



STATE OF NEBRASKA
Office of the Attorney General

2115 STATE CAPITOL BUILDING
LINCOLN, NE 68509-8920
(402) 471-2682
TDD (402) 471-2682
FAX (402) 471-3297 or (402) 471-4725

MIKE HILGERS
ATTORNEY GENERAL

The Honorable Brendan Carr
The Honorable Anna M. Gomez
The Honorable Olivia Trusty
Federal Communications Commission
45 L Street NE
Washington, DC 20002

RE: *Potential Conditional approval of TP-Link Systems, Inc.*
WC Docket No. 18-89, ET Docket No. 21-232, EA Docket No. 21-233

Dear Chairman Carr and Commissioners Gomez and Trusty,

We, the undersigned state Attorneys General, write to express our concerns regarding reports that TP-Link Systems Inc. (“TP-Link”) is seeking conditional approval to sell new router models in the U.S.¹ The importance of safe and secure routers cannot be overstated. As the FCC’s March 23, 2026, Public Notice explained, “[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,” but “[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

As state officials charged with enforcing laws prohibiting unfair and deceptive acts and practices (“UDAP laws”), we write to notify you of three primary concerns we have regarding TP-Link and to offer to work to jointly resolve our concerns about remedying past and ongoing state-law violations in conjunction with your conditional-approval review. First, TP-Link has represented that its routers are secure, when in truth TP-Link has sold routers with serious security vulnerabilities that Chinese state-affiliated groups and other bad actors have exploited. Second, TP-Link represents that it has separated all operational aspects, including its workforce and research and development, from China-based TP-Link Technologies Co. Ltd. (“TP-Link Technologies”) and that its routers are manufactured in Vietnam. But it has been reported that TP-Link still relies on major research and development and manufacturing operations in China that are intertwined with the state-sponsored technology ecosystem, and only 0.5% of TP-Link components are bought in Vietnam with all other inputs into its Vietnam plant imported from or through China. Moreover, TP-Link recently used a construction contractor for its Vietnam plant that

¹ <https://www.pcmag.com/news/facing-router-ban-tp-link-tells-fcc-its-investing-hundreds-of-millions>;
<https://www.fcc.gov/document/fcc-adds-routers-produced-foreign-countries-covered-list> (link to Public Notice).

² <https://docs.fcc.gov/public/attachments/DA-26-278A1.pdf> at PDF p. 7 (Appendix C at p. 1).

the U.S. government designated a Chinese military company. Third, TP-Link deceives consumers about the security of their data by burying in its privacy policies a broad ability to share consumer data, and TP-Link key individuals and facilities are subject to a 2017 Chinese law that requires providing access to Chinese intelligence agencies upon demand. TP-Link does not disclose this risk. Each of these presents a serious consumer-protection harm that must be remedied.

TP-Link's deceptive conduct is the subject of lawsuits against TP-Link filed by the Attorneys General of Nebraska³, Texas⁴, Florida⁵, Montana⁶, and Iowa.⁷ The lawsuits seek to hold TP-Link accountable for placing consumers at risk of exploitation by nefarious actors overseas, and to enjoin their continued misrepresentations regarding the safety and security of TP-Link routers.

I. TP-Link Has Made Misleading Security Representations While Its Routers Have Been Repeatedly Implicated In Serious Cyber Attacks

TP-Link has repeatedly made false and deceptive statements and omitted material information about its routers' security. Chinese state-affiliated hackers and other bad actors have exploited TP-Link routers in serious cyber-attack campaigns, and TP-Link's marketing has touted its security without adequately disclosing these risks to consumers. This is particularly concerning because many older TP-Link routers that consumers are still using⁸ do not have the ability to automatically update, so they often continue to be sitting ducks in consumers' homes. As AGs, we intend to prioritize getting meaningful relief for consumers who were deceived and still have unsecure routers in their homes. Below are some examples of deceptive conduct.

A. TP-Link Deceptively Advertised and Sold Routers That Have Been Used in the Quad 7 Botnet and Horse Shell Attacks By Chinese State Actors and By the Russian GRU

TP-Link's deceptive conduct concerning its TL-WR940N router provides a key example of conduct and consumer harm that must be remedied. TP-Link advertised this router as providing "[e]asy wireless security encryption at a push of [a] WPS button" and "Easy Setup and Use."⁹ TP-Link further stated that its Tether app "lets you manage [the TL-WR940N's] network settings ... including ... access

³ *State of Nebraska ex rel. Michael T. Hilgers v. TP-Link Systems Inc.*, Keith County District Court, Complaint filed 10/6/2026.

