu app has noted, "[Users'] personal data...is resold indiscriminately for marketing purposes, and in all probability available to Chinese Security authorities for data mining purposes. Chinese Government security agents or their AI computers might be looking at what products [users and their] family buy on TEMU as a source of leverage, influence, manipulation, 'cross-border remote justice,' surveillance, or more."[73]

119. Senator Tom Cotton recently noted, "Just like TikTok, Temu or any Chinese tech company must allow the Communist Party unfettered access to its data. This should be a non-starter for doing business in the United States."[74]

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

121. These laws are broad, open-ended, and inscrutably applied. Moreover, there is no independent judiciary in China that operates outside the control of the Chinese Communist Party. Thus, there is no meaningful mechanism in China to resist these demands.

122. Laws including, but not limited to, the National Security Law, Cybersecurity Law, and National Intelligence Law are part of "an interrelated package of national security, cyberspace, and law enforcement legislation" that "are aimed at strengthening the legal basis for China's

---

[73] Grizzly Research, *supra* note 7.

[74] Tom Cotton (@SenTomCotton), TWITTER (Feb. 12, 2024, 8:54 a.m.), https://twitter.com/SenTomCotton/status/1757055483217604697.

security activities and requiring Chinese and foreign citizens, enterprises, and organizations to cooperate with them."[75]

123. China's National Security Law places "the responsibility and duty to safeguard national security" on all "*[c]itizens of the People's Republic of China*, all State bodies and armed forces, all political parties and people's organizations, *enterprises*, undertakings, organizations and all other social organizations."[76]

124. The National Intelligence Law expounds on this responsibility, requiring all organizations and Chinese citizens to "cooperate with national intelligence efforts" and permits national intelligence institutions to collect information, question organizations and individuals, and take control of facilities and "communication[] tools."[77]

125. Experts across a variety of fields, including law, national security, and technology agree that Chinese laws require any individuals or entities in China or otherwise subject to Chinese law to cooperate with the Chinese government, including China's intelligence and security

---

[75] M. Scot Tanner, *Beijing's New National Intelligence Law: From Defense to Offense*, LAWFARE (July 20, 2017), https://bit.ly/3fXfB4A (referring to laws addressing "Counterespionage (2014), National Security (2015), Counterterrorism (2015), Cybersecurity (2016), and Foreign NGO Management (2016), as well as the Ninth Amendment to the PRC Criminal Law (2015), the Management Methods for Lawyers and Law Firms (both 2016), and the pending draft Encryption Law and draft Standardization Law"); *see also* M. Haldane, *What China's new data laws are and their impact on Big Tech*, SOUTH CHINA MORNING POST (Sept. 1, 2021), https://bit.ly/3zM0jX3 (describing later enacted Data Security Law and Personal Information Protection Law as being "built on the groundwork laid by the Cybersecurity Law"); W. Zheng, *Big data expert takes over as China's new cybersecurity chief*, SOUTH CHINA MORNING POST (Sept. 27, 2019), https://bit.ly/3t03fLR.

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

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

services, and that there is no meaningful way to resist these requirements, or any pressure brought to bear by the Party.[78]

126. Further, Chinese law enforcement and intelligence services interpret Chinese law as applying to any data, wherever it is stored, if China has a national security interest in that data.

127. In sum, any data stored *or accessed* by individuals or entities subject to Chinese laws can be accessed by the Chinese Government.

128. The geopolitical reality of a dominant e-commerce platform being controlled by an authoritarian regime drastically amplifies the harms and the stakes associated with Defendants' deceptive and unconscionable practices.

5. Defendants Are Violating Arkansans' Right to Privacy of Their Data

129. As a result of their multiple violations of users' data privacy, Defendants possess a host of critical, sensitive, and potentially dangerous PII, including the PII of Arkansans who have used the Temu app. Such PII can be supplemented over time with *additional* private and personally

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

identifiable user data and content, and all of this information has been, is, and will be used for economic and financial gain.

