

**UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF NEW YORK**

SEAN HILL, HOWARD PORTMAN, and
VISHAL SHAH, individually and on behalf of all
others similarly situated,

Plaintiffs,

v.

LOREX CORPORATION, a Delaware
Corporation, and LOREX TECHNOLOGY INC.,
a Canadian Company

Defendants.

Civil Action No.

CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

Plaintiffs Sean Hill, Howard Portman, and Vishal Shah (“Plaintiffs”), bring this Class Action Complaint against Defendants Lorex Corporation and Lorex Technology Inc. (collectively, “Lorex” or “Defendants”), individually and on behalf of all others similarly situated, and complains and alleges upon personal knowledge as to Plaintiffs’ own acts and experiences and, as to all other matters, upon information and belief, including an investigation conducted by Plaintiffs’ attorneys, as follows:

NATURE OF THE ACTION

1. Plaintiffs bought residential security cameras expecting private, secure home monitoring consistent with Defendants’ express representations.
2. Plaintiffs purchased Lorex cameras with the understanding that the products would protect their homes and private living spaces. Plaintiffs were misled. Instead, as alleged herein, Defendants exposed those spaces to undisclosed security and surveillance risks associated with foreign-controlled technology and legal regimes material to consumers’ purchasing decisions.
3. Lorex markets security cameras that rely on hardware, firmware, and backend systems supplied by Zhejiang Dahua Technology Co., Ltd. to U.S. consumers while representing

that the products protect consumer privacy.

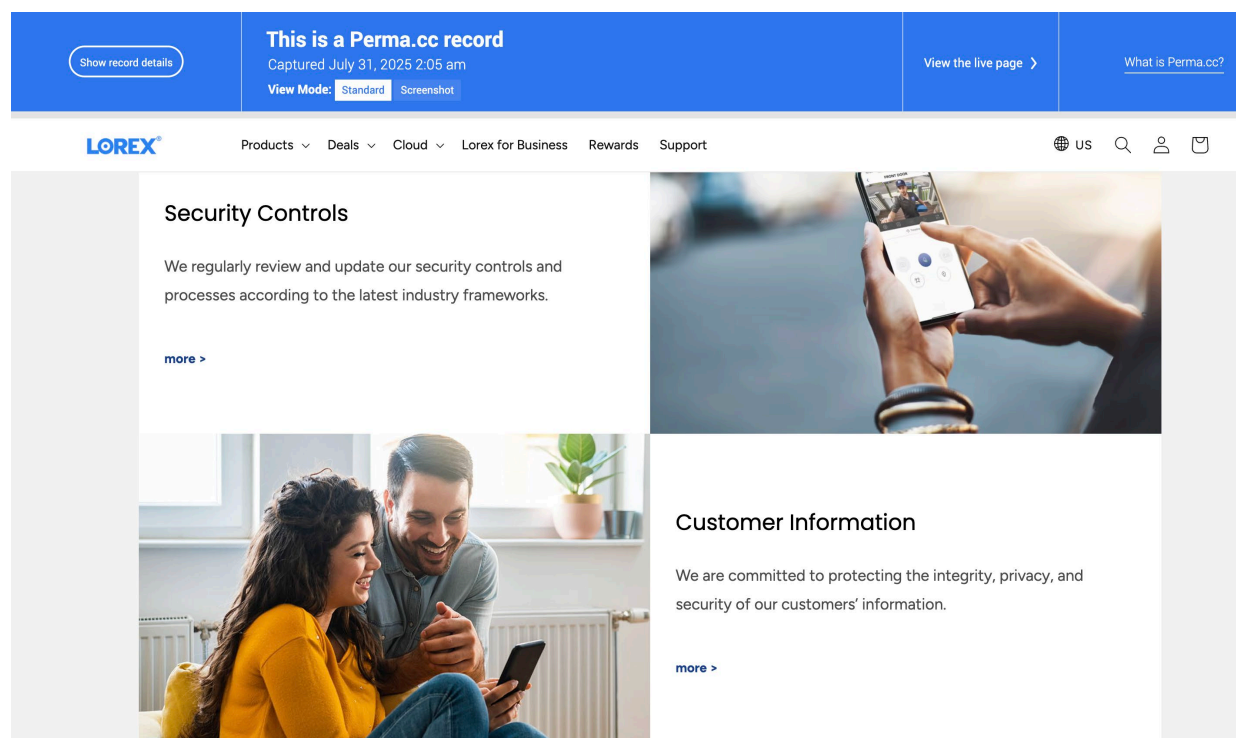
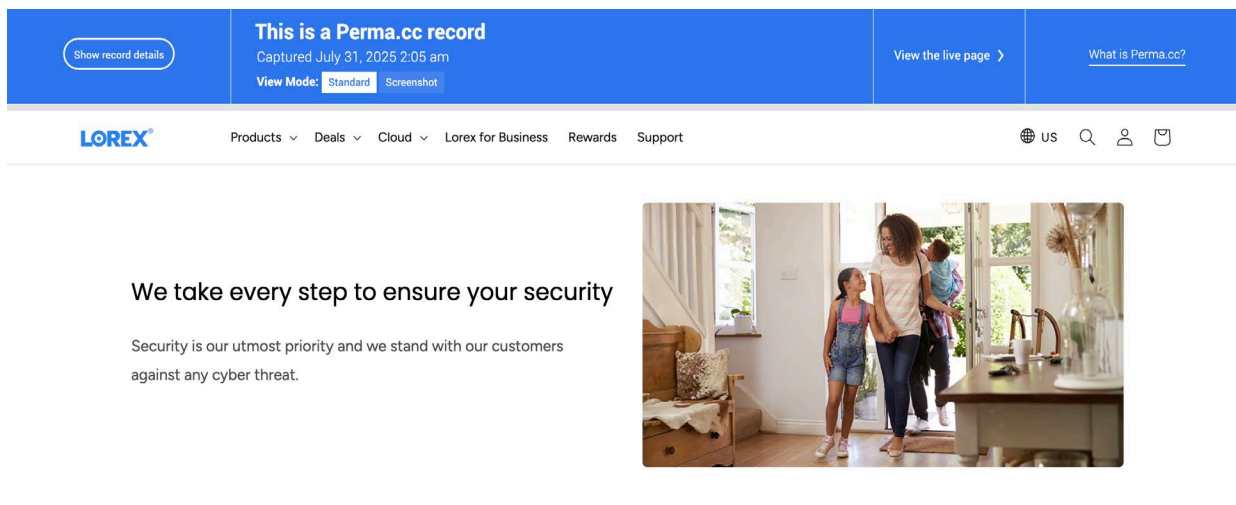
4. Defendants manufacture, distribute, and sell Lorex-branded home security cameras and surveillance systems throughout the United States, including through major retailers such as Costco, Best Buy, Home Depot, Kohl's, Office Depot, Amazon, and the Lorex website.¹ Lorex's product lines include its 2K Dual Lens Indoor Pan-Tilt Wi-Fi Security Camera, 2K Indoor Wi-Fi Camera, Floodlight Camera, and other indoor and outdoor security systems (collectively, the "Camera Products"). Camera Products are equipped with video recording, streaming, motion detection, and two-way audio capabilities.² This action seeks damages and equitable relief on behalf of consumers who purchased Lorex Camera Products in reliance on Defendants' false and misleading representations concerning the products' privacy and security features.