⁴ *The State of Texas v. TP-Link Systems Inc.*, Collin County District Court, Complaint filed 2/18/2026.

⁵ *Office of the Attorney General, State of Florida v. TP-Link Systems Inc.*, Tenth Judicial Circuit Court, Polk County, Complaint filed 10/6/2026.

⁶ *State of Montana, ex rel. Austin Knudsen v. TP-Link Systems Inc.*, First Judicial District Court, Lewis and Clark County, Complaint filed 10/6/2026.

⁷ *State of Iowa, ex rel. Attorney General Brenna Bird v. TP-Link Systems Inc.*, Polk County District Court, Complaint filed 10/6/2026.

⁸ <https://www.consumerreports.org/electronics-computers/wireless-routers/how-to-tell-when-its-time-to-replace-your-router-a5475786635/> (Richard Fisco, who oversees electronics testing for Consumer Reports, stating "consumers hold onto their router for dear life and for as long as possible").

⁹ <https://web.archive.org/web/20230329192916/https://www.tp-link.com/us/home-networking/wifi-router/tl-wr940n/>

control.”¹⁰ TP-Link sold this router through 2024, meaning that many of our states’ consumers are still using it.¹¹

Contrary to TP-Link’s security representations, the TL-WR940N contained a critical vulnerability (CVE-2023-50224) that was exploited by both Chinese state-affiliated hackers¹² and the Russian GRU foreign military intelligence agency.¹³ In other words, the router does not have proper “access control” because it allowed unauthorized actors to gain administrator access and conscript the router into an illegal botnet. And the router is not “easy [to] setup and use” but rather requires manually installing a patch that many users would not know to install to prevent it from being a security risk inside consumers’ homes. Consumers using the TL-WR940N router who have not updated it remain particularly vulnerable because it does not support automatic firmware updates. Instead, a user must manually update the firmware to patch this vulnerability.¹⁴

Microsoft reported that The Quad7 Botnet (aka CovertNetwork-1658) was able to gain control of the TL-WR940N and other TP-Link routers that “make up most of this network.”¹⁵ The network is then used to launch cyberattacks, such as “highly evasive password spray attacks” to gain credentials (i.e. logins) of targets such as “think tanks, government organizations, non-governmental organizations, law firms, defense industrial base, and others.”¹⁶ As TP-Link itself was forced to admit, “the Quad 7 ... botnet ... is used by Chinese threat actors for password spray attacks against Microsoft 365 accounts. The threat actor exploits vulnerabilities in the routers to gain remote code execution capability,” and the network is “predominantly TP-Link devices.”¹⁷

This episode also illustrates a concerning connection between the affected devices and security risks for American consumers from Chinese civil-military fusion, which TP-Link did not disclose to consumers despite touting its routers’ security. A 2023 article cited by TP-Link identified “HKVision software, software related to TP-Link Routers, and Dahua digital video recorders” as specifically being compromised in the Quad 7 botnet.¹⁸ Hikvision, Dahua, and TP-Link Technologies (which at the time was still formally affiliated with TP-Link) are now listed by the U.S. Department of Defense as “Chinese

¹⁰ <https://web.archive.org/web/20230329192916/https://www.tp-link.com/us/home-networking/wifi-router/tl-wr940n/>

¹¹ <https://web.archive.org/web/20260521160655/https://www.tp-link.com/us/support/faq/5058/>, <https://perma.cc/XRK7-WA3J> (last updated May 12, 2026); *see also* <https://perma.cc/F4B2-UR85> at 55 (listing end of sale as April 23, 2024 for v6 model).

¹² <https://www.tp-link.com/us/press/news/22295/>; <https://nvd.nist.gov/vuln/detail/CVE-2023-50224>; *see also* <https://web.archive.org/web/20260521160655/https://www.tp-link.com/us/support/faq/5058/> (showing this CVE applied to the TL-WR940N).

¹³ <https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/4453919/nsa-supports-fbi-in-highlighting-russian-gru-threats-against-routers/>; <https://media.defense.gov/2026/Apr/07/2003907743/-1/-1/0/I-260407-PSA.PDF>

¹⁴ *See* <https://www.tp-link.com/us/support/faq/2796/>, <https://perma.cc/G6RS-2YKS> (explaining how to manually update).

