Filed in Lancaster District Court
*** EFILED ***
Case Number: D02CI250002002
Transaction ID: 0023396611
Filing Date: 06/11/2025 04:28:29 PM CDT

IN THE DISTRICT COURT OF LANCASTER COUNTY, NEBRASKA

STATE OF NEBRASKA ex rel. MICHAEL T. HILGERS, Attorney General, *Plaintiff*, v. PDD HOLDINGS, INC. F/K/A PINDUODUO INC., and WHALECO, INC. D/B/A/ TEMU, *Defendants*.	Case No. CI 25-________ **COMPLAINT**

The State of Nebraska, *ex rel.* Michael T. Hilgers, Nebraska Attorney General, by and through the undersigned attorneys ("Attorney General," "State of Nebraska," or "State") brings this action against Defendants PDD Holdings Inc. f/k/a Pinduoduo Inc. and Whaleco Inc. d/b/a Temu ("Temu") (collectively, "Defendants"), for violations of the Consumer Protection Act, Neb. Rev. Stat. § 59-1601 et seq. ("CPA") and the Uniform Deceptive Trade Practices Act, Neb. Rev. Stat. § 87-301 et seq. ("UDTPA").

Temu has flooded the United States with cheap products, but those products come with a one-two punch to Americans. First, Temu's app operates as malware; its code is designed to exfiltrate an enormous amount of sensitive information, from access to a user's microphone, pictures, and messages, to information sufficient to track their movements. The app is further designed to avoid detection from white hat operators. This sensitive information that is unlawfully exfiltrated to Temu naturally flows to its powerful patron—the Chinese Communist Party. In the United States's great power competition with China, Temu presents yet another way in which China can extract and exploit information about Americans for its own purposes.

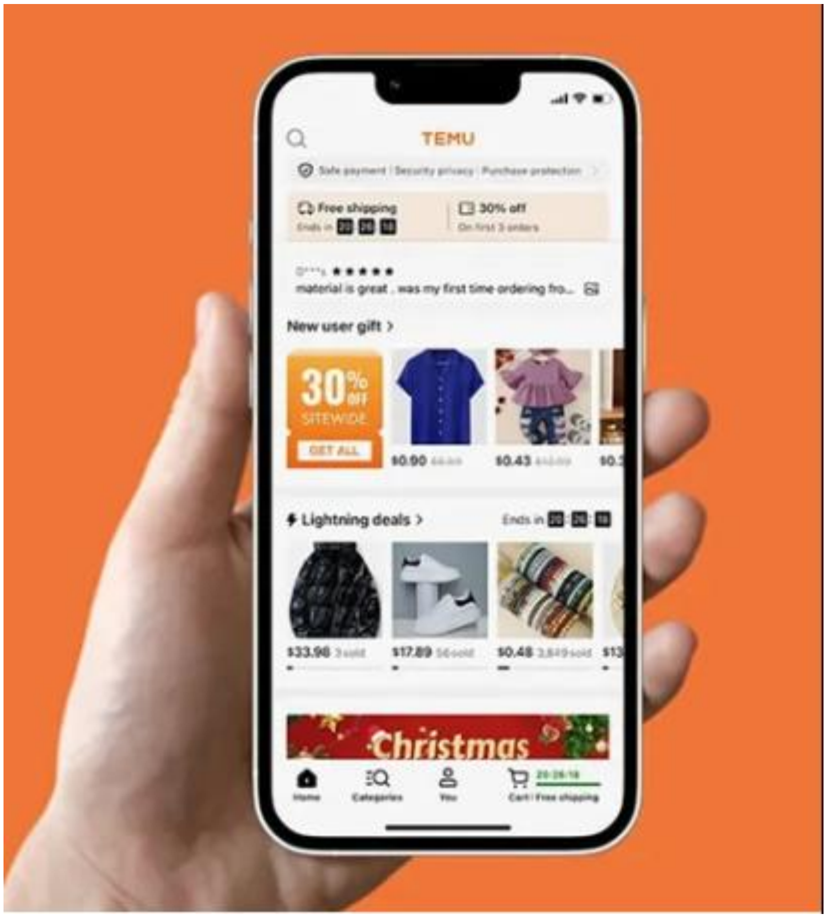
Second, Temu's platform fuels a whole host of other harms. The examples are legion: the platform is awash in products infringing copyrights and other intellectual property, Temu engages in "greenwashing," and it has platformed sellers who use forced labor for the production of goods.

As a consequence of these actions, and the deceptive statements and omissions intended to mislead Nebraskans and entice them to use its platform, the Attorney General brings this action. The Attorney General seeks to protect Nebraska consumers, brands, businesses, creators, and children from Temu's unlawful practices, hold Temu accountable, and put a stop to its conduct.

In support thereof, the State of Nebraska alleges the following:

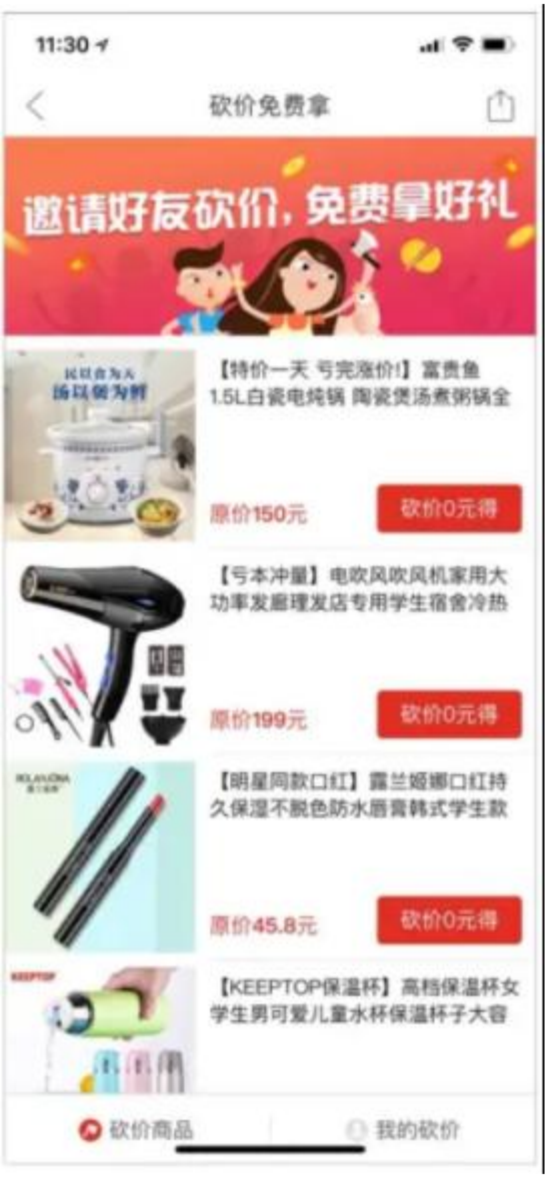
I. INTRODUCTION

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



D***s ★★★★★
material is great , was my first time ordering fro...

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



【特价一天 亏完涨价!】富贵鱼 1.5L白瓷电炖锅 陶瓷煲汤煮粥锅全

原价150元

【亏本冲量】电吹风吹风机家用大功率发廊理发店专用学生宿舍冷热

原价199元

【明星同款口红】露兰姬娜口红持久保湿不脱色防水唇膏韩式学生款

原价45.8元

【KEEPTOP保温杯】高档保温杯女学生男可爱儿童水杯保温杯子大容

3. 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 three separate advertisements that Temu aired during the 2024 Super Bowl, as well as two additional

advertisements aired immediately following the game.[1] The advertisements "featured animated characters using the app to transform their lives to the tune of 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]

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

5. Along with a bevy of cheap goods, Temu has brought with it a host of security and privacy concerns for Americans.

6. In mid-2023, for example, Apple suspended the Temu app from the Apple App Store for misrepresentations Temu had made regarding the descriptions about the types of data the app can access or collect from users, how it does so, and for what purposes it uses that data.[5] Similarly, Google suspended the Pinduoduo app (the forerunner of Temu and the app of its parent company)

[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) (available at https://www.businessinsider.com/temu-spends-millions-super-bowl-ads-effort-win-us-users-2024-2)

[2] *Id.*

[3] Sarah Perez, *Temu was the most-downloaded iPhone app in the US in 2023*, TechCrunch (Dec. 12, 2023) (available at https://techcrunch.com/2023/12/12/temu-was-the-most-downloaded-iphone-app-in-the-u-s-in-2023/)

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

[5] Clothilde Goujard, *Booming Chinese shopping app faces Western scrutiny over data security*, Politico (Jul. 24, 2023) (available at https://www.politico.eu/article/booming-chinese-shopping-app-temu-faces-western-scrutiny-over-data-security-2/)

from its Google Play Store in March 2023 after it was found to contain malware.[6]

7. A number of news outlets and technologists have engaged in their own, granular investigations. These investigations—involving review of the Temu app source code, documentation, network traffic and/or other dynamic or static analyses—revealed that the Temu app has multiple hallmarks of spyware and malware.

8. The State has conducted its own independent forensic investigation of the Temu app, including a review of its code.

9. The State's investigation has revealed that the Temu app is designed to collect sensitive user data without the user's knowledge or consent and is purposely designed so that it can evade detection of this type of data collection by third-party security researchers.

10. For example, Temu collects a shocking amount of sensitive user data ("Personally Identifiable Information," or "PII") well beyond what would be necessary in the ordinary course of business for an online shopping app. Some examples include a user's granular geolocation ("GPS"), lists of all other apps the user has installed on their phone and all of the accounts that a user has established with other apps on their phone, and the cellular data and WiFi networks the user's phone is connected to as well as all WiFi networks that are detected by the phone.

11. This exfiltration of data happens without a user's knowledge or consent. Not only does Temu fail to disclose the depth and breadth

[6] Helen Davidson, *Addictive, absurdly cheap and controversial: the rise of China's Temu app*, The Guardian (Oct. 5, 2023) (available at https://www.theguardian.com/world/2023/oct/06/addictive-absurdly-cheap-and-controversial-the-rise-of-chinas-temu-app)

of its data collection practices to consumers, Temu actively seeks to prevent its conduct from being discovered.

12. In fact, review of the Temu app's code shows that it is purposely designed to evade front-end security review. For example, Temu uses code to "sniff out" potential forensic tools or settings in order to determine whether it is being examined by a third-party reviewer.

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

14. The sensitive PII that Temu collects from Nebraska citizens is accessible by individuals and entities subject to Chinese law and beholden to China's communist regime. 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. Upon information and belief, the data Temu is illicitly collecting from Nebraska users is being sent to and used by the Chinese government.

15. 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 foreign adversaries" such as TikTok, WeChat, and Telegram—from government devices due to the significant threats posed to users' security and privacy.[7]

[7] Marvie Basilan, *After TikTok, Montana Bans WeChat, Temu And Telegram From Government Devices*, International Business Times (May 18, 2023) (available at

Likewise, Defendants are currently the subject of a congressional investigation based on "concerns about Temu and the amount of data collected."[8]

16. Defendants have sought to maximize their access to and collection of users' PII—both for profit and potentially for more nefarious geopolitical objectives—by employing unfair and deceptive trade practices. The app is designed, essentially, to hack users' mobile devices the moment it is downloaded, acquiring access to troves of sensitive information, in ways that are associated with pernicious spyware and malware.

17. In addition to Defendants' unsafe and illicit data collection, the Temu app is awash in products that flagrantly infringe upon, or simply copy outright, intellectual property owned by U.S.-based businesses large and small.[9] As of the date of this filing, Temu features dozens of what appear to be unlicensed products claiming to be from traditional Nebraska brands like Union Pacific, Cabela's, the University of Nebraska Cornhuskers, and the Creighton Bluejays.

18. Accordingly, the State brings this action pursuant to the CPA and UDTPA and seeks a preliminary and permanent injunction preventing Defendants from acquiring, maintaining, and otherwise utilizing the PII of Nebraska residents, preventing Defendants from allowing widespread intellectual property

https://www.ibtimes.com/after-tiktok-montana-bans-wechat-temu-telegram-government-devices-3694060).

[8] 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) (available at https://d1dth6e84htgma.cloudfront.net/CCP_Marketplace_Letter_to_Whaleco_Inc_Temu_7f921e1a67.pdf).

[9] Chow, Andrew. *Designers are Accusing Temu of Selling Copies of Their Work*. Time.com (Jan. 16, 2024) (available online at https://time.com/6342387/temu-copy-work/).

infringement to the detriment and confusion of Nebraska consumers, and further seeks civil penalties in light of Defendants' conduct as well as all other available relief allowed by law.

II. PUBLIC INTEREST

19. The Attorney General files this action in the public interest of the citizens of the State of Nebraska, bringing this lawsuit pursuant to the CPA, the UDTPA, and his statutory and common law authority, powers, and duties.

III. PARTIES

The State of Nebraska

20. The State of Nebraska, by and through its Attorney General, brings this action as the Chief Law Enforcement Officer of the State of Nebraska charged with the enforcement of the CPA and the UDTPA. The Attorney General brings this action on behalf of the people of the State of Nebraska to protect the State, its general economy, and its residents from Defendants' unlawful business practices.

PDD Holdings Inc. f/k/a Pinduoduo Inc.

21. Defendant PDD Holdings Inc. ("PDD Holdings") was founded in China in 2015 under the name Pinduoduo, and is registered in the Cayman Islands. It owns and operates a portfolio of businesses and is listed on the Nasdaq exchange in the United States. 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 (Co-Defendant 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.[10] However, it continues to have significant operations in China, with multiple subsidiaries located within that country.

22. PDD Holdings is traded on the NASDAQ stock exchange with the ticker name PDD and files annual reports with the U.S. Securities and Exchange Commission (SEC).

Whaleco Inc. d/b/a Temu

23. 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 operated by Defendant PDD Holdings.

Alter Ego and Single Enterprise Allegations

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

25. At all relevant times, Defendant PDD Holdings has directed the operations of Defendant Temu with respect to the Temu app, and Defendant Temu has reported to Defendant PDD Holdings. Defendant PDD Holdings has made, and continues to make, key strategy decisions for the Defendant Temu.

26. Defendant Temu and Defendant PDD Holdings have significant overlap of executive officers of each corporation.

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

27. Defendant PDD Holdings' most recent Form 20-F filing with the SEC state that the purpose of the Temu platform is to "primarily serve merchants in China, assisting them in reaching customers and growing sales."

28. This "primary" purpose of the Temu platform is accomplished by Defendant PDD Holdings directing the operations of Defendant Temu in the United States, and the State of Nebraska, to facilitate transactions between Nebraska consumers and Chinese merchants in part using data and information gathered about Nebraska consumers unlawfully, as described below.

29. Moreover, employees from PDD Holdings performed work on the Temu app, including software engineers who previously developed the Pinduoduo app for PDD Holdings.

30. Defendants' Temu app contains significant code overlap with Defendants' Pinduoduo app, including proprietary code and app programming components copied directly from the Pinduoduo app into the Temu app that are central to Defendants violation of Nebraska law, discussed infra at ¶¶ 106 through 110.

31. 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 the other Defendant, 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 Defendant and/or directed, authorized, affirmed, consented to, ratified, encouraged, approved, adopted and/or participated in the acts or transactions of the other Defendant.

32. 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, 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.

IV. JURISDICTION AND VENUE

33. At all times relevant to this Complaint, Defendants were in trade and commerce affecting consumers in Nebraska insofar as they operate an e-commerce platform (the Temu app) which has been intentionally directed towards, marketed to, and downloaded by citizens of the State of Nebraska. Defendants have engaged in myriad commercial transactions with Nebraska residents, taking payment from those residents in Nebraska-based commercial transactions and sending various products to those Nebraska residents, in the State of Nebraska. Defendants were—and remain—in possession of and/or have or have had control over sensitive PII of Nebraska residents.

34. This Court has personal jurisdiction over Defendants because the conduct and injuries from which the Complaint arose took place in Nebraska, harmed Nebraskans, and specifically targeted Nebraskans.

35. This Court has jurisdiction over the subject matter of this action under Neb. Rev. Stat. §§ 59-1608.01, 87-303.05(1), and 87-806 because Defendants, directly and through their subsidiaries, transacted business within the State of Nebraska at all times relevant to this Complaint.

36. The Attorney General, as Nebraska's chief law enforcement officer, is expressly authorized to enforce Nebraska's consumer protection laws, including the CPA and the UDTPA. Neb. Rev. Stat. §§ 59-1608; 59-1614; 87-806; 87-303.05; 87-303.11.

37. In addition to his express statutory authority, the Attorney General has standing to bring a legal action, in the name of the State, when the object of that action is a suit to vindicate the public interest.

38. Venue for this action properly lies in Lancaster County, Nebraska, pursuant to Neb. Rev. Stat. §§ 59-1608.01 and 87-806.

V. FACTUAL BACKGROUND

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

39. 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 gross merchandise value (GMV) in 2021, alone.