5. 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."³

¹ *Authorized Online Resellers*, LOREX, https://www.lorex.com/pages/authorized-resellers?srsltid=AfmBOorBGIZ8pTDjQNNv_qnF7MBbUGkyySwvbamUHZZOYc88kcoEQ5-m (last visited Jan. 6, 2026).

² *Wireless (Wi-Fi) Security Cameras & Systems*, LOREX, <https://www.lorex.com/collections/wireless-wi-fi-security-cameras-and-systems?srsltid=AfmBOoqc-18vLGjrStEm7CbK-md7r5C2KmISa0qzIS7CV4J0nGWyQUTYc>; *Lorex 1080p Wi-Fi Floodlight Security Camera*, LOREX, <https://www.lorex.com/products/1080p-wi-fi-floodlight-camera?srsltid=AfmBOoo9ICLnTwAlMiF3YWom9sD3ermmLhO9xgbdPwIbJ1OOItNEjDVP&> (last visited Jan. 6, 2026).

³ *See Committed To Your Security*, LOREX (Captured July 30, 2025, 4:35 pm) <https://perma.cc/79L4-78D3> (last visited Jan. 6, 2026).



Figures 1 & 2: Lorex representing that “security is our utmost priority” and that it is “committed to protecting the integrity, privacy, and security of our customers’ information”

6. 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.”⁴

⁴ See *Committed To Your Privacy*, LOREX (Captured July 30, 2025, 4:38 pm) <https://perma.cc/B3SS-Q6F4> (last visited Jan. 6, 2025).

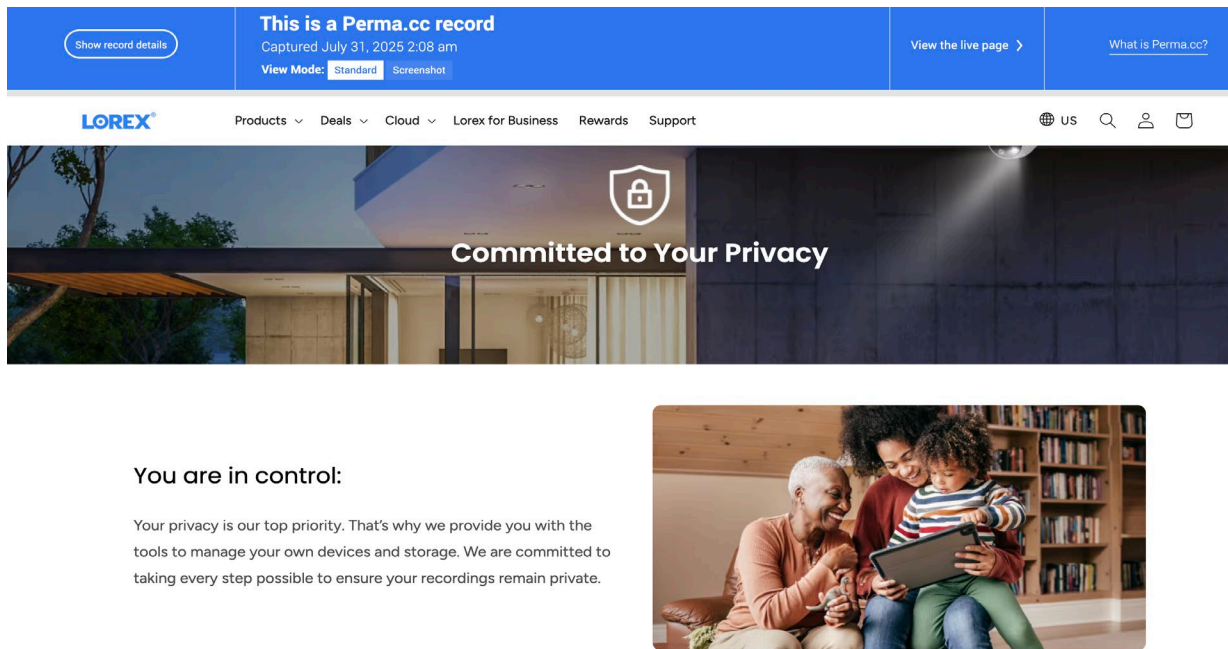


Figure 3: Lorex representing that “Your privacy is our top priority”