¹⁵ <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/>

¹⁶ <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 <https://web.archive.org/web/20250126092628/https://www.tp-link.com/us/support/faq/4365/>

¹⁸ <https://gi7w0rm.medium.com/the-curious-case-of-the-7777-botnet-86e3464c3ffd>
<https://web.archive.org/web/20250116213303/https://gi7w0rm.medium.com/the-curious-case-of-the-7777-botnet-86e3464c3ffd>

military companies.”¹⁹ This clear overlap of Chinese civil-military fusion and cyber-security risk from Chinese state-affiliated hackers is material to consumers, but it was never disclosed by TP-Link.

Chinese hackers have exploited the CVE-2023-50224 vulnerability in the TL-WR940N for other ends as well. Check Point Research reported that a Chinese state-sponsored actor it tracks as “Camaro Dragon” used a malicious firmware implant known as “Horse Shell,” tailored for the TL-WR940N and other TP-Link routers, that includes a custom backdoor enabling remote shell access, file transfer, and SOCKS tunneling.²⁰

In addition to Chinese state-affiliated hackers, the Russian GRU has exploited the same vulnerability to steal sensitive information.²¹ The FBI reports that “[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. These AitM attacks would allow the actors to see the [user’s] traffic unencrypted.”²² In other words, a user would think they are securely communicating with their Outlook Web Access, when the unencrypted content of their traffic is being disclosed to the GRU.

TP-Link’s conduct following the TL-WR940N’s security vulnerability becoming public was also deceptive. The 2023 security article that TP-Link cited specifically identified the TL-WR940N as having hardware that was subject to the vulnerability.²³ Despite previously citing this article, when TP-link listed routers that may be subject to this attack in April 2026, it did not include the TL-WR940N and falsely stated, “[a]ll the affected products have reached End-of-Life (EOL) status and no longer within TP-Link’s standard maintenance lifecycle.”²⁴ However, in May 2026, it had to admit that the TL-WR940N was also affected.²⁵

TP-Link also made deceptive statements and omissions related to other routers compromised by Quad 7. For example, TP-Link advertised multiple security features for the Archer C7 AC1750 (v2 and v3), including that it “provides secure Wi-Fi access for guests sharing your home or office network.”²⁶ TP-Link also advertised “[e]asy setup and management with Tether App.”²⁷ TP-Link also prepared a

¹⁹ <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>

²⁰ <https://research.checkpoint.com/2023/the-dragon-who-sold-his-camaro-analyzing-custom-router-implant/>; <https://blog.checkpoint.com/security/check-point-research-reveals-a-malicious-firmware-implant-for-tp-link-routers-linked-to-chinese-apt-group/>

²¹ <https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/4453919/nsa-supports-fbi-in-highlighting-russian-gru-threats-against-routers/>; <https://media.defense.gov/2026/Apr/07/2003907743/-1/-1/0/I-260407-PSA.PDF>

²² <https://media.defense.gov/2026/Apr/07/2003907743/-1/-1/0/I-260407-PSA.PDF>

²³ <https://gi7w0rm.medium.com/the-curious-case-of-the-7777-botnet-86e3464c3ffd> (“The TP-Link TL-WR940N, like many of the basic models we noticed were infected...”); <https://web.archive.org/web/20241224182608/https://gi7w0rm.medium.com/the-curious-case-of-the-7777-botnet-86e3464c3ffd>; see also <https://web.archive.org/web/20250126092628/https://www.tp-link.com/us/support/faq/4365/> (January 2025 TP-Link article that cites this report).

²⁴ <https://web.archive.org/web/20260410034756/https://www.tp-link.com/us/support/faq/5058/> (updated April 9, 2026).

²⁵ <https://web.archive.org/web/20260521160655/https://www.tp-link.com/us/support/faq/5058/> (last updated May 12, 2026).

