

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

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

Plaintiff,

v.

LOREX CORPORATION, A
DELAWARE CORPORATION;
AND LOREX TECHNOLOGY
INC., A CANADIAN COMPANY,

Defendants.

Case No: CI25-_____

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 the above-named Defendants (“Lorex,” or “Defendants”), to address a pattern of deceptive and unfair business practices related to the marketing and sale of Lorex home security cameras. Defendants represent that their cameras are “private by design,” “safe and secure,” and appropriate for use in sensitive spaces such as children’s bedrooms, while concealing material facts about their ongoing reliance on Zhejiang Dahua Technology Co., Ltd. (“Dahua”), a company sanctioned by the U.S. government for national security risks and human rights violations. The State seeks to obtain injunctive relief, restitution for consumers, civil penalties, and other equitable relief to address Defendants’ 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 Defendants’ cameras to Nebraska consumers.

INTRODUCTION

1. Lorex Corporation and Lorex Technology Inc. (collectively, “Lorex”) deceptively market security cameras manufactured by Zhejiang Dahua Technology Co., Ltd. (“Dahua”) to U.S. consumers as being protective of consumers’ privacy.

2. Lorex’s statements are misleading because Dahua’s involvement creates serious security and privacy risks. Rather than informing consumers of these risks, Lorex provides a misleading disclaimer that suggests any concerns are limited to use by the federal government. These marketing tactics are deceptive and unfair.

3. On Lorex’s website, under the security tab, it assures consumers that Lorex is “committed to protecting the integrity, privacy, and security of our customers’ information” and “We take every step to ensure your security.”¹

4. On its Privacy Commitment page, Lorex states: “Your privacy is our top priority. That’s why we provide you with the tools to manage your own devices and storage. We are committed to taking every step possible to ensure your recordings remain private.”²

5. On Lorex’s FAQ, under “Are Lorex wireless cameras secure?” the answer begins “Yes.”³

6. Lorex sells through Costco online, among other large retailers, and its product page for the Lorex 2K Dual Lens Indoor camera contains a statement: “Keep your recordings private and in your control” and that the product is “Private by design.”⁴

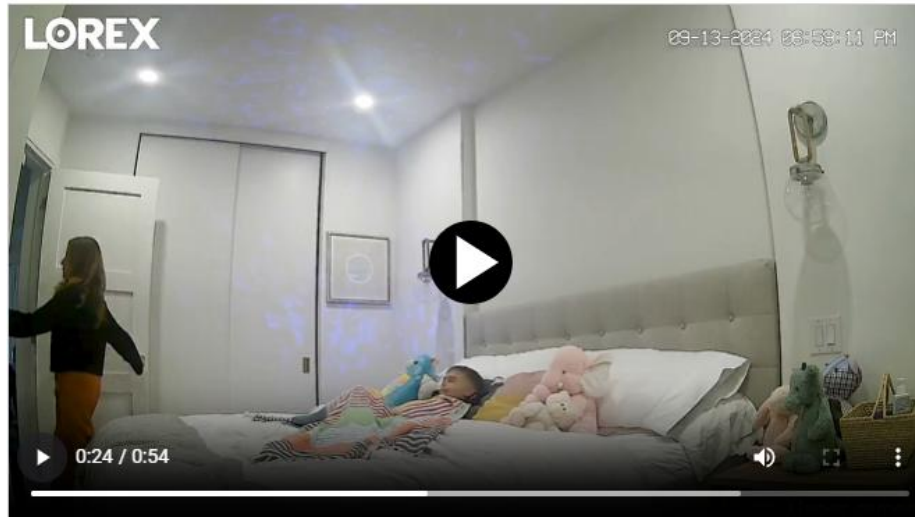
¹Emphasis added, <https://perma.cc/79L4-78D3>

² Emphasis added, <https://perma.cc/B3SS-Q6F4>

³ <https://perma.cc/HS6B-2VJC>

⁴ <https://www.costco.com/lorex-2k-dual-lens-indoor-pan-tilt-wi-fi-security-camera-2-pack.product.4000384381.html> [Last visited 7/30/2025]. Under Product Details tab, click on View More and scroll down to the picture of the Lorex Video Vault.

7. Lorex also represents to consumers that its high-definition cameras can be placed in extremely sensitive locations, such as the inside of a child's bedroom.⁵



8. Lorex's statements and representations (and others like them) are misleading because of Lorex's relationship with Dahua.

9. A bipartisan letter from the Congressional-Executive Commission on China ("CECC") stated, "Dahua still supplies all the component parts for the Lorex cameras and other surveillance equipment."⁶

10. The Lorex 2K Dual Lens Indoor camera sold on Costco.com, BestBuy.com, Kohls.com, and HomeDepot.com is nearly identical in appearance to Dahua "H5D-5F" and "H3D-3F" models.

⁵ <https://www.costco.com/lorex-2k-dual-lens-indoor-pan-tilt-wi-fi-security-camera-2-pack.product.4000384381.html>. Click on "View More" under Product Details, and view first video.

⁶ <https://www.cecc.gov/sites/evo-subsites/cecc.house.gov/files/documents/Costco%20Letter%20Signed.pdf>; see also <https://techcrunch.com/2023/11/01/lawmakers-costco-lorex-dahua-entity-list/>

	
<p>Dahua “H5D-5F” and “H3D-3F” models.⁷</p>	<p>Lorex 2K Dual Lens Indoor Pan-tilt Wi-Fi Security Camera for sale on Costco.com, BestBuy.Com, Kohls.com, and HomeDepot.com.⁸</p>

11. Another camera currently for sale on Amazon.com, Kohls.com, and OfficeDepot.com is the Lorex 2K Indoor Wi-Fi Security Camera, Model W461ASC-E.⁹

12. Researchers in Kentucky were able to analyze the camera’s firmware and discovered that it takes a technician to a login

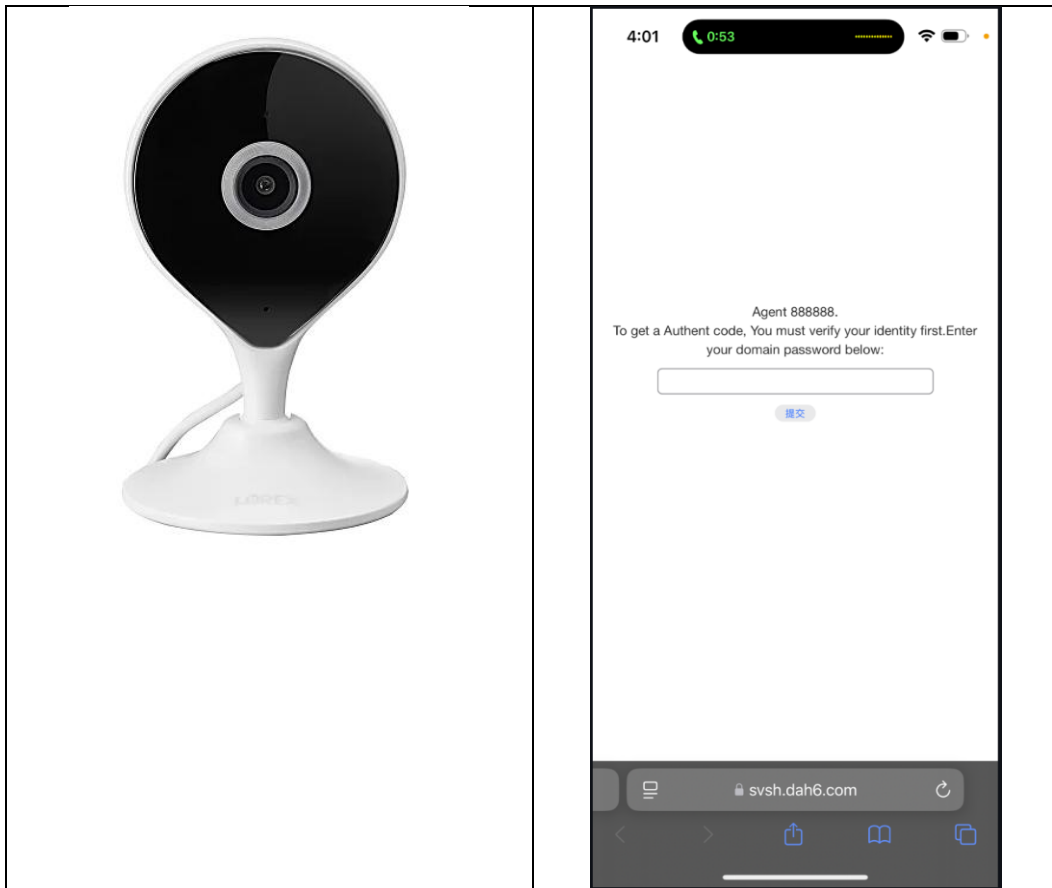
⁷ See <https://perma.cc/6QJ7-VSPC>; <https://perma.cc/EW9Y-K9ZW>