40. Among other business activities, PDD Holdings operates Pinduoduo, an e-commerce app created in China that offers consumer products across a spectrum of categories.

41. 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'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."[11]

42. 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,[12] thus incentivizing the proliferation of the app on social media platforms.

43. 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 in an effort 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' business operations, including several subsidiaries, continue to be located in China.

B. The Pinduoduo App Has Been Deemed to Be Malware by Security Experts and Was Banned From Google's App Marketplace.

44. On March 21, 2023, Google suspended the Pinduoduo app from the Google Play Store after malware issues were found on the app.[13] 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. For example, CNN conducted a detailed investigation in which it spoke to half a dozen cybersecurity teams from Asia, Europe and

[11] PDD Holdings, Form 20-F Annual Report (2022).

[12] *What is Temu*, NPR, Planet Money (March 22, 2024) (available at https://www.npr.org/transcripts/1197958526?ft=nprml&f=1197958526)

[13] Baranjot Kaur and Abinaya Vijayaraghavan, *Google suspends China's Pinduoduo app on security concerns*, Inside Retail (March 24, 2023)

the United States, as well as multiple former and current Pinduoduo employees. According to those sources, while many apps collect significant amounts of user data, sometimes without explicit consent, Pinduoduo took violations of privacy and data security "to the next level."[14]

45. Among other things, the expert sources found that the app was programmed to bypass users' cell phone security in order to monitor and record a user's activities across their phone—everything from "checking notifications," "monitor activities on other apps," and even "read private messages and change settings."[15]

46. According to one report by an IT security firm, "Pinduoduo requested as many as 83 permissions, including access to biometrics, Bluetooth, and Wi-Fi network information."[16] The purpose of this was, "to spy on users and competitors, allegedly to boost sales," according to a company insider.[17]

47. The Pinduoduo app also had the ability to spy on competitors by tracking activity on other apps on the user's phone and getting information from them, which is contrary to Apple's and Google's app store policies.[18]

[14] Nectar Gan, Yong Xiong and Juliana Liu, *'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) (available at https://www.cnn.com/2023/04/02/tech/china-pinduoduo-malware-cybersecurity-analysis-intl-hnk/index.html).

[15] *Id.*

[16] Nicholas Foisy, *Temu App Poses Potential Data Risk for Consumers*, Compass IT Compliance (Jun. 30, 2023) (available at https://www.compassitc.com/blog/temu-app-poses-potential-data-risk-for-consumers)

[17] *Id.*

[18] Nectar Gan, Yong Xiong and Juliana Liu, *'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) (available at https://www.cnn.com/2023/04/02/tech/china-pinduoduo-malware-cybersecurity-analysis-intl-hnk/index.html).

48. According to a current Pinduoduo employee, the company established a team of 100 engineers and product managers "to dig for vulnerabilities in Android phones, develop ways to exploit them – and turn that into profit."[19]

49. According to the company insider source, who requested anonymity for fear of reprisals, "[t]he goal was to reduce the risk of being exposed."[20]

50. Moreover, once the app was installed, the app was able to continue running in the background and prevent itself from being uninstalled.[21]

51. One security researcher interviewed by CNN described Pinduoduo as "the most dangerous malware" ever found among mainstream apps.[22]

52. 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. As discussed above, these functions were not accidental—they were intentionally built into the app.

53. Moreover, even after Defendants made changes to the Pinduoduo app in response to the suspension, 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.

[19] *Id.*
[20] *Id.*
[21] *Id.*
[22] *Id.*

54. On March 5, 2023, Pinduoduo issued a new update of its app, version 6.50.0, which purported to remove the exploits. Researchers who investigated the update confirmed, however, that the underlying code was still there and could be reactivated to carry out attacks.[23] Further, two days after the update, Pinduoduo disbanded the team of 100 engineers and product managers who had developed the exploits, according to a Pinduoduo source.[24]

55. Thereafter, most of the members on this team were transferred to work at Temu.[25]

C. In 2022, PDD Holdings Developed the Temu App, Which is Modeled on Pinduoduo—Including Through Its Design and Code—and Which Defendants Aggressively Market in the United States and in Nebraska.

56. In 2022, Defendants developed the Temu app, meant to be a global version of the Pinduoduo platform, with the United States as its principal market.[26]

57. Since that time, Defendants have heavily promoted the Temu app, including through television advertisements, large online ad campaigns, and sponsorships.

58. As described, *supra*, the same large team of software engineers and product managers from Pinduoduo—whose principal mission was to identify exploitations in the Android operating system and incorporate them into the app—were transitioned to working on

[23] *Id.*

[24] *Id.*

[25] *Id.*

[26] PDD Holdings, Form 20-F Annual Report (2022).

the Temu app within a year of Temu's introduction into the marketplace.[27]

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.[28]

60. 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.[29] As a result, the market capitalization of Defendant PDD Holdings has swelled to over $139 billion.[30]

61. Temu is responsible for tens of millions of shipments that are sent to the United States each year—including via purchases made, finalized, and received in Nebraska—through Temu's network of more than 80,000 China-based sellers participating in its online marketplace.[31]

[27] Nectar Gan, Yong Xiong and Juliana Liu, *'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) (available at https://www.cnn.com/2023/04/02/tech/china-pinduoduo-malware-cybersecurity-analysis-intl-hnk/index.html).

[28] https://selectcommitteeontheccp.house.gov/sites/evosubsites/selectcommitteeontheccp.house.gov/files/evo-media-document/fast-fashion-and-the-uyghur-genocide-interim-findings.pdf.

[29] Sarah Perez, *Temu was the most-downloaded iPhone app in the US in 2023*, TechCrunch (Dec. 12, 2023) (available at https://techcrunch.com/2023/12/12/temu-was-the-most-downloaded-iphone-app-in-the-u-s-in-2023/)

[30] https://finance.yahoo.com/quote/PDD/

[31] https://selectcommitteeontheccp.house.gov/sites/evo-subsites/selectcommitteeontheccp.house.gov/files/evo-media-document/fast-fashion-and-the-uyghur-genocide-interim-findings.pdf.

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

62. 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 Nebraska law.

63. This 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 access (undetected) 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. *See, supra.*

64. Indeed, in or about that same time period, 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 misleading users regarding how their data was being used: "Apple…said it had found that 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, said Apple. Temu also isn't letting users choose not to be tracked on the internet [which is an option that all apps in Apple's online marketplace are required to provide to users]."[32]

65. As one commentator observed following the State of Montana's decision to ban the app, the Temu app is "dangerous," due to the

[32] Clothilde Goujard, *Booming Chinese shopping app faces Western scrutiny over data security*, Politico (Jul. 24, 2023) (available at https://www.politico.eu/article/booming-chinese-shopping-app-temu-faces-western-scrutiny-over-data-security-2/)

fact that it "bypasses" phone security systems to read a user's private messages, make changes to the phone's settings and track notifications.[33]

66. The State's own forensic investigation of the Temu app reveals a host of troubling conduct, including but not limited to the following:

    a. The app is designed to allow for extensive data exfiltration from all corners of a user's mobile device.

    b. The app is designed to hide its exfiltration of sensitive information, both from users and even from any researcher who might be investigating the app's functionality.

    c. The app contains multiple portions of code that are recognized by cybersecurity professionals as hallmarks of spyware and malware.

    d. The app contains code that allows it to reconfigure itself even after having been downloaded to a user's phone, without the user's knowledge or consent.

    e. The app incorporates large swaths of Pinduoduo's previously banned code, wholesale.

67. These concerns are addressed more fully as follows:

i. Design and Programming That Intentionally Evades Scrutiny

[33] Marvie Basilan, *After TikTok, Montana Bans WeChat, Temu And Telegram From Government Devices*, International Business Times (May 18, 2023) (available at https://www.ibtimes.com/after-tiktok-montana-bans-wechat-temu-telegram-government- devices-3694060).

1. <u>Dynamic recompilation using the "Manwe" tool</u>

68. Multiple versions of the Temu app have a patching capability through a home-built framework known as "Manwe," which is an unpacking and patching tool (also called a software development kit or "SDK") also found in the malicious versions of Pinduoduo.

69. Manwe enables Temu to circumvent the protections of the Apple App Store or the Google Play Store, by directly patching the app on the device rather than through releasing updates via those stores.

70. The code's functionality is startling—it enables the app to change its behavior *on the user's phone*, without anyone being able to know, much less prevent, such a change.

71. This allows the Temu app to pass all required tests for approval into the Google Play Store or Apple App Store, while retaining the ability to reconfigure itself once it has been downloaded onto a user's device.

72. It thus becomes pointless for Google or Apple to vet Temu for security and privacy risks, because the app is capable of changing itself *after* going through those tests.

73. This is against app store policies, as it enables Temu to push unauthorized code via updates to user devices without Google's or Apple's knowledge—and of course, without the user's knowledge, either.

74. And, as noted below, Temu also borrowed code from Pinduoduo in the form of the ZipPatch library, see ¶ 109, *infra*, which also allows the app to update its code without pushing the update through Google or Apple.

2. Omission of data collection practices from the Temu app manifest file

75. Temu also has hidden its conduct by omitting requested permissions from the “manifest file” of the app.

76. A manifest file is required for every app,[34] and *must* contain certain information, including the permissions that the app needs in order to access protected parts of the system or other apps.[35] 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.”[36]

77. In apparent compliance with these requirements, Temu would either omit or remove the permission requests from the app and its manifest file; despite those omissions, the Temu app would still acquire the corresponding data by other means.

78. One glaring example involves location data. Starting no later than April 2023, Temu removed the permissions ACCESS_COARSE_LOCATION and ACCESS_FINE_LOCATION from its manifest. That omission logically means one thing: Temu was not collecting location data from its users.

79. However, during this time, Temu still was actively collecting user location, including by acquiring data that can be used to infer both approximate and precise location.

[34] Android, *App manifest overview*, Developers - Guides (available at https://developer.android.com/guide/topics/manifest/manifest-intro)

[35] *Id.*

[36] *Id.*

80. What this means is that Temu was creating the impression that it did not want nor use its customers' location data, but in reality was getting the information from sources that it did not need to disclose in the permission manifest.

81. It was not until version 2.4.1 of the app, released on or about September 8, 2023, that Temu reinserted the location data permissions into the app manifest. Tellingly, this change occurred two days after a report was published by a short-seller accusing Temu of a host of privacy-invasive conduct, including Temu's removal of ACCESS_COARSE_LOCATION and ACCESS_FINE_LOCATION from the manifest.

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

82. In addition, Defendants have sought to cover their tracks by removing from the public domain prior versions of files associated with the Temu app. Many websites archive APKs [*i.e.,* versions of an app] published in Google's Play Store, and it is common practice in the industry for developers to have prior APKs of their app exist on these sites. But the Temu app is typically absent from APK archives. Indeed, the historical Temu APKs have been removed from all websites within the jurisdiction of the U.S., making investigative research more difficult. Temu's removal of historical APKs is a highly suspicious deviation from the normal practice of app developers, suggesting that Temu is actively trying to thwart investigation into their app.

4. Detection of "root" access on a device

83. The Temu app checks a user's device to see whether it has "root" access, also known as "super user access." When someone has root

access to a device, they have the highest privilege level that can be given.

84. More importantly for purposes of this Complaint, when an app like Temu seeks to detect root access, it is in an attempt to avoid third-party scrutiny of the app's code. A cybersecurity researcher needs root access on his or her testing device to investigate and evaluate an app's security.

85. Thus, one purpose of an app trying to determine whether a device has root access[37] is to determine whether the app is being used in a "testing" environment. If the app—like Temu—determines that a device has root access, it can surmise that someone is looking into the app's code and therefore needs to hide any behaviors or functions that it does not want to be discovered.

86. The State has directly encountered this particular security countermeasure tool in the course of its own forensic investigation of the Temu app.

5. Searching for "debuggers"

87. Much like root access, security researchers—and security features on mobile devices—may employ a "debugger," which is a tool or program that enables researchers to view the application code while it is running. This is a critical tool for identifying malware that might be hidden within an app.[38]

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

[38] Srinivas, *Debugging for malware analysis*, InfoSec (Aug. 14, 2019) (available at https://www.infosecinstitute.com/resources/malware-analysis/debugging-for-malware-analysis/)

88. Calls in Temu's code include a query Debug.isDebuggerConnected(), which would alert the Temu app if a debugger is engaged on a user's device. Like the root access detection discussed above, this is intended to obstruct or obscure analysis of the app.

6. Code obfuscation

89. Temu employs "code obfuscation," which is the process of making an application difficult or impossible to decompile or disassemble, and the retrieved application code more difficult for humans to parse.[39]

90. Analysis of multiple versions of the Temu app show that the files, folders, classes, and functions of the Temu app are designed, named, and cross-referenced to each other in a highly complex way that is meant to hamper investigation of the malicious aspects of the app.

91. Further, analysis reveals that many of these obfuscated lines of code overlap with code from the Pinduoduo app, which has been imported wholesale in multiple instances to the Temu app.

7. Heavily-encrypted network traffic

92. The Temu app must send and receive information over the Internet in order to function on a user's device. This information is transmitted in what are colloquially known as "packets," and the sending and receiving of packets is known as "network traffic."

93. Ordinarily, apps protect information and data network traffic using a system called Transport Layer Security (TLS), which

[39] https://www.guardsquare.com/what-is-code-obfuscation

encrypts the data in such a way that it can be decrypted, read and understood by the user's device and the server communicating with the device, but cannot be decrypted, read, or understood by any other party that may handle or intercept the network traffic.

94. TLS is one pillar on which the modern Internet is built and is so secure that it is regularly relied on to protect the most sensitive types of personal information transmitted digitally, including financial and banking information and federally protected health information while that information is in transmission between a secure server and a user's device.

95. Even apps that deal with the most sensitive types of user data usually do not apply additional layers of encryption beyond TLS to data that is being transmitted between a user's device and the app's servers.

96. The Temu app, on the other hand, uses at least three layers of encryption beyond ordinary TLS to obfuscate data that the app transmits from a user's device to Temu's servers. This method of encrypting data applies the same encryption algorithm at least four times in succession, and essentially layers four distinct levels of encryption nested within each other like Russian dolls. When one layer of the encryption is decrypted, it contains some readable data and additional data that is further encrypted and requires a different hidden passkey to decrypt.

97. Critically, this multi-level of encryption makes it exceedingly difficult—and at times, entirely impossible—to see the precise data or even *types* of data that are being transmitted to and from the Temu app. In turn, this makes it easier for Temu to send surreptitiously acquired PII from a user's device without being caught.

98. The State's technical analysis has been able to decrypt some (but not all) of the layers of encryption the app applies to the data it transmits to Temu servers. The State's investigation discovered that some deeper layers of encrypted data transmitted to Temu's servers by the app contains information about the device that is never disclosed to the user, including specific information about the user, the device, and the way the user interacts with the device outside of the Temu app.

ii. Overlap with Pinduoduo Code

99. Analysis of the code of both the Pinduoduo app and the Temu app demonstrates the deep connection between Temu and its malware-ridden Chinese counterpart. The Temu app imported, wholesale, large swaths of code from Pinduoduo, including exact copies of code already deemed by experts to be malicious malware. Initial review provides the following examples:

1. <u>Package name overlap</u>

100. Multiple packages of code within the Temu app are lifted wholesale from Pinduoduo. Conceptually, a "package" is a way of organizing related code, much like the folders on one's computer that are used to keep files organized. Like the files on one's computer, packages must be named. Multiple packages in the Temu app begin with the naming convention "com.xumeng.pinduoduo," and are proprietary, non-public packages, meaning that they were developed by PDD and were copied wholesale from the Pinduoduo app and pasted into Temu.

2. <u>Further, specific code overlap</u>

101. Analysis reveals that thousands of lines of code overlap between Pinduoduo and Temu. It bears noting that in the Temu code, package names containing the overlapping code often are

obfuscated, while in Pinduoduo, they are not. This likely is in an effort to hide the fact that Temu contains Pinduoduo code.

102. The code that overlaps between Temu and Pinduoduo is not benign. For example, both Pinduoduo and Temu contain identical lines of code in the following classes, which in turn deal with the following functionality:

- PhoneInfoManager – the code in this class deals with device identifier collection—including IMEI and MAC Address. The precise data points collected, and the privacy-invasive impact of that collection, are discussed below.

- StorageUtils – the code in this class involves methods for access to user files on their mobile device.

- SecureNative – this code involves custom encryption (i.e., obscuring the two apps' activities).

- ZipPatch – this code is a native library that allows each app to update their respective code without requiring a publishing of the update to the Apple store or Google Play, or with the knowledge or consent of users.

3. SDK overlap

103. SDKs—otherwise known as Software Development Kits—are distinct libraries of code meant to perform specific functions. Some SDKs handle identifying and compiling statistics about app performance, others serve targeted ads, others render graphics in an app, etc. Temu and Pinduoduo have always had an overlap of multiple SDKs, with an overlap of 34, at their historical peak. One of the most pernicious overlaps of SDKs is the Manwe SDK, discussed above.