²⁶ <https://web.archive.org/web/20260331134655/https://www.tp-link.com/us/home-networking/wifi-router/archer-c7/>

²⁷ <https://web.archive.org/web/20260331134655/https://www.tp-link.com/us/home-networking/wifi-router/archer-c7/>

promotional video that told consumers purchasing the router it would “future-proof” their home networks, and this ad also reiterated that it provides “secure Wi-Fi access for guests sharing your home or office network.”²⁸ Contrary to these representations about “secure Wi-Fi access” and “future-proof[ing]” a network, consumers who purchased versions 2 or 3 of this router unwittingly became easy targets for the cyberattacks described above.²⁹ And like the TL-WR940N, versions 2 and 3 of the C7 do not support automatic firmware updates, so unless a user knows and is able to manually update their firmware, they remain vulnerable.³⁰

B. TP-Link Also Deceptively Sold Routers That Have Been Used in Multiple Botnet Operations, including the Flax Typhoon Attacks by Chinese State Actors

TP-Link also deceptively advertised the Archer AX21 (AX1800) router to consumers as offering “Refined Password Security” and a “New Level of Cyber Security” with the “latest Wi-Fi security protocol, WPA3.”³¹ TP-Link also deceptively advertised “easy setup”³² when v1 and v1.2 of its AX21 router did not offer automatic updates, so safely setting up the router included manually installing a patch that many users would not know to install. The AX21 was the bestselling WiFi 6 router on Amazon,³³ and the current version (v5) is still listed as Amazon’s choice.³⁴

In 2023, it was publicly disclosed through CVE-2023-1389, that versions 1 through 3 of the Archer AX21 router had a serious vulnerability that allowed a hacker to inject code on its web settings page and take control of the router. This vulnerability, which has been actively exploited by multiple botnet operations,³⁵ gives the hacker root access, and the hacker does not need to know the router’s login password to send this malicious command.³⁶ TP-Link admitted in April 2023 that the “AX21 has been added to the Mirai botnet[.]”³⁷ After this, it was used by the Flax Typhoon group, run by Chinese state-affiliated hackers, to carry out cyberattacks.³⁸ This means that TP-Link’s statements about “password security” were false or deceptive. Worse, versions 1 and 1.2 of the Archer AX21 did not support

²⁸ <https://www.youtube.com/watch?v=-PEWXGUQiQ8> at 1:00 (“future-proof”), 1:54 (“secure Wi-Fi access for guests”).

²⁹ <https://www.tp-link.com/us/support/faq/5058/>

³⁰ See generally <https://www.tp-link.com/en/support/faq/2796/>

³¹ <https://web.archive.org/web/20221006205422/https://www.tp-link.com/us/home-networking/wifi-router/archer-ax21/>

³² <https://web.archive.org/web/20221006205422/https://www.tp-link.com/us/home-networking/wifi-router/archer-ax21/>

³³ <https://gizmodo.com/forget-slow-wifi-amazon-just-cut-the-best-selling-wifi-6-tp-link-router-to-a-near-record-low-2000756849>

³⁴ <https://www.amazon.com/WiFi-6-Router-Gigabit-Wireless/dp/B08H8ZLKKK?tag=gizmodo08c-20&th=1>

³⁵ https://5gstore.com/blog/2026/04/12/router-security-by-the-numbers-10-years-of-cve-data/?srsId=AfmBOOrhT3UHxdajtiJaT1M1oO7L9U_NnCpUpIebnEdCJ6K-4PVgJpGg.

³⁶ <https://nvd.nist.gov/vuln/detail/cve-2023-1389> (“allowing an unauthenticated attacker to inject commands, which would be run as root, with a simple POST request”); <https://www.sentinelone.com/vulnerability-database/cve-2023-1389/> (same).

³⁷ <https://perma.cc/BNC8-C69P>

³⁸ <https://routerarena.com/news/FBI-remotely-resets-thousands-of-routers-to-disrupt-Flax-Typhoon-botnet> (“Specific hardware like the TP-Link Archer AX21 was a primary target due to a known vulnerability, CVE-2023-1389, which allows unauthenticated command injection.”); https://5gstore.com/blog/2026/04/12/router-security-by-the-numbers-10-years-of-cve-data/?srsId=AfmBOOrhT3UHxdajtiJaT1M1oO7L9U_NnCpUpIebnEdCJ6K-4PVgJpGg (“CVE-2023-1389, an unauthenticated command injection flaw in the popular Archer AX21 router ... has been actively exploited by at least six different botnet operations.”); <https://therecord.media/tp-link-router-vulnerability-botnets> (“The flaw — CVE-2023-1389 — ... affects the Archer AX21.”); <https://www.cybersecuritydive.com/news/-botnet-exploits-tp-link-router/742319/> (explaining for later attack that “[t]he flaw exploited by attackers is a command injection vulnerability tracked as CVE-2023-1389....”); see also <https://www.govtech.com/security/national-security-fears-prompt-federal-probe-of-tp-link> (showing AX21 router)

automatic firmware updates as a default. This means that these devices were not “easy [to] setup” but rather required manually downloading a firmware update.³⁹ And recently, TP-Link has obfuscated a security risk that it is clearly aware of by having its spokesperson state that it “‘has not been able to verify how its devices are affected, if at all,’ based on the information available to it.”⁴⁰

