

**IN THE DISTRICT COURT
OF KEITH COUNTY, NEBRASKA**

STATE OF NEBRASKA, ex rel.
MICHAEL T. HILGERS,
ATTORNEY GENERAL,

Plaintiff,

v.

TP-LINK SYSTEMS INC.,

Defendant.

Case No: CI 26-_____

COMPLAINT

COMES NOW, the State of Nebraska, ex rel. Michael T. Hilgers, Nebraska Attorney General, by and through the undersigned attorneys (“Attorney General,” “State,” or “Plaintiff”), and hereby brings this action against TP-Link Systems Inc. (“TP-Link” or “Defendant”), to address a pattern of deceptive and unfair business practices related to the marketing and sale of TP-Link routers, other devices, and related applications and services. TP-Link represents to its customers, among other things, that it can “cover[] all security scenarios” for network security; that it “maintain[s] network security and device security anytime anywhere”; that its devices are “well protected”; and that it “Handles All Your Concerns,” “Protects Comprehensively,” “Protects All Devices,” “Protects Everywhere,” and has “preventions against any potential cyber threats or attacks for your home network.”¹

TP-Link’s representations are false, misleading, deceptive, and conceal material facts about: (1) TP-Link’s past and ongoing ties to the People’s Republic of China (“PRC” or “China”), including a supply chain rooted in China and Chinese government subsidies; (2) TP-Link’s

¹ TP-Link, HomeShield, <https://www.tp-link.com/us/homeshield/> (last visited Sept. 18, 2026), archived at <https://perma.cc/M8ME-4EX7>.

repeated firmware vulnerabilities that Chinese state-sponsored hackers and other malicious actors have exploited to attack American consumers and businesses; and (3) the Chinese legal regime that governs TP-Link's Chinese facilities, affiliates, and personnel.

The State seeks to obtain injunctive relief, restitution for consumers, civil penalties, and other equitable relief to address Defendant's 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"), in connection with the advertisement, marketing, promotion, and sale of TP-Link's products and services to Nebraska consumers.

INTRODUCTION

1. A router serves as a consumer's virtual mouth and ears to the internet. What the consumer says to the internet comes out of the router's mouth, and what the internet says back goes through the router's ears. If compromised, it can whisper lies in both directions, impersonating the consumer and creating a foothold in the consumer's own home for state-sponsored cyberattacks. As the Federal Communications Commission has explained, "[c]ompromised routers can enable in-depth network surveillance, data exfiltration, botnet attacks, and unauthorized access to U.S. government or American businesses' networks."²

2. Such activity not only puts a consumer's internet connection at risk but also makes consumers involuntary participants in malicious campaigns carried out on behalf of foreign nations—something no Nebraska consumer would consent to.

3. Home- and small-office routers are typically housed within a consumer's own home or business and use the consumer's assigned IP address. Given the sensitive information that consumers

² FCC's Public Safety and Homeland Security Bureau Announces Addition of Routers Produced in Foreign Countries to FCC Covered List, WC Docket No. 18-89, Public Notice, DA 26-278, App. C at 1 (Mar. 23, 2026) ("Routers Public Notice").

send and receive over the internet via their routers, it is imperative that companies that manufacture and market routers speak truthfully about their devices' functions and security risks.

4. TP-Link has amassed a large market share of the routers that consumers and small businesses purchase at retail. According to congressional testimony, TP-Link controls at least 60 percent of the United States retail market for Wi-Fi systems and small-office/home-office routers.³

5. Recognizing the importance of security to its consumers, TP-Link repeatedly represents that its routers have robust protections and features. For example, TP-Link tells consumers that its built-in “HomeShield” service “covers all security scenarios,” “handles all your concerns” regarding “cyber virus intrusion” and “IoT device attacks,” and allows the user to “[c]heck the results of the scans and preventions against any potential cyber threats or attacks for your home network.”⁴ A version of TP-Link’s website available as recently as November 2025 represented that HomeShield provides a “100% safeguard” for network security.⁵

6. TP-Link also makes model-specific security representations about its routers. TP-Link advertised its TL-WR940N router as providing “[e]asy wireless security encryption at a push of [a] WPS button,” its Archer C7 as “provid[ing] secure Wi-Fi access for

³ End the Typhoons: How to Deter Beijing’s Cyber Actions and Enhance America’s Lackluster Cyber Defenses Before the H. Select Comm. on the Strategic Competition Between the U.S. and the Chinese Communist Party, 119th Cong. (Mar. 5, 2025) (statement of Rob Joyce, former Dir. of Cybersecurity, Nat’l Sec. Agency), <https://docs.house.gov/meetings/ZS/ZS00/20250305/117983/HHRG-119-ZS00-Wstate-JoyceR-20250305.pdf> (“TP-Link, the world’s largest manufacturer of commercial Wi-Fi and home routers has grown to at least 60% of the U.S. retail market for Wi-Fi systems and SoHo routers compared with about 10% of the market at the start of 2019.”).

⁴ TP-Link, HomeShield, <https://www.tp-link.com/us/homeshield/> (last visited Sept. 18, 2026), archived at <https://perma.cc/M8ME-4EX7>.

⁵ TP-Link, HomeShield (archived Nov. 14, 2025), <https://web.archive.org/web/20251114185316/https://www.tp-link.com/us/homeshield/>.

guests,” and its Archer AX21 as offering “Refined Password Security” and a “New Level of Cyber Security.”⁶

7. TP-Link’s representations to Nebraska consumers are false, deceptive, and unfair. First, TP-Link minimizes the risks to consumers from its longstanding and ongoing connections to China. By its own admission, TP-Link was not a separate company from its Chinese operations until 2024. China has been designated a foreign adversary by the U.S. government.⁷ Under China’s 2017 National Intelligence Law, Chinese companies and citizens are required to “support, assist, and cooperate with national intelligence efforts in accordance with law” and to “protect national intelligence work secrets they are aware of.”⁸ Under China’s 2021 Regulations on the Management of Security Vulnerabilities in Network Products (“RMSV”), Chinese tech providers and network operators are required to report (within 2 days) any newly discovered (“zero-day”) security vulnerabilities.⁹ A senior U.S. Department of Homeland Security

⁶ TP-Link, TL-WR940N Product Page (archived Mar. 29, 2023), <https://web.archive.org/web/20230329192916/https://www.tp-link.com/us/home-networking/wifi-router/tl-wr940n/>; TP-Link, Archer C7 Product Page (archived Mar. 31, 2026), <https://web.archive.org/web/20260331134655/https://www.tp-link.com/us/home-networking/wifi-router/archer-c7/>; TP-Link, Archer AX21 Product Page (archived Oct. 6, 2022), <https://web.archive.org/web/20221006205422/https://www.tp-link.com/us/home-networking/wifi-router/archer-ax21/>.

⁷ 15 C.F.R. § 791.4.

⁸ PRC National Intelligence Law art. 7 (as amended 2018), China Law Translate (June 27, 2017), <https://www.chinalawtranslate.com/en/national-intelligence-law-of-the-p-r-c-2017/>. The Chinese-language original has been rendered in varying English translations; *compare id.*, with https://cs.brown.edu/courses/cs180/sources/2017_06_28_China_NationalIntelligenceLawOfThePeoplesRepublicOfChina.pdf.

⁹ Stewart Scott et al., *Dragon Tails: Preserving International Cybersecurity Research*, Atlantic Council (Sept. 2022), <https://www.atlanticcouncil.org/in-depth-research-reports/report/preserving-international-cybersecurity-research/>; *see also* Suzanne Smalley, *China Could Be Reviewing Security Bugs Before Tech Companies Issue Patches, DHS Official Says*, CyberScoop (Aug. 10, 2022), <https://cyberscoop.com/dhs-official-chinese-rules-exploit/> (reporting remarks of DHS Under Secretary for Policy Robert Silvers).

(“DHS”) official has reported that China appears to use the RMSV to preview zero-day flaws before companies can develop fixes.

8. By TP-Link’s own admission, it was affiliated with a Chinese company until 2024, when it finalized its separation from TP-Link Technologies Co., Ltd. (“TP-Link Technologies”).

9. Even following its claimed split in mid-2024, TP-Link still makes misleading statements about its ties to China. TP-Link represents that “[a]s a company headquartered in the United States, no government – foreign or domestic – has access to and control over the design and production of our routers and other devices.”¹⁰ But much of TP-Link’s research, development, and manufacturing remains in China, entrenched in China’s state-sponsored technology ecosystem, with the company’s leadership acknowledging accolades and subsidies from the Chinese government.¹¹ And in June 2026, the U.S. Department of Defense designated TP-Link Technologies—the entity from which Defendant claims complete separation—a Chinese military company operating directly or indirectly in the U.S.¹²

10. TP-Link also represents that it manufactures its products for the U.S. market in its own factory in Vietnam, and that manufacturing in its own facilities “provides another layer of security and governance for the supply chain.”¹³ In truth, only 0.5% of the

¹⁰ TP-Link, Fact Sheet, <https://www.tp-link.com/us/landing/fact-sheet/> (last visited Sept. 18, 2026), archived at <https://perma.cc/9LWY-L3NU>.

¹¹ Kate O’Keeffe, *Wi-Fi Giant TP-Link’s US Future Hinges on Its Claimed Split From China*, Bloomberg (Apr. 11, 2025), <https://www.bloomberg.com/news/articles/2025-04-11/wi-fi-giant-tp-link-s-us-future-hinges-on-its-claimed-split-from-china>.

¹² Notice of Availability of Designation of Chinese Military Companies, 91 Fed. Reg. 35189, 35193 (June 10, 2026) (designating TP-Link Technologies Co., Ltd.); U.S. Dep’t of Def., Entities Identified as Chinese Military Companies Operating in the United States in Accordance with Section 1260H of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 (June 8, 2026), <https://media.defense.gov/2026/Jun/08/2003945537/-1/-1/1/ENTITIES-IDENTIFIED-AS-CHINESE-MILITARY-COMPANIES-OPERATING-IN-THE-UNITED-STATES-IN-ACCORDANCE-WITH-SECTION-1260H.PDF>.

¹³ TP-Link, Fact Sheet, <https://www.tp-link.com/us/landing/fact-sheet/> (last visited Sept. 18, 2026), archived at <https://perma.cc/9LWY-L3NU>; *see also* TP-Link, TP-Link Systems Inc. Sets the Record Straight Regarding Inaccurate Testimony at House

components in TP-Link’s Vietnamese plant by value are bought in Vietnam—all other inputs are imported from or through China. And a U.S.-designated Chinese military company performed recent construction at the Vietnam factory, further evidencing the deceptiveness of TP-Link’s assurances of additional security based on its Vietnam activities.¹⁴

11. Second, TP-Link deceives consumers into thinking their routers are secure, when this is simply not the case. TP-Link’s routers have contained critical, actively exploited firmware vulnerabilities. These security vulnerabilities were exploited by Chinese state hackers to weaponize consumers’ routers in the Volt and Flax Typhoon attacks according to congressional testimony. As Rob Joyce, the former Director of Cybersecurity of the National Security Agency, testified, “TP-Link routers were among the various brands exploited by Chinese state-sponsored hackers” in various attacks.¹⁵

12. Microsoft has likewise reported that a covert network comprised predominantly of compromised TP-Link routers has been

Select Committee on the CCP Hearing (Mar. 5, 2025) (“TP-Link manufactures our routers in Vietnam in our own facility, while others in our segment continue to outsource manufacturing to Chinese original design manufacturers.”), <https://www.tp-link.com/us/press/news/21656/>, archived at <https://perma.cc/U5HT-36AN>.