130. Meanwhile, Arkansans have incurred, and continue to incur, harm as a result of the invasion of privacy stemming from Defendants' deceptive and unconscionable acquisition and possession of their PII.

131. Arkansans have a reasonable expectation of privacy in the PII contained on their mobile devices, as well as in their autonomy interests of the mobile devices themselves.

132. Defendants' capacity for "near perfect surveillance," *Carpenter v. United States*, 585 U.S. 296, 312 (2018), is an extreme privacy violation. Defendants' unlawful intrusion into their users' privacy is made even more egregious and offensive by the fact that the Defendants are targeting and collecting information in a manner that is *intended to go undetected.*

133. Defendants have designed the Temu app to surreptitiously collect a wide range of data from Temu users. In addition, Defendants continue to take actions and have purposefully designed the Temu app to obscure and hide their unlawful collection of users' data.

134. Defendants' actions also adversely impact non-users of Temu who have had electronic communications with Temu users or whose data is stored on the device of a Temu user because their data is subject to harvesting by Defendants without their knowledge.

135. Many of the categories of data and information collected by Defendants are particularly sensitive. As just one example, Defendants collect physical and digital location tracking data that is highly invasive of Temu users' privacy rights. Over time, location data reveals private living patterns of Temu 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 Temu users' health, religion, politics, and intimate relationships.

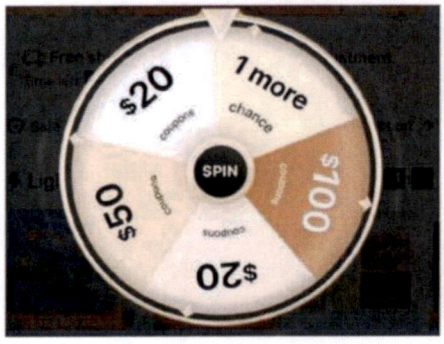
136. More generally, the various functions and aspects of the Temu app described above make clear that it is a malicious app designed to covertly harvest user data in violation of their privacy rights. [79]

6. Defendants Engage in Deceptive and Unconscionable Trade Practices in the Offer and Sale of Products on the Temu App

137. Defendants actively utilize deceptive and unconscionable practices to maximize the number of users who sign up to use the app, thereby maximizing the amount of data that Defendants can misappropriate.[80]

138. But beyond the privacy harms of the app, Defendants separately engage in deceptive and unconscionable business practices regarding the sale of goods on their platform.

139. Defendants seek to induce users to sign up for the Temu app with the promise of low-cost, high-quality goods manufactured in China. Defendants underscore this aspect of the platform through a variety of mechanisms such as pop-ups with wheels to spin for discounts, tokens to collect, and countdown clocks like those below.



[79] *Id.*

[80] *Id.*

140. These tactics have been wildly successful. "PDD's TEMU online marketplace is being reported as among the fastest growing apps in history."[81]

7. Deceptive Representations as to the Quality of Goods

141. Defendants' representations regarding the products sold on the Temu platform are false and serve only to further conceal its scheme to maximize the number of users who sign up to the platform and unwittingly subject their private data to theft by Defendants. For example, while Temu represents that it sells "affordable quality products," and indeed "the best products,"[82] there have been many complaints regarding the quality of goods sold on the site as well as the service provided by Temu.

142. The Better Business Bureau alone has received hundreds of complaints in the past year, earning Temu a rating of 2.1 out of 5 stars.[83] Users experience undelivered packages and poor customer service. Moreover, even when goods are delivered, they are often of low quality, contrary to Temu's marketing and representations.

143. For example, one analysis observed that "TEMU products as shipped often do not resemble the photos."[84] Users frequently receive low-quality merchandise when the photo on the app indicates that they would receive high-quality goods. Moreover, photos and product

---

[81] *Id.*

[82] Temu, *What is Temu?*, TEMU, https://www.temu.com/about-temu.html (last accessed June 18, 2024).