C. TP-Link Makes False and Deceptive Representations About Consumers’ Security Based on Its HomeShield Service And Materially Omits Disclosure of the 2021 Chinese Regulation that Companies Immediately Share Zero-Day Vulnerabilities

A third example of deceptive representations is TP-Link’s claims related to its HomeShield service. TP-Link currently tells consumers that its “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.”⁴¹ These statements are deceptive in assuring consumers that their routers can handle all security risks, when this is simply not true. It is also deceptive because it doesn’t disclose the risks—which HomeShield cannot address—of TP-Link’s Chinese facilities being subject to a requirement that they share zero-day vulnerabilities with the Chinese government within 2 days of discovering such vulnerability.

First, multiple routers that TP-Link advertised as having HomeShield had security vulnerabilities. For example, TP-Link advertised the Archer AXE75 with HomeShield and also represented that the AXE75 has “advanced security features that deliver a safe environment that protects your family and network’s data and privacy.”⁴² Yet the Archer AXE75 was vulnerable to CVE-2024-53375, which was classified as a high-severity vulnerability that allowed the hacker to execute commands on the router.⁴³ This router was also subject to another high-severity vulnerability, CVE-2025-15568, which allows the hacker to perform remote code execution in certain scenarios.⁴⁴

Similarly, the Archer AX53 advertises HomeShield and links to the HomeShield page with TP-Link’s representations about “cover[ing] all security scenarios” and “handl[ing] all [of the user’s] concerns.”⁴⁵ TP-Link also states on the AX53 webpage, “TP-Link HomeShield - Enhanced security defends against the latest cyber threats.” But this router was subject to CVE-2025-15607 and CVE-2025-15608.⁴⁶ Under the first of these, an authenticated attacker can take complete administrative control of the system. Under the second—which was labeled 9.8 (critical)—an attacker could create a Denial of Service (DoS), and under certain conditions, achieve remote code execution.⁴⁷ And other routers that

³⁹ See generally <https://www.tp-link.com/en/support/faq/2796/>

⁴⁰ <https://www.bloomberg.com/news/articles/2025-04-11/wi-fi-giant-tp-link-s-us-future-hinges-on-its-claimed-split-from-china>

⁴¹ <https://www.tp-link.com/us/homeshield/>; <https://perma.cc/M8ME-4EX7>

⁴² <https://www.tp-link.com/us/home-networking/wifi-router/archer-axe75/>

⁴³ <https://nvd.nist.gov/vuln/detail/CVE-2024-53375>

⁴⁴ <https://www.tp-link.com/us/support/faq/5005/>; <https://nvd.nist.gov/vuln/detail/cve-2025-15568>

⁴⁵ <https://www.tp-link.com/my/home-networking/wifi-router/archer-ax53/>

⁴⁶ <https://www.tp-link.com/us/support/faq/5025/>

⁴⁷ <https://nvd.nist.gov/vuln/detail/CVE-2025-15608>

also advertise HomeShield—including the Archer BE230, Archer AX73 and Deco BE25—were also subject to command-injection vulnerabilities.⁴⁸

Second, even when router vulnerabilities are eventually patched by TP-Link, this does not eliminate the risk during the time between when the vulnerability is first discovered and when it is patched. This can take several weeks or multiple months in many cases. On top of this, it also does not eliminate the risk that the Chinese government is made aware of the zero-day vulnerability before it is patched. 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 security vulnerabilities (so-called “zero-day” attacks).⁴⁹ The DHS has reported that China appears to use the RMSV to preview dangerous zero-day flaws before companies can develop fixes. HomeShield does not address that “concern[.]” and therefore TP-Link’s representations are deceptive and omit material information.⁵⁰

II. TP-Link’s Representations That It Separated from TP-Link Technologies and that Its Routers Are Manufactured in Vietnam Are Also Deceptive And Omit Material Information