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

104. As discussed above, 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 the sensitive PII contained therein.

1. Users' granular location data

105. Analysis reveals that the Temu app gains access to user's "fine" location—that is, the app gets user's real-time GPS location within an accuracy of at least 10 feet. As discussed above, the permission, ACCESS_FINE_LOCATION, historically was removed from the Temu app's Android manifest for a period of time in 2023, only to reappear after public reporting called out Temu for this conduct, demonstrating an intent to keep this functionality hidden from the public.

106. Regardless of whether Temu was or was not listing ACCESS_FINE_LOCATION (or ACCESS_COARSE_LOCATION, for that matter) at any point in its history, it was simultaneously acquiring data points from users that allowed Temu to determine users' location even without these permissions. In other words, Temu was collecting data that would enable it to bypass the location permissions in Android, and simply get its information in a different, more concealed, way.

107. Although recent versions of the app now include ACCESS_FINE_LOCATION, Temu has still never disclosed in its consumer-facing privacy policies that it collects a user's fine location data.

2. WiFi access points

108. The Temu app contains the permission ACCESS_WIFI_STATE, which enables it to collect the name and signal strength of WiFi networks utilized by the individual's device, as well as all WiFi networks that are near a user's device, whether or not the device is connected to those networks.

109. Collecting these data points over time enables the Temu app to create a detailed map of a user's travels throughout the day. When aggregated, these data points provide a detailed map of any place that Temu users have been, whether or not those users ever consented to providing geolocation data.

110. This type of data already has been used to create this kind of global mapping. Recently, the company Niantic announced that it would be building a "Large Geospatial Model" (LGM) that combines millions of scans taken from the smartphones of players of its popular app, Pokémon Go. As explained by Niantic's chief scientist, "Using the data our users upload when playing [our] games…we built high-fidelity 3D maps of the world, which include both 3D geometry (or the shape of things) and semantic understanding (what stuff in the map is, such as the ground, sky, trees, etc)."[40]

3. Microphone and camera access

111. Two permissions that Temu includes its app are requests for CAMERA and RECORD_AUDIO, surreptitiously granting the app access to all of the audio and visual recording and storage

[40] https://www.theverge.com/2024/11/19/24300975/niantic-pokemon-go-data-large-geospatial-model

functions of a user's device. These permissions are not adequately disclosed to users.

4. Intentional Android exploit: ActivityManager.getRunningTasks

112. The Temu app code contains the method ActivityManager.getRunningTasks. This method was actually deprecated by Android over a decade ago, with the release of Android 5.0 (Lollipop) on November 4, 2014. This was because of its ability to be exploited by developers seeking to acquire a user's personal information, largely in the form of being able to view a user's app usage patterns across their entire device (i.e., it enables Temu to view activity of *all* running apps on a user's phone, and not just activity related to the Temu app).[41]

113. What is particularly concerning about the inclusion of this method within Temu's code is that, as explained above, it was deprecated over a decade ago, [42] in November 2014. Because Temu was not founded until 2022, this means that there was *never* a benign reason for Temu to include this method in its code. Instead—and consistent with Defendants' employment of 100 engineers and product managers to identify and incorporate Android exploits into the Temu and Pinduoduo apps—the only reason to include this method is in furtherance of a purposeful and opportunistic exploit of users who have devices running older operating systems.

114. This analogizes to a thief walking down the street and trying the door of every car and house to see if they are locked. In

[41] https://www.droidcon.com/2022/02/08/accessing-app-usage-history-in-android/

[42] In the context of software development, "deprecated" refers to a feature, function, or method that is considered outdated or no longer recommended for use, but is still supported. While it still functions, its use is discouraged because newer, more efficient, or secure alternatives are available.

most instances, they will be, but in the rare event that a door is not locked (meaning a user is using an older device with an older operating system, as would be common in certain populations like elderly users), the thief can take advantage of this security lapse and take whatever they wish from inside.

115. Additionally, the use of ActivityManager.getRunningTasks allows Temu to collect runtime metadata from files on a device like "proc/self/maps," "proc/self/cmdline," and "proc/self/environ," which is a common technique to detect debuggers. *See* ¶¶ 94 and 95, *supra*.

5. Intentional Android exploit: android.telephony.TelephonyManager.listen( )

116. Android Developer documentation explains that this method "[p]rovides access to information about the telephony services on the device. Applications can use the methods in this class to determine telephony services and states, as well as to access some types of subscriber information. Applications can also register a listener to receive notification of telephony state changes."[43]

117. Telephony information, broadly, includes information about the telephony services such as subscriber ID, SIM serial number, phone network type, as well as the phone state (status of ongoing calls, phone number, etc.).

118. Critically, *both* android.telephony.TelephonyManager.listen() and ActivityManager.getRunningTasks have been identified as prima

[43] https://developer.android.com/reference/android/telephony/TelephonyManager

facie evidence of malware in at least one recent paper on digital security, which states

> android.telephony.TelephonyManager.listen() and android.app.ActivityManager.getRunningTasks() are sensitive APIs that can violate users' privacy" and are identified as useful heuristics when training models to identify malware at scale.[44]

6. Lists of all apps installed on user's device

119. Temu contains code that allows it to identify all of the applications installed on a user's device, via the method getPackageManager().getInstalledPackages.

120. Such behavior violates the "sandbox" established by both Apple and Google for their respective operating systems (iOS and Android). In short, sandboxing is a principle that keeps one app from gathering data about other apps on a user's device. This privacy-protective principle is self-explanatory: no one app has any need for—nor any business in obtaining—information about the other apps on an individual's device.

121. Additionally, Temu utilizes "query" commands, which seek information about various aspects of a user's device. Initially, Temu utilized broad terms, enabling it to get an exhaustive list of the installed applications on a user's device.

122. The State's analysis revealed that such queries would return data that includes, but is not limited to: (1) the name of

[44] Cai, *et al.* - *JOWMDroid: Android malware detection based on feature weighting with joint optimization of weight-mapping and classifier parameters,* Computers & Security, Vol. 100 (Jan. 2021), 102086

every installed app on a user's device; (2) likely install and update timestamps; (3) the version of the installed app; and (4) unknown flags and IDs for each entry.[45]

123. More recently, in response to efforts by Android to prevent this kind of behavior—that is, preventing one app from getting an exhaustive list of other apps on a user's device without the user's notice or consent—Temu has reigned in its queries to address specific apps. However, the queries still search for a wide array of specific apps across a continuum of categories. These apps and categories include, but are not limited to:

- Social Media and Messaging: WhatsApp, Facebook, Instagram, Snapchat, Signal, Telegram, Line, and Discord.
- Financial and Payment Apps: PayPal, Klarna, AfterPay, MobilePay, Toss, Swish, and Satispay.
- Miscellaneous: Google Play Store, Google Maps, and the Samsung Galaxy Store.

7. List of all of the accounts a user has stored on the phone

124. Forensic analysis also reveals that the Temu app has contained, at different points in time, the GET_ACCOUNTS permission. Per Android, this permission "[a]llows access to the list of accounts in the Accounts Service."[46]

[45] As explained in paragraphs 52-53, *supra*, the purpose of this data collection was done by Defendants in order "to spy on users and competitors, allegedly to boost sales."

[46] https://developer.android.com/reference/android/Manifest.permission#GET_ACCOUNTS

125. The Android developer guidance further explains that this means an app with this permission gets access to the device's AccountManager code, which is a "class [that] provides access to a centralized registry of the user's online accounts."[47]

126. Virtually everyone that has a smart device also has scores of apps that require having an account: social media, dating, banking, health, email, travel, mental wellbeing, exercise, entertainment—the list is practically infinite. Temu does not disclose to its users that it accesses the centralized registry of these online accounts.

8. Additional sensitive PII

127. Temu also 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. Some of the items of PII that Temu collects include:

128. **International Mobile Subscriber Identity ("IMSI")**: these are uniquely identifying data points that are associated with each mobile phone's unique SIM card. They also are instrumental in allowing an individual's device to switch from cell tower to cell tower as the individual moves. This means that if you have an individual's IMSI, you can track that individual without their knowledge or consent.

129. **Media Access Control ("MAC") Address**: a user's MAC address is a unique, 12-digit hexadecimal number assigned to a specific device (for example, e0:6c:4f:8b:aa:d7). A MAC address uniquely identifies your device to each network to which it connects. Therefore, like the IMSI discussed above, MAC

[47] https://developer.android.com/reference/android/accounts/AccountManager

addresses are used to track an individual's location as they move from WiFi network to WiFi network. For example, it has been shown that possible to use MAC addresses to track the wireless devices.

130. **International Mobile Equipment Identity ("IMEI")**: Like the other data elements described in this section, an IMEI is a unique identifier that is associated with a given individual's device. And, just like the above-identified PII, an IMEI can be used to identify a specific individual's location over time, along with that individual's usage of his or her device, more generally. Beyond unauthorized tracking, an IMEI can be used to clone an individual's device, leading to identity theft and other fraud.[48]

131. **Android Advertising ID ("AAID")**: this is a unique identifier used to track an individual's activity over time and across the various apps or websites he or she engages with. As the name suggests, it is used for advertising purposes—that is, data profilers will use this PII to record an individual's activity, and then draw inferences about the person based on that information (ostensibly in hopes of serving targeted ads to the person that are likely to result in a sale).

E. Users Do Not Consent to Defendants' Data Collection Practices.

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

[48] https://devicesafety.org/should-you-keep-your-imei-number-hidden-for-enhanced-mobile-security/

133. This is all the more egregious given that Defendants have issued a recent statement to the press in response to online commenters complaining about Temu's data practices, declaring: "At Temu, we prioritize the protection of privacy and are transparent about our data practices."[49]

134. But this is not true. Defendants cannot be said to apprise their users of their conduct. Indeed, Defendants have designed Temu to have secretive and obfuscated code and functions meant to expressly *hide* their conduct from users.

135. Temu's own disclosures to its consumers only confirm its intent to hide its conduct and cannot be said to establish consent on the part of their users. A survey of the operative Privacy Policies in effect from October 17, 2022 through the present show that Temu has kept the conduct challenged in this Complaint hidden from its users.

October 17, 2022[50]

Type of Data	Extent to Which Data Is Addressed in Privacy Policy
Microphone Access (¶ 111)	No mention of seeking microphone access (or of audio, generally)
Camera Access (¶ 111)	Temu states that it only acquires photos provided by the user, in the course of using the Temu platform: "Personal Information We Collect …

[49] Schulz, *What is Temu? What we know about the e-commerce company with multiple Super Bowl Ads*, USA Today (Feb. 12, 2024) (available at https://www.usatoday.com/story/money/2024/02/12/what-is-temu-super-bowl/72573203007/)

[50] Available at https://web.archive.org/web/20221127065309/https:/www.temu.com/privacy-and-cookie-policy.html

	Information You Provide to Us. Personal information you may provide to us through the Service or otherwise includes: … User-generated content, such as profile pictures, photos, images, videos, comments, questions, messages, and other content or information that you generate, transmit, or otherwise make available on the Service, as well as associated metadata.”
Location Data (¶¶ 78-80; 105-110; 127-131)	Temu states that it only collects location data through device data (which it states can only identify “general location”) or when a user provides authorization: “Automatic data collection. We, our service providers, and our business partners may automatically log information about you, your computer or mobile device, and your interaction over time with the Service, our communications and other online services, such as: … Device data, such as…general location information such as city, state or geographic area. … Location data when you authorize the Temu mobile app to access your device’s location.”
WiFi Access Points (¶¶ 108-110)	No mention of WiFi Access Points. The only time “Wi-Fi” appears in the document is under “Automatic data collection…Device data,” when Temu states that it collects “radio/network information (e.g., Wi-Fi, LTE, 3G).
User’s Activity on His or Her Device, Outside of Temu (¶¶ 112-115)	The only mention of acquiring user data from his or her activity outside of the Temu platform is as follows: “Automatic data collection. We, our service providers, and our business partners may automatically log information about you, your computer or mobile device, and your interaction over time with the Service, our communications and other online services, such as: …

	Online activity data, such as pages or screens you viewed, how long you spent on a page or screen, the website you visited before browsing to the Service, navigation paths between pages or screens, information about your activity on a page or screen, access times and duration of access, and whether you have opened our emails or clicked links within them.”
Phone State/Telephony (¶¶ 115-118)	Temu’s privacy policies make no mention that the app collects this type of data.
List of non-Temu apps or user accounts installed on a user’s device (¶¶ 119-126)	There is no mention of Temu’s collection of all installed apps or accounts on a user’s device, nor of the app-specific queries that Temu runs.
IMSI, MAC Address, IMEI, and AAID (¶¶ 127-131)	Temu states only that it collects “unique identifiers (including identifiers used for advertising purposes),” and does not explain either the specific identifiers it collects, nor does it disclose their sensitivity or their ability to be used to discern location information. “Automatic data collection. We, our service providers, and our business partners may automatically log information about you, your computer or mobile device, and your interaction over time with the Service, our communications and other online services, such as: … Device data, such as…unique identifiers (including identifiers used for advertising purposes)[.]”

February 13, 2023[51]

Type of Data	Extent to Which Data Is Addressed in Privacy Policy
Microphone Access (¶ 111)	No mention of seeking microphone access (or of audio, generally), with the exception of a notice at the end of the document titled “Information for California

[51] Available at https://web.archive.org/web/20230314181236/https:/www.temu.com/privacy-and-cookie-policy.html

	Residents…Right to correction…In the last 12 months, we've collected the following categories of personal information…Audio, electronic, visual, or similar information."
Camera Access (¶ 111)	Temu states that it only acquires photos provided by the user, in the course of using the Temu platform: "Personal Information We Collect … Information You Provide to Us. Personal information you may provide to us through the Service or otherwise includes: … User-generated content, such as profile pictures, photos, images, videos, comments, questions, messages, and other content or information that you generate, transmit, or otherwise make available on the Service, as well as associated metadata."
Location Data (¶¶ 78-80; 105-110; 127-131)	Temu states that it only collects location data through device data (which it states can only identify "general location") or when a user provides authorization: "Automatic data collection. We, our service providers, and our business partners may automatically log information about you, your computer or mobile device, and your interaction over time with the Service, our communications and other online services, such as: … Device data, such as…general location information such as city, state or geographic area. … Location data when you authorize the Temu mobile app to access your device's location."
WiFi Access Points (¶¶ 108-110)	No mention of WiFi Access Points. The only time "Wi-Fi" appears in the document is under "Automatic data collection…Device data," when Temu states that it collects "radio/network information (e.g., Wi-Fi, LTE, 3G).

User’s Activity on His or Her Device, Outside of Temu (¶¶ 112-115)	The only mention of acquiring user data from his or her activity outside of the Temu platform is as follows: “Automatic data collection. We, our service providers, and our business partners may automatically log information about you, your computer or mobile device, and your interaction over time with the Service, our communications and other online services, such as: … Online activity data, such as pages or screens you viewed, how long you spent on a page or screen, the website you visited before browsing to the Service, navigation paths between pages or screens, information about your activity on a page or screen, access times and duration of access, and whether you have opened our emails or clicked links within them.”
Phone State/Telephony (¶¶ 115-118)	Temu’s privacy policies make no mention that the app collects this type of data.
List of non-Temu apps or user accounts installed on a user’s device (¶¶ 19-126)	There is no mention of Temu’s collection of all installed apps or accounts on a user’s device, nor of the app-specific queries that Temu runs.
IMSI, MAC Address, IMEI, and AAID (¶¶ 127-131)	Temu states only that it collects “unique identifiers (including identifiers used for advertising purposes),” and does not explain either the specific identifiers it collects, nor does it disclose their sensitivity or their ability to be used to discern location information. “Automatic data collection. We, our service providers, and our business partners may automatically log information about you, your computer or mobile device, and your interaction over time with the Service, our communications and other online services, such as: … Device data, such as…unique identifiers (including identifiers used for advertising purposes)[.]”

136. In the February 2023 Privacy Policy, Temu separately mentions a "Privacy Notice Addendum to US Residents," but the text of that document does not appear in this Privacy Policy. Instead, Temu describes the document as follows:

> **Privacy Notice Addendum for US Residents**
> Residents of certain US states may have additional privacy rights under applicable state privacy laws. US users can learn more about which rights may be available to them and how to exercise those rights by reviewing US Privacy Notice Addendum for US Residents.

137. Temu's phrasing in the privacy policy does not indicate that the addendum might disclose additional data that Temu collects from users, but only that "[r]esidents of certain US states" might have additional rights available to them. This cannot be construed as a disclosure for any purpose, and nothing in the Privacy Policy would put a reader on notice that they should read the Addendum for a more transparent list of PII that Temu collects. Ultimately, this is irrelevant, as nothing in the Addendum remedies the defects in Temu's Privacy Policy regarding the data that Temu collects from users.