7. On Lorex’s Frequently Asked Questions (FAQ), under “Are Lorex wireless cameras secure?” the answer begins “Yes.”⁵

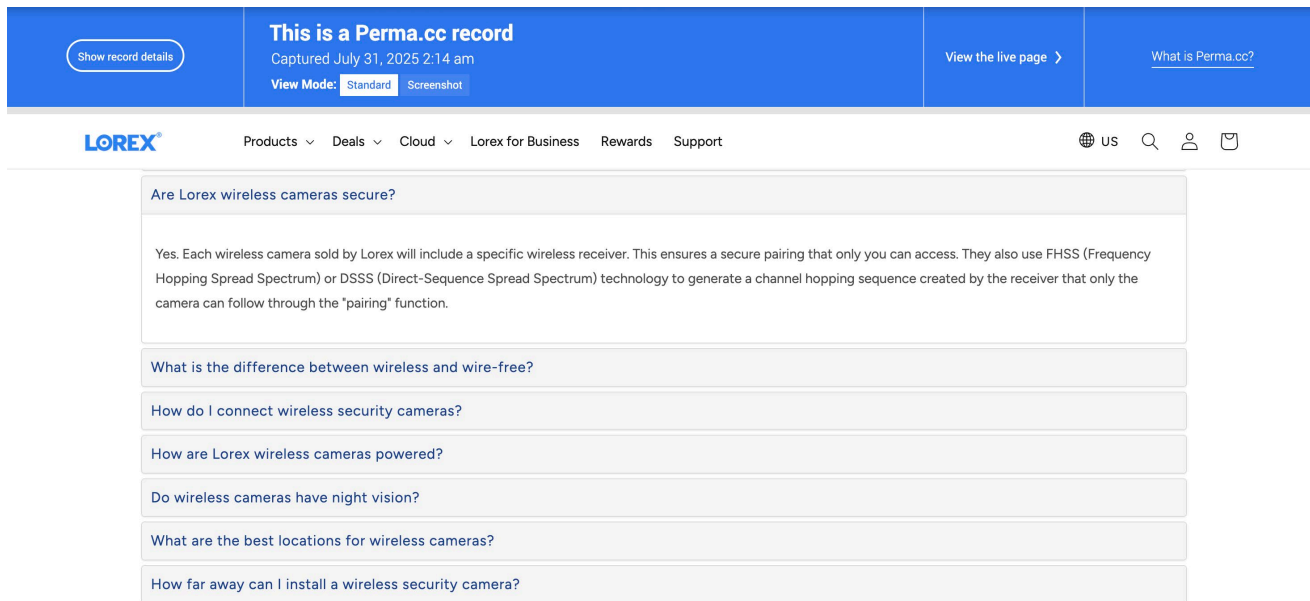


Figure 4: Lorex representing on its FAQ Page that their wireless cameras are secure

⁵See *Frequently Asked Question*, LOREX, (Captured July 30, 2025 4:44 pm) <https://perma.cc/HS6B-2VJC> (last visited Jan. 6, 2026).

8. The product page for the Lorex 2K Dual Lens Indoor camera contains a statements: “Keep your recordings private and in your control,” that the product is “Private by design[,]” and there is “Private Local Storage.”⁶



Smart security means control and ownership

We believe that personal control and ownership of data is the future of home security. Your data, your video, should remain yours—with only you controlling who has access to it.

Lorex Video Vault™ Technology is comprised of three components:



Private Local
Storage



In-Camera
Edge AI



Private by
Design

Together, these embody our commitment to keeping your data private.

Figure 5: Lorex representing that its cameras are “Private by Design.”

9. Lorex’s marketing and retail pages compound this deception by showing cameras in highly sensitive areas such as bedrooms and children’s nurseries. These depictions create the false impression of private and secure household surveillance, even though the cameras expose consumers’ most intimate spaces to potential foreign access.⁷

⁶ Lorex 2K Dual Lens Indoor Pan-Tilt Wi-Fi Security Camera (2-Pack), COSTCO, <https://www.costco.com/lorex-2k-dual-lens-indoor-pan-tilt-wi-fi-security-camera-2-pack.product.4000384381.html> (last visited Nov. 7, 2025). Under Product Details tab, click on View More and scroll down to the picture of the Lorex Video Vault.

⁷ Lorex 2K Dual Lens Indoor Pan-Tilt Wi-Fi Security Camera (2-Pack), COSTCO, <https://www.costco.com/lorex-2k-dual-lens-indoor-pan-tilt-wi-fi-security-camera-2-pack.product.4000384381.html> (last visited Jan. 6, 2026). Click on “View More” under Product Details, and view first video.

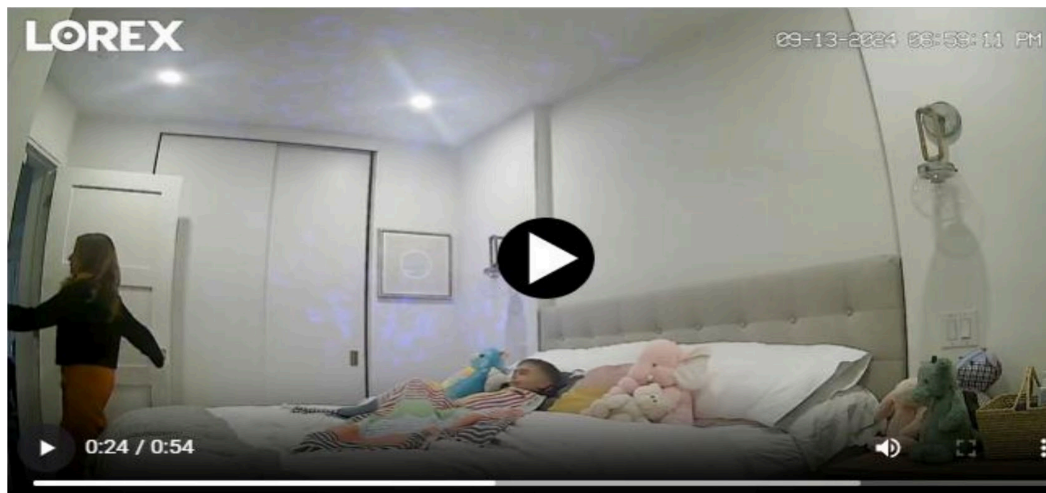


Figure 6: Lorex representing that its cameras are safe to use in a children's bedroom

10. Lorex's statements and representations are misleading because of Lorex's relationship with Zhejiang Dahua Technology Co., Ltd., whose products are restricted for use in the United States by the Federal Communications Commission.⁸ 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."⁹

11. The Lorex 2K Dual Lens Indoor camera offered for sale on Costco, Kohl's, and The Home Depot is nearly identical in appearance to the "H5D-5F" and "H3D-3F" camera models manufactured by Zhejiang Dahua Technology Co., Ltd.