Our second major concern is that TP-Link makes deceptive statements and omits material information when representing to our states’ consumers that it has separated from TP-Link Technologies, that the separation encompasses all research and development and production, and that no government has access to or control over the design and production of its routers. In reality, as Bloomberg News reported in April 2025, “much of the research, development and manufacturing operations of [the] U.S. company remain in China, entrenched in the country’s state-sponsored technology ecosystem, despite the restructuring.”⁵¹ We are also concerned that TP-Link makes deceptive statements and omissions to our states’ consumers related to its products being manufactured in Vietnam when only 0.5% of the components are bought in Vietnam, and all other inputs are imported from or through China, and when a Chinese military-fusion company was responsible for recent construction at TP-Link’s Vietnam factory.⁵²

A. TP-Link’s Representations Are Deceptive Because It Maintains Major Facilities in China and Continues to Participate in China’s State-Sponsored Technology Ecosystem

TP-Link represented in 2024 that its separation from TP-Link Technologies means that each “functions as a standalone entity” and the separation “encompasses all shareholdings and operational aspects, including ... workforce, research and development, [and] production[.]”⁵³ TP-Link also

⁴⁸ <https://www.tp-link.com/us/support/faq/4935/>

⁴⁹ <https://www.atlanticcouncil.org/in-depth-research-reports/report/preserving-international-cybersecurity-research/>

⁵⁰ <https://www.tp-link.com/us/homeshield/>; <https://perma.cc/M8ME-4EX7>

⁵¹ <https://www.bloomberg.com/news/articles/2025-04-11/wi-fi-giant-tp-link-s-us-future-hinges-on-its-claimed-split-from-china>

⁵² <https://www.bloomberg.com/news/articles/2025-11-22/wi-fi-giant-s-vietnam-factory-raises-questions-over-china-split>; <https://www.bloomberg.com/news/articles/2025-04-11/wi-fi-giant-tp-link-s-us-future-hinges-on-its-claimed-split-from-china>

⁵³ <https://www.tp-link.com/us/press/news/21130/>

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.”⁵⁴ An investigation by Bloomberg News, and TP-Link’s own 2024 Sustainability Report, show that these statements are deceptive. Bloomberg reported that “[w]hat TP-Link hasn’t advertised – but which Chinese corporate records and government announcements show – is 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.”⁵⁵

Per Bloomberg, TP-Link and TP-Link Technology’s “operations in China ... employ 11,000 people” compared to only “305 employees based in the U.S.”⁵⁶ Among these Chinese facilities and operations is a “massive research, development and manufacturing arm that has attracted Chinese government support and that continues to power TP-Link despite the reorganization.”⁵⁷ TP-Link even implicitly admitted that it is investing hundreds of millions in China. When Bloomberg asked about a \$180 million investment in a large engineering facility in Chengdu, a TP-Link spokesperson responded that it “has currently stopped increasing its investments in personnel, R&D, and manufacturing in China.” A purported policy to stop “increasing” investments above hundreds of millions of dollars is not the same thing as “separati[ng] all ... operational aspects, including ... research and development[and] production[.]”⁵⁸ TP-Link’s own 2024 Sustainability Report confirms that it has multiple important facilities remaining in China, including its “Shenzhen R&D Center, Shenzhen Manufacturing Center, Dongguan Manufacturing Center, [and] Shenzhen Guangqiao Manufacturing Center.”⁵⁹ Given this, TP-Link’s statements to American consumers are deceptive and omit material information.

Vividly illustrating the deceptive nature of TP-Link’s statements to consumers, Bloomberg reported that after TP-Link claimed to have split with TP-Link Technologies, “representatives from both the US- and China-based TP-Links attended a CCP event” in China and posted a picture 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, just with different logos reflecting the corporate split.”⁶⁰

Deceptive statements and omissions about a router manufacturer’s ties to China matter to consumers because China is designated by the United States as a foreign adversary,⁶¹ and China’s legal framework creates national-security and data-access risks for China-based entities and employees.

⁵⁴ <https://www.tp-link.com/us/landing/fact-sheet/>

⁵⁵ <https://www.bloomberg.com/news/articles/2025-04-11/wi-fi-giant-tp-link-s-us-future-hinges-on-its-claimed-split-from-china>

⁵⁶ <https://www.bloomberg.com/news/articles/2025-04-11/wi-fi-giant-tp-link-s-us-future-hinges-on-its-claimed-split-from-china>

⁵⁷ <https://www.bloomberg.com/news/articles/2025-04-11/wi-fi-giant-tp-link-s-us-future-hinges-on-its-claimed-split-from-china>