¹⁴ TP-Link, Fact Sheet, <https://www.tp-link.com/us/landing/fact-sheet/> (last visited Sept. 18, 2026), archived at <https://perma.cc/9LWY-L3NU>; Kate O’Keeffe, *Wi-Fi Giant TP-Link’s US Future Hinges on Its Claimed Split From China*, Bloomberg (Apr. 11, 2025), <https://www.bloomberg.com/news/articles/2025-04-11/wi-fi-giant-tp-link-s-us-future-hinges-on-its-claimed-split-from-china>; Kate O’Keeffe, *Wi-Fi Giant’s Vietnam Factory Raises Questions Over China Split*, Bloomberg (Nov. 22, 2025), <https://www.bloomberg.com/news/articles/2025-11-22/wi-fi-giant-s-vietnam-factory-raises-questions-over-china-split>; Notice of Availability of Designation of Chinese Military Companies, 91 Fed. Reg. 35189, 35191 (June 10, 2026) (designating China State Construction Engineering Corporation Limited).

¹⁵ End the Typhoons: How to Deter Beijing’s Cyber Actions and Enhance America’s Lackluster Cyber Defenses before the House Select Committee on the Strategic Competition Between the United States and the Chinese Communist Party, 119th Cong. (March 5, 2025) (statement of Rob Joyce), <https://docs.house.gov/meetings/ZS/ZS00/20250305/117983/HHRG-119-ZS00-Wstate-JoyceR-20250305.pdf>.

used by Chinese threat actors to conduct credential-theft attacks against American organizations.¹⁶

13. Nor are Chinese state actors the only ones exploiting TP-Link’s insecure routers. According to the FBI and NSA, Russia’s GRU foreign military intelligence agency has exploited a critical vulnerability in TP-Link’s TL-WR940N router to conduct adversary-in-the-middle attacks—attacks in which a consumer believes he or she is securely communicating with services such as Microsoft Outlook Web Access while the GRU views the traffic unencrypted.¹⁷

14. TP-Link’s deception regarding security also extends to default settings—which for many routers, including the Archer AX21 v1 and v1.20, do not support automatic firmware updates. TP-Link no longer provides updates for the AX21 v1 and v1.20 at all, contending that these models reached “end of life” in May 2024.¹⁸

15. Third, TP-Link reserves the right not only to collect Nebraska consumers’ personal data—including email addresses, location, and mobile phone identifiers—but also to share that data with “affiliates” to “comply with applicable laws” and to protect the rights of “others.”¹⁹ TP-Link’s conduct is deceptive because it does not

¹⁶ Microsoft Threat Intelligence, Chinese threat actor Storm-0940 uses credentials from password spray attacks from a covert network, Microsoft (October 31, 2024), <https://www.microsoft.com/en-us/security/blog/2024/10/31/chinese-threat-actor-storm-0940-uses-credentials-from-password-spray-attacks-from-a-covert-network/>.

¹⁷ Nat’l Sec. Agency, NSA Supports FBI in Highlighting Russian GRU Threats Against Routers (Apr. 7, 2026), <https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/4453919/nsa-supports-fbi-in-highlighting-russian-gru-threats-against-routers/>; Fed. Bureau of Investigation, Russian GRU Exploiting Vulnerable Routers to Steal Sensitive Information, Alert No. I-260407-PSA (Apr. 7, 2026), <https://media.defense.gov/2026/Apr/07/2003907743/-1/-1/0/I-260407-PSA.PDF>.

¹⁸ TP-Link, End of Life Products (FAQ No. 3562), <https://www.tp-link.com/us/support/faq/3562/> (last updated Sept. 18, 2026) (linking the EOL List for Home Network); TP-Link, End-of-Life Policy, <https://privacy.tp-link.com/web/website/policy> (last visited Sept. 18, 2026) (“TP-Link discontinues support and maintenance, including security updates, for such products.”)

¹⁹ TP-Link, Tether Privacy Policy (August 20, 2026), <https://privacy.tp-link.com/app/Tether/privacy>; TP-Link, Deco Privacy Policy (January 5, 2026),

disclose its Chinese affiliations and the impact of the 2017 Chinese National Intelligence Law that may expose any collected or shared data to potential access by PRC intelligence agencies under PRC law.

16. The federal government has taken notice. The U.S. Departments of Commerce, Defense, and Justice have reportedly opened investigations into TP-Link,²⁰ and federal officials have weighed banning the sale of TP-Link routers in the United States as an “unacceptable risk” to national security.²¹ In March 2026, the FCC’s Public Safety and Homeland Security Bureau announced the addition of routers produced in foreign countries to the FCC’s Covered List, and it has since been reported that TP-Link is seeking conditional FCC approval to sell new router models in the United States.²²

17. TP-Link’s conduct has placed Nebraska consumers at risk of harm by making their home and small-office networks vulnerable to exploitation and intrusion by foreign actors with a proven track record of nefarious conduct. That risk is ongoing: many consumers keep their routers for years, and many of the compromised TP-Link models in Nebraska homes do not support automatic firmware updates and no longer receive security support at all.²³

<https://privacy.tp-link.com/app/Deco/privacy>; TP-Link, Tapo Privacy Policy (January 23, 2026), <https://privacy.tp-link.com/app/tapo/privacy> (each last visited Sept. 22, 2026).

²⁰ Heather Somerville, Dustin Volz, and Aruna Viswanatha, *U.S. Weighs Ban on China-Made TP-Link Routers*, The Wall Street Journal (December 18, 2024).

²¹ Kate O’Keeffe, Josh Sisco, and Kate Sullivan, *US Weighs Action Against China-Linked Router Giant TP-Link*, Bloomberg (October 9, 2025).

²² FCC’s Public Safety and Homeland Security Bureau Announces Addition of Routers Produced in Foreign Countries to FCC Covered List, WC Docket No. 18-89, Public Notice, DA 26-278 (Mar. 23, 2026), <https://docs.fcc.gov/public/attachments/DA-26-278A1.pdf>; Michael Kan, *Facing Router Ban, TP-Link Tells FCC It’s Investing Hundreds of Millions in the US*, PCMag (Apr. 23, 2026), <https://www.pcmag.com/news/facing-router-ban-tp-link-tells-fcc-its-investing-hundreds-of-millions>.

²³ Nicholas De Leon, *How to Tell When It’s Time to Replace Your Router*, Consumer Reports (Apr. 30, 2021), <https://www.consumerreports.org/electronics-computers/wireless-routers/how-to-tell-when-its-time-to-replace-your-router-a5475786635/> (last visited Sept. 18, 2026) (quoting Richard Fisco, who oversees

18. The Attorney General brings this action to enjoin TP-Link's unlawful practices; obtain appropriate relief for Nebraska consumers; and protect Nebraskans from having their privacy and security further jeopardized by TP-Link's deceptive, unfair, and unconscionable acts.

AUTHORITY & PUBLIC INTEREST

19. The Nebraska Attorney General is responsible for enforcing the CPA, UDTPA, and other state and federal laws that affect Nebraska consumers.

20. Under Neb. Rev. Stat. § 59-1608, the Attorney General may bring an action in the name of the State of Nebraska against any person to restrain and prevent the doing of any act prohibited by the CPA.

21. Under Neb. Rev. Stat. § 87-303.05, the Attorney General may apply for and obtain, in an action in any district court of Nebraska, a temporary restraining order, or injunction, or both, prohibiting such person from continuing or engaging in any deceptive trade practice, or doing any act in furtherance thereof.

22. The Attorney General has reasonable cause to believe that Defendant has violated the CPA and UDTPA and brings this action in the public interest because Defendant has deceived, misled, and caused harm to Nebraska consumers.

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

electronics testing for Consumer Reports, as stating that “consumers hold onto their router for dear life and for as long as possible”)

PARTIES

24. The State of Nebraska, by and through its Attorney General and on behalf of all of Nebraska’s citizens and consumers, is the Plaintiff in this action.

25. The Attorney General of Nebraska is Nebraska’s Chief Law Enforcement Officer. The Attorney General is expressly authorized to enforce Nebraska’s consumer protection laws, including both the Consumer Protection Act and the Uniform Deceptive Trade Practices Act. Neb. Rev. Stat. §§ 59-1608(1), 87-303.05(1).

26. In addition to that express statutory authority, the Attorney General has standing to bring legal action, in the name of the State, when the object of that action is a suit to vindicate the public interest. *See, e.g., State ex rel. Meyer v. Peters*, 188 Neb. 817, 819–21, 199 N.W.2d 738, 739–41 (1972); *State v. Pacific Express Co.*, 80 Neb. 823, 115 N.W. 619, 620–23 (1908).

27. Defendant is a foreign corporation that has identified its corporate headquarters as being located at 10 Mauchly, Irvine, CA 92618,²⁴ and its principal address as 5 Peters Canyon Road, Suite 300, Irvine, CA 92606.²⁵

28. TP-Link transacts business in Nebraska by marketing, offering, and selling TP-Link-branded routers and other devices, and related applications and services, to Nebraska consumers. These retailers include Amazon, Best Buy, Costco, Walmart, Target, Home Depot, Lowe’s, Sam’s Club, Staples, Office Depot, Nebraska Furniture Mart, and others. *See* <https://www.tp-link.com/us/where-to-buy/>.

29. At all relevant times, Defendant acted directly and through its affiliates, agents, and related entities to advertise, promote, import, and sell TP-Link devices in Nebraska, and is

²⁴ TP-Link, Corporate Information, <https://www.tp-link.com/us/about-us/corporate-information/> (last visited Sept. 18, 2026).

²⁵ Cal. Sec’y of State, Business Search, <https://bizfileonline.sos.ca.gov/search/business> (search “TP-Link” and click on TP-Link Systems Inc.) (last visited Sept. 18, 2026).

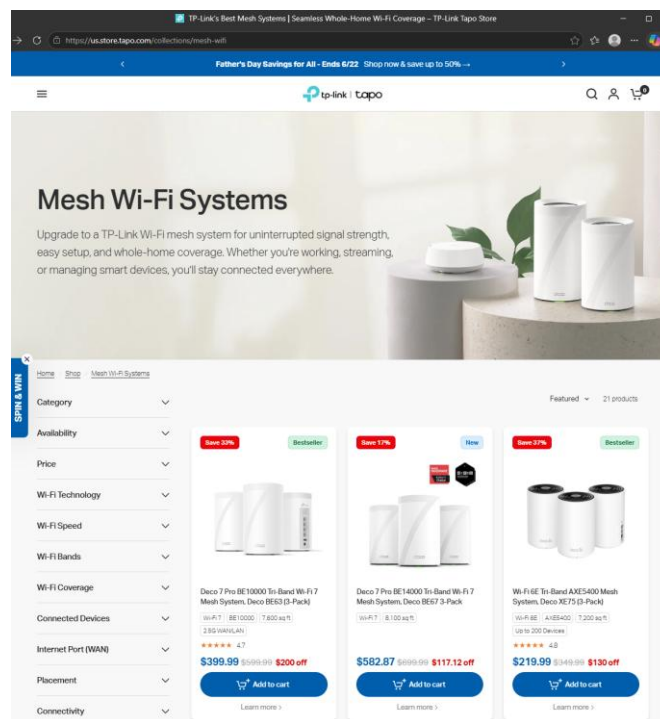
responsible for the deceptive and unfair practices alleged in this Complaint.