[83] Nicholas Kaufman, *Shein, Temu, and Chinese e-Commerce: Data Risks, Sourcing Violations, and Trade Loopholes*, Issue Brief prepared by the research staff at the U.S.-China Economic and Security Review Commission (Apr. 14, 2023), https://www.uscc.gov/sites/default/files/2023-04/Issue_Brief-Shein_Temu_and_Chinese_E-Commerce.pdf (last accessed June 18, 2024).

[84] Grizzly Research, *supra* note 7.

descriptions are sometimes simply copied directly from other sellers on sites like Amazon, bearing no relationship to the actual goods being sold.[85] In addition, while Defendants claim that they use "world-class manufacturers" and have a "zero tolerance policy against counterfeits,"[86] Temu frequently sells counterfeit, knock-off products in violation of the law. For example, it recently was reported that Temu was selling knockoff Air Jordans on the site and continued to do so even after the issue came to light.[87]

8. False-Reference Pricing

144. Temu further engages in a deceptive act known as "false-reference pricing," in which a retailer represents to a prospective customer that a product is on sale at a steep discount when the "discounted price" is the product's regular market price. Specifically, the seller provides two prices that the customer can compare a former list price or MSRP, which is inflated or was never real to begin with, and a "reduced" current price, which is the product's normal market price.

9. Sign-Up Scams to Lure New Users or to Induce Existing Users to Reel in Their Friends

145. Defendants utilize additional deceptive marketing techniques to induce users to sign up for the platform and grant Defendants access to user data. For example, Defendants run what has been described as an "affinity scam" or "chain letter" like tactic where users are

[85] Jennifer Ortakales Dawkins, *Temu sellers are now even copying product photos, descriptions, and entire Amazon storefronts, lawsuits allege*, BUSINESS INSIDER (July 11, 2023), https://www.businessinsider.com/temu-sellers-are-counterfeiting-amazon-listings-and-storefronts-2023-7 (last accessed June 18, 2024).

[86] Temu, *Temu's Commitments*, TEMU, https://www.temu.com/commitments.html (last accessed June 18, 2024).

[87] Dawkins, *supra* note 85.

repeatedly urged to sign up their friends and acquaintances to expand the number of users whose data Defendants may then access through the app.

146. Temu offers credit and free items to users who get their friends and acquaintances to sign up for the app. Temu then repeatedly spams users to get their family and friends to give Temu their personal information.[88]

147. Temu users are bombarded by notifications and spam from third parties other than Defendants. These emails and notifications occur even after users delete the app from their devices and even when users seek to block such notifications.

148. Moreover, Temu has utilized online "influencers" to harvest new users on an even larger scale.[89]

10. Fake Reviews

149. Defendants attract and maintain users through other fraudulent means. For example, Temu pays users to provide reviews, which skews the reviews more positively.

150. Reviews are categorized in a deceptive manner with reviews characterized as "five star" positive reviews when in reality they contain extremely negative comments about the platform.[90]

---

[88] Grizzly Research, *supra* note 7.

[89] *Id.*

[90] *Id.*

11. Gamification

151. As illustrated by its gamified nature, Temu is designed to be highly addictive.[91] The more time users spend on the app, the more data is available for covert collection by Defendants in violation of users' right to privacy in their personal data.

152. As one analyst observes, the addictive tactics extend not only to users' continued use of the platform, but also inducing individuals to sign up for the app.[92]

12. Collection of Personal Information from Minors, Including Minors Under the Age of 13

153. These practices are particularly abusive, given that many of the users of Temu are minors, including minors under the age of 13. At all relevant times, Defendants have been aware that minors, including minors under the age of 13, are using the Temu platform.

154. Nonetheless, Defendants failed to take adequate measures to protect minor users from these abusive tactics or to ensure that minor users, including minor users under the age of 13, had parental consent before they used the Temu platform. Nor did Defendants implement adequate age verification procedures or other procedures to confirm that minor users were acting with the consent of their parents in using the Temu platform or adequate opt-out rights or rights to delete collected information.