⁸ <https://www.costco.com/lorex-2k-dual-lens-indoor-pan-tilt-wi-fi-security-camera-2-pack.product.4000384381.html>; <https://www.bestbuy.com/site/lorex-2k-dual-lens-indoor-pan-tilt-wi-fi-security-camera-white/6587859.p?skuId=6587859>; <https://www.kohls.com/product/prd-7462714/lorex-2k-dual-lens-indoor-pan-tilt-wi-fi-security-camera.jsp>; <https://www.homedepot.com/p/Lorex-2K-Dual-Camera-Pan-Tilt-Indoor-Security-Camera-W463AQD-E/332823101>.

⁹ <https://perma.cc/PKP4-QBLY>. Clicking on the first hyperlink on this page “Lorex makes a cheap” takes the user to: <https://perma.cc/K3ZK-42FA>. This same model number is for sale at <https://www.kohls.com/product/prd-6378004/lorex-2k-indoor-wi-fi-security-camera.jsp>; <https://www.officedepot.com/a/products/7842911/Lorex-2K-QHD-Indoor-Wi-Fi/#Specs>. And a camera with the same name is available at https://www.amazon.com/Lorex-Indoor-Wi-Fi-Security-Camera/dp/B0CPT8QXCL?ref=ast_sto_dp.

prompt at svsh.dah6.com.¹⁰ That domain is associated with Dahua, not Lorex.¹¹

13. While there is nothing inherently nefarious about a login, the fact that it goes through Dahua further illustrates Dahua’s involvement and control over both the hardware and software of these devices.



¹⁰ <https://perma.cc/PKP4-QBLY>. Scroll down to “Scanning the QR takes you to a support login that appears internal to Lorex.”

¹¹ See <https://www.godaddy.com/whois/results.aspx?domain=dah6.com> (listing the “Organization” for Registrant as 浙江大华技术股份有限公司). That translates to Zhejiang Dahua Technology Co., Ltd. See <https://translate.google.com/?sl=zh-CN&tl=en&text=%E6%B5%99%E6%B1%9F%E5%A4%A7%E5%8D%8E%E6%8A%80%E6%9C%AF%E8%82%A1%E4%BB%BD%E6%9C%89%E9%99%90%E5%85%AC%E5%8F%B8&op=translate>. In addition, the dah6.com website redirects to dahuatech.com. See <https://web.archive.org/web/20250711114605/dah6.com>.

Lorex 2K Indoor Wi-Fi Security Camera currently for sale at Amazon.com, Kohls.com, and OfficeDepot.com.	Support login associated with dah6.com—a domain owned by Dahua—that researchers accessed when analyzing the Lorex camera’s firmware.
---------------------------------------------------------------------------------------------------------	--------------------------------------------------------------------------------------------------------------------------------------

14. Lorex’s failure to disclose Dahua’s involvement and associated risks is deceptive and unfair.

15. The federal government—including the Department of Defense (“DOD”) under the FY 2021 National Defense Authorization Act (“NDAA”) and the Federal Communications Commission (“FCC”) under the 2021 Secure Equipment Act (“SEA”)—has added Dahua to lists of companies that pose security concerns and whose products are subject to restrictions.

16. In fact, Dahua previously owned Lorex and only decided to sell it the day before the FCC announced that it would block Dahua from further product approvals in the U.S.¹²

17. Dahua cameras have experienced multiple security vulnerabilities and other risks that a reasonable consumer would find significant when evaluating Lorex’s express representations about privacy.

18. These include backdoor and other vulnerabilities and documented human-rights violations.

19. The CECC has stated: “Lorex products are ... a known security risk to U.S. customers because critical vulnerabilities are regularly discovered in Dahua products, including unauthorized

¹² Order dated November 11, 2022, released November 25, 2022.
<https://docs.fcc.gov/public/attachments/FCC-22-84A1.pdf>

viewing of video and audio feeds and archives, as well as unauthorized network access and remote tampering with settings.”¹³

20. The CECC further noted: “No data collected can be withheld from PRC authorities should they request it for intelligence purposes—a vulnerability that your U.S. and global customers should be notified of.”¹⁴

21. Despite this, Lorex adds only a misleading disclaimer to certain webpages that suggests the cameras are appropriate for home and business use.

22. For example, Costco’s online page for Lorex products contains a disclaimer under “Product Details” that states: “Lorex products are designed for consumer and business use only and not for US federal governments, federally-funded projects or contractors subject to NDAA.”¹⁵

23. Lorex posts this same disclaimer on its FAQ page under a cryptically worded header, “What is Lorex’s response to the NDAA?”¹⁶

24. A reasonable consumer would interpret these disclaimers as stating that any concern is limited to federal government use, and the disclaimers are therefore misleading.

25. By presenting their products as “private by design” while concealing Dahua’s ongoing involvement and the serious risks of surveillance and exploitation, and by making deceptive assurances of

¹³ <https://www.cecc.gov/sites/evo-subsites/cecc.house.gov/files/documents/Costco%20Letter%20Signed.pdf>; see also <https://techcrunch.com/2023/11/01/lawmakers-costco-lorex-dahua-entity-list/>

¹⁴ <https://www.cecc.gov/sites/evo-subsites/cecc.house.gov/files/documents/Costco%20Letter%20Signed.pdf>

¹⁵ *E.g.*, <https://www.costco.com/lorex-fusion-nvr-with-two-4k-180-panoramic-lens-and-two-4k-bullet-cameras.product.4000272398.html>.

¹⁶ <https://perma.cc/HS6B-2VJC>

security, Lorex has engaged in unfair and deceptive trade practices in violation of the CPA and UDTPA.

26. Lorex's conduct has placed Nebraska consumers at serious risk of harm by making their most intimate images and private locations vulnerable to exploitation and intrusion by foreign actors with a proven track record of nefarious and untrustworthy conduct.

27. The Attorney General brings this action to enjoin Defendants, hold them accountable, and to protect Nebraskans from having their intimate images and privacy further jeopardized by Lorex's egregious and unconscionable acts.

AUTHORITY & PUBLIC INTEREST

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

29. 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.

30. 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 engaging in any deceptive trade practices or engaging therein, or doing any act in furtherance thereof.

31. The Attorney General has reasonable cause to believe that Defendants have violated the CPA and UDTPA and brings this action in the public interest because Defendants have deceived, misled, and caused financial harm to consumers from Nebraska and other states.

32. 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.

PARTIES

33. 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.

34. 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).

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

36. Defendant Lorex Corporation is a Delaware corporation with its principal office located at 999 Corporate Blvd., Suite 110, Linthicum, Maryland 21090. Lorex Corporation is ultimately owned by Skywatch, a Taiwanese company. Lorex transacts business in Nebraska by marketing, offering, and selling Lorex-branded security cameras to Nebraska consumers, including through national retailers such as Costco, Best Buy, Home Depot, Kohl's, Office Depot, and Amazon.com.

37. Defendant Lorex Technology Inc. is a Canadian company with its headquarters located at 250 Royal Crest Court, Markham, Ontario L3R 3S1, Canada. Lorex Technology Inc. is an intermediate

parent of Lorex Corporation and is affiliated with Zhejiang Dahua Technology Co., Ltd. (“Dahua”), a Chinese technology company sanctioned by the United States government. Lorex Technology Inc. likewise transacts business in Nebraska by marketing, offering, and selling Lorex-branded security cameras to Nebraska consumers.