JURISDICTION AND VENUE

30. At all times relevant to this Complaint, Defendant was engaged in trade and commerce affecting consumers in Nebraska insofar as it marketed, offered, and sold routers and other products and services to Nebraska residents.

31. TP-Link at all relevant times directly offered and sold routers and other products to Nebraska consumers through its own online websites, including <https://us.store.tp-link.com> and <https://us.store.tapo.com/>.

32. For example, TP-Link directly sells its Deco mesh router systems to consumers in Nebraska.²⁶



²⁶ TP-Link, Deco Mesh Wi-Fi Systems, TP-Link Store, <https://us.store.tapo.com/collections/mesh-wifi> (last visited Sept. 22, 2026), archived at <https://perma.cc/2CAV-E297>.

33. These offers and sales also involve TP-Link specifically touting both its HomeShield service and its various apps, such as its Tether App.²⁷

TP-Link HomeShield: TP-Link's premium security service keeps your home network safe with cutting-edge network and IoT protection. Free features: 1) Basic Network Security including Security Scan and IoT Device Identification; 2) Basic Parental Controls; 3) Quality of Service; 4) Basic Weekly/Monthly Reports. Visit TP-Link's website for more information.

As discussed below, TP-Link's statements regarding these products and services—which it directly sells to Nebraska consumers—are unfair and deceptive and violate the CPA and UDTPA.

34. TP-Link also sells its products and services to Nebraska consumers through online retailers and large national chains.

²⁷ TP-Link, HomeShield & Tether App, TP-Link Store, <https://us.store.tp-link.com> (last visited Sept. 18, 2026), archived at <https://perma.cc/4HNX-YWG5>.

35. TP-Link also directly offers applications such as TP-Link Tether, TP-Link Tapo, TP-Link Deco, and Kasa Smart on Apple’s App Store and Google’s Play Store to Nebraska consumers.²⁸ In addition, the Apple and Google Play stores indicate that these programs also involve “in-app purchases” by consumers.

36. This Court has personal jurisdiction over Defendant because Defendant purposefully availed itself of the privilege of conducting business in Nebraska by advertising and selling thousands of devices to consumers in Nebraska, as well as software to consumers in Nebraska. The conduct and injuries from which this Complaint arises took place in Nebraska, harmed Nebraskans, and targeted Nebraskans.

37. This Court has jurisdiction over the subject matter of this action under Neb. Rev. Stat. §§ 59-1608, 59-1608.01, and 87-303.05, because Defendant has engaged in unfair, deceptive, and unconscionable acts or practices in Nebraska in violation of the CPA and UDTPA.

38. Venue is proper in this Court pursuant to Neb. Rev. Stat. §§ 25-403.01 and 25-403.02 because Defendant transacts business in Nebraska, advertises and sells products to Nebraska residents, the unlawful acts and practices alleged herein caused injury to consumers in this county and throughout the State, and all defendants are nonresidents of this state.

FACTUAL ALLEGATIONS

I. TP-Link Is a China-Founded Company That Remains Dependent on China in Critical Ways

39. TP-Link is a global provider of networking and smart home devices for consumers and small to mid-size organizations. TP-

²⁸ Google Play Store for Android, TP-Link Tether, https://play.google.com/store/apps/details?id=com.tplink.tether&hl=en_US (last visited Sept. 18, 2026); App Store for iPhone, Kasa Smart, <https://apps.apple.com/us/app/kasa-smart/id1034035493> (last visited Sept. 18, 2026).

Link was founded in 1996 by brothers Zhao Jiaxing (“Cliff Chao”) and Zhao Jianjun (“Jeffrey Chao”) in Shenzhen, China, and expanded into the United States market in 2008 by establishing TP-Link USA. By 2016, TP-Link Technology’s reported global revenues (which included the U.S. market) exceeded \$2 billion.

40. TP-Link is a dominant player in the United States’ networking and smart home technology market. According to congressional testimony, TP-Link has a 60 percent or greater share of the United States consumer retail market for Wi-Fi systems and small-office/home-office routers.²⁹ TP-Link’s smartphone applications are ranked among the top downloads in Apple’s App Store “Utilities” category, and TP-Link’s sponsored Amazon listings show tens of thousands of monthly purchases.

41. After more than a decade in the U.S. market, TP-Link announced it had restructured the company into two distinct operations. By 2024, Cliff Chao retained operating control of TP-Link’s Chinese sales through the entity TP-Link Technologies, and Jeffrey Chao became the CEO and owner of Defendant TP-Link Systems Inc. (herein “TP-Link”). TP-Link represented to Nebraskans that this divide “encompass[ed] all shareholdings and operational aspects, including legal entities, workforce, research and development, production, marketing, and customer service.”³⁰

42. In March of 2025, TP-Link again represented to Nebraskans that it had “entirely different ownership, management, and operations” than TP-Link Technologies.³¹ TP-Link also presently

²⁹ End the Typhoons: How to Deter Beijing’s Cyber Actions and Enhance America’s Lackluster Cyber Defenses before the House Select Committee on the Strategic Competition Between the United States and the Chinese Communist Party, 119th Cong. (2025), (statement of Rob Joyce).

³⁰ TP-Link, TP-Link Corporation Group Announces Completion of Corporate Restructuring, Marking a New Era in Its Future Evolution (May 11, 2024), <https://www.tp-link.com/us/press/news/21130/>.

³¹ TP-Link, TP-Link Systems Inc. Sets the Record Straight Regarding Inaccurate Testimony at House Select Committee on the CCP Hearing (March 5, 2025), <https://www.tp-link.com/us/press/news/21656/>.

represents that “[a]s a company headquartered in the United States, no government – foreign or domestic – has access to and control over the design and production of our routers and other devices.”³²

43. Despite its representation that it had completely separated from China, TP-Link admits elsewhere that it “still has substantial operations in mainland China.”³³

44. In fact, the scale of TP-Link’s remaining Chinese operations dwarfs its U.S. presence. According to Bloomberg News, the operations of TP-Link and TP-Link Technologies in China employ approximately 11,000 people, compared to roughly 305 employees based in the United States. Bloomberg reported that “much of the research, development and manufacturing operations of [the] new U.S. company remain in China, entrenched in the country’s state-sponsored technology ecosystem, despite the restructuring.”³⁴ The relatively low number of U.S. employees is consistent with current statistics on LinkedIn, which show only 484 associated members, defined as “LinkedIn members who’ve listed TP-Link Systems Inc. as their current workplace on their profile.”³⁵ One former employee wrote on Glassdoor.com in June 2026, that “Despite efforts to present itself as an American employer, my experience was that TP-Link remains fundamentally a Chinese company operating in the United States. ... U.S.-based leaders often appeared to have less authority than their titles suggested, with major decisions ultimately controlled elsewhere. Transparency was limited, organizational changes were frequent, and priorities often shifted without clear explanation.”³⁶

³² TP-Link, Fact Sheet, <https://www.tp-link.com/us/landing/fact-sheet/> (last visited Sept. 18, 2026), archived at <https://perma.cc/9LWY-L3NU>.

³³ Kate O’Keeffe, *Wi-Fi Giant TP-Link’s US Future Hinges on Its Claimed Split From China*, Bloomberg (Apr. 11, 2025), <https://www.bloomberg.com/news/articles/2025-04-11/wi-fi-giant-tp-link-s-us-future-hinges-on-its-claimed-split-from-china>.

³⁴ *Id.*

³⁵ <https://www.linkedin.com/company/tp-link/about/>

³⁶ <https://www.glassdoor.com/Reviews/Employee-Review-TP-Link-Systems-Inc-E10762893-RVW104415054.htm>

45. TP-Link has operational control over at least four major facilities in China used to manufacture, research, and develop its devices: TP-Link’s Shenzhen Research and Development Center, Shenzhen Manufacturing Center, Dongguan Manufacturing Center, and Shenzhen Guangqiao Manufacturing Center. Further, TP-Link is building a fifth engineering facility in Chengdu, China.³⁷

46. TP-Link has implicitly admitted its continuing Chinese investments. When asked by Bloomberg in April 2025 about a \$180 million investment in the Chengdu engineering facility, TP-Link’s spokesperson stated only that the company “has currently stopped increasing its investments in personnel, R&D, and manufacturing in China.” A purported policy to stop increasing investments is not a separation of “all . . . operational aspects, including . . . research and development[and] production,” as TP-Link represented to the public.³⁸

47. Jeffrey Chao has admitted that TP-Link’s Chinese facilities and subsidiaries have “recently received state accolades and benefits.”³⁹ The Chinese government utilizes subsidies, such as lucrative tax breaks, free land, and expedited permitting for industrial facilities.⁴⁰

48. That relationship—and dependence—runs deeper than financial support. Hunan, a Chinese province, announced that TP-

³⁷ TP-Link, 2024 Sustainability Report, <https://static-page.tp-link.com/sustainability/pdf/TP-Link%202024%20Sustainability%20Report.pdf> (last visited Sept. 18, 2026).

³⁸ Kate O’Keeffe, *Wi-Fi Giant TP-Link’s US Future Hinges on Its Claimed Split From China*, *Bloomberg* (Apr. 11, 2025), <https://www.bloomberg.com/news/articles/2025-04-11/wi-fi-giant-tp-link-s-us-future-hinges-on-its-claimed-split-from-china>; TP-Link, TP-Link Corporation Group Announces Completion of Corporate Restructuring, Marking a New Era in Its Future Evolution (May 11, 2024), <https://www.tp-link.com/us/press/news/21130/>.

³⁹ Kate O’Keeffe, *Wi-Fi Giant TP-Link’s US Future Hinges on Its Claimed Split From China*, *Bloomberg* (Apr. 11, 2025), <https://www.bloomberg.com/news/articles/2025-04-11/wi-fi-giant-tp-link-s-us-future-hinges-on-its-claimed-split-from-china>.

⁴⁰ Christine Clark, *Accelerating the Energy Revolution by Working with China*, *UC San Diego Today* (June 18, 2024), <https://today.ucsd.edu/story/accelerating-the-clean-energy-revolution-by-working-with-china>, (last visited Sept. 18, 2026).

Link's Vietnamese factory was one of its "Key Projects for Foreign Investment and Cooperation." The notice reportedly identified a company—which the U.S. government has designated as a Chinese military company—as working to expand TP-Link's manufacturing, research, and development facilities in Vietnam.⁴¹

49. In June 2026, the U.S. Department of Defense identified TP-Link Technologies—the Chinese entity from which Defendant claims complete separation—as a Chinese military company operating directly or indirectly in the United States under Section 1260H of the National Defense Authorization Act for Fiscal Year 2021.⁴²

50. Even after TP-Link represented to Nebraska consumers that it completely split from TP-Link Technologies, representatives of both companies reportedly attended a Chinese Communist Party event together in China and posted a photograph on social media showing the two employees standing next to each other under the party's hammer-and-sickle emblem, each holding "TP-Link" signs bearing their respective corporate logos.⁴³

51. Reporting and trade data show that TP-Link has imported items into the United States from China for years. TP-Link's shipments from Lianzhou Technologies Co., Ltd. have departed from Shanghai, China to Long Beach, California, as recently as January of 2026. On information and belief, TP-Link Systems Inc. has imported

⁴¹ Kate O'Keeffe, *Wi-Fi Giant's Vietnam Factory Raises Questions Over China Split*, Bloomberg (November 22, 2025), <https://www.bloomberg.com/news/articles/2025-11-22/wi-fi-giant-s-vietnam-factory-raises-questions-over-china-split>.