155. Anyone can use Temu without verifying his or her age, and indeed many children use the Temu platform, including children under 13 years old. Temu sells a wide variety of products that are marketed to children such as children's toys and clothing. Defendants have

---

[91] James Titcomb, *Here comes Temu, China's 'scary' bargain-basement Amazon killer*, The Telegraph (Jul. 1, 2023), https://web.archive.org/web/20230705172831/https://www.telegraph.co.uk/business/2023/07/01/temu-china-bargain-basement-amazon-rival-retail-online-shop/ (last accessed June 18, 2024).

[92] Grizzly Research, *supra* note 7.

increased their revenue and profits by marketing these products to minors and by collecting minors' personal data when minors accessed the Temu platform.

156. Many of the advertisements for products on Temu are directed toward children, sometimes in inappropriate ways. For example, the United Kingdom's Advertising Standards Authorities recently found that certain Temu advertisements inappropriately sexualized children.[93] Likewise, a consumer group in the United Kingdom found that Temu was selling age-restricted weapons such as survival knives and axes that were illegal for children to possess without any age verification.[94] Others have observed that Temu is filled with smoking and drug paraphernalia that is sold to any customer, without age verification.

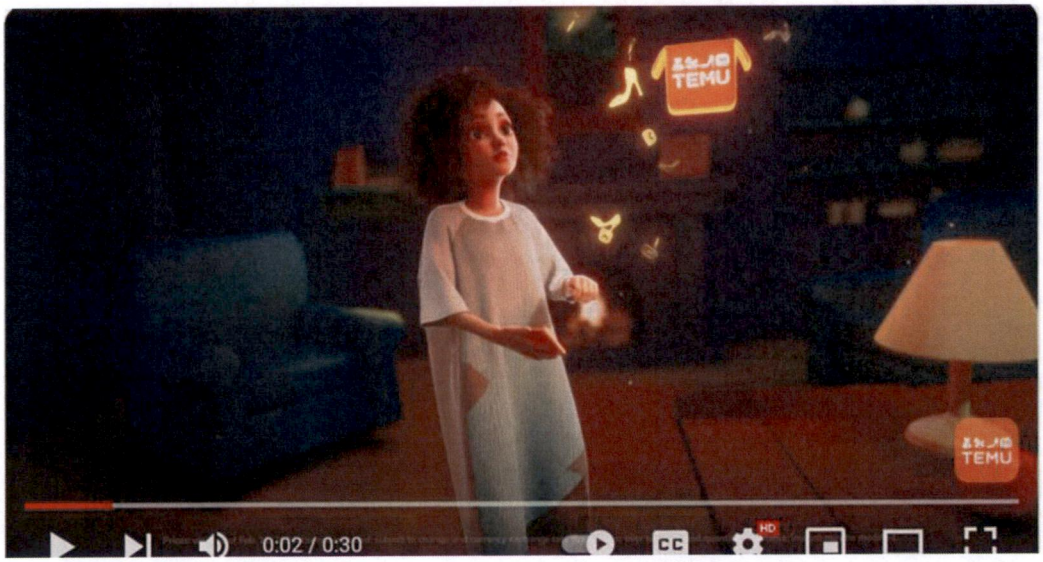
157. Temu recently ran an animated advertisement multiple times during the 2024 Super Bowl that featured a young-looking protagonist who uses magic to bestow low-priced Temu products on everyone she encounters. Attorneys General from several states as well as members of Congress urged CBS not to run the ad given ongoing investigations by Congress into Temu and the company's documented relationship with the Chinese Communist Party. As one congresswoman who objected to the advertisement observed, it "looked like it belonged on a children's show."[95]

---

[93] *Adverts for online shopping platform Temu banned for sexualising a child and objectifying women*, SkyNews (Nov. 1, 2023), https://news.sky.com/story/adverts-for-online-shopping-platform-temu-banned-for-sexualising-a-child-and-objectifying-women-12997811 (last accessed June 18, 2024).

[94] Sarah Marsh, *Weapons banned in UK apparently found on shopping app Temu*, THE GUARDIAN (Nov. 16, 2023), https://www.theguardian.com/money/2023/nov/17/weapons-banned-in-uk-apparently-found-on-shopping-app-temu-which (last accessed June 18, 2024).