January 1, 2025[52]

Type of Data	Extent to Which Data Is Addressed in Privacy Policy
Microphone Access (¶ 118)	No mention of seeking microphone access (or of audio, generally), except for a discussion about customer service: "Customer Support Activity

[52] Available at https://www.temu.com/ie/privacy-and-cookie-policy.html.

	When you communicate with our customer service team through our customer support functions in the mobile application/on the website, either with a customer service agent or with our virtual assistant (via the chatbot or hotline), through social media, or any other means, we will collect your communication history with us which includes any text, images, video, audio, or supporting documents exchanged between us.”
Camera Access (¶ 118)	Temu removed its prior language quoted above and now says the following: “What Information Do We Collect … User-generated content When you provide product reviews and ratings on the Service, we collect this information, including any accompanying images, videos or text, as well as associated metadata.”
Location Data (¶¶ 85-87; 112-117, 134-138)	Temu removed its prior language quoted above and now states as follows, regarding location: “What Information Do We Collect … General location data We collect your approximate location based on your technical information (e.g., IP address).”
Wi-Fi Access Points (¶¶ 115–117)	Temu removed its prior language quoted above and has not provided substitute language.
User’s Activity on His or Her Device, Outside of Temu (¶¶ 119-122)	Temu removed its prior language quoted above and now states: “Information collected automatically To enhance your experience with the Service and support the other purposes for which we collect Personal Data as outlined in this Privacy Policy, we automatically process information about you, your computer or mobile device, your interactions with the Service, and our communications over time, such as:

	… Device data We collect Personal Data 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 where we have a legal basis for doing so). … Service usage information We collect Personal Data about your interactions with the Service, including the items in your shopping cart, your order pages you view, your duration on a page, the source from which you arrived at a page, your interactions with a page, your searched text and images, your browsing history, whether you opened our emails, and whether you clicked the links within our emails. We also collect service-related, diagnostic, and performance information, including crash reports and performance logs."
Phone State/Telephony (¶¶ 123–125)	Temu's privacy policies make no mention that the app collects this type of data.
List of non-Temu apps or user accounts installed on a user's device (¶¶ 126–133)	There is no mention of Temu's collection of all installed apps or accounts on a user's device, nor of the app-specific queries that Temu runs.
IMSI, MAC Address, IMEI, and AAID (¶¶ 134–138)	Temu now states that it collects "unique identifiers (including identifiers used for advertising purposes where we have a legal basis for doing so)," and does not explain either the specific identifiers it collects, nor does it disclose their sensitivity or their ability to be used to discern location information.

F. Defendants Are Violating Nebraska Consumers' Right to Privacy of Their Data.

138. As the immediately foregoing sections make clear, Temu (1) collects a host of privacy invasive PII and that (2) it purposely

designed its app *and* its customer disclosure in a way to keep its conduct hidden.

139. 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 Nebraskans who have used the Temu app. Such PII can be supplemented over time with *additional* private and personally identifiable user data and content, and all of this information has been, is, and will be used in the past, the present, and the future for economic and financial gain.

140. Meanwhile, Nebraskans 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.

141. Nebraskans 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.

142. Invasion of privacy has been recognized as a common law tort for over a century. *See Matera v. Google Inc.*, 15-CV-0402, 2016 WL 5339806, at *10 (N.D. Cal, Sept. 23, 2016) (citing Restatement (Second) of Torts §§ 652A-I for the proposition that "the right to privacy was first accepted by an American court in 1905, and 'a right to privacy is now recognized in the great majority of the American jurisdictions that have considered the question'"); *see also* Restatement (Second) of Torts § 652B (defining an intrusion claim as follows: "One who intentionally intrudes, physically or otherwise, upon the solicitude 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.")

143. As Justice Brandeis explained in his seminal article, *The Right to Privacy*, "[t]he common law secures to each individual the right of determining, ordinarily, to what extent his thoughts, sentiments, and emotions shall be communicated to others." Samuel D. Warren & Louis Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 198 (1890). The Supreme Court similarly recognized the primacy of privacy rights, explaining that the Constitution operates in the shadow of a "right to privacy older than the Bill of Rights." *Griswold v. Connecticut*, 381 U.S. 479, 486 (1965).

144. More recently, the Supreme Court explicitly recognized the reasonable expectation of privacy an individual has in his or her cell phone, and the PII generated therefrom, in its opinion in *Carpenter v. United States*, 138 S. Ct. 2206 (2018). There, the Court held that continued access of an individual's cell phone location data constituted a search under the Fourth Amendment because "a cell phone—almost a "feature of human anatomy[]"—tracks nearly exactly the movements of its owner . . . A cell phone faithfully follows its owner beyond public thoroughfares and into private residences, doctor's offices, political headquarters, and other potentially revealing locales . . . Accordingly, when the Government tracks the location of a cell phone it achieves near perfect surveillance, as if it had attached an ankle monitor to the phone's user." *Id.* at 2218 (internal citations omitted).

145. And, even more recently, the Northern District of California, in an order denying a motion to dismiss an intrusion upon seclusion claim for the exfiltration of PII in different mobile apps, held that "current privacy expectations are developing, to say the least, with respect to a key issue raised in these cases – whether the data subject owns and controls his or her personal information, and whether a commercial entity that secretly harvests it commits a highly offensive or egregious act."

McDonald v. Kiloo ApS, 385 F. Supp.3d 1022, 1035 (N.D. Cal. 2019). The *McDonald* court's reasoning was subsequently adopted in the District of New Mexico in analogous litigation. *See New Mexico ex rel. Balderas v. Tiny Lab Prods.*, 457 F. Supp. 3d 1103, 1127 (D.N.M. 2020), *on reconsideration*, No. 18-854 MV/JFR, 2021 WL 354003 (D.N.M. Feb. 2, 2021).

146. It is precisely because of Defendants' capacity for "near perfect surveillance" that courts have consistently held that time-honored legal principles recognizing a right to privacy in one's affairs naturally apply to online monitoring. 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*.

147. As discussed above, Defendants have designed the Temu app to 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.

148. 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.

149. 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. "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."[53] 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. 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.

G. Defendants Have Collected Personal Information from Minors, Including Minors under the Age of Thirteen

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

151. 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 thirteen, had parental consent before they used the Temu platform. Nor did Defendants implement adequate age verification procedures or procedures to confirm that minor users were acting with the

[53] Christopher Cole, *Sens. Prod Zuckerberg: Why Keep Tracking User Locations?*, Law360 (Nov. 19, 2019) (available at https://www.law360.com/consumerprotection/articles/1221312)

consent of their parents in using the Temu platform or adequate opt-out rights or rights to delete collected information.

152. Anyone can use Temu without verifying his or her age, and indeed many children use the Temu platform, including children under thirteen years old. Temu sells a wide variety of products that are marketed to children such as children's toys and clothing. Defendants have increased their revenue and profits by marketing these products to minors and by collecting minors' personal data when minors accessed the Temu platform.

153. 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.[54] 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.[55] Others have observed that Temu is filled with smoking and drug paraphernalia that is sold to any customer, without age verification.

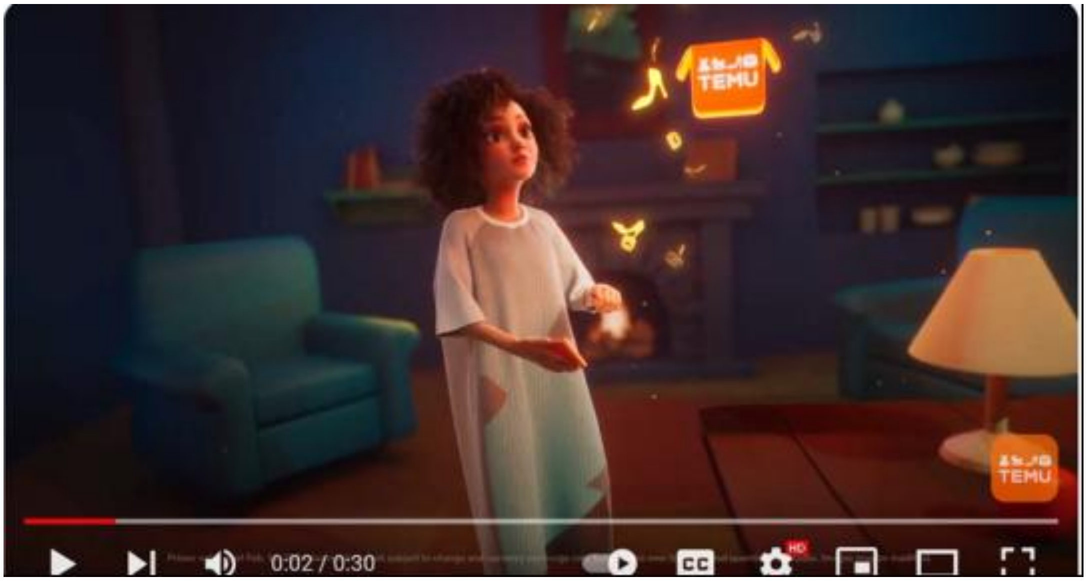
154. Finally, Temu recently ran an advertisement multiple times during the 2024 Super Bowl that featured a young-looking animated cartoon protagonist in an animated cartoon world who uses magic to bestow low-priced Temu products on everyone she

[54] *Adverts for online shopping platform Temu banned for sexualising a child and objectifying women*, SkyNews (Nov. 1, 2023) (available at https://news.sky.com/story/adverts-for-online-shopping-platform-temu-banned-for-sexualising-a-child-and-objectifying-women-12997811).

[55] Sarah Marsh, *Weapons banned in UK apparently found on shopping app Temu*, The Guardian (Nov. 16, 2023) (available at https://www.theguardian.com/money/2023/nov/17/weapons-banned-in-uk-apparently-found-on-shopping-app-temu-which)

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."[56]

155. 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. Yet 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.



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

156. Temu's data collection procedures with respect to minors have also been a specific concern of government authorities. 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.[57]

157. 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.

H. Temu Subjects User Data to Misappropriation By Chinese Authorities.

158. While the mere act of invading users' privacy in the manner described above is enough to sustain the State's claims without any further allegations, there are additional, egregious privacy harms that Nebraskans have suffered at the hands of Defendants. Namely, Temu's parent is a China-based company that is subject to Chinese law that requires companies to provide user data—including Nebraskans' data in Defendants' possession—to the government upon request.

159. Senator Pete Ricketts recently noted: "Under Chinese law, all Chinese companies must do the bidding of the Chinese Communist Party."[58]

[57] 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) (available at https://d1dth6e84htgma.cloudfront.net/CCP_Marketplace_Letter_to_Whaleco_Inc_Temu_7f921e1a67.pdf).

[58] https://www.ricketts.senate.gov/news/press-releases/ricketts-comments-on-supreme-court-upholding-tiktok-law-americas-national-security-comes-first/.

160. 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.

161. 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.

162. Laws including, but not limited to, the National Security Law, Cybersecurity Law, and National Intelligence Law are part of "an interrelated package of national security, cyberspace, and law enforcement legislation" that "are aimed at strengthening the legal basis for China's security activities and requiring Chinese and foreign citizens, enterprises, and organizations to cooperate with them."[59]

163. 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

[59] 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.

political parties and people's organizations, *enterprises*, undertakings, organizations and all other social organizations."[60]

164. 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."[61]

165. Specifically, the National Intelligence Law provides that "[a]ll organizations and citizens shall support, assist, and cooperate with national intelligence efforts in accordance with law, and shall protect national intelligence work secrets they are aware of."[62]

166. Article 14 provides that "[n]ational intelligence work institutions lawfully carrying out intelligence efforts may request that relevant organs, organizations, and citizens provide necessary support, assistance, and cooperation."[63]

167. Article 16 provides that these institutions "may enter relevant restricted areas and venues; may learn from and question relevant institutions, organizations, and individuals; and may read or collect relevant files, materials or items."[64]

168. Article 17 provides that "[a]s necessary for their work, the staff of national intelligence work institutions may, in accordance

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

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

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

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

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

with relevant national provisions, have priority use of, or lawfully requisition, state organs', organizations' or individuals' transportation or communications tools, premises and buildings . . . ."[65]

169. Against this backdrop are numerous laws and regulations designed to form a comprehensive cybersecurity regime. The "chief engineer at the [Ministry of Public Security's] Cybersecurity Bureau," Guo Qiquan, described the scheme as intended to "cover every district, every ministry, every business and other institution, basically covering the whole society. It will also cover all targets that need [cybersecurity] protection, including all networks, information systems, cloud platforms, the internet of things, control systems, big data and mobile internet."[66]

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

171. "China's Cybersecurity Law lays the foundation for a cybersecurity review of network products and services, also known as the Cybersecurity Review Regime."[67]

172. The Cybersecurity Law applies broadly to, among others, "network operators," which can encompass not only "telecommunications or internet service providers (ISPs)" but also "anyone who uses [information communication and technology] systems."[68]

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

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

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

[68] *Id.*

173. Article 28 of China's Cybersecurity Law requires these "network operators" to cooperate with national intelligence activities, as well as criminal investigations. Specifically, Article 28 provides that, "Network operators shall provide technical support and assistance to public security organs and national security organs that are safeguarding national security and investigating criminal activities in accordance with the law."[69]

174. Article 49 further provides that "network operators shall cooperate with cybersecurity and informatization departments and relevant departments in conducting implementation of supervision and inspections in accordance with the law."[70]

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

176. For example, Article 35 provides that "[c]ritical information infrastructure operators purchasing network products and services that might impact national security shall undergo a national security review organized by the State cybersecurity and informatization departments and relevant departments of the State Council."[71]

177. Article 37 further provides:

> [c]ritical information infrastructure operators that gather or produce personal information or important data during operations within the mainland territory of the People's Republic of China, shall store it within

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

[70] CYBERSECURITY LAW, art. 49.

[71] CYBERSECURITY LAW, art. 35.

> mainland China. Where due to business requirements it is truly necessary to provide it outside the mainland, they shall follow the measures jointly formulated by the State cybersecurity and informatization departments and the relevant departments of the State Council to conduct a security assessment; where laws and administrative regulations provide otherwise, follow those provisions.[72]

178. Since the law's enactment, authorities have issued regulations expanding its scope.[73]

179. Exactly what type of organization may be designated a "critical information infrastructure operator" is not always clear. However, authorities' use of the applicable procedures indicates that tech companies and platforms could be subject to an invasive cybersecurity review, and that authorities' power to require a company to take any action pursuant to a cybersecurity review—even if justified only after the fact—could have significant consequences for its business.[74]

180. For example, in July 2021, just a few days after the Chinese ride-hailing service Didi raised billions of dollars in a New York

[72] CYBERSECURITY LAW, art. 37.

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

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

IPO, the Cyberspace Administration of China (CAC), a "merged party-state institution listed under the Central Committee of the Chinese Communist Party,"[75] initiated a cybersecurity review of Didi. The CAC further "suspended new user registrations during the review" and ordered the removal of the company's applications from app stores in China.[76] Although the law and related regulations did not explicitly apply to Didi in advance of the review, CAC published a list of proposed new rules applying the cybersecurity review requirements to Didi *after* it began its review.[77] CAC eventually imposed a $1.2 billion fine on the company.[78]

181. The Data Security Law applies in China as well as to "data handling activities outside the mainland territory of the PRC [that] harm the national security, the public interest, or the lawful rights and interests of citizens or organizations of the PRC.[79]

182. Article 24 provides that "[t]he State is to establish a data security review system and conduct national security reviews for data handling activities that affect or may affect national security."[80]

183. Further, Article 31 applies "[t]he provisions of the Cybersecurity Law . . . to the outbound security management of

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

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

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

[78] *Id.*

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

[80] DATA SECURITY LAW, art. 24.

important data collected or produced by critical information infrastructure operators operating within the mainland territory of the PRC."[81]

184. Under the Data Security law, even "a company holding data belonging to a US citizen stored on a Chinese server may not be able to legally hand over that data to the US government without proper approval."[82] More specifically, under Article 35, whether operating critical information infrastructure or not, companies "are prohibited from providing any data *stored* in China, regardless of the data's sensitivity level and whether or not the data was initially *collected* in China, to any foreign judicial or law enforcement agency without the prior approval of the relevant [Chinese Government] authorities."[83]

185. 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 services, and that there is no meaningful way to resist these requirements, or any pressure brought to bear by the Party.[84]

[81] DATA SECURITY LAW, art. 31.

[82] 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.

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

[84] *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*,

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

187. In sum, any data stored *or accessed* by individuals or entities subject to Chinese laws, as written and as interpreted and applied by Chinese government officials, is not safe from access by the Chinese government, for any use it deems fit.

188. 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.

I. Defendants Acknowledge That They Risk Being Subject to China's Laws Regarding Users' Data in Their Possession

189. None of the above is speculation or hyperbole. In a filing to the SEC on April 28, 2025,[85] Pinduoduo (1) acknowledges that

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).