⁴² Notice of Availability of Designation of Chinese Military Companies, 91 Fed. Reg. 35189, 35193 (June 10, 2026) (designating TP-Link Technologies Co., Ltd.); U.S. Dep't of Def., *Entities Identified as Chinese Military Companies Operating in the United States in Accordance with Section 1260H of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021* (June 8, 2026), <https://media.defense.gov/2026/Jun/08/2003945537/-1/-1/1/ENTITIES-IDENTIFIED-AS-CHINESE-MILITARY-COMPANIES-OPERATING-IN-THE-UNITED-STATES-IN-ACCORDANCE-WITH-SECTION-1260H.PDF>.

⁴³ Kate O'Keeffe, *Wi-Fi Giant TP-Link's US Future Hinges on Its Claimed Split From China*, Bloomberg (Apr. 11, 2025), <https://www.bloomberg.com/news/articles/2025-04-11/wi-fi-giant-tp-link-s-us-future-hinges-on-its-claimed-split-from-china>.

shipments from its Chinese-affiliated companies, such as TP-Link Technologies and Lianzhou Technologies Co., Ltd.⁴⁴

52. On information and belief, TP-Link also utilizes TP-Link USA Corporation to import from China. According to trade information, TP-Link USA Corporation has had shipments from Shanghai, China as recently as December of 2025.⁴⁵ This further shows TP-Link's connection to China regardless of the corporate entity used to receive the goods.

II. China's Legal Regime Compels Cooperation with PRC Intelligence, Including Nearly Contemporaneous Disclosure of Zero-Day Security Vulnerabilities

53. The U.S. government has designated China a foreign adversary of the United States. 15 C.F.R. § 791.4.

54. Article 7 of China's 2017 National Intelligence Law requires that Chinese organizations and citizens "support, assist, and cooperate with national intelligence efforts in accordance with law" and "protect national intelligence work secrets they are aware of." Article 14 of the same law provides that Chinese intelligence institutions "may request that relevant organs, organizations, and citizens provide necessary support, assistance, and cooperation."⁴⁶

55. DHS has warned American businesses that this law "forms the baseline of the modern data collection regime, and compels

⁴⁴ ImportGenius, Lianzhou Technologies Co., Ltd., <https://www.importgenius.com/suppliers/lianzhou-technologies-co-ltd> (last visited Sept. 18, 2026); ImportInfo, TP-LINK SYSTEMS INC, <https://www.importinfo.com/tp-link-systems-inc> (last visited Sept. 18, 2026); ImportInfo, TP-LINK USA CORPORATION, <https://www.importinfo.com/tp-link-usa-corporation> (last visited Sept. 18, 2026).

⁴⁵ ImportInfo, TP-LINK USA CORPORATION, <https://www.importinfo.com/tp-link-usa-corporation>, (last visited Sept. 18, 2026).

⁴⁶ PRC National Intelligence Law arts. 7, 14 (as amended 2018), China Law Translate (June 27, 2017), <https://www.chinalawtranslate.com/en/national-intelligence-law-of-the-p-r-c-2017/>; accord https://cs.brown.edu/courses/cs180/sources/2017_06_28_China_NationalIntelligenceLawOfThePeoplesRepublicOfChina.pdf.

all PRC firms and entities to support, assist, and cooperate with the PRC intelligence services, creating a legal obligation for those entities to turn over data collected abroad and domestically to the PRC.” DHS further explained that the law “establishes a system of incentives for compliance and penalties for non-compliance,” including that a person who “obstructs . . . state intelligence work” “shall be dismissed, investigated and/or detained.”⁴⁷

56. Under China’s 2021 RMSV, Chinese network-product providers and network operators must report newly discovered security vulnerabilities to China’s Ministry of Industry and Information Technology within a mere two days of discovery. A senior DHS official has stated that the Chinese government appears to use this vulnerability-disclosure rule to preview dangerous zero-day flaws before technology companies can deploy fixes.⁴⁸

57. The risks from these laws matter to Nebraska consumers. A company whose research, development, manufacturing, personnel, and affiliates are subject to this regime cannot truthfully assure consumers that their routers, networks, and personal data are protected from “any” cyber threats, or that “no government” has access to or control over the design and production of its devices.

III. TP-Link’s Representations That It Separated from China and Manufactures Its Product in Vietnam Are Deceptive and Omit Material Information

58. TP-Link represents that it “manufacture[s] products for the U.S. market in its own factory in Vietnam” and that

⁴⁷ U.S. Dep’t of Homeland Sec., Data Security Business Advisory 6 (Dec. 22, 2020), https://www.dhs.gov/sites/default/files/publications/20_1222_data-security-business-advisory.pdf.

⁴⁸ Stewart Scott et al., Dragon Tails: Preserving International Cybersecurity Research, Atlantic Council (Sept. 2022), <https://www.atlanticcouncil.org/in-depth-research-reports/report/preserving-international-cybersecurity-research/>; Suzanne Smalley, China Could Be Reviewing Security Bugs Before Tech Companies Issue Patches, DHS Official Says, CyberScoop (Aug. 10, 2022), <https://cyberscoop.com/dhs-official-chinese-rules-exploit/> (reporting remarks of DHS Under Secretary for Policy Robert Silvers).

“[m]anufacturing products in TP-Link facilities with our own employees provides another layer of security and governance for the supply chain serving the U.S. market and beyond.”⁴⁹ In a 2023 announcement, TP-Link claimed that “all product manufacturing” related to its smart home products was handled by its Vietnamese entity Lian Yue Vietnam Co. Ltd.⁵⁰

59. In 2025, after the House Select Committee on the Chinese Communist Party held a hearing discussing TP-Link’s relation to Chinese state-sponsored cyberattacks, TP-Link represented that it “manufactures [its] routers in Vietnam in [its] own facility.”⁵¹

60. The reality behind TP-Link’s Vietnamese manufacturing claims tells a different story. Only 0.5% of the components used in TP-Link’s Vietnamese factory by value are bought in Vietnam; all other inputs are imported from or through China. Bloomberg reported this figure based on trade data, and TP-Link confirmed it.⁵²

61. TP-Link’s Vietnam facility also has connections to the Chinese military. TP-Link recently used a construction contractor for its Vietnam plant—China State Construction Engineering Corporation—that the U.S. Department of Defense has designated a Chinese military company.⁵³

⁴⁹ TP-Link, Fact Sheet, <https://www.tp-link.com/us/landing/fact-sheet/> (last visited Sept. 21, 2026), archived at <https://perma.cc/9LWY-L3NU>.

⁵⁰ TP-Link, BFG Group Announcement (September 19, 2023).

⁵¹ TP-Link, TP-Link Systems Inc. Sets the Record Straight Regarding Inaccurate Testimony at House Select Committee on the CCP Hearing (Mar. 5, 2025), <https://www.tp-link.com/us/press/news/21656/>.

⁵² Kate O’Keeffe, *Wi-Fi Giant TP-Link’s US Future Hinges on Its Claimed Split From China*, Bloomberg (Apr. 11, 2025), <https://www.bloomberg.com/news/articles/2025-04-11/wi-fi-giant-tp-link-s-us-future-hinges-on-its-claimed-split-from-china>; Kate O’Keeffe, *Wi-Fi Giant’s Vietnam Factory Raises Questions Over China Split*, Bloomberg (Nov. 22, 2025), <https://www.bloomberg.com/news/articles/2025-11-22/wi-fi-giant-s-vietnam-factory-raises-questions-over-china-split>.

⁵³ Notice of Availability of Designation of Chinese Military Companies, 91 Fed. Reg. 35189, 35191 (June 10, 2026) (designating China State Construction Engineering Corporation Limited); see also Kate O’Keeffe, *Wi-Fi Giant’s Vietnam Factory Raises Questions Over China Split*, Bloomberg (Nov. 22, 2025),

62. TP-Link omits material facts to deceive consumers into thinking its Vietnamese-assembled products and its supply chain are unaffiliated with China, a designated foreign adversary. The reality is that TP-Link continues to operate its supply chain with deep Chinese connections, Chinese governmental support, and Chinese exports. The final assembly of components sourced from or through China in Vietnam does not cure the company's deceptive statements and material omissions regarding its Chinese dependence and affiliations.

IV. TP-Link Makes False and Deceptive Security Representations While Its Routers Have Been Repeatedly Exploited in Serious Cyberattacks

63. TP-Link represents to consumers that its networking devices robustly protect their privacy and security. Those representations are false or deceptive.

A. The TP-Link TL-WR940N and Archer C7 Routers: Exploited by the Quad7 Botnet and the Russian GRU

64. TP-Link advertised its TL-WR940N router as providing “[e]asy wireless security encryption at a push of [a] WPS button” and “Easy Setup and Use,” and represented that its Tether app “lets you manage [the router’s] network settings . . . including . . . access control.” TP-Link sold versions of this router through 2024, and on information and belief many Nebraska consumers still use it.⁵⁴

65. Contrary to TP-Link’s representations, the TL-WR940N contained a critical vulnerability. TP-Link has admitted that CVE-

<https://www.bloomberg.com/news/articles/2025-11-22/wi-fi-giant-s-vietnam-factory-raises-questions-over-china-split>.

⁵⁴ TP-Link, TL-WR940N Product Page (archived Mar. 29, 2023), <https://web.archive.org/web/20230329192916/https://www.tp-link.com/us/home-networking/wifi-router/tl-wr940n/>; TP-Link, FAQ No. 5058 (last updated May 12, 2026), <https://www.tp-link.com/us/support/faq/5058/>, archived at <https://web.archive.org/web/20260521160655/https://www.tp-link.com/us/support/faq/5058/> and <https://perma.cc/XRK7-WA3J>; see also <https://perma.cc/F4B2-UR85>, at 55 (listing end of sale of the TL-WR940N v6 plus model as Apr. 23, 2024).