[95] *Temu's ad controversy: Here's what you need to know*, CNBC (Feb. 12, 2024), https://www.cnbc.com/video/2024/02/12/temus-ad-controversy-heres-what-you-need-to-know.html (last accessed June 18, 2024).



158. Thus, notwithstanding Temu's statement in its terms of service that "[c]hildren under 13 years are not permitted to use Temu or the Services," Defendants possess actual knowledge that children under the age of 13 are on the Temu app—and indeed, Defendants actively seek out this audience. Defendants also indiscriminately and surreptitiously mine those children's PII, without providing notice to parents of those children and without obtaining the parents' verifiable consent.

159. Temu's data collection procedures with respect to minors have also been a specific concern of government authorities. Thus, for example, in their ongoing investigation of Temu, members of Congress recently sent a letter to Defendants specifically requesting information regarding Temu's data collection practices with respect to minors.[96]

160. Children under the age of 13 are particularly vulnerable to the harms caused by Defendants' conduct complained of herein, and Defendants' conduct violates longstanding societal norms meant to protect children, and to preserve parents' autonomy to ensure the same.

[96] McMorris Rodgers, *supra* note 15.

V. CAUSES OF ACTION

COUNT 1

Arkansas Deceptive Trade Practices Act,
Ark. Code Ann. § 4-88-107, *et seq.*
(Privacy Harms)

161. The State repeats and incorporates by reference each allegation contained in the preceding paragraphs. Ark. R. Civ. P. 10(c).

162. Defendants are "persons" within the meaning of Ark. Code Ann. § 4-88-102(6).

163. The Temu app is a "service" within the meaning of Ark. Code Ann. § 4-88-102(8), and Defendants are engaged in the offer and sale of "goods" within the meaning of Ark. Code Ann. § 4-88-102(5).

164. Defendants knowingly engaged in the conduct detailed above and challenged by this action.

165. The ADTPA prohibits, among other things, the following:

a. "Knowingly making a false representation as to the characteristics, ingredients, uses, benefits, alterations, source, sponsorship, approval, or certification of goods or services." Ark. Code Ann. § 4-88-107(1);

b. "Advertising the goods or services with the intent not to sell them as advertised." Ark. Code Ann. § 4-88-107(a)(3);

c. "Knowingly taking advantage of a consumer who is reasonably unable to protect his or her interest because of...ignorance." Ark. Code Ann. § 4-88-107(a)(8)(B); and,

d. "Engaging in any other unconscionable, false, or deceptive act or practice in business, commerce, or trade." Ark. Code Ann. § 4-88-107(a)(10).

166. The conduct complained of herein violates each of the above-identified provisions of the ADPTA. Defendants have created an app purported to be an e-commerce platform, which in reality is designed to collect users' PII in a manner that is unknown—and due to the intentional design of the Temu app—unknowable. Defendants utilize deception—in the forms of misrepresentation, omission, and deliberate concealment—to mask the Temu app's behavior, hide the fact that PII is being siphoned from the user's device, and prevent the user from knowing that said PII is subject to unfettered use by other individuals and an adversarial government.

167. Defendants conduct is so extreme that the two dominant app marketplaces—Apple and Google—have had to intervene due to the privacy harms (and the misrepresentations, omissions, and concealment in furtherance of those harms) visited upon users, including users in Arkansas.

168. The fact that the Temu app's privacy-violative conduct is executed through code—that is, in a manner that is invisible to the layperson—makes the conduct complained of all the more egregious, as there is no way for Arkansans to know the full extent of the nature of the privacy harms visited upon them by the app. Indeed, Defendants' conduct is especially egregious in light of the lengths to which they go to prevent independent third parties—including security researchers, Google, and Apple—from uncovering their bad acts.

COUNT 2

Arkansas Deceptive Trade Practices Act,
Ark. Code Ann. § 4-88-108, *et seq.*
(Privacy Harms)

169. The State repeats and incorporates by reference each allegation contained in the preceding paragraphs. Ark. R. Civ. P. 10(c).