[85] https://www.sec.gov/ix?doc=/Archives/edgar/data/1737806/000141057825000951/pdd-20241231x20f.htm

Temu is one of its platforms,[86] and (2) states, in a section titled "Risks Related to Doing Business in China," the following:

a. "A significant portion of our assets and operations is located in China. Accordingly, our business, financial condition, results of operations and prospects may be influenced to a significant degree by political, economic and social conditions in China generally."

b. "Our operations in China are governed by PRC laws and regulations. Our PRC subsidiaries are subject to laws and regulations applicable to foreign investment in China."

c. "We only have contractual control over the Pinduoduo platform. We do not directly own the Pinduoduo platform due to the restrictions on foreign investment in businesses providing value-added telecommunications services in China, including e-commerce services and internet content-related services. This may significantly disrupt our business, subject us to sanctions, compromise enforceability of related contractual arrangements, or have other harmful effects on us."

d. "The PRC governmental authorities have also promulgated laws and regulations relating to cybersecurity review. The Data Security Law, the Regulations on the Protection of Critical Information Infrastructure, and the Cybersecurity Review Measures promulgated by the PRC authorities (collectively, the 'Cybersecurity Laws')[.]"

[86] "[R]eferences in this annual report to…'our platforms' are to the Pinduoduo platform and the Temu platform."

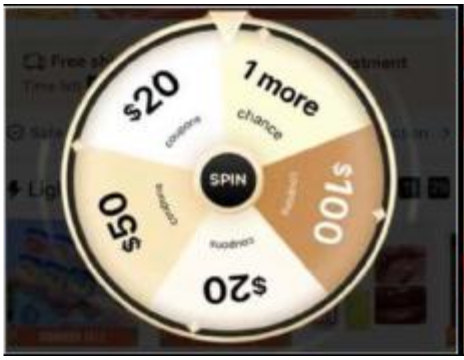
e. "[W]e may…be subject to cybersecurity review obligations if the Cybersecurity Review Office decides to initiate a review against us on the grounds that we are deemed to be an operator engaged in offering network products and services or data processing activities that affect or may affect national security, though our ability to control and assess the likelihood of whether this happens is limited."

J. Defendants Also Engage in Deceptive and Unconscionable Trade Practices in the Offer and Sale of Products on the Temu App, and the Resolution of Consumer Complaints.

190. Defendants actively utilize deceptive and unconscionable practices in order to maximize the number of users who sign up to use the app, thereby maximizing the amount of data that Defendants can misappropriate. According to one commentator, "TEMU is a notoriously bad actor in its industry. We see rampant user manipulation, chain-letter-like affinity scams to drive signups, and overall, the most aggressive and questionable techniques to manipulate large numbers of people to install the app."[87]

191. 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.

[87] *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 (Sep. 6, 2023) (available at 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/)



192. These tactics have been wildly successful: "PDD's TEMU online marketplace is being reported as among the fastest uptaken apps in history."[88]

193. However, 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,"[89] there have been many complaints regarding the quality of goods sold on the site as well as the service provided by Temu.

i. Deceptive Representations as to the Quality of Goods

194. 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.[90] Users experience undelivered packages and poor

[88] *Id.*

[89] Temu, *What is Temu?* (available at https://www.temu.com/about-temu.html)

[90] 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) (available at https://www.uscc.gov/sites/default/files/2023-04/Issue_Brief-Shein_Temu_and_Chinese_E-Commerce.pdf)

customer service. Moreover, even when goods are delivered, they are often of low quality, contrary to Temu's marketing and representations.

195. For example, one analysis observed that "TEMU products as shipped often do not resemble the photos."[91] Users frequently receive low-quality, cheaply-made merchandise when the photo on the app indicates that they would receive high-quality goods. Moreover, photos and product descriptions are sometimes simply copied directly from other sellers on sites like Amazon, bearing no relationship to the actual goods being sold.[92] In addition, while Defendants claim that they use "world-class manufacturers" and have a "zero tolerance policy against counterfeits,"[93] 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 (more on Temu's sale of unlicensed goods below).[94]

ii. False Reference Pricing

[91] *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 (Sep. 6, 2023) (available at 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/).

[92] Jennifer Ortakales Dawkins, *Temu sellers are now even copying product photos, descriptions, and entire Amazon storefronts, lawsuits allege*, Business Insider (Jul. 11, 2023) (available at https://www.businessinsider.com/temu-sellers-are-counterfeiting-amazon-listings-and-storefronts-2023-7)

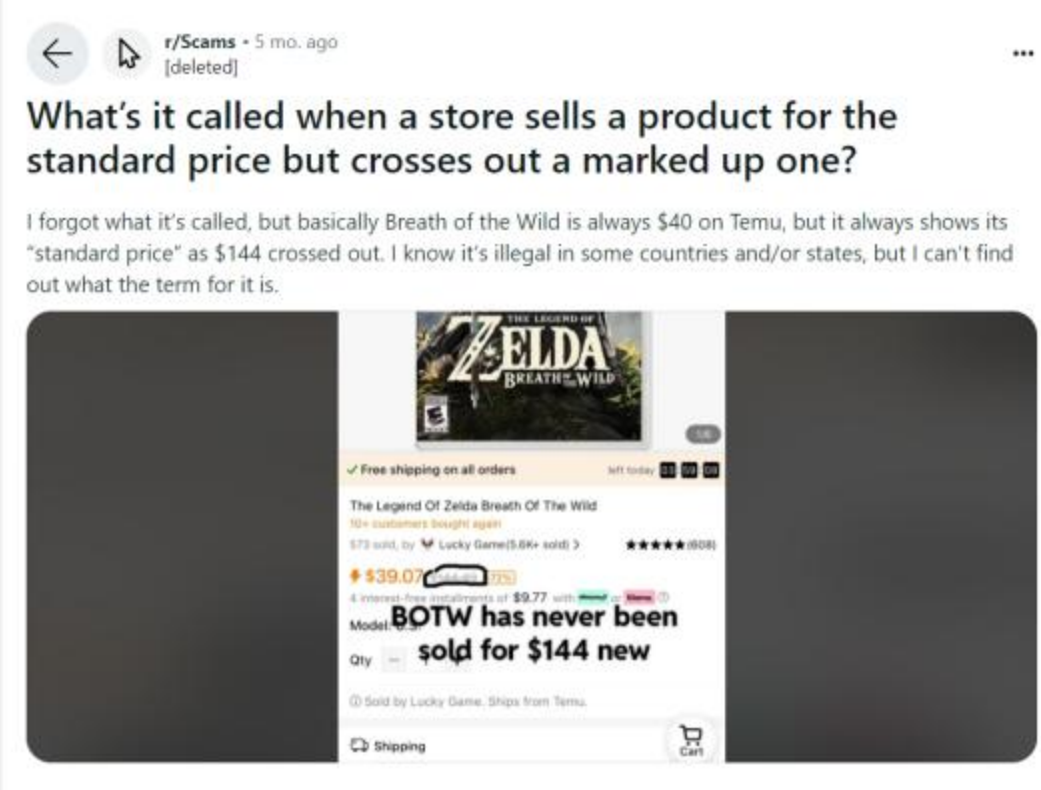
[93] Temu, *Temu's Commitments*, (available at https://www.temu.com/commitments.html)

[94] Jennifer Ortakales Dawkins, *Fake Jordans are all over Temu even after the knockoffs were removed from Shein*, Business Insider (Jun. 16, 2023) (available at https://www.businessinsider.com/shein-and-temu-listed-fake-air-jordans-for-under-50-2023-6)

196. 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—for example by providing two prices that the customer can compare to each other: a former list price or manufacturer's suggested retail price ("MSRP") and a supposedly reduced current price—when in reality the "full price" is inflated, or was never real to begin with, while the "discounted" price is merely the product's regular or market price.

197. Defendants engage in such false reference pricing on Temu. One such example was identified in the social media platform Reddit, regarding the sale of the popular video game "Zelda: Breath of the Wild" or "BOTW." In a post[95] titled "*What's it called when a store sells a product for the standard price but crosses out a marked up one?*" a user noted that Temu was claiming the purportedly discounted price of $40 for the video game was misleading, because the game never actually retailed for the advertised "standard" price of $144:

[95] https://www.reddit.com/r/Scams/comments/179oq5y/whats_it_called_when_a_store_sells_a_product_for/



r/Scams • 5 mo. ago
[deleted]

What's it called when a store sells a product for the standard price but crosses out a marked up one?

I forgot what it's called, but basically Breath of the Wild is always $40 on Temu, but it always shows its "standard price" as $144 crossed out. I know it's illegal in some countries and/or states, but I can't find out what the term for it is.

THE LEGEND OF
ZELDA
BREATH OF THE WILD
Free shipping on all orders
left today
The Legend Of Zelda Breath Of The Wild
10+ customers bought again
Lucky Game(5.6K+ sold)
★★★★★(608)
$39.07
4 interest-free installments of $9.77 with
Model:
Qty
Sold by Lucky Game. Ships from Temu.
Shipping
Cart

BOTW has never been sold for $144 new

iii. Charges and Delivery for Goods Not Ordered

198. Numerous consumers have complained to the Better Business Bureau and other consumer watchdog organizations about receiving mysterious packages from Temu that they did not order and Temu charging the consumers for those purchases and other items that they did not order.

199. These fraudulent deliveries and charges occur frequently after consumers make comparatively small purchases from Temu, and then much larger charges and deliveries are made using the same information the consumer provided Temu during checkout for their legitimate purchase.

iv. Use of Forced Labor

200. In addition, while Defendants claim that they seek to "[d]o good for the world," are "honest, ethical and trustworthy," and are "socially responsible,"[96] a recent report found that much of the merchandise sold on Temu is likely being produced using forced labor provided by China's Uyghur minority held against their will in camps in the Chinese province of Xinjiang.[97] As the *Los Angeles Times* noted in a recent exposé, such practices are not only deceptive, but they violate federal law: "Products made in China's western province of Xinjiang are being sold to U.S. consumers through the online shopping platform Temu, in breach of a ban that forbids goods from the region due to links to forced labor, according to research by a global supply chain verification firm." As one expert noted in the article, "It's a systematic violation of U.S. trade policies."[98]

201. As the article explains, "Citing what the U.S. State Department has called 'horrific abuses' against the Uyghur people of Xinjiang, who are predominantly Muslim, federal officials banned the importation of cotton from the region in 2021 and expanded the law and its enforcement to all Xinjiang products last year under the Uyghur Forced Labor Prevention Act. Statements from former detainees and reports from an array of researchers and advocacy groups have alleged that the Chinese government put more than 1 million people in detention camps in the region and that laborers in fields and factories were forced or coerced."[99]

[96] Temu, *What is Temu?* (available at https://www.temu.com/about-temu.html)

[97] Sheridan Prasso, *Most-downloaded app in App Store sells products linked to forced labor in China, analysis shows*, L.A. Times (Jun. 15, 2023) (available at https://www.latimes.com/business/story/2023-06-15/temu-sells-products-linked-to-forced-labor-in-china).

[98] *Id.*

[99] *Id.*

202. The U.S. government has also expressed concerns that Temu is selling Chinese goods to consumers in the United States that are manufactured using forced labor. For example, the Congressional U.S.-China Economic and Security Review Commission issued a report noting that Temu posed "risks and challenges to U.S. regulations, laws and principles of market access" resulting from such direct-to-consumer sales.[100] Likewise, Representative Mike Gallagher, former chair of the House Select Committee on the Chinese Communist Party, and the panel's top Democrat, Raja Krishnamoorthi, who represents Illinois' 8th Congressional district, sent letters to Temu asking for information concerning whether the company is importing products derived from forced labor in China.

203. The House Select Committee on the Chinese Communist Party recently issued an Interim Report regarding its findings to date, entitled "Fast Fashion and the Uyghur Genocide." The report concludes that "Temu does not have any system to ensure compliance with the Uyghur Forced Labor Prevention Act (UFLPA). This all but guarantees that shipments from Temu containing products made with forced labor are entering the United States on a regular basis, in violation of the UFLPA."[101] The report concluded that Temu is actively seeking to avoid the protections in place to prevent the sale of goods manufactured with forced labor: "Temu's business model … is to avoid bearing

[100] 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) (available at https://www.uscc.gov/sites/default/files/2023-04/Issue_Brief-Shein_Temu_and_Chinese_E-Commerce.pdf)

[101] Select Committee on the Chinese Communist Party, *Fast Fashion and the Uyghur Genocide: Interim Findings* (Mar. 23, 2023) (available at https://selectcommitteeontheccp.house.gov/sites/evo-subsites/selectcommitteeontheccp.house.gov/files/evo-media-document/fast-fashion-and-the-uyghur-genocide-interim-findings.pdf).

responsibility for compliance with the UFLPA and other prohibitions on forced labor while relying on tens of thousands of Chinese suppliers to ship goods direct to U.S. consumers."[102] Moreover, the report observed that "Temu admitted that it does not expressly prohibit third party sellers from selling products based on their origin in the Xinjiang Autonomous Region."[103]

204. The committee's report was issued after it held hearings at which it received expert testimony regarding the "genocide of the Uyghur people and other minorities." As recounted in the report, "The Committee received first-hand witness testimony and expert reports about the CCP's atrocities, which include imprisonment, torture, rape, forced sterilization, and the widespread exploitation of the Uyghur people in forced labor."[104]

205. The committee noted that the hearings provided evidence that Temu ships "millions of packages" to the United States "duty free" and "without providing [U.S. Customs & Border Protection] with sufficient data regarding the contents of the packages."[105] The committee concluded: "In light of the sheer volume of shipments sent to the United States through its website, Temu's failure to take any meaningful steps with respect to preventing the importation of goods with forced labor is striking."[106]

206. These unscrupulous practices have allowed Defendants to maximize their access to user data through the false promise of low-cost, high-quality goods. Moreover, they further demonstrate that Defendants' real business is not providing a platform for the sale of quality merchandise but rather obtaining access to user

[102] *Id.*
[103] *Id.*
[104] *Id.*
[105] *Id.*
[106] *Id.*

data under false pretenses, which they then misappropriate and seek to monetize.

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

207. 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 "affinity scam" or "chain letter"-like tactics where users are repeatedly urged to sign up their friends and acquaintances in order to expand the number of users whose data Defendants may then access through the app.

208. Among other things, Temu offers credit and free items to users who get their friends and acquaintances to sign up for the app. "Those who do register are subjected to a bombardment of emails and app notifications."[107] "[O]nce you give TEMU your personal information, you will be repeatedly spammed, hounded, nagged, and bribed to get your friends and family to give TEMU their personal information. When users fall down this rabbit hole (getting that Nintendo Switch absolutely free), TEMU sends a torrent of popup sequences milking users for 'just one more contact'."[108] In addition, Temu users are bombarded by notifications and spam from third parties other than Defendants. These emails and notifications occur even after users delete the

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

[108] *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 (Sep. 6, 2023) (available at 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/).

app from their devices and even when users seek to block such notifications.

209. Moreover, Temu has utilized online "influencers" to harvest new users on an even larger scale. "There are now literally thousands of so-called 'influencers' hawking TEMU referrals on Reddit, YouTube, TikTok, and also Minecraft, Roblox, Discord… the pitch is: 'You don't have to buy anything, just sign up!'" "If you have a social media presence, TEMU will figure that out and will start to spam you – every day – to induce you to create videos promoting TEMU, for which they promise to pay."[109]

vi. Fake Reviews

210. Defendants attract and maintain users through other fraudulent means. For example, "TEMU … compensates users to write reviews," which are then "obviously skewed positive." Moreover, 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. For example, one report cited a so-called "five star" review stating that "What this company is doing is illegal" and constitutes "fraud," that the company relies on "lies and deceptions", and that "[c]ountless reviews are clearly negative, yet it shows that the person gave the item 5 stars which is impossible."[110] Other users have reported that "Some items are legit pretty good, but I've ordered from these sites and most is total crap. I just wish I wouldn't waste my time if the reviews were more truthful. I've noticed sometimes the text of the review is negative, yet the rating is 5 stars," and that when a user tries

[109] *Id.*

[110] *Id.*

to give an item a one-star rating, the rating is automatically "upgraded" to a 5-star rating.[111]

vii. Intellectual Property and Product Source-Related Deception

211. Temu claims to be "committed to protecting everyone's intellectual property and [to] have a comprehensive policy to that end." Temu's intellectual property (IP) policies and practices are anything but "comprehensive." Rather, the platform is designed and operated in manners that make IP enforcement difficult and allow infringement to thrive. Temu's claims are woefully misleading in light of the actual details of Temu's policy, Temu's procedures for reporting IP violations, Temu's automated promotion of infringing products, and the literally countless products that are available for purchase from the Temu store that infringe on IP rights.[112]

212. Nebraska consumers who shop on Temu are harmed by the proliferation of counterfeit and often low-quality imitations. Further, Nebraska brands, businesses, and creators who invest time and resources in developing products and brand reputation are harmed by Temu's lack of meaningful protections, which are far from "comprehensive." This is especially true for smaller businesses and creators who are less likely to be able to afford legal fees to navigate Temu's cumbersome reporting processes let alone keep up with the slew of infringing listings. And while the

[111] Shein, Temu, etc. – What's up with the 5 star reviews for EVERYTHING?!, Reddit.com (August 10, 2023) (available at https://www.reddit.com/r/FrugalFemaleFashion/comments/15niiki/shein_temu_etc_whats_up_with_the_5_star_reviews/).