38. At all relevant times, Defendants acted in concert to advertise, promote, and sell Lorex cameras in Nebraska. Defendants share common business purposes, operate as a single enterprise, and are collectively responsible for the deceptive and unfair practices alleged in this Complaint.

JURISDICTION AND VENUE

39. At all times relevant to this Complaint, Defendants were engaged in trade and commerce affecting consumers in Nebraska insofar as they marketed, offered, and sold home security cameras to Nebraska residents through online retailers and large national chains, including Costco, Nebraska Furniture Mart, Best Buy, Home Depot, Kohl’s, Office Depot, and Amazon.com.

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

41. 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 Defendants have engaged in unfair, deceptive, and unconscionable acts or practices in Nebraska in violation of the CPA and UDTPA.

42. Venue is proper in this Court pursuant to Neb. Rev. Stat. §§ 25-403.01 and 25-403.02 because Defendants transact business in Nebraska, advertise and sell products to Nebraska residents, and the

unlawful acts and practices alleged herein caused injury to consumers in this county and throughout the State.

FACTUAL ALLEGATIONS

I. Dahua Is a Prohibited Company With Repeated Security Issues

43. Zhejiang Dahua Technology Co., Ltd. (“Dahua”) is a Chinese company¹⁷ that was designated as a “Chinese military company” by the U.S. Department of Defense (“DOD”) under the FY21 National Defense Authorization Act (“NDAA”), which means DOD has determined that Dahua is, or is owned or controlled by, a military-civil fusion contributor for the Chinese military.¹⁸

44. Dahua is also listed on the U.S. Department of Commerce’s Entity List for its role in mass surveillance of Uyghurs in Xinjiang, restricting U.S. exports of technology to the company.¹⁹

45. Additionally, Section 889 of the 2019 NDAA lists “video surveillance and telecommunications equipment” produced by Dahua, or any subsidiary or affiliate, as “Covered Telecommunications Equipment or Services,” prohibiting them in federal contracts and

¹⁷ See, e.g., Joint Petitioners’ Brief, Document #2002808 at PDF page 5 (internal page iii), *Dahua v. FCC*, Case No. #23-1032 (D.C. Cir.).

¹⁸ <https://media.defense.gov/2025/Jan/07/2003625471/-1/-1/1/ENTITIES-IDENTIFIED-AS-CHINESE-MILITARY-COMPANIES-OPERATING-IN-THE-UNITED-STATES.PDF>. The Department of Commerce lists its addresses as: Dahua Technology, 807, Block A, Meike Building No. 506, Beijing South Road, New City, Urumqi, Xinjiang, China; 1199 Bin'an Road, Binjiang High-tech Zone, Hangzhou, China; and 6/F, Block A, Dacheng Erya, Huizhan Avenue, Urumqi, China; and No. 1187, Bin'an Road, Binjiang District, Hangzhou City, Zhejiang Province, China. <https://www.ecfr.gov/current/title-15/subtitle-B/chapter-VII/subchapter-C/part-744/appendix-Supplement%20No.%204%20to%20Part%20744>

¹⁹ <https://www.federalregister.gov/documents/2019/10/09/2019-22210/addition-of-certain-entities-to-the-entity-list>; <https://www.sdmag.com/articles/97227-hikvision-and-dahua-barred-from-selling-to-us-government-agencies>; <https://www.cnn.com/2019/10/07/us-names-hikvision-chinese-security-bureaus-to-economic-blacklist.html?msockid=081d56a036cb68da37fd43db37aa69aa>.

grant-funded projects due to cybersecurity and national security risks.²⁰

46. The Federal Communications Commission (“FCC”) has also listed, as of March 12, 2021, “Video surveillance and telecommunications equipment produced by Dahua Technology Company, to the extent it is used for the purpose of public safety, security of government facilities, physical security surveillance of critical infrastructure, and other national security purposes, including telecommunications or video surveillance services provided by such entity or using such equipment.”²¹

47. In 2021, Congress passed the Secure Equipment Act (“SEA”), which directed the FCC to no longer approve any equipment on the Covered List for marketing or sale within the United States related to critical infrastructure.²²

48. The FCC therefore banned “the authorization of [Dahua’s] products for marketing and sale in the United States, to the extent that the products are used ‘for the purpose of ... physical security surveillance of critical infrastructure.’”²³ The D.C. Circuit recently affirmed in part and vacated in part for the FCC “to comport its definition [of ‘critical infrastructure’] and justification for it with the statutory text of the NDAA.”²⁴

49. Additionally, Australia removed Dahua cameras from government facilities, citing national security threats and human rights violations, as Dahua has been “directly implicated in the alleged human rights abuses and mass surveillance of Uyghurs in Xinjiang.”²⁵

²⁰ <https://www.congress.gov/115/bills/hr5515/BILLS-115hr5515enr.pdf?download=1>; <https://www.ndia.org/policy/issues/cyber/section-889>.

²¹ <https://www.fcc.gov/supplychain/coveredlist>

²² *Hikvision USA, Inc. v. Fed. Commc’ns Comm’n*, 97 F.4th 938, 940 (D.C. Cir. 2024).

²³ *Hikvision USA, Inc. v. Fed. Commc’ns Comm’n*, 97 F.4th 938, 944 (D.C. Cir. 2024).

²⁴ *Hikvision USA, Inc. v. Fed. Commc’ns Comm’n*, 97 F.4th 938, 950 (D.C. Cir. 2024).

²⁵ <https://www.bbc.com/news/world-australia-64577641>.

50. In addition to its presence on government lists, experts have criticized Dahua for purposefully creating a “backdoor wiretapping vulnerability.”²⁶

51. Dating back to 2019, years before Dahua was even designated as a Chinese Military Company,²⁷ U.S. researchers at The Internet Protocol Video Market (“IPVM”) discovered “that millions of [Dahua] cameras have been carrying the potential to be used as eavesdropping devices—even when the audio on the camera is disabled.”²⁸

52. IPVM is a respected authority on surveillance technology, recognized by Time magazine as a “leading source of information on the harms of facial-recognition technology.”²⁹

53. IPVM has released directory lists of numerous U.S. and Canadian companies that are engaging in original equipment manufacturing (OEM) or white-labeling of Dahua (and other Chinese-manufactured) cameras.³⁰

54. According to IPVM, it only lists OEMs it has “verified by examining shipping records, product documentation, or testing products.”³¹

55. And according to IPVM, Dahua is an OEM for Lorex.³²

²⁶ <https://ipvm.com/reports/security-exploits;>
[https://www.forbes.com/sites/zakdoffman/2019/08/03/update-now-warning-as-eavesdropping-risk-hits-millions-of-chinese-made-cameras/.](https://www.forbes.com/sites/zakdoffman/2019/08/03/update-now-warning-as-eavesdropping-risk-hits-millions-of-chinese-made-cameras/)

²⁷ [https://www.defense.gov/News/Releases/Release/Article/3180636/dod-releases-list-of-peoples-republic-of-china-prc-military-companies-in-accord/.](https://www.defense.gov/News/Releases/Release/Article/3180636/dod-releases-list-of-peoples-republic-of-china-prc-military-companies-in-accord/)

²⁸ [https://www.forbes.com/sites/zakdoffman/2019/08/03/update-now-warning-as-eavesdropping-risk-hits-millions-of-chinese-made-cameras/.](https://www.forbes.com/sites/zakdoffman/2019/08/03/update-now-warning-as-eavesdropping-risk-hits-millions-of-chinese-made-cameras/)

²⁹ [https://time.com/collection/time100-ai/6308784/john-honovich/.](https://time.com/collection/time100-ai/6308784/john-honovich/)

³⁰ [https://ipvm.com/reports/dahua-oem.](https://ipvm.com/reports/dahua-oem)

³¹ [https://ipvm.com/reports/dahua-oem.](https://ipvm.com/reports/dahua-oem)

³² [https://ipvm.com/reports/dahua-oem;](https://ipvm.com/reports/dahua-oem) [https://www.costco.com/lorex-fusion-4k%2b-wired-system-with-4-4k-deterrence-spotlight-cameras.product.4000272248.html.](https://www.costco.com/lorex-fusion-4k%2b-wired-system-with-4-4k-deterrence-spotlight-cameras.product.4000272248.html)