⁸ One Hundred Eighteenth Congress Representative Christopher H. Smith, Chair & Representative Jeff Merkley, CoChair, *Letter to Costco Wholesale Corp.*, CECC (Oct. 31, 2023) <https://www.cecc.gov/sites/evo-subsites/cecc.house.gov/files/documents/Costco%20Letter%20Signed.pdf> (last visited Jan. 6, 2026); see also Zack Whittaker, *Lawmakers say Costco's decision to continue selling banned China surveillance tech is 'puzzling'*, TECHCRUNCH (Nov. 1, 2023 9:25 AM PDT), <https://techcrunch.com/2023/11/01/lawmakers-costco-lorex-dahua-entity-list/> (last visited Jan. 6, 2026).

⁹ *Id.*



Figure 7: Lorex 2K Dual Lens Indoor camera and Dahua “H5D-5F” and “H3D-3F” models

12. The Lorex 2K Indoor Wi-Fi Security Camera, Model W461ASC-E is a camera for sale, as of this filing, on Amazon.com, Kohls.com, and OfficeDepot.com.¹⁰

13. Researchers conducted firmware analysis and identified a pathway that connects to a login prompt hosted at svsh.dah6.com.¹¹ That domain is associated with Dahua, not Lorex.¹²

14. Although a login prompt is not inherently improper, the fact that it routes through Zhejiang Dahua Technology Co., Ltd. further demonstrates Dahua’s involvement in, and control¹³ over, both the hardware and software of these devices.

¹⁰ See, <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, Lorex 2K Indoor Wi-Fi Security Camera, KOHL’S, <https://www.kohls.com/product/prd-6378004/lorex-2k-indoor-wi-fi-security-camera.jsp> ; Lorex 2K QHD Indoor Wi-Fi Camera, OFFICE DEPOT, <https://www.officedepot.com/a/products/7842911/Lorex-2K-QHD-Indoor-Wi-Fi/#Specs> . And a camera with the same name is available at Lorex Indoor Wi-Fi Security Camera, AMAZON, https://www.amazon.com/Lorex-Indoor-WiFiSecurity-Camera/dp/B0CPT8QXCL?ref=ast_sto_dp . (last visited Jan. 6, 2026).

¹¹ See <https://perma.cc/PKP4-QBLY>. Scroll down to “Scanning the QR takes you to a support login that appears internal to Lorex.” (last visited Jan. 14, 2026).

¹² GoDaddy WHOIS Lookup for dah6.com, <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). The name translates to Zhejiang Dahua Technology Co., Ltd. See GOOGLE TRANSLATE, <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>. The dah6.com domain redirects to Dahua’s main site. See INTERNET ARCHIVE: WAYBACK MACHINE, <https://web.archive.org/web/20250711114605/dah6.com> (last visited Jan. 14, 2026).

¹³ As alleged herein, “control” refers to Dahua’s ability to design, update, authenticate, and service the hardware and firmware used in Lorex Camera Products, including through backend systems and credentialed access points. Not all such access is malicious; still, the undisclosed technical control and legal obligations materially contradict Lorex’s privacy and security representations.

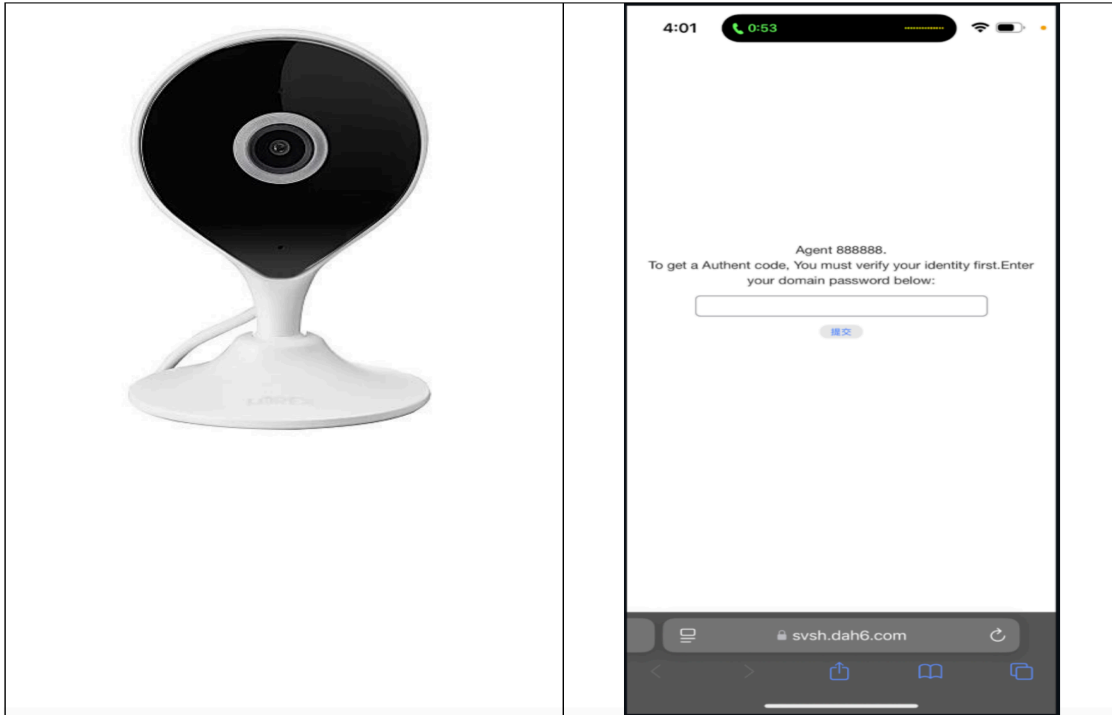


Figure 8: Lorex 2K Indoor Wi-Fi Security Camera currently for sale at Amazon.com, Kohls.com, and OfficeDepot.com. and Support login associated with dah6.com—a domain owned by Dahua—that researchers accessed when analyzing the Lorex camera's firmware.