[112] *What Is Temu? Read Before You 'Shop Like a Billionaire'*, PC Mag (January 15, 2025) (available at https://www.pcmag.com/explainers/what-is-temu-read-before-you-shop-like-a-billionaire).

proliferation of counterfeit and infringing products on Temu is no secret, Temu has a profit incentive to keep allowing the slew.

213. In order for an IP rightsholder to merely request that Temu review an infringing product, the rightsholder is required to create a Temu customer account before gaining access to the Temu Intellectual Property Complaint Portal. To submit a removal request, the rightsholder is then required to enter extensive information about each specific product listing that violates their intellectual property. Notably, Temu commonly generates multiple, sometimes dozens, of separate and independent listings for identical products with differences only in price, shipping speed, and other minor details. Temu offers no ability for IP rightsholders to report these identical products except for locating each listing separately and providing Temu with each specific listing URL link to Temu's own listing of the product. IP watchdog groups warn that rightsholders who submit multiple URLs to Temu at once can expect Temu to take significantly longer to provide any response to those complaints than submitting only a single URL in a complaint.[113]

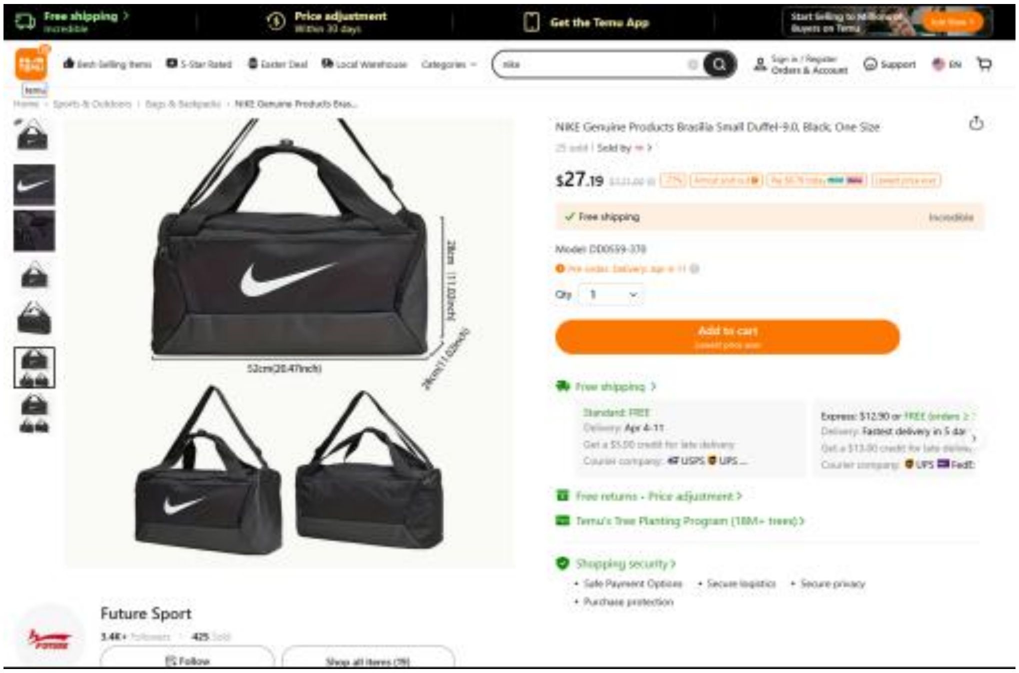
214. As a result of Temu's convoluted and ineffective IP protection policy, the Temu store is rife with unlicensed products listed for sale bearing protected trademark images. Countless brands are impersonated on the store, including Nike[114], Disney[115],

[113] *Why Removing Counterfeit Listings on Temu Matters*, IPMoat.ai (available at https://ipmoat.ai/blogs/how-to-guides/how-to-remove-copied-product-listings-from-temu) (Last accessed 3/31/2025).

[114] See Figure A, available at https://www.temu.com/-small-duffel-9-0--size-g-601099966059247.html (Last accessed 3/31/2025).

[115] See Figure B, available at https://www.temu.com/1pc---wooden-sculpture-creative-cartoon-design-with--gesture-ideal-for-home-office-or--perfect-gift-for-birthdays-christmas-valentines-thanksgiving-collectible-statue-made-of--wood-decorative-no-electricity-needed-g-601100033356476.html (Last accessed 3/31/2025).

Microsoft[116], Amazon[117], and (closer to home) Runza[118] and the University of Nebraska[119].



NIKE Genuine Products Brasilia Small Duffel-9.0, Black, One Size

Sold by

$27.19

✓ Free shipping Incredible

Model: DD0559-370

Qty 1

Free shipping >

Standard: FREE
Delivery: Apr 4-11
Get a $5.00 credit for late delivery
Courier company: USPS UPS ...

Express: $12.90 or FREE (orders ≥
Delivery: Fastest delivery in 5 da
Get a $13.00 credit for late delive
Courier company: UPS FedE

Free returns · Price adjustment >

Temu's Tree Planting Program (18M+ trees) >

Shopping security >

- Safe Payment Options
- Secure logistics
- Secure privacy
- Purchase protection

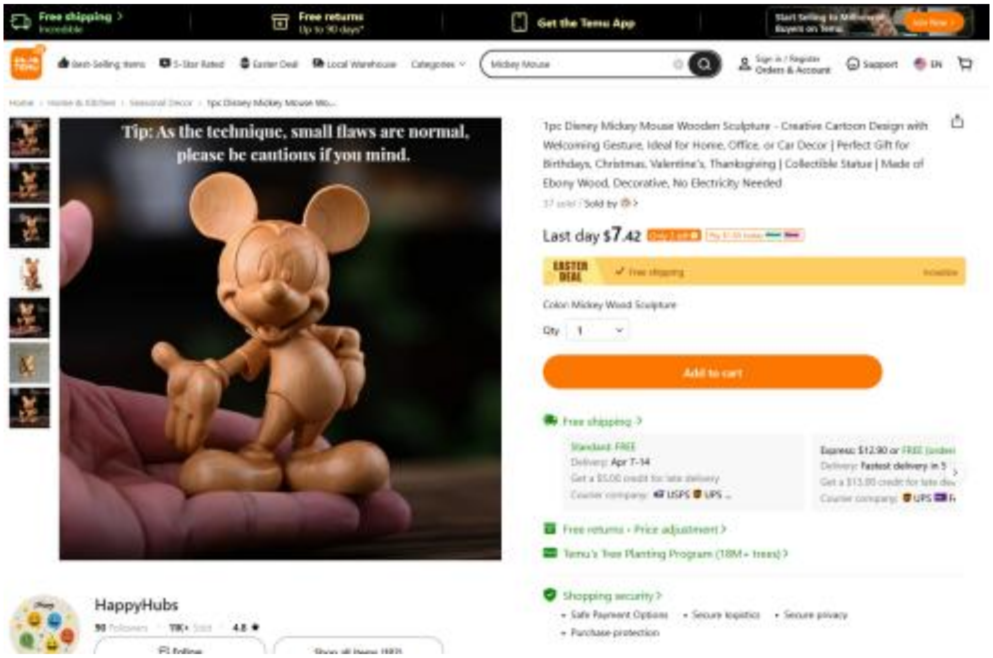
Figure A

[116] See Figure C, available at https://www.temu.com/vintage---metal-sign-1pc-8x8-inch-aluminum-wall-art-for-home-decor--cave-cafe-office-waterproof-fade-resistant-rust-proof-indoor-outdoor-signage-g-601099703019525.html (Last accessed 3/31/2025).

[117] See Figure D, available at https://www.temu.com/--logo-baseball-cap-adjustable-snapback--polyester-black-with-orange-print-unisex--for-men-women-casual-outdoor-wear--headgear-minimalist-baseball-cap-polyester-cap-g-601100203355238.html (Last accessed 3/31/2025).

[118] See Figure E, available at https://www.temu.com/-love-and--sandwich-pattern-t-shirt--cotton-casual-round-neck-slightly-elastic-formal-wear-knitted-fabric-suitable-for---men-and-women-can-wear-g-601099828002639.html (Last accessed 3/31/2025).

[119] See Figure F, available at https://www.temu.com/1pc---polyester-single-sided-red-white-ideal-for-outdoor-use-outdoor-decor-college-theme-durable-polyester-college-flags-g-601100245629436.html (Last accessed 3/31/2025).



1pc Disney Mickey Mouse Wooden Sculpture - Creative Cartoon Design with Welcoming Gesture, Ideal for Home, Office, or Car Decor | Perfect Gift for Birthdays, Christmas, Valentine's, Thanksgiving | Collectible Statue | Made of Ebony Wood, Decorative, No Electricity Needed

37 sold | Sold by ›

Last day $7.42

Color: Mickey Wood Sculpture

Qty 1

Standard: FREE
Delivery: Apr 7-14
Get a $5.00 credit for late delivery
Courier company: USPS UPS ...

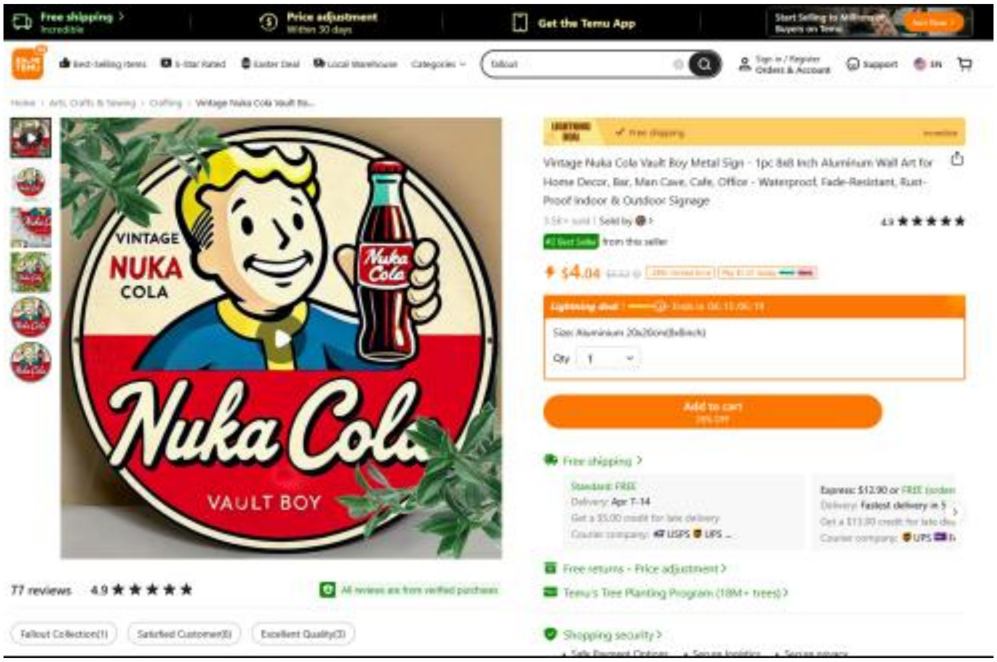
Express: $12.90 or FREE (order
Delivery: Fastest delivery in 5
Get a $13.00 credit for late de
Courier company: UPS F

- Safe Payment Options
- Secure logistics
- Secure privacy
- Purchase protection

HappyHubs

90 Followers | 11K+ Sold | 4.8 ★

Figure B



Vintage Nuka Cola Vault Boy Metal Sign - 1pc 8x8 Inch Aluminum Wall Art for Home Decor, Bar, Man Cave, Cafe, Office - Waterproof, Fade-Resistant, Rust-Proof Indoor & Outdoor Signage

3.5K+ sold | Sold by ›

4.9 ★★★★★

from this seller

$4.04

Size: Aluminium 20x20cm(8x8inch)

Qty 1

Standard: FREE
Delivery: Apr 7-14
Get a $5.00 credit for late delivery
Courier company: USPS UPS ...

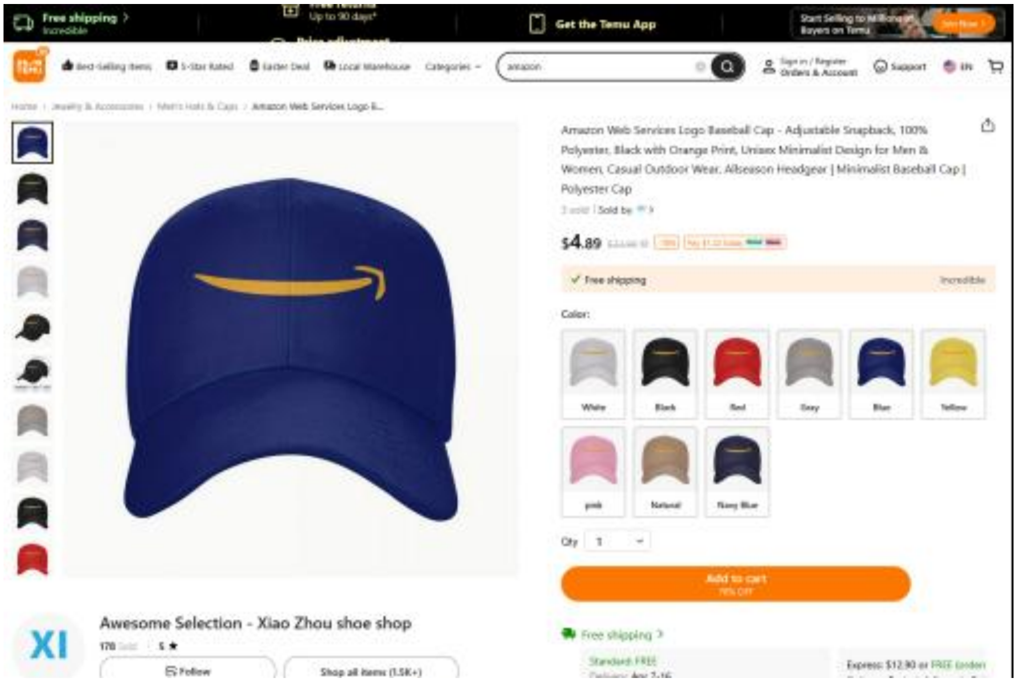
Express: $12.90 or FREE (order
Delivery: Fastest delivery in 5
Get a $13.00 credit for late de
Courier company: UPS F

77 reviews 4.9 ★★★★★

All reviews are from verified purchases

- Safe Payment Options
- Secure logistics
- Secure privacy

Figure C



Amazon Web Services Logo Baseball Cap - Adjustable Snapback, 100% Polyester, Black with Orange Print, Unisex Minimalist Design for Men & Women, Casual Outdoor Wear, Allseason Headgear | Minimalist Baseball Cap | Polyester Cap

Sold by

$4.89

✓ Free shipping Incredible

Awesome Selection - Xiao Zhou shoe shop

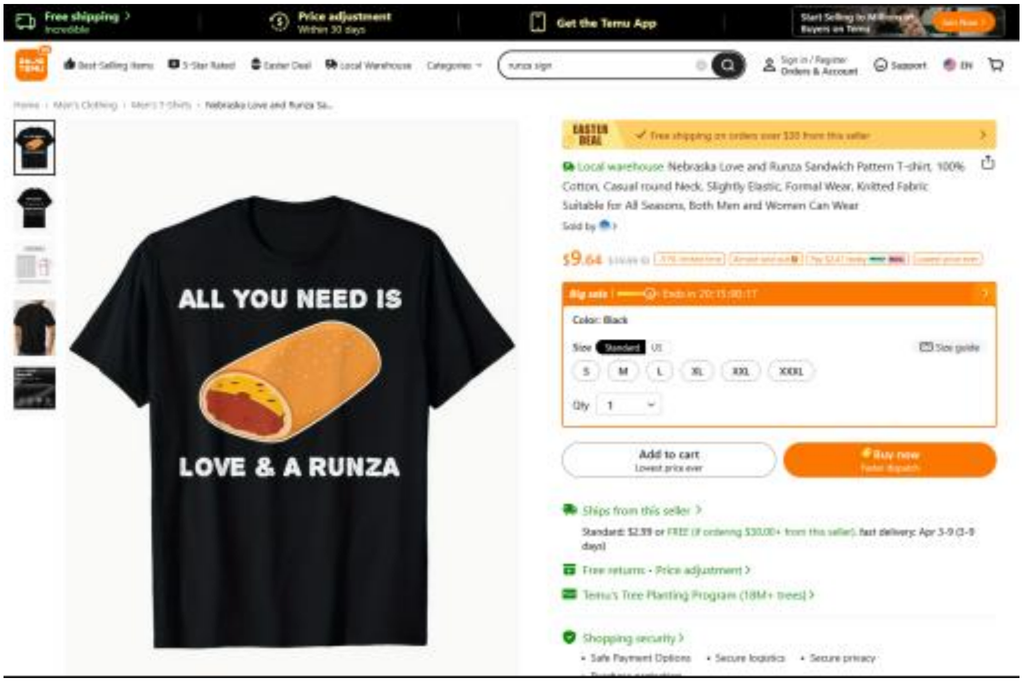
178 sold 5 ★

Standard: FREE

Delivery: Apr 7-16

Express: $12.90 or FREE (orders

Figure D



✓ Free shipping on orders over $30 from this seller

Local warehouse Nebraska Love and Runza Sandwich Pattern T-shirt, 100% Cotton, Casual round Neck, Slightly Elastic, Formal Wear, Knitted Fabric Suitable for All Seasons, Both Men and Women Can Wear