⁵⁸ <https://www.tp-link.com/us/press/news/21130/>

⁵⁹ Page 29, https://static-page.tp-link.com/sustainability/pdf/TP-Link%202024%20Sustainability%20Report.pdf?_gl=1*1rc5oq8*_gcl_au*NDIxNTg5NTMwLjE3ODExOTUxOTA.*_ga*ODc5MDc4NjE1LjE3ODExOTUxODk.*_ga_X5XJFE5K24*cZ3ODI3NzY2MTEkbzMzJGcxJHqXNzgyNzc5NjU5JGo2MCRsMCRoMA

⁶⁰ <https://www.bloomberg.com/news/articles/2025-04-11/wi-fi-giant-tp-link-s-us-future-hinges-on-its-claimed-split-from-china>

⁶¹ *See, e.g.*, 15 C.F.R. § 791.4.

Article 7 of China’s 2017 National Intelligence Law contains broad support-and-cooperation language for organizations and citizens,⁶² and China’s vulnerability-management rules require network-product providers to report newly discovered vulnerabilities to MIIT within a short period and requires certain disclosures within 2 days.⁶³ The Department of Defense’s June 2026 § 1260H materials further heighten the consumer-protection concern by identifying TP-Link Technologies as a Chinese military company under the statutory framework.⁶⁴ Simply put, our laws prohibit making deceptive statements to consumers that a router—key hardware they put in their homes and businesses—is simply a Vietnam-manufactured product sold by an American Company with no material China-related operational dependencies or legal risks, when this is not true.

B. TP-Link’s Claim That Its Routers Are Manufactured In Vietnam Also Deceives Consumers Related to the Role of China In Such Manufacturing

TP-Link represents that it “manufacture[s] products for the U.S. market in its own factory in Vietnam” and that “[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.”⁶⁵ These statements are deceptive and omit material information.

First, the amount of manufacturing that occurs in Vietnam appears to be minimal because only 0.5% of TP-Link components are bought in Vietnam, with all other inputs into its Vietnam plant imported from or through China. Bloomberg reported this fact based on trade data and TP-Link confirmed it.⁶⁶ Second, TP-Link’s Vietnam facility has connections to the Chinese military that TP-Link does not disclose to consumers. TP-Link recently used a construction contractor, China State Construction Engineering Corporation (“CSCEC”), that the U.S. government designated a Chinese military company.⁶⁷

III. TP-Link’s Disclosures Related to Use of Consumer Data Materially Omit the Risks to Consumers from China’s 2017 Intelligence Law

TP-Link’s disclosures related to sharing consumer data are deceptive because they reserve a broad power to share consumer data and do not disclose that TP-Link key employees and facilities appear to be subject to Chinese national intelligence laws. TP-Link’s routers and other products can be operated using mobile applications such as TP-Link Tether app and TP-Link Deco app. These applications can

⁶² <https://www.chinalawtranslate.com/en/national-intelligence-law-of-the-p-r-c-2017/>

⁶³ <https://www.atlanticcouncil.org/in-depth-research-reports/report/preserving-international-cybersecurity-research/>

⁶⁴ <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>; <https://www.federalregister.gov/documents/2026/06/10/2026-11571/notice-of-availability-of-designation-of-chinese-military-companies>.

⁶⁵ <https://www.tp-link.com/us/landing/fact-sheet/>

⁶⁶ <https://www.bloomberg.com/news/articles/2025-04-11/wi-fi-giant-tp-link-s-us-future-hinges-on-its-claimed-split-from-china>; <https://www.bloomberg.com/news/articles/2025-11-22/wi-fi-giant-s-vietnam-factory-raises-questions-over-china-split>.

⁶⁷ <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>; *see also* <https://www.bloomberg.com/news/articles/2025-11-22/wi-fi-giant-s-vietnam-factory-raises-questions-over-china-split>

be integral for users to successfully set up and manage their devices, as well as related TP-Link services such as HomeShield.⁶⁸

In the Tether Privacy Policy, TP-Link first states that it “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.”⁶⁹ TP-Link then specifically carves out the right to share information with its “authorized partners, including affiliates ... to: ... comply with applicable laws.”⁷⁰ And then it further provides that it “may share information ... (c) where otherwise necessary to protect our rights, interests, and/or property (including, without limitation, to enforce our agreements), or the rights, interests, and/or property of our agents, independent contractors, customers, and others.”⁷¹ Similar carve-outs are included in the terms of service for TP-Link’s services such as Deco,⁷² Tapo,⁷³ and Kasa.⁷⁴