56. Further, according to IPVM, “Dahua cybersecurity history has numerous vulnerabilities, many rated as critical, and it regularly fails to provide complete lists of affected models or firmware versions.”³³

57. Experts describe this “backdoor” vulnerability as “intentional,” stating the backdoor has been “‘placed into the product by the vendor’ by using hard-coded credentials in firmware for cameras.”³⁴

58. Examples exposing Dahua’s pattern of security vulnerabilities include the following:

- a. July 23, 2025 — National Vulnerability Database Number, Common Vulnerabilities and Exposures (“CVE”) Number CVE-2025-31700. “Attackers could exploit a buffer overflow vulnerability by sending specially crafted malicious packets, potentially causing service disruption (e.g., crashes) or remote code execution (RCE). Some devices may have deployed protection mechanisms such as Address Space Layout Randomization (ASLR), which reduces the likelihood of successful RCE exploitation. However, denial-of-service (DoS) attacks remain a concern.”³⁵
- b. January 2023 — Dahua DSS Software³⁶ 12 Vulnerabilities Discovered and Analyzed. IPVM discovered and reported 12 CVEs impacting around 3,100 devices, with potential for chain attacks resulting in system takeover. A number of hidden features, some of which allow Server-Side Request Forgery (SSRF), Remote

³³ <https://ipvm.com/reports/security-exploits>.

³⁴ <https://ipvm.com/reports/security-exploits>.

³⁵ <https://nvd.nist.gov/vuln/detail/CVE-2025-31700>

³⁶ DSS Software refers to Digital Surveillance System, which is “all-in-one Central Management System (CMS) / Video Management System (VMS) that encompasses a wide range of features and functions within video surveillance.” <https://dahuawiki.com/DSS>

Code Execution (RCE), and unchecked ICMP requests, can be used for Distributed Denial of Service (DDoS) attacks.³⁷

- c. January 2022 — Dahua Broken Access Control Vulnerability. A critical-level vulnerability rated 9.8/10.0 by NIST that Dahua originally reported as only 8.1. It allows attackers to reset device passwords. Dahua refused to publish an advisory on its U.S. site or disclose which North American models were affected, and an advisory published on its international site has since been removed.³⁸
- d. September 2021 — Dahua New Critical Vulnerabilities 2021.³⁹ Two new critical-level vulnerabilities rated 9.8/10.0 that allow authentication bypass without valid credentials. Dahua’s response raised several distinct concerns that contradicted industry standards: 1) Dahua assigned lower severity ratings of 8.1 and 7.3 over the objections of the discovering researcher by manipulating CVSS criteria, later updated to 9.8 by NIST; 2) Dahua released a patch in July 2021 described as “*Fix some tiny bugs*” with no mention of the vulnerabilities; 3) Dahua subsequently waited two months before informing users of the vulnerabilities in September 2021.”⁴⁰
- e. May 2020 — Dahua Critical Cloud Vulnerabilities. Dahua and 22 OEMs were discovered to have hard-coded cloud keys/passwords which could be used to gain full access to cloud connected equipment.⁴¹

³⁷ <https://ipvm.com/reports/security-exploits>.

³⁸ <https://ipvm.com/reports/security-exploits>.

³⁹ <https://ipvm.com/reports/dahua-21-critical>.

⁴⁰ <https://ipvm.com/reports/security-exploits>.

⁴¹ <https://ipvm.com/reports/security-exploits>.

- f. March 2017 — Dahua cameras and DVRs/NVRs allowed unauthorized remote admin access to Dahua devices by downloading an unprotected configuration file containing usernames and passwords, an exploit the researcher who discovered it said worked ‘like a damn Hollywood hack, click on one button and you are in.’ It worked by downloading an unprotected configuration file containing usernames and passwords, and its design indicated it was intentional. The vulnerability received DHS ICS-CERT's highest score of 10.0/10.0 and affected over 1 million Dahua devices globally.⁴²

59. These security risks must be understood in the context of prior PRC state-sponsored hacking campaigns using “living off the land” (LOTL) tactics, which allow undetected monitoring of computer and camera activity. Because Dahua is a Chinese military company manufacturing these products, it may be facilitating LOTL techniques to capture information without users knowing.⁴³

II. Lorex Sells Through Large Retailers and Makes Misleading Representations About the Privacy Design of Its Products

60. Defendant Lorex Corporation is a Delaware corporation headquartered in Maryland and is ultimately owned by Skywatch, a Taiwanese company.⁴⁴

⁴² <https://ipvm.com/reports/security-exploits>; see also <https://www.cisa.gov/news-events/ics-advisories/icsa-17-124-02>.

⁴³ <https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a>; <https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-144a>; <https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/3669159/combating-cyber-threat-actors-perpetrating-living-off-the-land-intrusions/>; <https://www.cisa.gov/sites/default/files/2025-03/Joint-Guidance-Identifying-and-Mitigating-LOTL508.pdf>.

⁴⁴ <https://sen.news/dahua-sells-lorex-for-us72-million/>; see also <https://www.dahuasecurity.com/newsEvents/pressRelease/7717>. One of Skywatch’s major investors is Inventec, a publicly traded Taiwanese company, and Skywatch’s CEO is still listed

61. According to the State of Maryland business search, Lorex Corporation's principal office is located at 999 Corporate Blvd., Suite 110, Linthicum, Maryland 21090.⁴⁵

62. Lorex's FAQ also states that its office is located in Linthicum, Maryland;⁴⁶ however, the most recent address provided on product specifications may be a Regus office space in Columbia, Maryland.⁴⁷

63. Lorex has an intermediate parent, Lorex Technology Inc., which is a Canadian company headquartered at 250 Royal Crest Court, Markham, Ontario L3R 3S1, Canada.

64. Lorex has historically had distribution through large retail companies including Costco, Best Buy, Home Depot, Kohl's, and Office Depot.⁴⁸ Lorex also lists products on Amazon.com.

a. Representations on Lorex's Own Webpages

65. Lorex has multiple misleading representations on its own web pages.

66. On Lorex's website, under the security tab, it assures consumers that Lorex is "committed to protecting the integrity,

as a Senior VP at Inventec. https://isourcing-trade.com/en/company_data.php?id=337#:~:text=Skywatch%20IoT%20platform%20has%20been,Taiwan%20Telecom%20IoT%20platform%20market; see also <https://www.linkedin.com/in/wei-chao-chen-b4b0bb1/?originalSubdomain=tw>; page 21, <https://esg.inventec.com/uploads/files/shares/annualreport/2023AnnualReport.pdf>.

⁴⁵ <https://egov.maryland.gov/BusinessExpress/EntitySearch/Business>. According to the BBB, Lorex Corporation's address is 7055 Troy Hill Drive, Suite 400, Elkridge, MD 21075. <https://www.bbb.org/us/md/elkridge/profile/security-cameras/lorex-corporation-0011-90270768>. The BBB page lists the alternate names Lorex By FLIR, FLIR Lorex Inc, and Lorex Technology Inc

⁴⁶ <https://perma.cc/HS6B-2VJC>

⁴⁷ A recent product specification page lists Lorex Corporation's address as 10440 Little Patuxent Parkway, Ste, 300, Columbia, MD 21044, United States. <https://content.syndigo.com/asset/d3521e89-58ea-45f9-9487-b29806458c86/original.pdf>. See <https://maps.app.goo.gl/1sH6QeWhkS6dMJcs9>.