15. Lorex's omission of Dahua's involvement, and the risks associated with that relationship, constitutes deceptive and unfair conduct.

16. Pursuant to the FY 2021 National Defense Authorization Act ("NDAA"), the Department of Defense ("DOD") has identified Zhejiang Dahua Technology Co., Ltd. as a company posing security concerns.

17. Pursuant to the 2021 Secure Equipment Act ("SEA"), the Federal Communications Commission ("FCC") has restricted the authorization of Dahua's products.¹⁴

18. In fact, Zhejiang Dahua Technology Co., Ltd. previously owned Lorex and decided

¹⁴ *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 (Public Law 116-283)*, U.S. DEPARTMENT OF DEFENSE, <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 (last visited Jan. 6, 2026).

to sell it the day before the Federal Communications Commission announced that it would block further Dahua product approvals in the United States.¹⁵

19. Zhejiang Dahua Technology Co., Ltd. cameras have faced documented security vulnerabilities and associated risks that a reasonable consumer would find significant in evaluating Lorex’s express privacy representations.

20. Such risks include documented backdoor access, additional security vulnerabilities, and documented human rights violations.

21. In a letter to Costco, the CECC wrote that: “Lorex products are ... 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.”¹⁶

22. The CECC further noted: “No data collected can be withheld from [People’s Republic of China (“PRC”)] authorities should they request it for intelligence purposes—a vulnerability that your U.S. and global customers should be notified of.”¹⁷

23. Despite this, Lorex includes only a misleading disclaimer on certain webpages that suggests the cameras are appropriate for home and business use.

24. 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

¹⁵ *Order*, FCC 22-84, at 1 (Nov. 11, 2022) (released Nov. 25, 2022), <https://docs.fcc.gov/public/attachments/FCC-22-84A1.pdf> (last visited Jan. 6, 2026).

¹⁶ *One Hundred Eighteenth Congress Representative Christopher H. Smith, Chair & Representative Jeff Merkley, CoChair, Letter to Costco Wholesale Corp.*, CECC (last visited Jan. 6, 2026); see also Zack Whittaker, *Lawmakers say Costco’s decision to continue selling banned China surveillance tech is ‘puzzling’*, TECHCRUNCH (last visited Jan. 6, 2026).

¹⁷ *One Hundred Eighteenth Congress Representative Christopher H. Smith, Chair & Representative Jeff Merkley, CoChair, Letter to Costco Wholesale Corp.*, CECC (last visited Jan. 6, 2026).

and not for US federal governments, federally-funded projects, or contractors subject to NDAA.”¹⁸

25. Lorex also places this same disclaimer on its FAQ page under a header that does not clearly describe its substance, “What is Lorex’s response to the NDAA?”¹⁹

26. A reasonable consumer would understand these disclaimers to mean that any concern is limited to federal government use; as a result, the disclaimers are misleading.

27. Lorex’s conduct constitutes unfair and deceptive acts and practices under consumer protection statutes, including UDTPA. Lorex marketed its products as “private by design,” yet failed to disclose Dahua’s ongoing involvement and the resulting surveillance and exploitation risks, and provided deceptive assurances of security.

28. Information concerning the identity of the entities supplying camera hardware, firmware, and backend infrastructure, as well as associated security risks and government restrictions, is material to reasonable consumers purchasing surveillance products for use inside private living spaces.

29. Had Plaintiffs and Class Members known that Lorex cameras relied on Zhejiang Dahua Technology Co., Ltd.’s hardware, firmware, and backend systems, or that the products posed heightened security and privacy risks, they would not have purchased the cameras or would have paid substantially less for them.

30. Plaintiffs and Class Members paid a price premium for Lorex Camera Products based on representations that the products were private, secure, and suitable for use in sensitive home environments. That premium would not have been paid had Defendants disclosed Dahua’s involvement, associated risks, or the limitations of the products’ privacy protections.

¹⁸ E.g., *Lorex Fusion NVR With Two 4K 180° Panoramic Lenses and Two 4K Bullet Cameras*, COSTCO, <https://www.costco.com/lorex-fusion-nvr-with-two-4k-180-panoramic-lens-and-two-4kbullet-cameras.product.4000272398.html> (last visited Jan. 6, 2026).

¹⁹ See, LOREX, <https://perma.cc/HS6B-2VJC> (last visited Jan. 6, 2026).

31. Plaintiffs bring this action on behalf of a class consisting of all individuals in the United States who purchased Lorex Camera Products for personal or household use, and not for resale, during the applicable statute of limitations period.

PARTIES

32. Plaintiff Sean Hill is a citizen of the State of New York. In or around August 2015, Plaintiff Hill purchased three Lorex home security cameras at a P.C. Richard & Son retail location. Plaintiff Hill installed the cameras on the exterior of his residence and used the FLIR Cloud application to manage the system. Plaintiff Hill has retained possession of the devices and preserved their hardware, firmware, software configurations, and current settings in substantially the same condition. Plaintiff Hill alleges that, if he had been aware of Dahua-related hardware vulnerabilities and/or subsequent government sanctions that affect the system's security and longevity, he would not have purchased the cameras or would have paid a substantially lower price.

33. Plaintiff Howard Portman is a citizen of Tarzana, California. In or around 2023, Plaintiff Portman purchased a digital video recorder and four Lorex home security cameras directly from Lorex's website for a total purchase price of approximately \$1,000. Plaintiff Portman installed the cameras on the exterior of his residence and used the Lorex Classic App to manage the system. In making his purchase, Plaintiff Portman relied on Lorex's representations that the products were "private by design" and "safe and secure," including marketing emails emphasizing privacy. Plaintiff Portman alleges that, if he had been aware of Dahua-related hardware vulnerabilities and/or subsequent government sanctions that affect the system's security and longevity, he would not have purchased the cameras or would have paid a substantially lower price.