When providing for this broad right to share consumer information, TP-Link does not disclose to consumers that key employees and affiliates are Chinese citizens or entities subject to China’s 2017 National Intelligence Law. Under Article 7 of that law, Chinese companies and citizens are required to “support, assist, and cooperate with national intelligence efforts in accordance with law” and also to “protect national intelligence work secrets they are aware of.”⁷⁵ Moreover, Article 14 of that law provides that “National intelligence work institutions lawfully carrying out intelligence efforts may request that relevant organs, organizations, and citizens provide necessary support, assistance, and cooperation.”⁷⁶ The U.S. Department of Homeland Security (“DHS”) issued a Data Security Business Advisory, which stated that this law “forms the baseline of the modern data collection regime, and compels 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.”⁷⁷ DHS further stated that this 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.”⁷⁸ The U.S. National Security Advisor reiterated these risks from the 2017 National Intelligence Law and also tied it specifically to “the goals of the PRC’s Military-Civil Fusion (MCF) strategy.”⁷⁹

⁶⁸ Paragraph 3, <https://www.tp-link.com/us/support/faq/2997/>

⁶⁹ Paragraph 3, <https://privacy.tp-link.com/app/Tether/privacy>

⁷⁰ Paragraph 3, <https://privacy.tp-link.com/app/Tether/privacy>

⁷¹ Paragraph 3, <https://privacy.tp-link.com/app/Tether/privacy>

⁷² Paragraph 3, <https://privacy.tp-link.com/app/Deco/privacy>

⁷³ Paragraph 3, <https://privacy.tp-link.com/app/tapo/privacy>

⁷⁴ Paragraph 3, <https://privacy.tp-link.com/app/kasa/privacy>

⁷⁵ 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/>; accord

https://cs.brown.edu/courses/cs180/sources/2017_06_28_China_NationalIntelligenceLawOfThePeoplesRepublicOfChina.pdf

⁷⁶ <https://www.chinalawtranslate.com/en/national-intelligence-law-of-the-p-r-c-2017/>

⁷⁷ Page 6, https://www.dhs.gov/sites/default/files/publications/20_1222_data-security-business-advisory.pdf

⁷⁸ Page 6, https://www.dhs.gov/sites/default/files/publications/20_1222_data-security-business-advisory.pdf

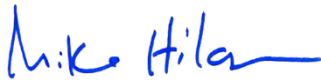
⁷⁹ <https://trumpwhitehouse.archives.gov/briefings-statements/statement-national-security-advisor-robert-c-obrien-011521-2/>

Therefore, when TP-Link states that it may share information when necessary to protect its rights or the rights of “others,” there is a specific China-related risk that would be material to many consumers. TP-Link deceptively omits any mention of this risk.

IV. Conclusion

We stand ready to work with the FCC to protect American consumers. Our consumer-protection concerns are focused on ensuring that 1) previously harmed consumers are protected from further depredation and 2) going forward, consumers are protected from exploitation by the Chinese Communist Party. We appreciate your work on these issues and look forward to continued coordination.

Sincerely,



Mike Hilgers
Nebraska Attorney General



Steve Marshall
Alabama Attorney General



Chris Carr
Georgia Attorney General



Raúl Labrador
Idaho Attorney General



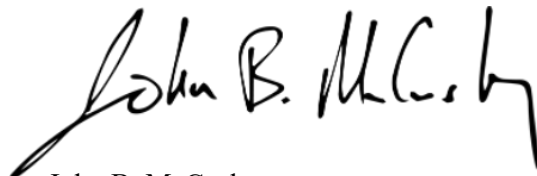
Kris Kobach
Kansas Attorney General



Liz Murrill
Louisiana Attorney General



Austin Knudsen
Montana Attorney General



John B. McCuskey
West Virginia Attorney General



Brenna Bird
Iowa Attorney General



Drew Wrigley
North Dakota Attorney General



Cori Mills
Acting Alaska Attorney General



Tim Griffin
Arkansas Attorney General



David Sunday, Jr.
Pennsylvania Attorney General



Alan Wilson
South Carolina Attorney General



Marty Jackley
South Dakota Attorney General



Jonathan Skrmetti
Tennessee Attorney General



Derek Brown
Utah Attorney General



Russell Coleman
Kentucky Attorney General



Todd Rokita
Indiana Attorney General



Ken Paxton
Texas Attorney General

A handwritten signature in blue ink, appearing to read 'A. Wilson'.

Andy Wilson
Ohio Attorney General