2023-50224 affects the TL-WR940N. This vulnerability has been exploited by the operators of the Quad7 botnet—tracked by Microsoft as CovertNetwork-1658 and attributed by Microsoft to Chinese threat actors—and by Russia’s GRU.⁵⁵

66. Microsoft reported in October 2024 that CovertNetwork-1658—comprised predominantly of compromised TP-Link routers—was used to conduct “highly evasive password spray attacks” against targets including “think tanks, government organizations, non-governmental organizations, law firms, [and the] defense industrial base,” and that a Chinese threat actor known as Storm-0940 used credentials obtained from those attacks to intrude into targeted organizations. Password spraying is when a hacker attempts to gain unauthorized access by using a password across several accounts at once. TP-Link itself acknowledged that “the Quad 7 . . . botnet . . . is used by Chinese threat actors for password spray attacks against Microsoft 365 accounts,” that “[t]he threat actor exploits vulnerabilities in the routers to gain remote code execution capability,” and that the network is “predominantly TP-Link devices.”⁵⁶ This overlap is itself

⁵⁵ TP-Link, Press Release No. 22295, *An Important Update for TP-Link Customers Regarding Recent CVE-2023-50224 Reporting* (May 1, 2026), <https://www.tp-link.com/us/press/news/22295/>; Nat’l Inst. of Standards & Tech., CVE-2023-50224 Detail, National Vulnerability Database, <https://nvd.nist.gov/vuln/detail/CVE-2023-50224> (last visited Sept 21, 2026); TP-Link, FAQ No. 5058 (last updated May 12, 2026), <https://www.tp-link.com/us/support/faq/5058/>, archived at <https://web.archive.org/web/20260521160655/https://www.tp-link.com/us/support/faq/5058/> and <https://perma.cc/XRK7-WA3J> (identifying CVE-2023-50224 as applicable to the TL-WR940N); Fed. Bureau of Investigation, Russian GRU Exploiting Vulnerable Routers to Steal Sensitive Information, Alert No. I-260407-PSA (Apr. 7, 2026), <https://media.defense.gov/2026/Apr/07/2003907743/-1/-1/0/I-260407-PSA.PDF>; Microsoft Threat Intelligence, Chinese Threat Actor Storm-0940 Uses Credentials from Password Spray Attacks from a Covert Network, Microsoft (Oct. 31, 2024), <https://www.microsoft.com/en-us/security/blog/2024/10/31/chinese-threat-actor-storm-0940-uses-credentials-from-password-spray-attacks-from-a-covert-network/>; TP-Link, FAQ No. 4365 (archived Jan. 26, 2025), <https://web.archive.org/web/20250126092628/https://www.tp-link.com/us/support/faq/4365/>.

⁵⁶ Microsoft Threat Intelligence, Chinese Threat Actor Storm-0940 Uses Credentials from Password Spray Attacks from a Covert Network, Microsoft (Oct. 31, 2024), [https://www.microsoft.com/en-us/security/blog/2024/10/31/chinese-threat-actor-storm-](https://www.microsoft.com/en-us/security/blog/2024/10/31/chinese-threat-actor-storm-0940-uses-credentials-from-password-spray-attacks-from-a-covert-network/)

material and undisclosed: in June 2026, the U.S. Department of Defense identified TP-Link Technologies, Hangzhou Hikvision Digital Technology Co., Ltd., and Zhejiang Dahua Technology Co., Ltd.—all three compromised in the same overall botnet—as Chinese military companies, a civil-military-fusion connection TP-Link deceptively omits despite touting its routers’ security.⁵⁷

67. The FBI and NSA report that the GRU has exploited compromised routers to conduct adversary-in-the-middle attacks: “[t]he GRU provides fraudulent DNS answers for specific domains and services – including Microsoft Outlook Web Access – enabling adversary-in-the-middle (AitM) attacks against encrypted traffic if users navigate through a certificate error warning.” In other words, a consumer would believe he or she is securely communicating with Outlook Web Access while the unencrypted content of the traffic is disclosed to the GRU.⁵⁸

0940-uses-credentials-from-password-spray-attacks-from-a-covert-network/; TP-Link, FAQ No. 4365 (archived Jan. 26, 2025), <https://web.archive.org/web/20250126092628/https://www.tp-link.com/us/support/faq/4365/>.

⁵⁷ Gi7w0rm, The Curious Case of the 7777 Botnet, Medium (Oct. 19, 2023), <https://gi7w0rm.medium.com/the-curious-case-of-the-7777-botnet-86e3464c3ffd>, archived at <https://web.archive.org/web/20250116213303/https://gi7w0rm.medium.com/the-curious-case-of-the-7777-botnet-86e3464c3ffd>; Notice of Availability of Designation of Chinese Military Companies, 91 Fed. Reg. 35189, 35192–94 (June 10, 2026) (designating Hangzhou Hikvision Digital Technology Co., Ltd., TP-Link Technologies Co., Ltd., and Zhejiang Dahua Technology Co., Ltd.); U.S. Dep’t of Def., Entities Identified as Chinese Military Companies Operating in the United States in Accordance with Section 1260H of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 (June 8, 2026), <https://media.defense.gov/2026/Jun/08/2003945537/-1/-1/1/ENTITIES-IDENTIFIED-AS-CHINESE-MILITARY-COMPANIES-OPERATING-IN-THE-UNITED-STATES-IN-ACCORDANCE-WITH-SECTION-1260H.PDF>.

⁵⁸ Nat’l Sec. Agency, NSA Supports FBI in Highlighting Russian GRU Threats Against Routers (Apr. 7, 2026), <https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/4453919/nsa-supports-fbi-in-highlighting-russian-gru-threats-against-routers/>; Fed. Bureau of Investigation, Russian GRU Exploiting Vulnerable Routers to Steal Sensitive Information, Alert No. I-260407-

68. The TL-WR940N does not have proper “access control”—it allows unauthorized actors to gain administrator access and conscript the router into an illegal botnet. Nor is it “[e]asy [to] [s]etup and [u]se”: the router does not support automatic firmware updates, so protecting it requires manually installing a patch that many users would not know to install.⁵⁹

69. TP-Link’s conduct after this vulnerability became public compounded the deception. In April 2026, TP-Link published a list of routers affected by these attacks that omitted the TL-WR940N and stated that “[a]ll the affected products have reached End-of-Life (EOL) status and [are] no longer within TP-Link’s standard maintenance lifecycle.” In May 2026, TP-Link was forced to admit that the TL-WR940N was also affected—even though a 2023 security analysis that TP-Link itself had previously cited specifically identified the TL-WR940N.⁶⁰

70. TP-Link likewise advertised the Archer C7 AC1750 (versions 2 and 3) as “provid[ing] secure Wi-Fi access for guests sharing your home or office network” and offering “[e]asy setup and management with Tether App.” TP-Link also promoted the Archer C7 in an online video advertisement telling consumers that purchasing

PSA (Apr. 7, 2026), <https://media.defense.gov/2026/Apr/07/2003907743/-1/-1/0/I-260407-PSA.PDF>.

⁵⁹ TP-Link, FAQ No. 2796, <https://www.tp-link.com/us/support/faq/2796/>, archived at <https://perma.cc/G6RS-2YKS> (explaining how to update firmware manually).

⁶⁰ Gi7w0rm, *The Curious Case of the 7777 Botnet*, Medium (Oct. 19, 2023), <https://gi7w0rm.medium.com/the-curious-case-of-the-7777-botnet-86e3464c3ffd>, archived at <https://web.archive.org/web/20250116213303/https://gi7w0rm.medium.com/the-curious-case-of-the-7777-botnet-86e3464c3ffd>; TP-Link, FAQ No. 4365 (archived Jan. 26, 2025), <https://web.archive.org/web/20250126092628/https://www.tp-link.com/us/support/faq/4365/> (January 2025 TP-Link article citing that report); TP-Link, FAQ No. 5058 (updated Apr. 9, 2026), archived at <https://web.archive.org/web/20260410034756/https://www.tp-link.com/us/support/faq/5058/>; TP-Link, FAQ No. 5058 (last updated May 12, 2026), <https://www.tp-link.com/us/support/faq/5058/>, archived at <https://web.archive.org/web/20260521160655/https://www.tp-link.com/us/support/faq/5058/> and <https://perma.cc/XRK7-WA3J>.

the router would “future-proof” their home network and reiterating that it “provides secure Wi-Fi access for guests sharing your home or office network.”⁶¹ Contrary to those representations, versions 2 and 3 of the Archer C7 were compromised in the Quad7 botnet operations, and neither version supports automatic firmware updates.⁶² The Archer C7 was also one of the TP-Link Routers hacked by the GRU.⁶³

B. The Archer AX21: Exploited in the Flax Typhoon Attacks

71. TP-Link advertised the Archer AX21 (AX1800) router as offering “Refined Password Security” and a “New Level of Cyber Security” with the “latest Wi-Fi security protocol, WPA3,” along with “easy setup.” The AX21 was the bestselling Wi-Fi 6 router on Amazon, and its current version (v5) remains listed as “Amazon’s Choice,” underscoring the continued prominence of the AX21 product line among consumers.⁶⁴

72. In 2023, it was publicly disclosed that versions 1 through 3 of the AX21 contained a critical vulnerability, CVE-2023-1389, allowing an unauthenticated attacker—i.e. an attacker that does not know the router’s password—to nonetheless inject malicious

⁶¹ TP-Link, Archer C7 Promotional Video, YouTube, <https://www.youtube.com/watch?v=-PEWXGUQiQ8>, at 1:00 (“future-proof”), 1:54 (“secure Wi-Fi access for guests”).

⁶² TP-Link, Archer C7 Product Page (archived Mar. 31, 2026), <https://web.archive.org/web/20260331134655/https://www.tp-link.com/us/home-networking/wifi-router/archer-c7/>; TP-Link, FAQ No. 5058, <https://www.tp-link.com/us/support/faq/5058/>; see generally TP-Link, FAQ No. 2796, <https://www.tp-link.com/en/support/faq/2796/>.

⁶³ FBI Says Russian Hackers Hijacked Old Wi-Fi Routers, Fox News (June 14, 2026), <https://noticias.foxnews.com/tech/fbi-says-russian-hackers-hijacked-old-wi-fi-routers.amp>

⁶⁴ TP-Link, Archer AX21 Product Page (archived Oct. 6, 2022), <https://web.archive.org/web/20221006205422/https://www.tp-link.com/us/home-networking/wifi-router/archer-ax21/>; *Forget Slow WiFi, Amazon Just Cut the Best-Selling WiFi 6 TP-Link Router to a Near Record Low*, Gizmodo (May 10, 2026), <https://gizmodo.com/forget-slow-wifi-amazon-just-cut-the-best-selling-wifi-6-tp-link-router-to-a-near-record-low-2000756849>; TP-Link AX1800 Wi-Fi 6 Router (ArcherAX21 V5), Amazon, <https://www.amazon.com/WiFi-6-Router-Gigabit-Wireless/dp/B08H8ZLKKK> (last visited Sept. 21, 2026).

commands. TP-Link admitted in April 2023 that the “AX21 has been added to the Mirai botnet Arsenal.” The vulnerability has been actively exploited by multiple botnet operations, including by the Chinese state-affiliated Flax Typhoon group, whose botnet the FBI ultimately disrupted on information and belief through a court-authorized operation remotely resetting thousands of compromised routers.⁶⁵

73. TP-Link’s marketing created a false impression of security for consumers: a router advertised for “Refined Password Security” allowed attackers to gain root access with no password at all.