Sold by

$9.64

Big sale | Ends in 20:15:00:17

Color: Black

Ships from this seller

Standard: $2.99 or FREE (if ordering $30.00+ from this seller), fast delivery: Apr 3-9 (3-9 days)

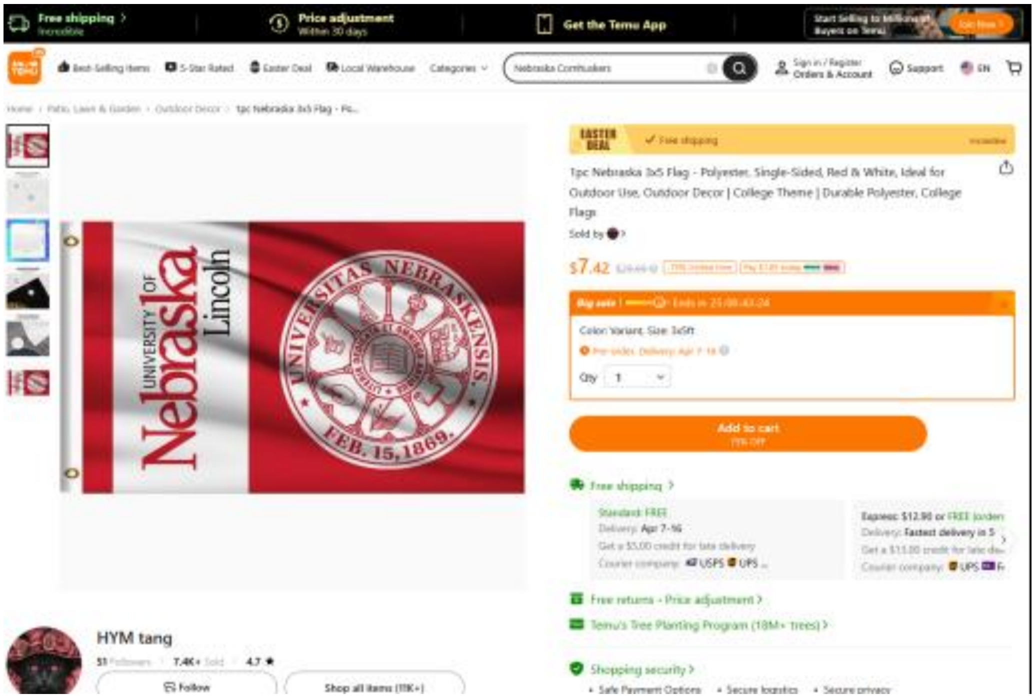
Free returns · Price adjustment

Temu's Tree Planting Program (18M+ trees)

Shopping security

- Safe Payment Options
- Secure logistics
- Secure privacy

Figure E



Home › Patio, Lawn & Garden › Outdoor Decor › 1pc Nebraska 3x5 Flag - Fo...

1pc Nebraska 3x5 Flag - Polyester, Single-Sided, Red & White, Ideal for Outdoor Use, Outdoor Decor | College Theme | Durable Polyester, College Flags

Sold by ●›

$7.42

Color: Variant, Size: 3x5ft

Qty 1

Free shipping ›

Standard: FREE
Delivery: Apr 7-16
Get a $5.00 credit for late delivery
Courier company: USPS UPS ...

Express: $12.90 or FREE (orders
Delivery: Fastest delivery in 5
Get a $13.00 credit for late de...
Courier company: UPS F...

Free returns · Price adjustment ›

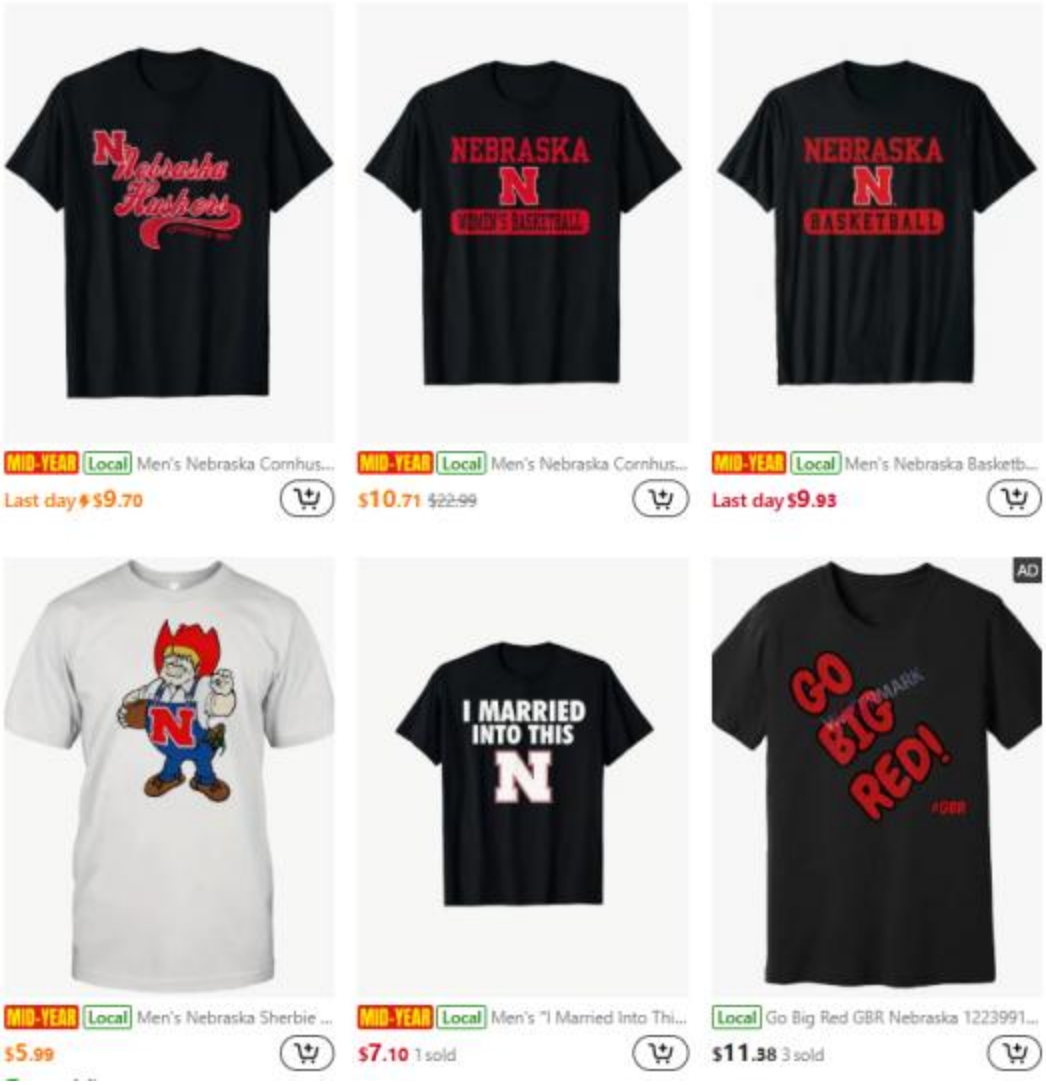
Temu's Tree Planting Program (18M+ trees) ›

Shopping security ›
- Safe Payment Options
- Secure logistics
- Secure privacy

HYM tang
51 Followers | 7.4K+ Sold | 4.7 ★

Figure F

215. A recent search on Temu for "Nebraska huskers" also resulted in numerous product listings that appear to be infringing (see Figure G below). Many of these listings also include a "local" tag. While consumers may reasonably assume this means these products originate locally, this is not true. Temu misleadingly uses the "local" tag for products shipped from warehouses located in the United States. These products could originate from foreign countries, such as China, but Temu passes them off as local goods because the products are temporarily stored for distribution in the United States. This tag is inherently misleading. Nebraska consumers are not necessarily shopping from local manufacturers, creators, designers, or stores by purchasing "local" products on Temu.



MID-YEAR Local Men's Nebraska Cornhus...
Last day $9.70

MID-YEAR Local Men's Nebraska Cornhus...
$10.71 ~~$22.99~~

MID-YEAR Local Men's Nebraska Basketb...
Last day $9.93

MID-YEAR Local Men's Nebraska Sherbie ...
$5.99

MID-YEAR Local Men's "I Married Into Thi...
$7.10 1 sold

Local Go Big Red GBR Nebraska 1223991...
$11.38 3 sold

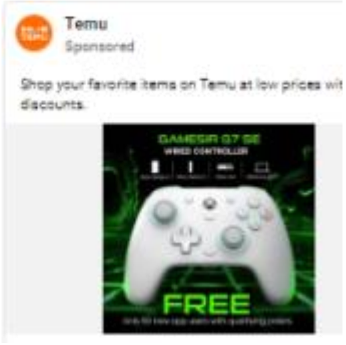
Figure G

216. Unlicensed and infringing products are nevertheless falsely presented to consumers as authentic and licensed by the true owners of those brands, many of which are also misleadingly labelled as "local."

217. Not only does Temu offer infringing products for sale, but Temu creates its own advertisements for unlicensed products as well. On information and belief, Temu produces auto-generating

ads to consumers that contain unlicensed and infringing products.

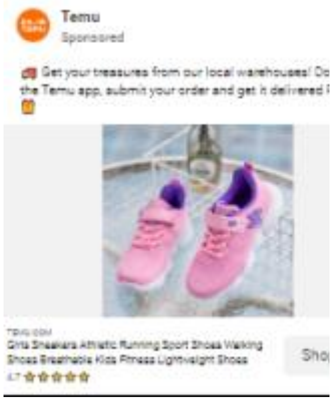
218. For example, in just a few minutes of searching the Facebook Ad Library, the Attorney General's Office came across numerous ads being run by Temu itself on Facebook that advertised products that infringe well-known brands, including Xbox[120], Sketchers[121], and Disney's Lilo and Stich Merchandise[122]. Screenshots of those ads are below.



Temu

Sponsored

Shop your favorite items on Temu at low prices wit discounts.



Temu

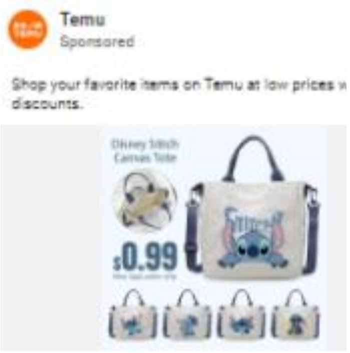
Sponsored

Get your treasures from our local warehouses! Do the Temu app, submit your order and get it delivered !

TEMU.COM

Girls Sneakers Athletic Running Sport Shoes Walking Shoes Breathable Kids Fitness Lightweight Shoes

4.7 ★★★★★



Temu

Sponsored

Shop your favorite items on Temu at low prices w discounts.

219. Temu also advertises infringing products in Nebraska. For example, after browsing on the Temu website, one user encountered Temu banner ads embedded on the website for WOWT, First Alert 6, in Omaha. These banner ads displayed hats purportedly for sale on Temu bearing trademarked images and logos. Notably, when the user refreshed the website, the Temu banner ads also refreshed, offering new copyright infringing images each time, including Chevron[123], Indian Motorcycles[124],

[120] https://www.facebook.com/ads/library/?id=489370897185094

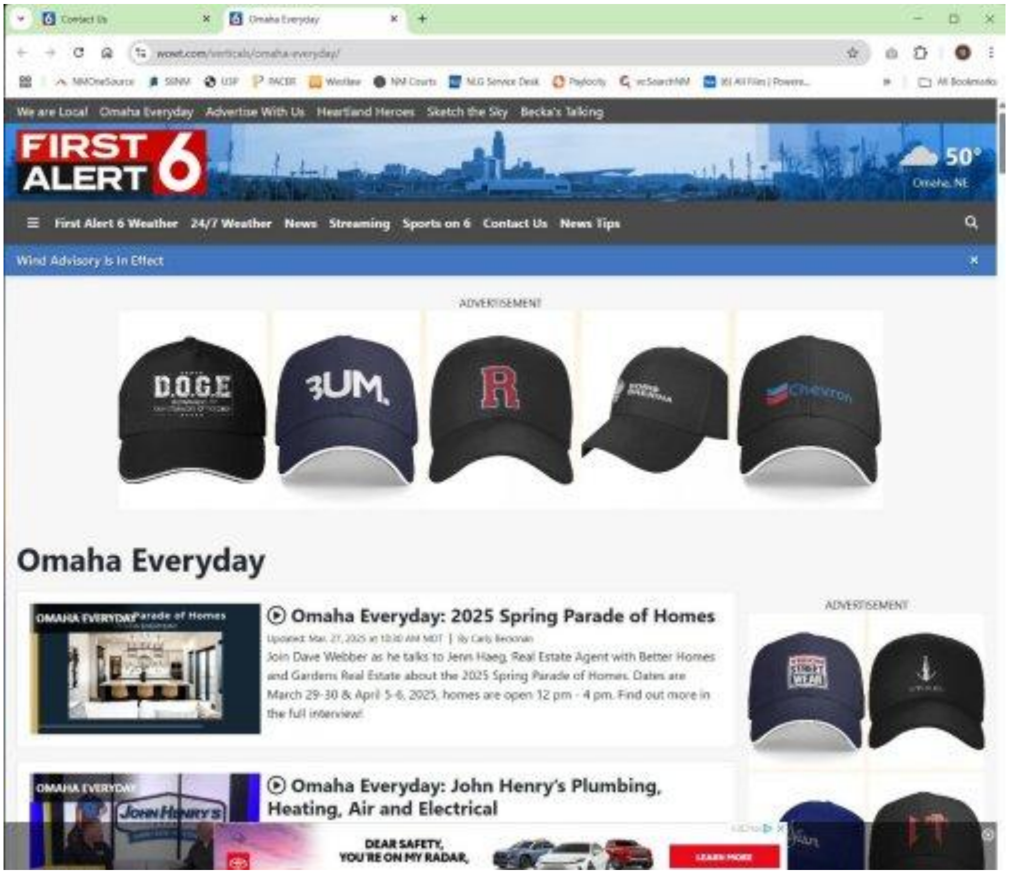
[121] https://www.facebook.com/ads/library/?id=498679473018532

[122] https://www.facebook.com/ads/library/?id=512805074562820

[123] See Figure H.

[124] See Figure I.

and Isuzu[125]. When the user clicked on the images of the infringing hats, the user was redirected to Temu store listings for the hats bearing the infringing logos.



Omaha Everyday

Omaha Everyday: 2025 Spring Parade of Homes

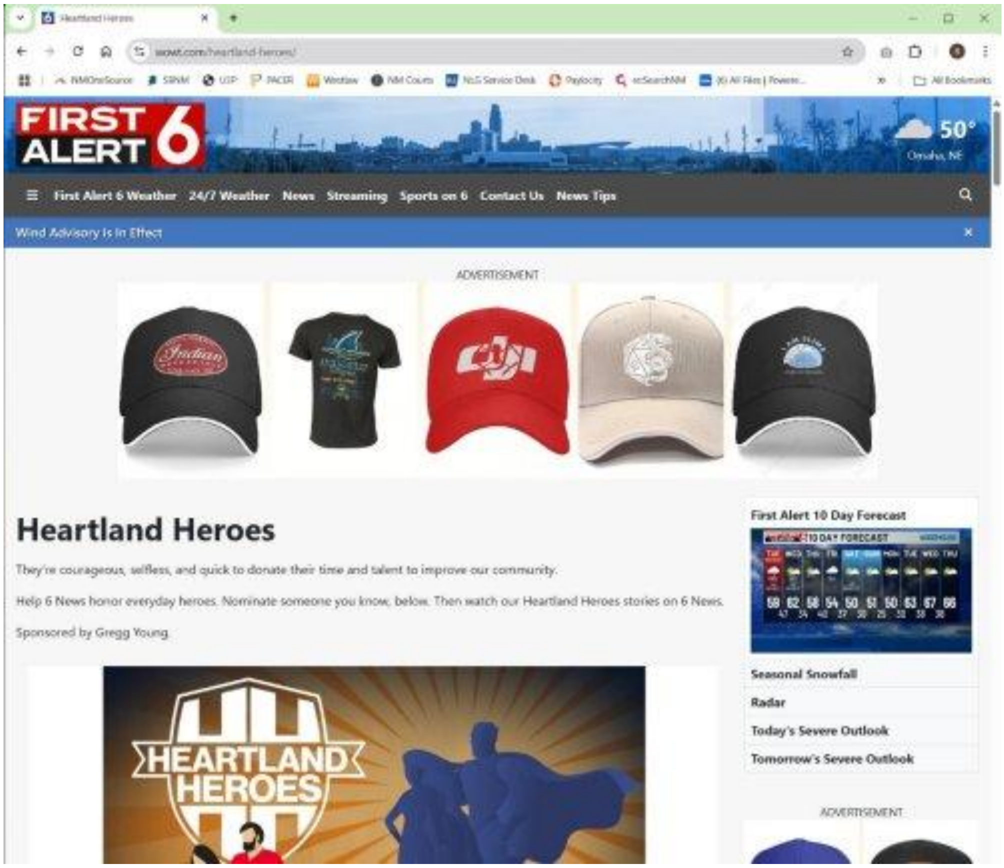
Updated: Mar. 27, 2025 at 10:30 AM MDT | By Carly Beckman

Join Dave Webber as he talks to Jenn Haeg, Real Estate Agent with Better Homes and Gardens Real Estate about the 2025 Spring Parade of Homes. Dates are March 29-30 & April 5-6, 2025, homes are open 12 pm - 4 pm. Find out more in the full interview!