⁴⁸ <https://techcrunch.com/2023/11/01/lawmakers-costco-lorex-dahua-entity-list/>

privacy, and security of our customers' information" and "We take every step to ensure your security."⁴⁹

67. On its Privacy Commitment page, Lorex states: "Your privacy is our top priority. That's why we provide you with the tools to manage your own devices and storage. We are committed to taking every step possible to ensure your recordings remain private."⁵⁰

68. On Lorex's FAQ, under "Are Lorex wireless cameras secure?" the answer begins "Yes."⁵¹

b. Representations on Costco's Webpages for Lorex Products

69. One of Lorex's most significant retail relationships is through Costco.

70. Lorex's website states that "[f]or over a decade, Costco has carried a wide variety of Lorex products, including security cameras and systems."⁵²



⁴⁹ <https://perma.cc/79L4-78D3>

⁵⁰ <https://perma.cc/B3SS-Q6F4>

⁵¹ <https://perma.cc/HS6B-2VJC>

⁵² <https://perma.cc/GEZ4-DCPT>

**i. Costco was questioned specifically in a letter by
Members of Congress in 2023**

71. TechCrunch reported that in October 2023, Representative Christopher Smith and Senator Jeff Merkley, the co-chairs of the Congressional-Executive Commission on China (“CECC”),⁵³ sent a letter to Costco.⁵⁴

72. That letter stated in part: “Lorex products are also a known security risk to U.S. customers because critical vulnerabilities are regularly discovered in Dahua products, including unauthorized viewing of video and audio feeds and archives, as well as unauthorized network access and remote tampering with settings. While Dahua denies it shares any data and claims its products are safe, the PRC’s 2017 National Intelligence Law requires Dahua to support national intelligence work. No data collected can be withheld from PRC authorities should they request it for intelligence purposes—a vulnerability that your U.S. and global customers should be notified of. The recent sale of Lorex to a Taiwanese company Skywatch does not allay our concerns or immediately change the security risks posed to U.S. companies and consumers moving forward, as Dahua still supplies all the component parts for the Lorex cameras and other surveillance equipment.

The material and reputational risks associated with selling Lorex equipment are something your company recognizes. After an IPVM report showed that Lorex video surveillance kits sold in Costco bore “Made in the USA” labels, the kits were later re-labeled as “Made in China.” Nevertheless, they stayed on Costco’s shelves, with no further

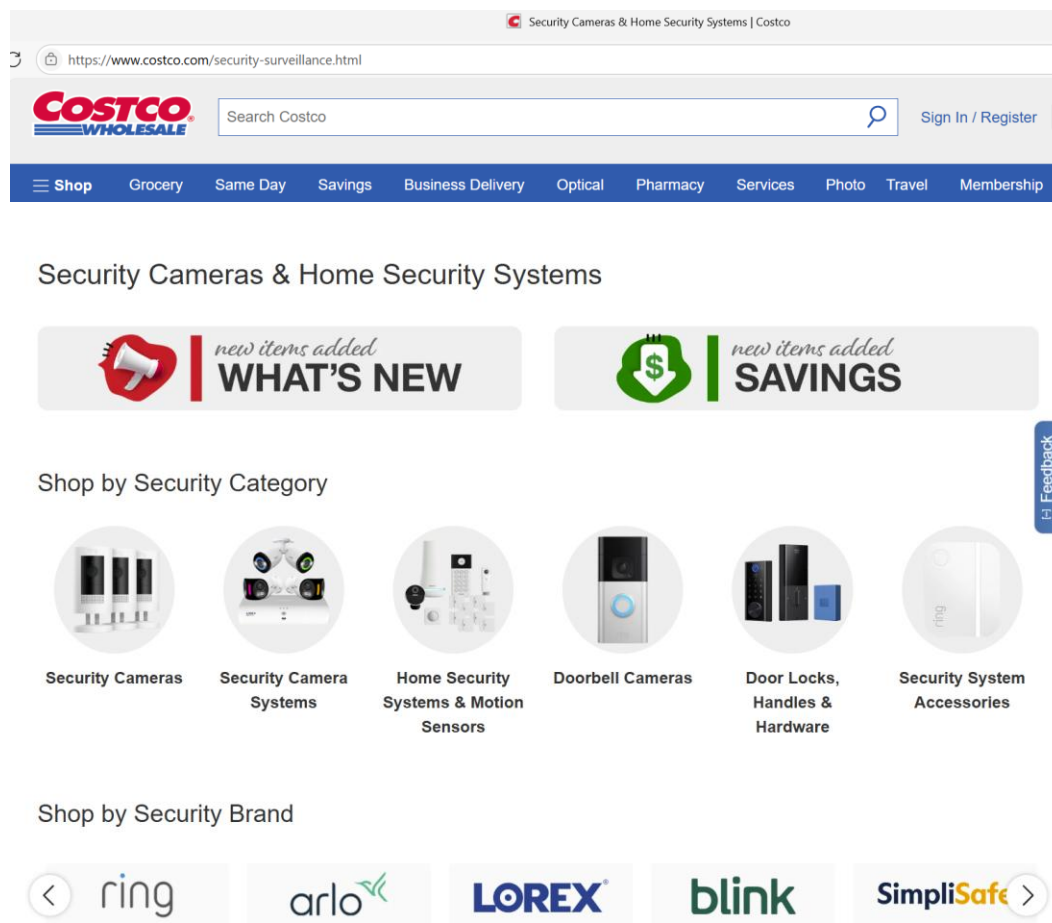
⁵³ See <https://www.cecc.gov/>

⁵⁴ <https://www.cecc.gov/sites/evo-subsites/cecc.house.gov/files/documents/Costco%20Letter%20Signed.pdf>; see also <https://techcrunch.com/2023/11/01/lawmakers-costco-lorex-dahua-entity-list/>

explanation of who was responsible for this mistake or why the Lorex name stayed on Dahua equipment.”⁵⁵

ii. Lorex and Costco’s Website Make Misleading Representations About Privacy

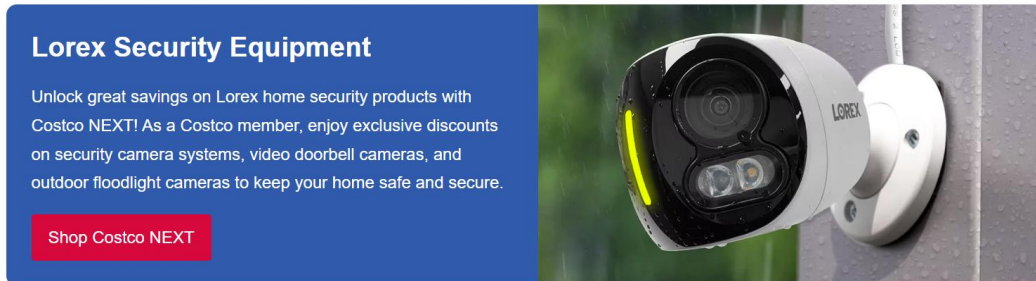
73. Nonetheless, the Costco online website still prominently displays Lorex products—with Lorex listed alongside such other major brands as Ring, Arlo, and Blink.⁵⁶




⁵⁵ <https://www.cecc.gov/sites/evo-subsites/cecc.house.gov/files/documents/Costco%20Letter%20Signed.pdf>, at page 2.

⁵⁶ <https://www.costco.com/security-surveillance.html>





74. Costco highlights the Lorex brand in particular.



75. As of July 30, 2025, Costco's website listed two Lorex products: the \$750 Lorex Fusion NVR with Two 4K 180° Panoramic Lens and Two 4K Bullet Cameras; and the \$150 Lorex 2K Dual Lens Indoor Pan-tilt Wi-Fi Security Camera, 2-pack.⁵⁷

Three images of Lorex security equipment: two bullet cameras, a Fusion NVR system with two bullet cameras, and a 2-pack of indoor pan-tilt cameras.