74. Versions 1 and 1.20 of the AX21 did not support automatic firmware updates as a default setting. To be protected, a consumer had to know about the vulnerability and manually download and install a firmware patch. And even consumers who installed TP-Link’s Tether app received notice of this critical security update only as a red dot on a menu within the app. TP-Link no longer provides updates for the AX21 v1 and v1.20, contending these models reached “end of life” in May 2024. TP-Link has continued to obfuscate, claiming it “has not been able to verify how its devices are affected, if at all.”⁶⁶

⁶⁵ Nat’l Inst. of Standards & Tech., CVE-2023-1389 Detail, National Vulnerability Database, <https://nvd.nist.gov/vuln/detail/cve-2023-1389> (last visited Sept. 21, 2026); SentinelOne, CVE-2023-1389, SentinelOne Vulnerability Database, <https://www.sentinelone.com/vulnerability-database/cve-2023-1389/>; <https://perma.cc/BNC8-C69P> (TP-Link statement that the “AX21 has been added to the Mirai botnet Arsenal”); Router Security by the Numbers: 10 Years of CVE Data, 5Gstore Blog (Apr. 12, 2026), <https://5gstore.com/blog/2026/04/12/router-security-by-the-numbers-10-years-of-cve-data/>; Lulzim A., *FBI Remotely Resets Thousands of Routers to Disrupt Flax Typhoon Botnet*, RouterArena, <https://routerarena.com/news/FBI-remotely-resets-thousands-of-routers-to-disrupt-Flax-Typhoon-botnet>; see also Daryna Antoniuk, *Botnets continue exploiting year-old flaw in unpatched TP-Link routers*, The Record (Apr. 16, 2024), <https://therecord.media/tp-link-router-vulnerability-botnets>; Elizabeth Montalbano, *Emerging botnet exploits TP-Link router flaw posing risk to US organizations*, Cybersecurity Dive (Mar. 12, 2025), <https://www.cybersecuritydive.com/news/-botnet-exploits-tp-link-router/742319/>.

⁶⁶ See generally TP-Link, FAQ No. 2796, <https://www.tp-link.com/en/support/faq/2796/>; Kate O’Keefe, *Wi-Fi Giant TP-Link’s US Future Hinges on Its Claimed Split From China*, Bloomberg (Apr. 11, 2025),

C. HomeShield Does Not “Cover[] All Security Scenarios”

75. TP-Link represents that its routers, such as the Archer BE9700 router offered through national retailers that serve Nebraska consumers, feature “Network Security with HomeShield.” HomeShield is a “built-in service” that purports to provide consumers with privacy and security controls over their homes’ and businesses’ networks. TP-Link currently represents that HomeShield “covers all security scenarios,” that it handles all concerns regarding “cyber virus intrusion” and “IoT device attacks,” and that users can “[c]heck the results of the scans and preventions against any potential cyber threats or attacks for your home network.” A version of TP-Link’s website available as recently as November 2025 further represented that HomeShield provides a “100% safeguard” for network security.⁶⁷ Consumers trust TP-Link’s representations when considering which device to purchase. TP-Link knows this, and TP-Link knows of its devices’ plethora of vulnerabilities.

76. TP-Link’s HomeShield representations are belied by vulnerabilities in the very routers TP-Link advertises with HomeShield. TP-Link advertised the Archer AXE75 with HomeShield and represented that it has “advanced security features that deliver a safe environment that protects your family and network’s data and privacy.” Yet the AXE75 was subject to CVE-2024-53375, a high-severity vulnerability allowing an attacker to execute commands on the router, and CVE-2025-15568, which allows remote code execution in certain scenarios. Other routers TP-Link advertises with

<https://www.bloomberg.com/news/articles/2025-04-11/wi-fi-giant-tp-link-s-us-future-hinges-on-its-claimed-split-from-china>.

⁶⁷ Current version: TP-Link, HomeShield, <https://www.tp-link.com/us/homeshield/> (last visited Sept. 22, 2026), archived at <https://perma.cc/M8ME-4EX7>; TP-Link, HomeShield (archived Nov. 14, 2025), <https://web.archive.org/web/20251114185316/https://www.tp-link.com/us/homeshield/>.

HomeShield—including the Archer BE230, Archer AX73, and Deco BE25—were likewise subject to command-injection vulnerabilities.⁶⁸

77. HomeShield also cannot address a risk that TP-Link never discloses to consumers: Even when TP-Link eventually patches a vulnerability—which can take weeks or months—later patching does not eliminate the risk that the Chinese government learns of the zero-day flaw first. Under the RMSV, described in Section II above, Chinese technology providers and network operators must report newly discovered vulnerabilities to the Chinese government within two days. A service that purports to “cover[] all security scenarios” and “handle[] all your concerns” while its provider’s Chinese facilities and affiliates are subject to that regime is deceptive and omits material information from consumers.⁶⁹

78. Former FCC Commissioner Michael O’Rielly wrote that TP-Link’s “Chinese investment structures” warranted inquiry and that its products “had more than their fair share” of vulnerabilities.⁷⁰

79. Rob Joyce, the former Director of Cybersecurity of the National Security Agency, has testified that “TP-Link routers were

⁶⁸ TP-Link, Archer AXE75 Product Page, <https://www.tp-link.com/us/home-networking/wifi-router/archer-axe75/> (last visited Sept. 22, 2026); Nat’l Inst. of Standards & Tech., CVE-2024-53375 Detail, National Vulnerability Database, <https://nvd.nist.gov/vuln/detail/CVE-2024-53375> (last visited Sept. 22, 2026); TP-Link, FAQ No. 5005, <https://www.tp-link.com/us/support/faq/5005/>; Nat’l Inst. of Standards & Tech., CVE-2025-15568 Detail, National Vulnerability Database, <https://nvd.nist.gov/vuln/detail/cve-2025-15568> (last visited Sept. 22, 2026); TP-Link, FAQ No. 4935, <https://www.tp-link.com/us/support/faq/4935/>.

⁶⁹ Stewart Scott et al., *Dragon Tails: Preserving International Cybersecurity Research*, Atlantic Council (Sept. 2022), <https://www.atlanticcouncil.org/in-depth-research-reports/report/preserving-international-cybersecurity-research/>; Suzanne Smalley, China Could Be Reviewing Security Bugs Before Tech Companies Issue Patches, DHS Official Says, CyberScoop (Aug. 10, 2022), <https://cyberscoop.com/dhs-official-chinese-rules-exploit/> (reporting remarks of DHS Under Secretary for Policy Robert Silvers); TP-Link, HomeShield, <https://www.tp-link.com/us/homeshield/> (last visited Sept. 22, 2026), archived at <https://perma.cc/M8ME-4EX7>.

⁷⁰ Michael O’Rielly, *Chinese Wireless Routers: The Next Entry Point for State-Sponsored Hackers?*, Hudson Institute (March 2024), https://s3.amazonaws.com/media.hudson.org/030724_ORielly_Chinese_Routers_Hackers_Memo.pdf.

among the various brands exploited by Chinese state-sponsored hackers” in various attacks.⁷¹

80. The Chairman of the United States House of Representatives’ Select Committee on the Chinese Communist Party, John Moolenaar, wrote to Secretary Gina Raimondo of the United States Department of Commerce, warning of TP-Link devices’ vulnerabilities and requesting an investigation: “TP-Link’s unusual degree of vulnerabilities and required compliance with PRC law are in and of themselves disconcerting. When combined with the PRC government’s use of routers like TP-Link to perpetrate extensive cyberattacks in the United States, it becomes significantly alarming.”⁷²

81. Cyber threat intelligence researchers with Check Point Research reported in May 2023 that a Chinese state-sponsored hacking group known as Camaro Dragon deployed a malicious firmware implant—containing a custom backdoor named “Horse Shell”—on TP-Link routers, including the TL-WR940N, enabling the attackers to maintain persistent access, build anonymous attack infrastructure, and move laterally into compromised networks.⁷³

82. TP-Link’s Archer router series, along with other models, also has had firmware vulnerabilities reported by the National Institute of Standards and Technology, including a directory traversal vulnerability (CVE-2015-3035) that can allow attackers access to files on the device. The Cybersecurity and Infrastructure Security Agency

⁷¹ End the Typhoons: How to Deter Beijing’s Cyber Actions and Enhance America’s Lackluster Cyber Defenses Before the H. Select Comm. on the Strategic Competition Between the U.S. and the Chinese Communist Party, 119th Cong. (Mar. 5, 2025) (statement of Rob Joyce), <https://docs.house.gov/meetings/ZS/ZS00/20250305/117983/HHRG-119-ZS00-Wstate-JoyceR-20250305.pdf>.

⁷² Rep. John Moolenaar and Rep. Raja Krishnamoorthi, Letter to Department of Commerce Secretary Raimondo (August 13, 2024).

⁷³ Itay Cohen and Radoslaw Madej, The Dragon Who Sold His Camaro: Analyzing Custom Router Implant, Check Point Research (May 16, 2023), <https://research.checkpoint.com/2023/the-dragon-who-sold-his-camaro-analyzing-custom-router-implant/>.

(“CISA”) added that vulnerability to its Known Exploited Vulnerabilities Catalog, confirming it has been exploited in the wild.⁷⁴

83. In April 2025, CISA has cataloged SQL injection vulnerabilities in TP-Link firmware. These vulnerabilities allow “an unauthenticated attacker to inject malicious SQL statements via the username and password fields.”⁷⁵

84. Despite TP-Link representing that its networking devices protect consumers’ privacy and security, the experts have made the opposite clear. TP-Link’s routers have vulnerabilities that hostile state actors have exploited to reach into consumers’ homes and businesses. Though these issues have been reported on and warned of for years, TP-Link’s websites, blogs, and advertisements continue to falsely represent to consumers that its products “protect[] comprehensively.”⁷⁶ These representations were and are false, deceptive, and material to Nebraska consumers.

D. TP-Link’s Pattern of Critical Vulnerabilities Continues

85. TP-Link’s security failures are not confined to past incidents. Throughout 2026 researchers have continued to disclose critical vulnerabilities across TP-Link’s camera, router, and cloud-management product lines.

86. In August 2026, TP-Link disclosed a family of vulnerabilities in 2026—CVE-2025-30237 through CVE-2025-30241—affecting its Aginet line of ISP-managed mesh routers, gateways, and modems, which internet service providers distribute directly to homes

⁷⁴ National Institute of Standards and Technology, CVE-2015-3035 Detail, National Vulnerability Database, <https://nvd.nist.gov/vuln/detail/cve-2015-3035> (last visited Sept. 22, 2026); Cybersecurity and Infrastructure Security Agency, Known Exploited Vulnerabilities Catalog (CVE-2015-3035 added March 25, 2022), <https://www.cisa.gov/known-exploited-vulnerabilities-catalog>.

⁷⁵ Cybersecurity and Infrastructure Security Agency, Vulnerability Summary for the Week of April 14, 2025, <https://www.cisa.gov/news-events/bulletins/sb25-111> (last visited Sept. 22, 2026).

⁷⁶ TP-Link, HomeShield, <https://www.tp-link.com/us/homeshield/> (last visited Sept. 22, 2026), archived at <https://perma.cc/M8ME-4EX7>.

and small businesses.⁷⁷ The lead vulnerability, CVE-2025-30237, is rated high severity (CVSS 8.7) and results from missing authorization checks on internal server endpoints, allowing an unauthenticated attacker with network access to bypass login screens and gain full control of the device.

87. On September 3, 2026, TP-Link published a security advisory disclosing CVE-2026-18167, a high-severity (CVSS 7.7) stack-based buffer overflow in the EasyMesh module of its Archer AX55 (v4) router.⁷⁸ The Archer AX55 is one of TP-Link’s best-selling Wi-Fi 6 routers, and the AX55 has received “Amazon’s Choice.”⁷⁹ An attacker on the router’s local network could exploit the flaw to crash the router or, in some circumstances, execute arbitrary code on the device.

88. In late-August 2026, TP-Link likewise disclosed CVE-2026-9254, a high-severity (CVSS 8.7) command-injection vulnerability in the parental-control feature of the Archer BE800, Archer BE3600, and Archer AX75 routers.⁸⁰ The flaw permits an unauthenticated attacker on the local network to inject commands that execute with root privileges.