Omaha Everyday: John Henry's Plumbing, Heating, Air and Electrical

Figure H

[125] See Figure J.



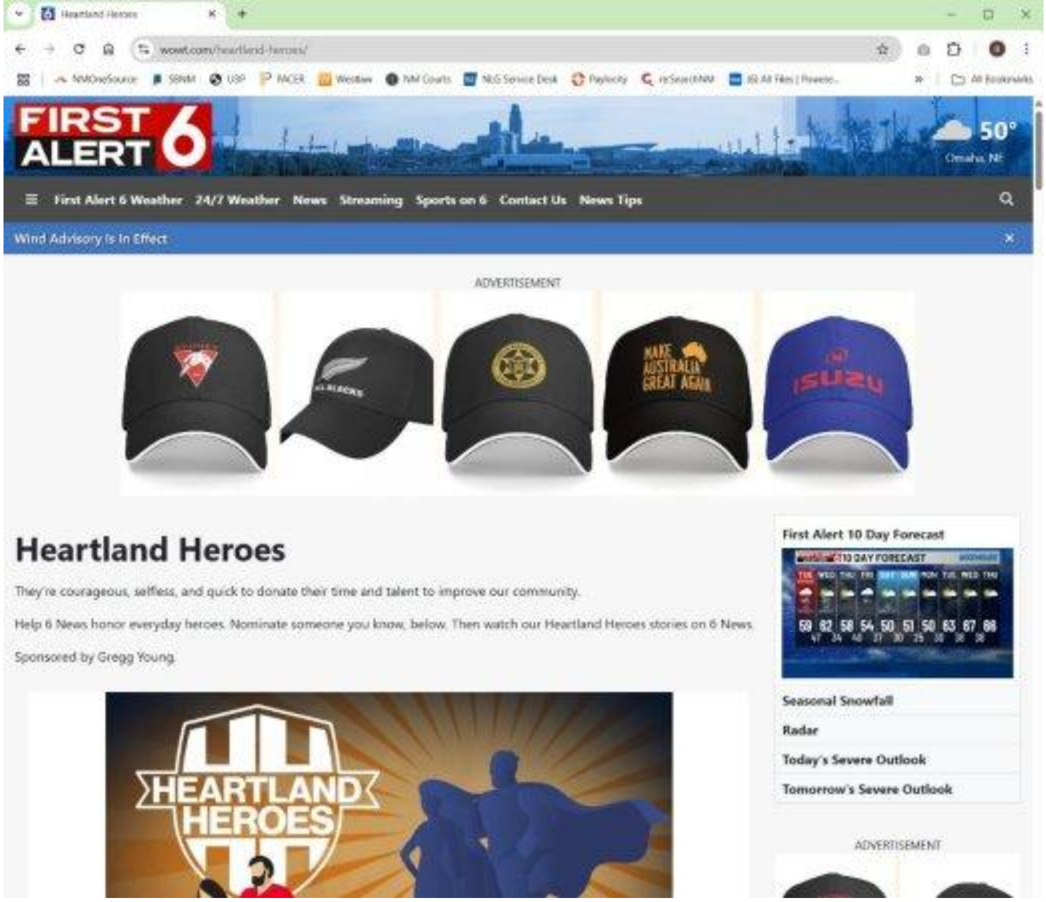
Heartland Heroes

They're courageous, selfless, and quick to donate their time and talent to improve our community.

Help 6 News honor everyday heroes. Nominate someone you know, below. Then watch our Heartland Heroes stories on 6 News.

Sponsored by Gregg Young.

Figure I



Heartland Heroes

They're courageous, selfless, and quick to donate their time and talent to improve our community.

Help 6 News honor everyday heroes. Nominate someone you know, below. Then watch our Heartland Heroes stories on 6 News.

Sponsored by Gregg Young.

Figure J

viii. "Greenwashing"

220. In order to further incentivize consumers to purchase products on its site, Temu also deceptively represents that it donates a portion of sales through the app to charity as part of a "Tree Planting Program," by placing information about that program immediately below the "Add to cart" button, "Free shipping" information, and "Free returns" information on the product page.

221. Temu claims that it has planted "18M+ trees," through a charity called "Trees for the Future," without disclosing any

information about what portion of each sale is donated to charity. Temu claims that donations to Trees for the Future are "funded by users worldwide who donate by clicking 'Donate with Temu' at checkout *and by Temu*."[126] (Emphasis added). Trees for the Future displays its "Corporate Partners" on its website, ranking them by the "number of trees planted" by each partner. The charity lists eleven "Corporate Partners" that have "planted" more than 1-million trees. Temu is listed as the third largest "tree planter," with "18-million trees planted". According to Trees for the Future's 2023audited financial statements, the charity received $12.9 million in total contributions and grants in 2023.[127]

222. On information and belief, Temu's annual revenue in 2023 was approximately $18 billion. Even assuming that the donations to Trees for the Future are funded entirely by Temu from its business revenue, and none of the donations were funded by individual Temu customers making the donations *in addition* to payment for purchases from Temu, the most generous possible calculation of Temu's own contributions to Trees for the Future would account for less than one third of one hundredth of one percent (.03%) of Temu's total revenue in 2023. This ratio is not disclosed to customers when they make a purchase from Temu.

VI. CLAIMS

<u>COUNT 1:</u>
VIOLATIONS OF THE CONSUMER PROTECTION ACT PRIVACY HARMS
(Neb. Rev. Stat. § 59-1602 et seq.)

[126] https://www.temu.com/tree-landing.html (last accessed 3/31/2025).

[127] Trees for the Future Independent Audit Report 2023, Nov. 15, 2024 (available at https://trees.org/wp-content/uploads/2024/11/TREES-2023-Audit-Report.pdf) (last accessed 3/31/25).

223. The State of Nebraska re-alleges the facts above and incorporates them herein by reference.

224. Defendants are "persons" within the meaning of the Consumer Protection Act, Neb. Rev. Stat. § 59-1601(1).

225. Defendants conduct "trade or commerce" within the meaning of the Consumer Protection Act, Neb. Rev. Stat. § 59-1601(2).

226. The Consumer Protection Act, § 59-1602, prohibits acts and practices that are "unfair" or "deceptive" in the conduct of any trade or commerce.

227. An act or practice is unfair if it is offensive to public policy, immoral, unethical, oppressive, unscrupulous, or falls within some common law, statutory, or other established concept of unfairness, or causes substantial injury to consumers.

228. An act or practice is deceptive if it possesses the tendency or capacity to mislead or creates the likelihood of deception.

229. The conduct complained of herein violates the CPA. 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—potentially 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.

230. 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 Nebraska.

231. 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 Nebraskans 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.

232. Each and every instance of unfair conduct and each and every instance of deceptive conduct constitutes a separate and independent violation of the Consumer Protection Act, Neb. Rev. Stat. § 59-1602.

COUNT 2:
VIOLATIONS OF THE CONSUMER PROTECTION ACT
COMMERCIAL HARMS
(Neb. Rev. Stat. § 59-1602 et seq.)

233. The State of Nebraska re-alleges the facts above and incorporates them herein by reference.

234. Defendants are "persons" within the meaning of the Consumer Protection Act, Neb. Rev. Stat. § 59-1601(1).

235. Defendants conduct "trade or commerce" within the meaning of the Consumer Protection Act, Neb. Rev. Stat. § 59-1601(2).

236. The Consumer Protection Act, § 59-1602, prohibits acts and practices that are “unfair” or “deceptive” in the conduct of any trade or commerce.

237. An act or practice is unfair if it is offensive to public policy, immoral, unethical, oppressive, unscrupulous, or falls within some common law, statutory, or other established concept of unfairness, or causes substantial injury to consumers.

238. An act or practice is deceptive if it possesses the tendency or capacity to mislead or creates the likelihood of deception.

239. As described in Section G above, Defendants engaged in commercial related deceptive acts or practices in violation of the Consumer Protection Act, § 59-1602.

240. Each and every instance unfair conduct and each and every instance of deceptive conduct constitutes a separate and independent violation of the Consumer Protection Act, Neb. Rev. Stat. § 59-1602.

COUNT 3:

VIOLATIONS OF THE UNIFORM DECEPTIVE TRADE PRACTICES ACT PRIVACY HARMS (Neb. Rev. Stat. § 87-301 et seq.)

241. The State of Nebraska re-alleges the facts above and incorporates them herein by reference.

242. Section 87-302(a) of the Uniform Deceptive Trade Practices Act specifies multiple practices, which when conducted in the course of business, constitutes a deceptive trade practice, including, without limitation:

a. Representing that goods or services have characteristics, uses, and benefits that they do not have; Neb. Rev. Stat. § 87-302(a)(5)

b. Representing that goods or services do not have characteristics, uses, and benefits that they do have; Neb. Rev. Stat. § 87-302(a)(6).

c. Representing that goods or services are of a particular standard, quality, or grade if they are of another; Neb. Rev. Stat. § 87-302(a)(8)

d. Knowingly making a false or misleading statement in a privacy policy, published on the Internet or otherwise distributed or published, regarding the use of personal information submitted by members of the public. Neb. Rev. Stat. § 87-302(a)(15).

243. An unconscionable act or practice by a supplier in connection with a consumer transaction is also a violation of the Unform Deceptive Trade Practices Act, Neb. Rev. Stat. § 87-303.01(1).

244. The unconscionability of an act or practice is a question of law for the court. § 87-303.01(2).

245. Defendants are "persons" within the meaning of the Uniform Deceptive Trade Practices Act, Neb. Rev. Stat. § 87-301(19).

246. The conduct complained of herein constitutes both deceptive and unconscionable practices under the UDTPA. 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—potentially 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.

247. 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 Nebraska.

248. 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 Nebraskans 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.

249. Each and every instance of a deceptive trade practice and each and every instance of an unconscionable trade practice constitutes a separate and independent violation of the Uniform Deceptive Trade Practices Act. Neb. Rev. Stat. §§ 87-302 and 87-303.01.

COUNT 4:

VIOLATIONS OF THE UNIFORM DECEPTIVE TRADE PRACTICES ACT

COMMERCIAL HARMS
(Neb. Rev. Stat. § 87-301 et seq.)

250. The State of Nebraska re-alleges the facts above and incorporates them herein by reference.

251. Section 87-302(a) of the Uniform Deceptive Trade Practices Act specifies multiple practices, which when conducted in the course of business, constitutes a deceptive trade practice, including, without limitation:

a. Passing off goods or services as those of another; Neb. Rev. Stat. § 87-302(a)(1)

b. Causing likelihood of confusion or of misunderstanding as to the source, approval, or certification of goods or services; Neb. Rev. Stat. § 87-302(a)(2);

c. Causing likelihood of confusion or of misunderstanding as to affiliation, connection, or association with, or certification by, another; Neb. Rev. Stat. § 87-302(a)(3);

d. Using deceptive representations or designations of geographic origin in connection with goods or services; Neb. Rev. Stat. § 87-302(a)(4);

e. Representing that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits, or quantities that they do not have or that a person has a sponsorship, approval, status, affiliation, or connection that [it] does not have; Neb. Rev. Stat. § 87-302(a)(5);

f. Representing that goods or services are of a particular standard, quality, or grade, or that goods are of a particular style or model, if they are of another; Neb. Rev. Stat. § 87-302(a)(8);

g. Advertising goods or services with intent not to sell them as advertised or advertises the price in any manner calculated or tending to mislead or in any way deceive a person; Neb. Rev. Stat. § 87-302(a)(10);

h. Making false or misleading statements of fact concerning the reasons for, existence of, or amounts of price reductions; Neb. Rev. Stat. § 87-302(a)(12);

i. With respect to a sale or lease to a natural person of goods or services purchased or leased primarily for personal, family, household, or agricultural purposes, using or employing any referral or chain referral sales technique, plan, arrangement, or agreement; Neb. Rev. Stat. § 87-302(a)(14); and

j. In connection with the solicitation of funds or other assets for any charitable purpose, or in connection with any solicitation which represents that funds or assets will be used for any charitable purpose, using or employing any deception, fraud, false pretense, false promise, misrepresentation, unfair practice, or concealment, suppression, or omission of any material fact. Neb. Rev. Stat. § 87-302(a)(21).

252. An unconscionable act or practice by a supplier in connection with a consumer transaction is also a violation of the Unform Deceptive Trade Practices Act, Neb. Rev. Stat. § 87-303.01(1).

253. The unconscionability of an act or practice is a question of law for the court. § 87-303.01(2).

254. Defendants are “persons” within the meaning of the Uniform Deceptive Trade Practices Act, Neb. Rev. Stat. § 87-301(19).

255. As described in Section G above, Defendants engaged in commercial related deceptive acts or practices and unconscionable acts or practices in violation of the Consumer Protection Act, § 59-1602.

256. Each and every instance of a deceptive trade practice and each and every instance of an unconscionable trade practice constitutes a separate and independent violation of the Uniform Deceptive Trade Practices Act. Neb. Rev. Stat. §§ 87-302 and 87-303.01.

VII. PRAYER FOR RELIEF

WHEREFORE, Plaintiff respectfully requests that the Court enter judgment against Defendants and enter an Order:

1. Finding that Defendants violated the CPA, Neb. Rev. Stat. § 59-1602; and the UDTPA §§ 87-302-303 by engaging in the unlawful acts and practices alleged herein, and permanently enjoining Defendants from continuing to engage in such unlawful acts and practices;

2. Requiring Defendants to pay civil penalties pursuant to Neb. Rev. Stat. §§ 59-1614 and 87-303.11, and pay direct economic damages for each affected Nebraska resident pursuant to Neb. Rev. Stat. § 87-806;

3. Requiring Defendants to pay restitution to affected Nebraska residents pursuant to Neb. Rev. Stat. §59-1608(2) and § 87-303.05(1);

4. Requiring Defendants to pay all costs and fees for the prosecution and investigation of this action pursuant to Neb. Rev. Stat. §§ 59-1608 and 87-303(b);

5. Enjoining Defendants from committing or continuing to commit further deceptive or unconscionable trade practices pursuant to Neb. Rev. Stat. § 87-303.05(1);

6. Enjoining Defendants from committing or continuing to commit further unfair or deceptive acts or practices pursuant to Neb. Rev. Stat. § 59-1608(1); and

7. Granting any such further relief as the Court may deem appropriate.

JURY DEMAND

The State demands a trial by jury on all issues so triable.

DATED: June 11, 2025

MICHAEL T. HILGERS, #24483
Nebraska Attorney General

By: *__/s/ Anna M. Anderson__*

Anna M. Anderson, #28080
Benjamin Swanson, #27675
Beatrice O. Strnad, #28045
CONSUMER PROTECTION BUREAU
OFFICE OF THE ATTORNEY GENERAL
2115 State Capitol
Lincoln, NE 68509-8920
Phone: (402) 471-2811
anna.anderson@nebraska.gov
benjamin.swanson@nebraska.gov
bebe.strnad@nebraska.gov

Brian E. McMath, *pro hac pending*

Brian L. Moore, *pro hac pending*
Michaela Hohweiler, #26826
NACHAWATI LAW GROUP
5489 Blair Road
Dallas, Texas 75231
Telephone: (214) 890-0711
bmcmath@ntrial.com
bmoore@ntrial.com
mhohwieler@ntrial.com

David F. Slade, *pro hac pending*
WADE KILPELA SLADE
1 Riverfront Place, Suite 745
North Little Rock, Arkansas 72114
slade@waykayslay.com

Attorneys for the State of Nebraska