Costco Members Receive Exclusive Value on Security Equipment from Lorex
Lorex - Costco Next

	Online Only	Online Only
		
	\$749.99	\$149.99
	Lorex Fusion NVR with Two 4K 180° Panoramic Lens and Two 4K Bullet Cameras	Lorex 2K Dual Lens Indoor Pan-tilt Wi-Fi Security Camera, 2-pack
	★★★★★ (58)	☆☆☆☆☆ (0)
	 Delivery Available	 Delivery Available
	<input type="checkbox"/> Compare	<input type="checkbox"/> Compare
Select Options	Add to Cart	Add to Cart

⁵⁷ <https://www.costco.com/security-surveillance.html?keyword=Lorex> [Last visited 7/30/2025]

76. The Lorex 2K Dual Lens Indoor camera design appears very similar to Dahua's "H5D-5F" and "H3D-3F" models.⁵⁸



77. The Costco page for this product states: "Keep your recordings private and in your control" and that the product is "Private by design."⁵⁹

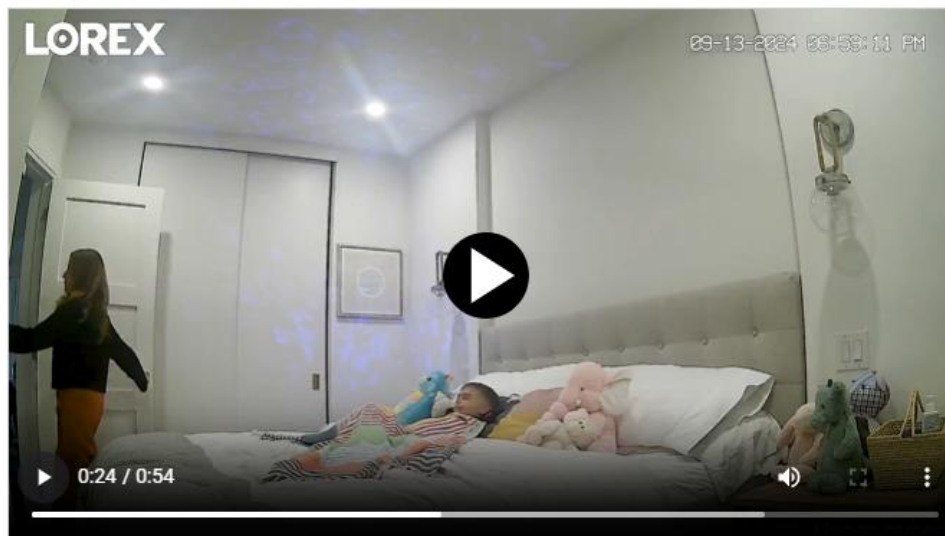


78. Lorex also represents that its cameras may be placed in extremely sensitive locations, including children's bedrooms.⁶⁰

⁵⁸ See <https://perma.cc/6QJ7-VSPC>; <https://perma.cc/EW9Y-K9ZW>

⁵⁹ <https://www.costco.com/security-surveillance.html?keyword=Lorex> [Last visited 7/30/2025]. Under product details, scroll down to the picture of the Lorex Video Vault.

⁶⁰ <https://www.costco.com/lorex-2k-dual-lens-indoor-pan-tilt-wi-fi-security-camera-2-pack.product.4000384381.html>. Click on "View More" under Product Details, and view first video.



79. On some pages, Costco includes a disclaimer: “From The Brand ... Lorex products are designed for consumer and business use only and not for US federal governments, federally-funded projects or contractors subject to NDAA.”⁶¹

80. A product specification contains a similar disclaimer.⁶²

81. This disclaimer shows actual knowledge by Lorex and/or Costco of security issues but provides no explanation as to why the disclaimer is significant.

82. A reasonable consumer would interpret the disclaimer to mean Lorex cameras are safe for household and business use.

iii. Costco’s Sale of Lorex Products May Conflict with Its Representations Regarding Human Trafficking and Anti-Slavery

83. Costco’s website may be misleading for an additional reason, which is that Costco has made express representations about

⁶¹ *E.g.*, <https://www.costco.com/lorex-fusion-nvr-with-two-4k-180-panoramic-lens-and-two-4k-bullet-cameras.product.4000272398.html> (Emphasis added).

⁶² <https://content.syndigo.com/asset/d3521e89-58ea-45f9-9487-b29806458c86/original.pdf>

its disclosure of human trafficking and anti-slavery. This website states that Costco “prohibits human rights abuses in [its] supply chain” including “human trafficking, physical abuse, [and] restricting freedom of movement.”⁶³

84. Given that Costco’s website had an express statement about the NDAA and it received a letter in October 2023 from the Congressional CECC, it is misleading for Costco not to disclose that Dahua is listed on the U.S. Department of Commerce’s Entity List for its role in mass surveillance of Uyghurs in Xinjiang.⁶⁴

c. Other Retailer Websites Also Contain Misleading Representations About Privacy

i. Best Buy

85. Best Buy offers multiple Lorex products on its website, including the Lorex 2K Dual Lens Indoor Pan-Tilt Wi-Fi Security Camera – White and the Lorex 2K Wi-Fi Smart Lightbulb Camera.⁶⁵

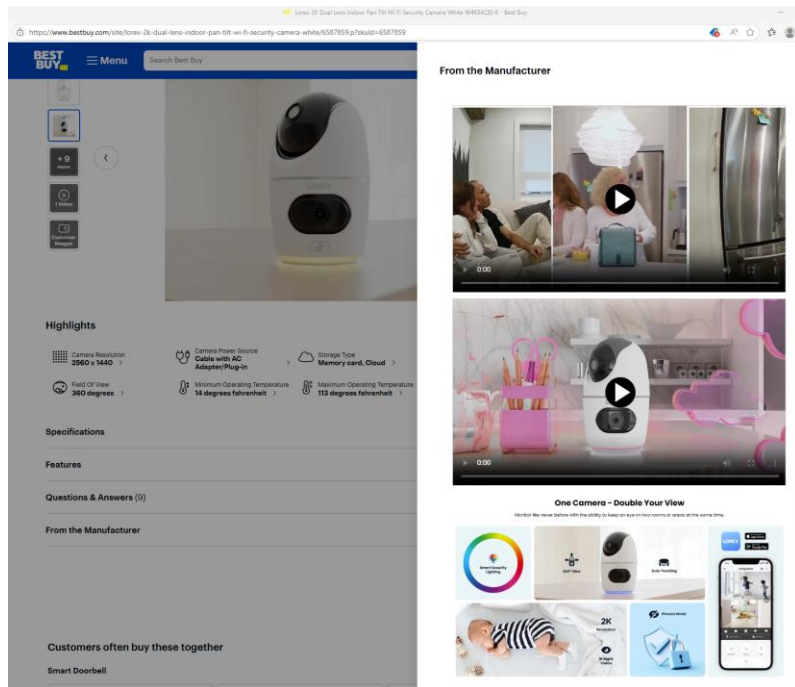
86. Under the “From the Manufacturer” tab, for the Lorex - 2K Dual Lens Indoor Pan-Tilt Wi-Fi Security Camera – White, it shows indoor use of the camera, including a couple watching TV, people in their kitchen, and a baby sleeping:⁶⁶

⁶³ <https://www.costco.com/disclosure-regarding-human-trafficking-and-anti-slavery.html>

⁶⁴ <https://www.federalregister.gov/documents/2019/10/09/2019-22210/addition-of-certain-entities-to-the-entity-list>; <https://www.sdmmag.com/articles/97227-hikvision-and-dahua-barred-from-selling-to-us-government-agencies>; <https://www.cnbc.com/2019/10/07/us-names-hikvision-chinese-security-bureaus-to-economic-blacklist.html?msockid=081d56a036cb68da37fd43db37aa69aa>.

⁶⁵ <https://www.bestbuy.com/site/shop/lorex-security-cameras>

⁶⁶ <https://www.bestbuy.com/site/lorex-2k-dual-lens-indoor-pan-tilt-wi-fi-security-camera-white/6587859.p?skuId=6587859>



Your indoor personal assistance

Home life can be chaotic with curious toddlers and mischievous pets. View your entire room and auto-track subjects utilizing the camera's pan and tilt abilities.

 Pan, Tilt and Digital Zoom

 Auto Tracking



Always know who's there

Stay one step ahead. Be notified when a person or an animal enters the camera's view.

 Person Detection

 Animal Detection

No second guessing

See the finest details day and night with 2K resolution video and IR (infrared) night vision in low-light settings.

2K 2K Resolution

 Black & White (IR) Night Vision



87. The first video under the “From the Manufacturer” tab also includes a short advertisement, that specifically includes having the camera in a child’s bedroom:



88. This is the type of deployment where a reasonable consumer would be most concerned about privacy.

89. The “From the Manufacturer” tab also states “Private by design,” including a bullet that lists “Enhanced Privacy features.”⁶⁷



⁶⁷ Click on From the Manufacturer and scroll down to the bottom.