34. Plaintiff Vishal Shah is a citizen of Schaumburg, Illinois. In or around May 2023, Plaintiff Shah purchased six Lorex home security cameras from Costco for approximately \$600. Plaintiff Shah installed the cameras around the exterior of his residence and used the Lorex Classic App to manage the system. In making his purchase, Plaintiff Shah relied on Lorex's representations that the cameras were "private" and "secure," as stated on the original product packaging and promotional materials. Plaintiff Shah encountered limitations that prevented multiple users from accessing the live feed, contrary to reasonable consumer expectations for a home monitoring product. Plaintiff Shah alleges that, if he had been aware of Dahua-related hardware vulnerabilities and/or subsequent government sanctions that affect the system's security and longevity, he would not have purchased the cameras or would have paid a substantially lower price.

35. Defendant Lorex Technology Inc. is a Canadian corporation with its principal place of business 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., a Chinese technology company sanctioned by the United States government. Lorex markets its Camera Products through major online retailers such as Amazon, Best Buy, Costco, and Home Depot, as well as through its own website, www.lorex.com. Lorex's Camera Products are marketed and sold to consumers in multiple U.S. states, including California, New York, and Illinois.

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 Corporation acts as the U.S. subsidiary and domestic distributor of Lorex Technology Inc. and is responsible for the marketing,

sale, and customer support of Lorex-branded products in the United States. Lorex Corporation manages Lorex’s U.S.-facing website, advertising, and consumer data collection systems.

37. Defendants Lorex Technology Inc., and Lorex Corporation, acted jointly to manufacture, label, market, and distribute the Camera Products described herein, including those falsely represented as “Private by Design” and “Safe and Secure.”²⁰ Together, Defendants collected, transmitted, and shared consumer data obtained through these products’ use. Each Defendant acted with the knowledge, approval, and/or under the direction of the others, within the course and scope of their agency relationships, and they are therefore jointly and severally liable for the acts and omissions alleged herein.

38. Defendant Lorex Corporation is a Delaware corporation headquartered in Maryland and is ultimately owned by Skywatch, a Taiwanese company.²¹

39. According to the State of Maryland business search, Lorex Corporation’s principal office is located at 999 Corporate Blvd., Suite 110, Linthicum, Maryland 21090.²²

40. Lorex’s FAQ also states that its office is located in Linthicum, Maryland,²³ however, the most recent address provided on product specifications may be a Regus office space

²⁰ Lorex Corporation, *Lorex Video Vault™ – Keep Your Security Footage Private*, Lorex Video Vault (Retail) (undated), <https://www.lorex.com/pages/lorexvideovault-retail?srsId=AfmBOoqMFJvZ8o-2CmKZw-sFIZQXkDRfpbyzV6-FQ1fQKSmdOs0t2R5d-convert> (last visited Jan. 6, 2026).

²¹ *Dahua to Sell Lorex for Around US\$72 Million to Taiwan-Based Cloud Services Firm*, DAHUA TECHNOLOGY (Nov. 24, 2022), <https://www.dahuasecurity.com/newsEvents/pressRelease/7717>; see also *Dahua Sells Lorex for US\$72 Million*, SEN (Nov. 28, 2022), <https://sen.news/dahua-sells-lorex-for-us72-million>; See also Inventec Corp., 2023 Annual Report 21 (2024), <https://esg.inventec.com/uploads/files/shares/annualreport/2023AnnualReport.pdf> (showing shareholding and corporate-governance disclosures). See also *Skywatch AIoT Platform Company Profile*, ISOURCING-TRADE, https://isourcing-trade.com/en/company_data.php?id=337 (identifying Inventec as a major investor in Skywatch). See also LinkedIn Profile of Wei-Chao Chen (Skywatch CEO & Senior VP at Inventec), <https://www.linkedin.com/in/wei-chao-chen-b4b0bb1/?originalSubdomain=tw> (last visited Jan. 6, 2026).

²² Maryland Business Express, Maryland Div. of Corporations, Business Entity Search, <https://egov.maryland.gov/BusinessExpress/EntitySearch/Business>; see also *Lorex Corporation*, BBB Business Profile, <https://www.bbb.org/us/md/elkridge/profile/security-cameras/lorex-corporation-0011-90270768> (last visited Nov. 7, 2025) (listing address as “7055 Troy Hill Dr., Suite 400, Elkridge, MD 21075” and alternate corporate names “Lorex By FLIR,” “FLIR Lorex Inc.,” and “Lorex Technology Inc.”).

²³ *Lorex Security Camera FAQ*, LOREX TECHNOLOGY INC., <https://perma.cc/HS6B-2VJC> (last visited Jan. 6, 2026).

in Columbia, Maryland.²⁴

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

JURISDICTION AND VENUE

42. This Court has subject matter jurisdiction over this class action under 28 U.S.C. § 1331 because this complaint asserts a claim arising under the laws of the United States. In addition, this Court has subject matter jurisdiction over this matter pursuant to 28 U.S.C. § 1332 of the Class Action Fairness Act of 2005 because: (i) there are 100 or more putative Class Members, (ii) the aggregate amount in controversy exceeds \$5,000,000.00, exclusive of interest and costs, and (iii) there is minimal diversity because Plaintiffs and Lorex are citizens of different states. This Court has supplemental jurisdiction over Plaintiffs' state law claims pursuant to 28 U.S.C. § 1367.

43. This Court has personal jurisdiction over Lorex because it has substantial aggregate contacts with this District, including engaging in conduct in this District that has a direct, substantial, reasonably foreseeable, and intended effect of causing injury to persons throughout the United States, including by marketing and selling Camera Products to consumers in this Judicial District, by placing Camera Products into the stream of commerce directed at this Judicial District, and because Lorex purposely availed itself of the laws of the United States and the State of New York. Furthermore, pursuant to the Terms of Service for Camera Products²⁵ (including the

²⁴ A recent product-specification page lists Lorex Corporation's address as 10440 Little Patuxent Parkway, Ste. 300, Columbia, MD 21044, United States. *See* Lorex Product Specification Sheet, <https://content.syndigo.com/asset/d3521e89-58ea-45f9-9487-b29806458c86/original.pdf> (last visited Jan. 6, 2026); *see also* Google Maps Listing for 10440 Little Patuxent Parkway, Columbia, MD, <https://maps.app.goo.gl/1sH6QeWhkS6dMJcs9> (last visited Jan. 6, 2026).