170. Defendants are "persons" within the meaning of Ark. Code Ann. § 4-88-102(6).

171. The Temu app is a "service" within the meaning of Ark. Code Ann. § 4-88-102(8), and Defendants are engaged in the offer and sale of "goods" within the meaning of Ark. Code Ann. § 4-88-102(5).

172. Defendants knowingly engaged in the conduct detailed above and challenged by this action.

173. The ADTPA prohibits the following:

a. "The act, use, or employment by a person of any deception, fraud, or false pretense...[w]hen utilized in connection with the sale or advertisement of any goods, services, or charitable solicitation." Ark. Code Ann. § 4-88-108(a)(1); and,

b. "The concealment, suppression, or omission of any material fact with intent that others rely upon the concealment, suppression, or omission... [w]hen utilized in connection with the sale or advertisement of any goods, services, or charitable solicitation." Ark. Code Ann. § 4-88-108(a)(2).

174. The conduct complained of herein violates each of the above-identified provisions of the ADPTA. Defendants have created an app purported to be an e-commerce platform, which in reality is designed to collect users' PII in a manner that is unknown—and due to the intentional design of the Temu app—unknowable. Defendants utilize deception—in the forms of misrepresentation, omission, and deliberate concealment—to mask the Temu app's behavior, hide the fact that PII is being siphoned from the user's device, and prevent the user from knowing that said PII is subject to unfettered use by an adversarial government.

175. Defendants conduct is so extreme that the two, dominant app marketplaces—Apple and Google—have had to intervene due to the privacy harms (and the misrepresentations,

omissions, and concealment in furtherance of those harms) visited upon users, including users in Arkansas.

176. The fact that the Temu app's privacy-violative conduct is executed through code—that is, in a manner that is invisible to the layperson—makes the conduct complained of all the more egregious, as there is no way for Arkansans to know the full extent of the nature of the privacy harms visited upon them by the app. Indeed, Defendants' conduct is especially egregious in light of the lengths to which they go to prevent independent third parties—including security researchers, Google, and Apple—from uncovering their bad acts.

COUNT 3

Arkansas Deceptive Trade Practices Act,
Ark. Code Ann. § 4-88-107, *et seq.*
(Commercial Harms)

177. The State repeats and incorporates by reference each allegation contained in the preceding paragraphs. Ark. R. Civ. P. 10(c).

178. Defendants are "persons" within the meaning of Ark. Code Ann. § 4-88-102(6).

179. The Temu app is a "service" within the meaning of Ark. Code Ann. § 4-88-102(8), and Defendants are engaged in the offer and sale of "goods" within the meaning of Ark. Code Ann. § 4-88-102(5).

180. Defendants knowingly engaged in the conduct detailed above and challenged by this action.

181. The ADTPA prohibits the following:

a. "Knowingly making a false representation as to the characteristics, ingredients, uses, benefits, alterations, source, sponsorship, approval, or certification of goods or services." Ark. Code Ann. § 4-88-107(1);

b. "Advertising the goods or services with the intent not to sell them as advertised." Ark. Code Ann. § 4-88-107(a)(3);

c. "Knowingly taking advantage of a consumer who is reasonably unable to protect his or her interest because of...ignorance." Ark. Code Ann. § 4-88-107(a)(8)(B); and,

d. "Engaging in any other unconscionable, false, or deceptive act or practice in business, commerce, or trade" Ark. Code Ann. § 4-88-107(a)(10)

182. Defendants engage in a host of business practices—specifically (1) Deceptive Representations as to the Quality of Goods; (2) False-Reference Pricing; (3) Sign-Up Scams to Lure New Users or to Induce Existing Users to Reel in Their Friends; (4) Fake Reviews; and (5) Gamification—that violate each of the above-identified provisions of the ADPTA.

COUNT 4

Arkansas Deceptive Trade Practices Act,
Ark. Code Ann. § 4-88-108, *et seq.*
(Commercial Harms)

183. The State repeats and incorporates by reference each allegation contained in the preceding paragraphs. Ark. R. Civ. P. 10(c).