90. The product specification includes the disclaimer: “Lorex products are designed for consumer and business use only and not for US federal governments, federally-funded projects or contractors subject to NDAA.”⁶⁸

91. The Lorex lightbulb camera page contains similar representations regarding Private by Design.⁶⁹

ii. Home Depot

92. Home Depot lists the Lorex 2K Dual Lens Indoor Pan-Tilt Wi-Fi Security Camera, as well as two PoE+ Switches.⁷⁰

93. Under “Highlights,” Home Depot’s listing states: “Safe and secure – in-camera ai and privacy mode.”⁷¹

⁶⁸ <https://content.syndigo.com/asset/d3521e89-58ea-45f9-9487-b29806458c86/original.pdf>

⁶⁹ <https://www.bestbuy.com/site/lorex-2k-wi-fi-smart-lightbulb-camera-white/6614839.p?skuId=6614839>. Click on “From the Manufacturer” and scroll down.

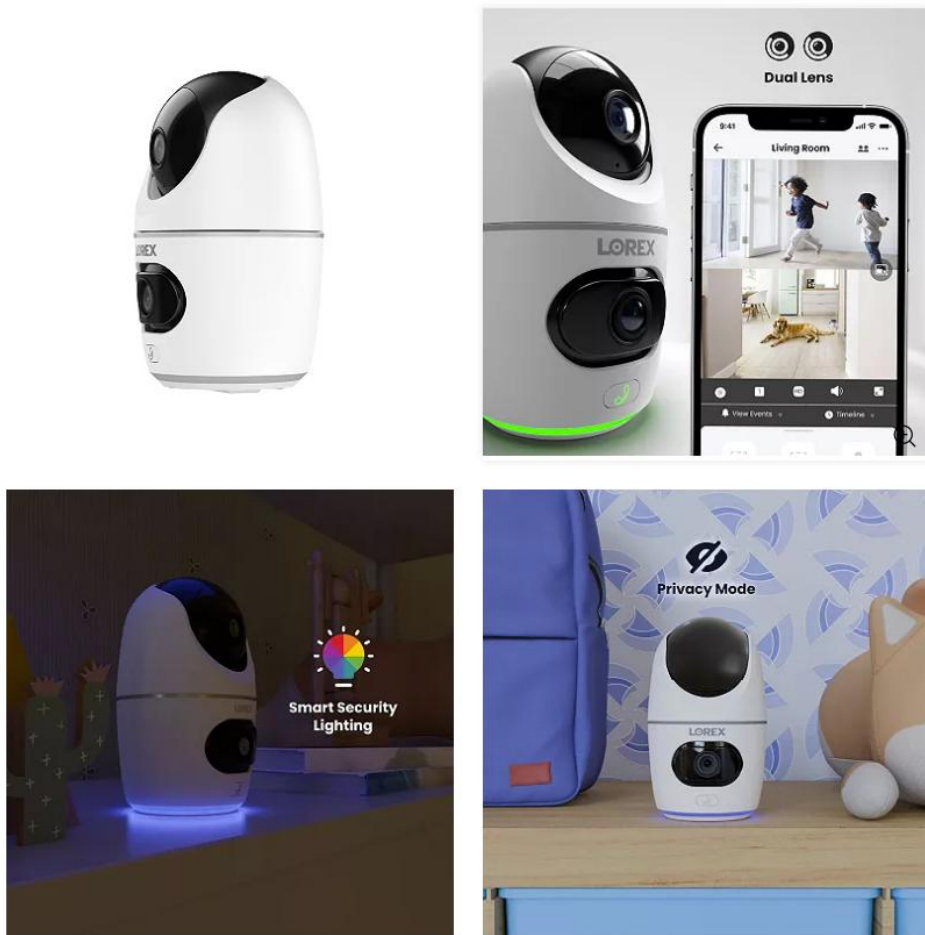
⁷⁰ <https://www.homedepot.com/b/Lorex/N-5vc1vZ2vj>

⁷¹ <https://www.homedepot.com/p/Lorex-2K-Dual-Camera-Pan-Tilt-Indoor-Security-Camera-W463AQD-E/332823101>. It is model # W463AQD-E and Internet # 332823101

iii. Kohl's

94. Kohl's appears to contain a large number of Lorex products for sale.⁷² This includes the Lorex 2K Dual Lens Indoor Pan-Tilt Wi-Fi Security Camera.⁷³

95. The Kohl's listing states: "Safe & secure – In-Camera AI & Privacy Mode."



⁷² <https://www.kohls.com/catalog/lorex.jsp?CN=Brand:Lorex>

⁷³ <https://www.kohls.com/product/prd-7462714/lorex-2k-dual-lens-indoor-pan-tilt-wi-fi-security-camera.jsp>

96. The page shows the camera installed in children’s rooms, including one labeled “Privacy Mode.”

97. Kohl’s also lists the Lorex 2K Indoor Wi-Fi Security Camera, which contains firmware that links to a Dahua-owned website.⁷⁴

98. That product listing states: “Keep your footage private and secure with built-in local storage.”⁷⁵

iv. Office Depot

99. Office Depot’s website lists a wide selection of Lorex cameras.⁷⁶

100. For the Lorex 2K QHD Indoor Wi-Fi Smart Security Camera With Person Detection, White, Office Depot includes the disclaimer: “Lorex products are designed for consumer and business use only and not for US federal governments, federally-funded projects or contractors subject to NDAA.”⁷⁷

101. The page also contains the statements: “Keep your security footage where it belongs. Private, at home, and in your control” and “Private by Design.”⁷⁸

v. Amazon.com

102. Amazon.com lists numerous Lorex products for sale.

103. For example, the Lorex 4MP Pan & Tilt Indoor Smart Security Camera – Wireless 2K Wi-Fi Camera with Person Detection, Privacy Mode, 2-Way Talk, Smart Home Compatibility, 360° Pan/Tilt

⁷⁴ <https://www.kohls.com/product/prd-6378004/lorex-2k-indoor-wi-fi-security-camera.jsp>

⁷⁵ *Id.* Click on “more” under product details.

⁷⁶ <https://www.officedepot.com/b/security-cameras/Brand--Lorex/N-509546>

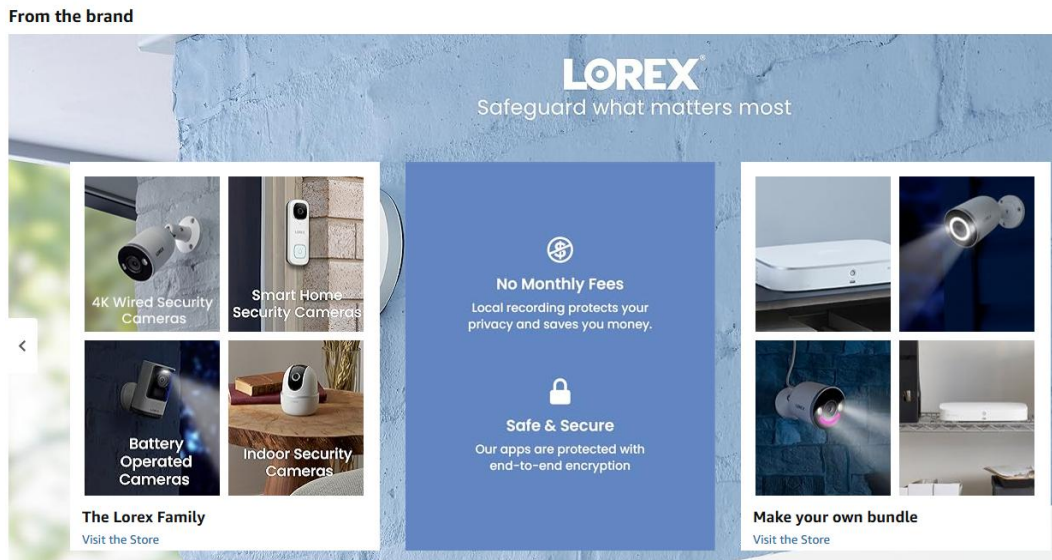
⁷⁷ <https://www.officedepot.com/a/products/7842911/Lorex-2K-QHD-Indoor-Wi-Fi/#MoreInfo>

⁷⁸ *Id.*

View – Free 16GB Micro SD identifies the seller as “Lorex Technology Inc.”⁷⁹

104. Under “About this item,” Amazon’s listing states: “Keep your footage private and secure with built-in local storage with 16 GB MicroSD card included (upgradable to 256GB).”