²⁵23, https://www.lorex.com/policies/terms-of-service?srsId=AfmBOopUQLMcXhrrJC31gA10NNEiK_0Vn6e-cwuMAaencTjdg9jftse23
https://www.lorex.com/policies/terms-of-service?srsId=AfmBOopUQLMcXhrrJC31gA10NNEiK_0Vn6e-

cameras purchased and used by Plaintiffs) (the “Terms”), Defendants submitted to the jurisdiction of any federal or state court, including ones located in New York, NY, which is within this Judicial District. Section 17 of the Terms read:

For purchasers based in the U.S., all matters relating to the Terms and any dispute or claim arising therefrom or related thereto (in each case, including non-contractual disputes or claims), shall be governed by and construed in accordance with the internal laws of the State of New York, without giving effect to any choice or conflict of law provision or rule (whether of the State of New York or any other jurisdiction). Any legal suit, action or proceeding arising out of, or related to, the Terms shall be instituted exclusively in the federal courts of the United States or the courts of the State of New York, in each case located in the City and County of New York, although Lorex retains the right to bring any suit, action or proceeding against you for breach of the Terms in your country of residence or any other relevant country. You waive any and all objections to the exercise of jurisdiction over you by such courts and to venue in such courts.

44. In accordance with 28 U.S.C. § 1391, venue is proper in this District because the parties consented to jurisdiction of this Court, Lorex transacts business in this District, and Lorex has intentionally availed itself of the laws and markets within this District. Furthermore, venue is proper in this Judicial District pursuant to 28 U.S.C. § 1391(b) because the Terms provides that any claim, dispute, action, cause of action, issue, or request for relief relating to the EULA will be governed by the laws of New York, without giving effect to any conflicts of laws principles that require the application of the laws of a different jurisdiction.

FACTUAL ALLEGATIONS

I. Dahua Is a Company Subject to Federal Restrictions and Documented Security Issues

45. Zhejiang Dahua Technology Co., Ltd. is a Chinese corporation headquartered in Hangzhou, Zhejiang Province, PRC. Dahua designs, develops, and licenses the underlying

[cwuMAaencTjdg9jfTse](https://www.lorex.com/policies/terms-of-service?srsId=AfmBOopUQLMcXhrrJC31gA10NNEiK_0Vn6e-cwuMAaencTjdg9jfTse) Terms and Condition of Sale, LOREX, (Sept. 28, 2023) https://www.lorex.com/policies/terms-of-service?srsId=AfmBOopUQLMcXhrrJC31gA10NNEiK_0Vn6e-cwuMAaencTjdg9jfTse

hardware, firmware, and cloud-based infrastructure used in Lorex Camera Products. Dahua provides the technological framework through which Lorex’s devices operate, including storage servers, software integrations, and data management systems that transmit, process, and store user information.

46. Pursuant to the NDAA, the DOD designated Dahua as a “Chinese military company,”²⁶ which signifies that DOD has determined Dahua to be, or to be owned or controlled by, a military-civil fusion contributor to the Chinese military.²⁷

47. The U.S. Department of Commerce has placed Dahua on its Entity List due to Dahua’s role in mass surveillance of Uyghurs in Xinjiang, thereby restricting the export of U.S. technology to Dahua.²⁸

48. 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 grant-funded projects due to cybersecurity and national security risks.²⁹

49. The FCC also includes Dahua on its list of equipment and services covered by

²⁶ 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.) (last visited Jan. 6, 2026).

²⁷ <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> (last visited Jan. 6, 2026).

²⁸ Addition of Certain Entities to the Entity List, 84 Fed. Reg. 54,005 (Oct. 9, 2019), <https://www.federalregister.gov/documents/2019/10/09/2019-22210/addition-of-certain-entities-to-the-entity-list>; see also Hikvision and Dahua Barred from Selling to U.S. Government Agencies, SDM MAG., <https://www.sdmmag.com/articles/97227-hikvision-and-dahua-barred-from-selling-to-us-government-agencies>; see also Sam Meredith, U.S. Names Hikvision, Chinese Security Bureaus to Economic Blacklist, CNBC (Oct. 7, 2019), <https://www.cnbc.com/2019/10/07/us-names-hikvision-chinese-security-bureaus-to-economic-blacklist.html> (last visited Jan. 6, 2026).

²⁹ John S. McCain National Defense Authorization Act for Fiscal Year 2019, Pub. L. No. 115-232, <https://www.congress.gov/115/bills/hr5515/BILLS-115hr5515enr.pdf?download=1>; (last visited Jan. 6, 2026).

Section 2 of the Secure Networks Act as posing an unacceptable risk to the national security of the United States or the security and safety of United States persons. The FCC list provides, in part: “[v]ideo 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.”³⁰

50. In 2021, Congress passed the 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.³¹

51. The FCC 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.’”³² 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.”³³

52. 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.”³⁴

53. In addition to its presence on government lists, experts have criticized Dahua for

³⁰ *Covered List*, FCC, <https://www.fcc.gov/supplychain/coveredlist> (last visited Jan. 6, 2026).

³¹ *Hikvision USA, Inc. v. Fed. Comm’n Comm’n*, 97 F.4th 938, 940 (D.C. Cir. 2024).