89. In September 2026, security researchers at OPSWAT disclosed two vulnerabilities in TP-Link’s popular Tapo C120 and C200 smart security cameras. CVE-2026-15315, rated high severity (CVSS 8.7), is an authentication-bypass vulnerability that permits an unauthenticated attacker on the same local network to obtain a valid administrator session without a password, enabling an attacker to alter device settings or view live and recorded video feeds. CVE-2026-

⁷⁷ TP-Link, Security Advisory: Multiple Vulnerabilities in ISP-Managed TP-Link Networking Products (CVE-2025-30237 to CVE-2025-30241), <https://www.tp-link.com/us/support/faq/5239/> (last visited Sept. 23, 2026).

⁷⁸ TP-Link, Security Advisory: Multiple Vulnerabilities in TP-Link Archer AX55 (CVE-2026-18167 & CVE-2026-18330), <https://www.tp-link.com/us/support/faq/5279/> (last visited Sept. 23, 2026).

⁷⁹ https://www.amazon.com/dp/B09G5W9R6R?ref=clp_hp_h_pc&th=1

⁸⁰ TP-Link, Security Advisory: Multiple Command Injection Vulnerabilities in Archer Products (CVE-2026-9254, CVE-2026-16348, CVE-2026-78541), <https://www.tp-link.com/us/support/faq/5264/> (last visited Sept. 23, 2026).

15316, also rated high severity (CVSS 7.1), permitted an attacker to crash or restart the camera's security service by sending malformed data. OPSWAT reported both vulnerabilities to TP-Link on April 16, 2026; TP-Link did not release a patch until August 18, 2026—more than four months later.⁸¹

90. In August 2026, researchers with Forescout disclosed fifteen new vulnerabilities in TP-Link's Omada business-networking ecosystem, including CVE-2025-9289.⁸² The vulnerabilities stem in part from hard-coded cryptographic keys and predictable device serial numbers in TP-Link's Zero-Touch Provisioning feature, which the researchers found could be exploited to spoof and hijack client devices, inject code into TP-Link's administrative cloud dashboards, and exfiltrate data.

V. TP-Link's Data Practices and Privacy Policies Deceive Consumers by Omitting the Risks from China's Intelligence Laws

91. TP-Link's mobile applications collect consumers' personal data and claim to provide customization and control of their privacy and security settings, and its privacy policies reserve broad rights to share that data. But TP-Link fails to disclose a critical fact: TP-Link's Chinese facilities, affiliates, and personnel are subject to PRC national intelligence laws mandating cooperation with PRC intelligence efforts, exposing American consumer data to potential PRC access. By

⁸¹ OPSWAT, Authentication Bypass and Denial-of-Service Vulnerabilities: OPSWAT Discovers CVE-2026-15315 & CVE-2026-15316 in TP-Link Tapo Cameras (2026), <https://www.opswat.com/blog/authentication-bypass-and-dos-vulnerabilities-opswat-discovers-cve-2026-15315-cve-2026-15316-in-tp-link-tapo-cameras>; TP-Link, Security Advisory: Multiple Vulnerabilities in Tapo C120 and C200 (CVE-2026-15315 & CVE-2026-15316), <https://www.tp-link.com/us/support/faq/5248/> (last visited Sept. 23, 2026).

⁸² Forescout, New TP-Link Router Vulnerabilities: Exploiting Zero Touch Provisioning (2026), <https://www.forescout.com/blog/new-tp-link-router-vulnerabilities-exploiting-zero-touch-provisioning/>; TP-Link, Security Advisory: Response to Research Concerning TP-Link Zero Touch Provisioning (ZTP) Technologies, <https://support.omadanetworks.com/us/document/130627/> (last visited Sept. 23, 2026).

omitting this material fact, TP-Link misleads consumers and fails to obtain informed consent regarding their data within its portfolio of networking and smart home device applications.

92. TP-Link offers applications such as TP-Link Tether, TP-Link Tapo, TP-Link Deco, and Kasa Smart on Apple’s App Store and Google’s Play Store. These applications can be required to operate TP-Link devices, are integral to setup and management of TP-Link services such as HomeShield, and grant consumers the ability to customize and control privacy and security settings. These apps are used with a wide range of TP-Link networking and smart home devices, such as cameras, fans, lights, and routers.⁸³

93. The Tether Privacy Policy states that TP-Link “may share your personal information internally and externally with suppliers, advisors, or partners for our legitimate business purposes, and only on a need-to-know basis.” It carves out the right to share information with “authorized partners, including affiliates . . . to: . . . comply with applicable laws,” and “where otherwise necessary to protect our rights, interests, and/or property . . . or the rights, interests, and/or property of our agents, independent contractors, customers, and others.” TP-Link’s Deco, Tapo, and Kasa policies contain similar carve-outs.⁸⁴

94. TP-Link’s Kasa Smart app points to a “Kasa Privacy Policy (US)” that informs consumers of TP-Link’s data collection and use practices. Since at least January of 2024, this policy has informed consumers of TP-Link’s collection of data, including email, location, and mobile phone identifier. But, under its section titled “How we share personal data,” TP-Link states that it “may share information

⁸³ App Store for iPhone, Kasa Smart, <https://apps.apple.com/us/app/kasa-smart/id1034035493> (last visited Sept. 22, 2026).

⁸⁴ TP-Link, Tether Privacy Policy ¶ 3 (Aug. 20, 2026), <https://privacy.tp-link.com/app/Tether/privacy>; TP-Link, Deco Privacy Policy ¶ 3 (Jan. 5, 2026), <https://privacy.tp-link.com/app/Deco/privacy>; TP-Link, Tapo Privacy Policy ¶ 3 (Jan. 23, 2026), <https://privacy.tp-link.com/app/tapo/privacy>; TP-Link, Kasa Privacy Policy (US) (Jan. 29, 2024) ¶ 3, <https://privacy.tp-link.com/app/kasa/privacy> (each last visited Sept. 22, 2026).

where we have a good faith belief that such disclosure is necessary to (a) comply with an applicable law or legal process”⁸⁵

95. China’s 2017 National Intelligence Law compels Chinese organizations and citizens to support, assist, and cooperate with PRC intelligence efforts—a legal obligation DHS has described as compelling PRC entities “to turn over data collected abroad and domestically to the PRC”—backed by penalties including dismissal, investigation, and detention.⁸⁶ The U.S. National Security Advisor has separately explained that the National Intelligence Law advances the goals of the PRC’s “Military-Civil Fusion (MCF) strategy.”⁸⁷

96. TP-Link employs this same omission across its entire suite of applications. The privacy policies are nearly identical on this issue, allowing the collection of personal information such as email, location, and mobile phone identifier while reserving the right to share information to comply with “applicable law or legal process” and to protect the rights of “others.”⁸⁸ None of these policies discloses that TP-Link’s Chinese affiliations subject American consumer data to potential access by PRC intelligence agencies. When TP-Link reserves the right to share data to “comply with applicable laws” or protect the rights of “others,” there is a specific China-related risk lurking behind those words that would be material to many consumers.

97. The risks discussed in the previous paragraph also show the deceptiveness of TP-Link’s representations to consumers that “[a]s

⁸⁵ TP-Link, Kasa Privacy Policy (US) (Jan. 29, 2024), <https://privacy.tp-link.com/app/kasa/privacy> (last visited Sept. 22, 2026).

⁸⁶ PRC National Intelligence Law (as amended in 2018), China Law Translate (June 27, 2017), <https://www.chinalawtranslate.com/en/national-intelligence-law-of-the-p-r-c-2017/> (last visited Sept. 22, 2026).

⁸⁷ Statement by National Security Advisor Robert C. O’Brien (Jan. 15, 2021), <https://trumpwhitehouse.archives.gov/briefings-statements/statement-national-security-advisor-robert-c-obrien-011521-2/>.

⁸⁸ TP-Link, Tether Privacy Policy (August 20, 2026), <https://privacy.tp-link.com/app/Tether/privacy>; TP-Link, Deco Privacy Policy (January 5, 2026), <https://privacy.tp-link.com/app/Deco/privacy>; TP-Link, Tapo Privacy Policy (January 23, 2026), <https://privacy.tp-link.com/app/tapo/privacy> (each last visited Sept. 22, 2026).

a company headquartered in the United States, no government – foreign or domestic – has access to and control over the design and production of our routers and other devices.”⁸⁹

VI. Federal and State Authorities Have Recognized the Risks Posed by TP-Link Devices

98. In December of 2024, it was publicly reported that the U.S. Departments of Commerce, Defense, and Justice had opened investigations into TP-Link concerning national security risks posed by its routers.⁹⁰

99. In October of 2025, it was reported that federal officials had concluded that TP-Link’s ties to China may pose an “unacceptable risk” and were weighing a proposed plan to ban the sale of TP-Link routers in the United States.⁹¹

100. On March 23, 2026, the FCC’s Public Safety and Homeland Security Bureau announced the addition of routers produced in foreign countries to the FCC’s Covered List, explaining that “[r]outers are the key networking device that enable American homes, schools, businesses, critical infrastructure providers, and emergency services to connect to the internet every day,” and that “[c]ompromised routers can enable in-depth network surveillance, data exfiltration, botnet attacks, and unauthorized access to U.S. government or American businesses’ networks.”⁹²

⁸⁹ TP-Link, Fact Sheet, <https://www.tp-link.com/us/landing/fact-sheet/> (last visited Sept. 22, 2026), archived at <https://perma.cc/9LWY-L3NU>.

⁹⁰ Heather Somerville, Dustin Volz & Aruna Viswanatha, *U.S. Weighs Ban on China-Made TP-Link Routers*, Wall St. J. (Dec. 18, 2024).

⁹¹ Kate O’Keeffe, Josh Sisco & Kate Sullivan, *US Weighs Action Against China-Linked Router Giant TP-Link*, Bloomberg (Oct. 9, 2025).

⁹² FCC’s Public Safety and Homeland Security Bureau Announces Addition of Routers Produced in Foreign Countries to FCC Covered List, WC Docket No. 18-89, Public Notice, DA 26-278, App. C at 1 (Mar. 23, 2026), <https://docs.fcc.gov/public/attachments/DA-26-278A1.pdf>.

101. It has since been reported that TP-Link is seeking conditional approval from the FCC to sell new router models in the United States.⁹³

102. In June 2026, the Department of Defense’s designations under Section 1260H identified TP-Link Technologies as a Chinese military company, alongside Hikvision and Dahua, whose devices were compromised in the same Quad7 botnet as TP-Link’s routers.⁹⁴

CAUSES OF ACTION

COUNTS I–VI: VIOLATIONS OF THE CONSUMER PROTECTION ACT BY TP-LINK SYSTEMS INC. – DECEPTIVE AND UNFAIR BUSINESS PRACTICES

(Neb. Rev. Stat. § 59-1601 et seq.)

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

104. Defendant TP-Link is a “person” within the meaning of the CPA, Neb. Rev. Stat. § 59-1601(1).

105. Defendant conducted “trade and commerce” within the meaning of the CPA, Neb. Rev. Stat. § 59-1601(2), by advertising,

⁹³ Michael Kan, *Facing Router Ban, TP-Link Tells FCC It’s Investing Hundreds of Millions in the US*, PCMag (Apr. 23, 2026), <https://www.pcmag.com/news/facing-router-ban-tp-link-tells-fcc-its-investing-hundreds-of-millions>.