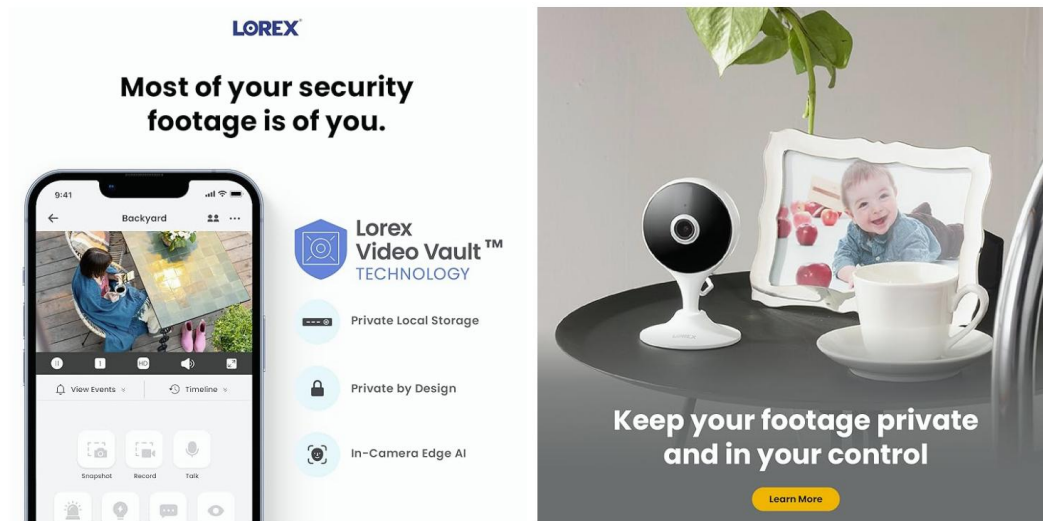
105. Under the “From the brand” heading, Amazon shows a padlock graphic and the statements: “Safe & Secure” and “Our apps are protected with end-to-end encryption.”



106. The Lorex store on Amazon.com contains additional representations about privacy.⁸⁰

⁷⁹ https://www.amazon.com/Lorex-Security-Detection-Two-Way-Control/dp/B0CPT61DMG?ref=ast_sto_dp

⁸⁰ <https://www.amazon.com/stores/Lorex/page/E7453005-0B96-4A82-8188-A18E40241FDB>



107. Amazon also sells the same 2K Indoor Wi-Fi Security Camera that researchers found contained firmware associated with Dahua.

CAUSES OF ACTION

108. Lorex has routinely withheld material information and misled consumers in connection with the marketing, advertisement, and sale of its cameras and other surveillance equipment. The Attorney General brings this action to expose Lorex’s misleading and deceptive behavior, to prevent Lorex from continuing to jeopardize Nebraskans’ privacy and security, and to hold them accountable for their repeated violations of Nebraska’s consumer protection laws.

COUNTS I–V: VIOLATIONS OF THE CONSUMER PROTECTION ACT BY LOREX CORPORATION AND LOREX TECHNOLOGY INC. – DECEPTIVE AND UNFAIR BUSINESS PRACTICES (Neb. Rev. Stat. § 59-1602 et seq.)

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

110. Defendants Lorex Corporation and Lorex Technology Inc. are “persons” within the meaning of the CPA, Neb. Rev. Stat. § 59-1601(1).

111. Defendants conducted “trade and commerce” within the meaning of the CPA, Neb. Rev. Stat. § 59-1601(2), by advertising, marketing, offering for sale, and selling Lorex-branded cameras to Nebraska consumers.

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

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

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

115. 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.

116. Defendants 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 or by implication, that Lorex cameras are “private by design” and “safe and secure” despite known security flaws and vulnerabilities;
- b. Marketing Lorex cameras as suitable for sensitive areas, including children’s bedrooms, without disclosing Dahua’s ongoing involvement and the associated surveillance risks;

- c. Concealing material facts about Defendants' reliance on Dahua, a company sanctioned by the U.S. government for national security and human rights violations;
- d. Using disclaimers that misleadingly suggest risks are limited to federal government use while assuring Nebraska consumers their products are private and secure; and
- e. Selling cameras through major U.S. retailers while failing to disclose material facts about security vulnerabilities and Dahua's control.

117. Defendants' actions constitute deceptive and unfair acts or practices in the conduct of trade or commerce in violation of Neb. Rev. Stat. § 59-1602. Each and every sale, offer for sale, advertisement, misrepresentation, omission, and deceptive statement in connection with the sale of their cameras and other surveillance equipment constitutes a separate and independent violation of the CPA.

**COUNTS VI-X: VIOLATIONS OF THE UNIFORM DECEPTIVE
TRADE PRACTICES ACT BY LOREX CORPORATION AND
LOREX TECHNOLOGY INC. – UNCONSCIONABLE BUSINESS
PRACTICES (Neb. Rev. Stat. § 87-303.01)**

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

119. Defendants Lorex Corporation and Lorex Technology Inc. are "persons" within the meaning of the UDTPA, Neb. Rev. Stat. § 87-301(19).

120. 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).

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

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

- a. Continuing to market and sell Lorex products in Nebraska despite knowledge that Dahua has been sanctioned by the U.S. government for national security and human rights concerns;
- b. Exploiting consumer trust by advertising Lorex cameras for use in children's bedrooms and other sensitive locations while aware of ongoing surveillance vulnerabilities;
- c. Failing to disclose that Lorex cameras are dependent on Dahua hardware and software components subject to backdoors and critical flaws;
- d. Marketing and selling Lorex products while aware of Dahua's placement on the U.S. Entity List for human rights violations, and failing to disclose that fact to consumers; and
- e. Using disclaimers that shift responsibility to consumers while affirmatively creating the false impression that products are safe for household use.

123. Defendants' marketing, advertisement, offer for sale, and sale of cameras and other surveillance equipment despite known security flaws and vulnerabilities constitute unconscionable acts and practices in violation of Neb. Rev. Stat. § 87-303.01. 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 XI-XV: VIOLATIONS OF THE UNIFORM DECEPTIVE
TRADE PRACTICES ACT BY LOREX CORPORATION AND
LOREX TECHNOLOGY INC. – UNFAIR AND DECEPTIVE
BUSINESS PRACTICES (Neb. Rev. Stat. § 87-301 *et seq.*)**

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

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

126. Defendants are “persons” within the meaning of the UDTPA, Neb. Rev. Stat. § 87-301(19).

127. Defendants 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 Lorex cameras have characteristics, benefits, or qualities they do not have, including that they are “private by design” and “secure”;
- b. Misrepresenting that Lorex cameras are of a particular standard, quality, or grade, with respect to the degree of safety and security that consumers can expect;
- c. Causing a likelihood of confusion or of misunderstanding as to the source of the component parts of their cameras and other surveillance equipment;
- d. Causing a likelihood of confusion or of misunderstanding as to Lorex’s affiliation, connection, or association with Dahua; and

- e. Advertising cameras and other surveillance equipment for sale with assurances of privacy, safety, and security despite Lorex's known security flaws and vulnerabilities.

128. 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 their cameras and other surveillance equipment constitutes a separate and independent violation of the UDTPA. Neb. Rev. Stat. §§ 87-302, 87-303.01(1).

PRAYER FOR RELIEF

WHEREFORE, the State of Nebraska requests that this Court:

129. Permanently enjoin and restrain Defendants, their 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).

130. Permanently enjoin and restrain Defendants, their 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).

131. Permanently enjoin and restrain Defendants, their 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.

132. Permanently enjoin and restrain Defendants, their 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.

133. Order Defendants 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.

134. Order Defendants to restore to every person any money acquired by Defendants as a result of their 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.

135. Order Defendants 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).

136. Order such other and further relief as the Court deems just and equitable.

DATED this 23rd day of September, 2025.

STATE OF NEBRASKA, Plaintiff

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

BY: Derek T. Bral
Derek T. Bral, #26767
Tyrone E. Fahie, #28125
Beatrice O. Strnad, #28045

Assistant Attorneys General
1445 K Street, Room 2115

Lincoln, NE 68508

Telephone: (402) 471-2682

Fax: (402) 471-4725

derek.bral@nebraska.gov

tyrone.fahie@nebraska.gov

bebe.strnad@nebraska.gov

Attorneys for the Plaintiff