184. Defendants are "persons" within the meaning of Ark. Code Ann. § 4-88-102(6).

185. The Temu app is a "service" within the meaning of Ark. Code Ann. § 4-88-102(8), and Defendants are engaged in the offer and sale of "goods" within the meaning of Ark. Code Ann. § 4-88-102(5).

186. Defendants knowingly engaged in the conduct detailed above and challenged by this action.

187. The ADTPA prohibits, among other things, the following:

a. "The act, use, or employment by a person of any deception, fraud, or false pretense," ... "[w]hen utilized in connection with the sale or advertisement of any goods, services, or charitable solicitation." Ark. Code Ann. § 4-88-108(a)(1); and,

b. "The concealment, suppression, or omission of any material fact with intent that others rely upon the concealment, suppression, or omission" ... "[w]hen utilized in connection with the sale or advertisement of any goods, services, or charitable solicitation." Ark. Code Ann. § 4-88-108(a)(2).

188. Defendants engage in a host of business practices that violate each of the above-identified provisions of the ADTPA, specifically: (1) Deceptive Representations as to the Quality of Goods; (2) False-Reference Pricing; (3) Sign-Up Scams to Lure New Users or to Induce Existing Users to Reel in Their Friends; (4) Fake Reviews; and (5) Gamification.

189. These deceptive and unconscionable trade practices in Counts 1 through 4 have harmed, and continue to harm, Arkansans.

190. Pursuant to Ark. Code Ann. § 4-88-113(a)(1), the State is entitled to a preliminary and permanent injunction prohibiting Defendants from continuing to engage in these deceptive business practices described in Counts 1 through 4.

191. Pursuant to Ark. Code Ann. § 4-88-113(a)(3), the State is entitled to civil penalties not to exceed $10,000 for each violation of the ADTPA in Counts 1 through 4.

192. Pursuant to Ark. Code Ann. § 4-88-113(e), for compensation for services to investigate and prosecute Defendants' violations of the ADTPA, the Attorney General is entitled to all expenses reasonably incurred in the investigation and prosecution of this suit, including but not limited to, expenses for expert witnesses, attorney's fees, and costs on Counts 1 through 4.

COUNT 5

Arkansas Personal Information Protection Act, Ark. Code Ann. § 4-110-101, *et seq.*

193. The State repeats and incorporates by reference each allegation contained in the preceding paragraphs. Ark. R. Civ. P. 10(c).

194. Defendants are a "business" pursuant to Ark. Code Ann. § 4-110-103(2)(A).

195. Defendants receive "personal information" from Arkansas residents through the use of the Temu app, pursuant to Ark. Code Ann. § 4-110-103(7).

196. Defendants "own or license" said "personal information," pursuant to Ark. Code Ann. § 4-110-103(6).

197. Defendants maintain "records" pursuant to Ark. Code Ann. § 4-110-103(8).

198. Defendants have failed to "implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information from unauthorized access, destruction, use, modification, or disclosure." Ark. Code Ann. § 4-110-104(b).

199. These violations are twofold: first, Defendants' surreptitious and unconsented-to acquisition of users' personal information amounts to its own "unauthorized access [and] use [and] disclosure" of Arkansas residents' personal information.

200. Second, Defendants are beholden under controlling Chinese law to make any and all personal information—including personal information of Arkansans—available to the Chinese government immediately and without qualification upon request.

201. Pursuant to Ark. Code Ann. § 4-110-108, violations of the Arkansas Personal Information Protection Act are "punishable by action of the Attorney General under the provisions of § 4-88-101 *et seq.*"

202. Pursuant to Ark. Code Ann. § 4-88-113(a)(1), the State is entitled to a preliminary and permanent injunction prohibiting Defendants from continuing to acquire users' PII in the manner described in this Complaint.

203. Pursuant to Ark. Code Ann. § 4-88-113(a)(3), the State is entitled to civil penalties not to exceed $10,000 for each violation of the ADTPA.