⁹⁴ Gi7w0rm, *The Curious Case of the 7777 Botnet*, Medium (Oct. 19, 2023), <https://gi7w0rm.medium.com/the-curious-case-of-the-7777-botnet-86e3464c3ffd>, archived at <https://web.archive.org/web/20250116213303/https://gi7w0rm.medium.com/the-curious-case-of-the-7777-botnet-86e3464c3ffd>; Notice of Availability of Designation of Chinese Military Companies, 91 Fed. Reg. 35189, 35192–94 (June 10, 2026) (designating Hangzhou Hikvision Digital Technology Co., Ltd., TP-Link Technologies Co., Ltd., and Zhejiang Dahua Technology Co., Ltd.); U.S. Dep’t of Def., *Entities Identified as Chinese Military Companies Operating in the United States in Accordance with Section 1260H of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021* (June 8, 2026), <https://media.defense.gov/2026/Jun/08/2003945537/-1/-1/1/ENTITIES-IDENTIFIED-AS-CHINESE-MILITARY-COMPANIES-OPERATING-IN-THE-UNITED-STATES-IN-ACCORDANCE-WITH-SECTION-1260H.PDF>.

marketing, offering for sale, and selling TP-Link-branded devices to Nebraska consumers.

106. The CPA, Neb. Rev. Stat. § 59-1602, prohibits “unfair or deceptive acts or practices in the conduct of any trade or commerce.”

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

108. 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.

109. Defendant engaged in deceptive and/or unfair acts or practices in violation of the CPA, Neb. Rev. Stat. § 59-1602, by, without limitation:

- a. Representing, expressly and by implication, that TP-Link devices are secure—including that HomeShield “covers all security scenarios,” “handles all your concerns,” and provides “preventions against any potential cyber threats or attacks,” and formerly that HomeShield provides a “100% safeguard,” and including model-specific representations regarding the TL-WR940N, Archer C7, Archer AX21, and Archer AXE75—despite known, critical, and actively exploited security flaws and vulnerabilities, which representations were false, or at minimum created a deceptive net impression of security;
- b. Representing that TP-Link manufactures its products for the U.S. market in its own Vietnamese facility and that such manufacturing “provides another layer of security and governance for the supply chain,” when only 0.5% of components by value are bought in Vietnam, all other inputs are imported from or through China, and a U.S.-designated Chinese military company performed recent construction at the facility;

- c. Omitting material facts about TP-Link's ongoing reliance on Chinese manufacturing, research and development, subsidies, suppliers, and affiliates;
- d. Omitting, while reserving broad contractual rights to share consumer data, that Defendant's Chinese facilities, affiliates, and personnel are subject to PRC intelligence laws that expose Nebraska consumers' personal data to potential access by PRC intelligence agencies under PRC law;
- e. Selling devices to Nebraska consumers while failing to disclose material facts about repeated critical security vulnerabilities, including vulnerabilities exploited by Chinese state-sponsored hackers and the Russian GRU, and about China's two-day vulnerability-disclosure mandate applicable to Defendant's Chinese operations; and
- f. Making false or deceptive statements after vulnerabilities became public, including TP-Link's April 2026 representation that all products affected by the Quad7 attacks had reached end-of-life status, which omitted the TL-WR940N until TP-Link corrected the omission in May 2026.

110. TP-Link's actions constitute deceptive and unfair acts or practices in the conduct of trade or commerce in violation of Neb. Rev. Stat. § 59-1602. TP-Link's violations are continuing. Each and every sale, offer for sale, advertisement, misrepresentation, omission, and deceptive statement in connection with the sale of Defendant's products and services constitutes a separate and independent violation of the CPA.

**COUNTS VII-XII: VIOLATIONS OF THE UNIFORM
DECEPTIVE TRADE PRACTICES ACT BY TP-LINK SYSTEMS
INC. – UNCONSCIONABLE BUSINESS PRACTICES**

(Neb. Rev. Stat. § 87-303.01)

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

112. Defendant TP-Link is a “person” within the meaning of the UDTPA, Neb. Rev. Stat. § 87-301(19).

113. An unconscionable act or practice by a supplier in connection with a consumer transaction constitutes a violation of the UDTPA, Neb. Rev. Stat. § 87-303.01(1).

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

115. Defendant engaged in unconscionable acts and practices in violation of Neb. Rev. Stat. § 87-303.01 by, without limitation:

- a. Continuing to market and sell TP-Link devices in Nebraska as secure despite knowledge that its devices have been exploited in state-sponsored cyberattack campaigns, including by Chinese threat actors and the Russian GRU, against American consumers, businesses, and critical infrastructure;
- b. Exploiting consumer trust by marketing its devices as the secure guardian of consumers’ home networks while aware of ongoing, repeated, and critical vulnerabilities;
- c. Ceasing security support for router models—including the TL-WR940N, Archer C7 (v2 and v3), and Archer AX21 (v1 and v1.20)—that TP-Link knows remain in consumers’ homes, that do not support automatic firmware updates, and that contain known, actively exploited vulnerabilities;
- d. Failing to disclose that TP-Link devices are dependent on Chinese components, facilities, and affiliates subject to PRC laws mandating cooperation with PRC intelligence services and two-day disclosure of security vulnerabilities to the Chinese government;
- e. Marketing and selling TP-Link products while aware of federal investigations and governmental designations

concerning the national security risks of its devices, and failing to disclose those facts to consumers; and

- f. Using vague privacy policies and manufacturing representations that shift responsibility to consumers while affirmatively creating the false impression that its products are safe, secure, and unaffiliated with China.

116. Defendant's marketing, advertisement, offer for sale, and sale of its products and services despite known security flaws and vulnerabilities constitute unconscionable acts and practices in violation of Neb. Rev. Stat. § 87-303.01. The unconscionability of the acts and practices is enhanced by the information asymmetry between TP-Link and its consumers regarding security vulnerabilities, the difficulty of self-protection on models lacking automatic updates, and TP-Link's market dominance.

117. Each and every sale, offer for sale, advertisement, omission of material fact, and deceptive representation constitutes a separate and independent violation of the UDTPA. Neb. Rev. Stat. § 87-303.01(1).

**COUNTS XIII–XVII: VIOLATIONS OF THE UNIFORM
DECEPTIVE TRADE PRACTICES ACT BY TP-LINK SYSTEMS
INC. – UNFAIR AND DECEPTIVE BUSINESS PRACTICES**

(Neb. Rev. Stat. § 87-301 et seq.)

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

119. Section 87-302(a) of the UDTPA specifies multiple practices, which when conducted in the course of a person's business, constitute a deceptive trade practice.

120. Defendant is a "person" within the meaning of the UDTPA, Neb. Rev. Stat. § 87-301(19).

121. Defendant engaged in deceptive and/or unfair trade practices in violation of the UDTPA, Neb. Rev. Stat. § 87-302, by, without limitation:

- a. Representing, expressly or by implication, that TP-Link products and services have characteristics, uses, benefits, or qualities they do not have, including that they provide robust security—that HomeShield “covers all security scenarios” and provides “preventions against any potential cyber threats or attacks,” that the TL-WR940N provides “access control,” and that the Archer AX21 offers “Refined Password Security”;
- b. Representing that TP-Link devices are of a particular standard, quality, or grade when they are of another, with respect to the degree of safety and security that consumers can expect;
- c. Using deceptive representations of geographic origin in connection with goods, by affirmatively representing that TP-Link manufactures its products in its own Vietnamese facility as a supply-chain security measure, when the facility performs final assembly of components imported almost entirely from or through China;
- d. Causing a likelihood of confusion or of misunderstanding as to the source of the component parts of its devices; and
- e. Causing a likelihood of confusion or of misunderstanding as to TP-Link’s affiliation, connection, or association with TP-Link Technologies and other Chinese entities, including entities designated as Chinese military companies.

122. Each and every advertisement, offer for sale, sale, misrepresentation, omission, or failure to disclose a material fact in connection with the promotion and sale of Defendant’s products and services constitutes a separate and independent violation of the UDTPA. Neb. Rev. Stat. §§ 87-302, 87-303.01(1).

DEMAND FOR JURY TRIAL

123. The State of Nebraska demands a jury on all matters triable by jury pursuant to Nebraska Revised Statutes.

PRAYER FOR RELIEF

WHEREFORE, the State of Nebraska requests that this Court:

- A. Permanently enjoin and restrain Defendant, its agents, employees, and all other persons and entities, corporate or otherwise, in active concert or participation with any of them, from engaging in conduct described in the Complaint that violates the Consumer Protection Act, pursuant to Neb. Rev. Stat. § 59-1608(1).
- B. Permanently enjoin and restrain Defendant, its agents, employees, and all other persons and entities, corporate or otherwise, in active concert or participation with any of them, from engaging in unfair or deceptive acts or practices, in violation of the Consumer Protection Act, pursuant to Neb. Rev. Stat. § 59-1608(1).
- C. Permanently enjoin and restrain Defendant, its agents, employees, and all other persons and entities, corporate or otherwise, in active concert or participation with any of them, from engaging in conduct described in the Complaint that violates the Uniform Deceptive Trade Practices Act, pursuant to Neb. Rev. Stat. § 87-303.05.
- D. Permanently enjoin and restrain Defendant, its agents, employees, and all other persons and entities, corporate or otherwise, in active concert or participation with any of them, from engaging in deceptive or unconscionable acts or practices, in violation of the Uniform Deceptive Trade Practices Act, pursuant to Neb. Rev. Stat. § 87-303.05.
- E. Order Defendant to make clear and conspicuous disclosures to Nebraska consumers, in connection with the marketing

and sale of its networking and smart home devices, regarding the sourcing of its products and components, its ties to China, and known exploited vulnerabilities affecting its devices.

- F. Order Defendant to pay civil penalties for each violation of the Consumer Protection Act and the Uniform Deceptive Trade Practices Act, pursuant to Neb. Rev. Stat. §§ 59-1614 and 87-303.11.
- G. Order Defendant to restore to every person any money acquired by Defendant as a result of its violations of the Consumer Protection Act and the Uniform Deceptive Trade Practices Act, pursuant to Neb. Rev. Stat. §§ 59-1608(2) and 87-303.05(1), including restitution and disgorgement of ill-gotten gains.
- H. Order Defendant to pay the State's costs and attorney's fees in this matter, pursuant to Neb. Rev. Stat. §§ 59-1608(1) and 87-303.05(1)(b).
- I. Order such other and further relief as the Court deems just and equitable.

DATED this 6th day of October 2026.

STATE OF NEBRASKA, Plaintiff.

BY: MICHAEL T. HILGERS, #24483
Nebraska Attorney General

BY: /s/ Derek T. Bral
Derek T. Bral, #26767
Erik W. Fern, #23733
Assistant Attorneys General
Consumer Protection Bureau Chief
NEBRASKA ATTORNEY GENERAL'S OFFICE
1445 K Street, Room 2115
Lincoln, NE 68509-8920
Telephone: (402) 471-1928
Fax: (402) 471-4725
derek.bral@nebraska.gov
erik.fern@nebraska.gov

Brunn (Beau) Roysden*, AZ Bar No. 028698
Culper Law PLLC
111 W. Marshall Ave.
Phoenix, AZ 85013
Telephone: 602-315-7545
beau@culper.law

**Pro Hac Vice forthcoming*

Attorneys for State of Nebraska