204. Pursuant to Ark. Code Ann. § 4-88-113(e), the Attorney General is entitled to all expenses reasonably incurred in the investigation and prosecution of this suit, including but not limited to, expenses for expert witnesses, attorney's fees, and costs.

COUNT 6

Unjust Enrichment

205. The State repeats and incorporates by reference each allegation contained in the preceding paragraphs. Ark. R. Civ. P. 10(c).

206. The State brings this count for unjust enrichment against Defendants pursuant to its common law and *parens patriae* authority.

207. As a direct and proximate result of the unlawful conduct described above, Defendants have been and will continue to be unjustly enriched.

208. Defendants have benefited from their unlawful acts, realizing billions of dollars in revenues and profits through the collection, accumulation, harvesting, use, and monetization of vast amounts of Arkansans' PII.

209. Defendants have further been enriched via deceptive conduct in the sale of goods to Arkansas consumers.

210. It would be inequitable and not in good conscience for Defendants to retain any ill-gotten gains earned as a result of the conduct alleged herein, which gains would not exist but for the victimization of users, by Defendants, in the State of Arkansas.

211. Defendants have retained this significant benefit despite their knowledge and understanding of the harms described herein.

212. Arkansans have suffered and will continue to suffer significant detriments, in the form both of privacy harms and financial harms as described herein, because of Defendants' continued practices relating to the Temu app.

213. The State requests an order from the Court compelling Defendants to disgorge proceeds that they unjustly received, including but not limited to the value of the intellectual property derived therefrom, because of its collection, harvesting, use, and monetization of Arkansans' PII, as well as the profits realized from deceptive sales practices, that Defendants obtained knowing that such conduct caused significant detriment to Arkansans.

VI. JURY DEMAND

214. The State demands a trial by jury.

VII. PRAYER FOR RELIEF

215. Based on the unlawful acts described herein, the State of Arkansas is entitled to an Order from this Court:

a. Declaring Defendants' actions unlawful, unconscionable, and deceptive to Arkansas consumers under Ark. Code Ann. § 4-88-101, *et seq.*;

b. Declaring Defendants' actions to be in violation of Ark. Code Ann. § 4-110-101, *et seq.*;

c. Declaring that Defendants were unjustly enriched;

d. Preliminarily and permanently enjoining Defendants from continuing to treat Arkansas consumers unlawfully, unconscionably, and deceptively in the ways described herein;

e. Awarding the State civil penalties of $10,000 per violation of the ADTPA;

f. Awarding all other monetary and equitable relief deemed proper by the Court;

g. Awarding the State its expenses for expert witnesses, reasonable and necessary costs incurred in pursuing this action, including reasonable attorneys' fees, and prejudgment and post-judgment interest at the highest lawful rates; and,

h. Granting such other and further relief as this Court deems just and appropriate.

Respectfully submitted,

TIM GRIFFIN
ATTORNEY GENERAL

By: 

Charles J. Harder, ABN 86080
Deputy Attorney General
Telephone: (501) 682-4058
Facsimile: (501) 681-8118
Chuck.Harder@ArkansasAG.gov

Matthew M. Ford, ABN 2013180
Senior Assistant Attorney General
Telephone: (501) 320-3069
Facsimile: (501) 682-8118
Matthew.Ford@ArkansasAG.gov

Brittany Edwards, ABN 2016235
Senior Assistant Attorney General
Telephone: (501) 682-8114
Facsimile: (501) 682-8118
Brittany.Edwards@ArkansasAG.gov

Philip D. Carlson*
Brian E. McMath*
Brian L. Moore*
Nachawati Law Group
5489 Blair Road
Dallas, Texas 75231
Telephone: (214) 890-0711
bmoore@ntrial.com
pcarlson@ntrial.com
bmcmath@ntrial.com

*To be admitted pro hac vice

David F. Slade, ABN 2013143
Wade Kilpela Slade
1 Riverfront Place, Suite 745
North Little Rock, Arkansas 72114
slade@waykayslay.com