³² *Id.*

³³ *Id.*

³⁴ *Australia to remove Chinese surveillance cameras amid security fears*, BBC (Feb. 9, 2023), <https://www.bbc.com/news/world-australia-64577641> (last visited Jan. 6, 2026).

purposefully creating a “backdoor ‘wiretapping vulnerability.’”³⁵

54. Dating back to 2019, years before Dahua was designated as a Chinese Military Company,³⁶ 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.”³⁷

55. 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.”³⁸

56. IPVM has released directory lists of numerous U.S. and Canadian companies that are engaging in original equipment manufacturing (OEM) or white-labeling³⁹ of Dahua (and other Chinese-manufactured) cameras.⁴⁰

57. According to IPVM, it only lists OEMs it has “verified by examining shipping records, product documentation, or testing products,”⁴¹ and IPVM has listed Dahua as an OEM for Lorex.⁴²

58. Further, IPVM has concluded that “Dahua cybersecurity history has numerous vulnerabilities, many rated as critical, and it regularly fails to provide complete lists of affected

³⁵ Zak Doffman, *Update NOW — Warning as Eavesdropping Risk Hits Millions of Chinese-Made Cameras*, FORBES (Aug. 3, 2019), <https://www.forbes.com/sites/zakdoffman/2019/08/03/update-now-warning-as-eavesdropping-risk-hits-millions-of-chinese-made-cameras/> (last visited Jan. 6, 2026).

³⁶ DOD Releases List of People’s Republic of China (PRC) Military Companies in Accordance With Section 1260H of the National Defense Authorization Act for Fiscal Year 2021, U.S. Dep’t of Def., Oct. 5, 2022, <https://www.war.gov/News/Releases/Release/Article/3180636/dod-releases-list-of-peoples-republic-of-china-prc-military-companies-in-accord/> (last visited Jan. 6, 2026).

³⁷ Zak Doffman, *Warning As Millions Of Chinese-Made Cameras Can Be Hacked to Spy on Users*, FORBES (Aug. 3, 2019), <https://www.forbes.com/sites/zakdoffman/2019/08/03/update-now-warning-as-eavesdropping-risk-hits-millions-of-chinese-made-cameras/> (last visited Jan. 6, 2026).

³⁸ Astha Rajvanshi, *John Honovich*, TIME100 AI (Sept. 7, 2023), <https://time.com/collection/time100-ai/6308784/john-honovich/> (last visited Jan. 6, 2026).

³⁹ White-labeling occurs when a company purchases a product from a manufacturer like Dahua and applies its own branding to it for retail sale.

⁴⁰ Dahua OEM Directory, IPVM, <https://ipvm.com/reports/dahua-oem> (last visited Jan. 6, 2026).

⁴¹ *Id.*

⁴² *Id.*

models or firmware versions.”⁴³

59. 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.”⁴⁴

60. 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.”⁴⁵
- b. January 2023 — Dahua DSS Software⁴⁶ 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 Code Execution (RCE), and unchecked ICMP

⁴³ *Security Exploits*, IPVM, <https://ipvm.com/reports/security-exploits> (last visited Jan. 6, 2026).

⁴⁴ *Id.*

⁴⁵ CVE-2025-31700, National Vulnerability Database, NIST, <https://nvd.nist.gov/vuln/detail/CVE-2025-31700> (last visited Jan. 6, 2026).

⁴⁶ 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” DahuaWiki, <https://dahuawiki.com/DSS> (last visited Jan. 6, 2026).

requests, can be used for Distributed Denial of Service (DDoS) attacks.⁴⁷

- 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.⁴⁸
- d. September 2021 — Dahua New Critical Vulnerabilities 2021.⁴⁹ 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.”⁵⁰
- 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.⁵¹
- f. March 2017 — Dahua cameras and DVRs/NVRs allowed unauthorized

⁴⁷ *Security Exploits*, IPVM, <https://ipvm.com/reports/security-exploits> (last visited Jan. 6, 2026).

⁴⁸ *Id.*

⁴⁹ *Dahua 21 Critical Vulnerabilities Report*, IPVM, <https://ipvm.com/reports/dahua-21-critical> (last visited Jan. 6, 2026).

⁵⁰ *Security Exploits*, IPVM, (last visited Jan. 6, 2026).

⁵¹ *Id.*

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.⁵²

61. These security risks must be evaluated in light of documented PRC state-sponsored hacking campaigns involving “living off the land” (“LOTL”) techniques, which allow hackers to covertly monitor users’ computer, network, and camera activity. As a Chinese military company that manufactures these products, Dahua may be positioned to facilitate LOTL-based data capture without user awareness.⁵³

62. These designations, restrictions, and documented vulnerabilities are material to consumers purchasing network-connected surveillance products for use inside private living spaces. Reasonable consumers would expect disclosure of any ongoing technical control, legal obligations, or security risks associated with entities subject to foreign intelligence and national security regimes. Lorex did not disclose these facts.

⁵² *Id.*; see also Dahua Technology Co., Ltd Digital Video Recorders and IP Cameras, CISA, <https://www.cisa.gov/news-events/ics-advisories/icsa-17-124-02> (last visited Jan. 6, 2026).

⁵³ CISA, *PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure*, Cybersecurity Advisory AA24-038A (Feb. 7, 2024), <https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-038a>; see also CISA, *People’s Republic of China State-Sponsored Cyber Actor Living Off the Land to Evade Detection*, Cybersecurity Advisory AA23-144A (May __, 2023), <https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-144a>; see also NSA, *Combating Cyber Threat Actors Perpetrating Living Off the Land Intrusions*, Press Release (Feb. 7, 2024), <https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/3669159/combating-cyber-threat-actors-perpetrating-living-off-the-landintrusions/>; see also CISA et al., *Joint Guidance: Identifying and Mitigating Living Off the Land Techniques* (Feb. 7, 2024), <https://www.cisa.gov/sites/default/files/2025-03/Joint-Guidance-Identifying-andMitigating-LOTL508.pdf> (last visited Jan. 6, 2026).

A. Foreign Adversary Legal Obligations and Network-Connected Surveillance Products

The following statutory and regulatory framework is alleged to provide context for Plaintiffs' claims concerning material omissions, technical control, and the reasonableness of consumer reliance on Defendants' privacy representations.

i. PRC Legal Obligations Requiring Cooperation With State Authorities

63. Under multiple statutes enacted by the PRC, organizations and individuals are subject to affirmative legal obligations to support, assist, and cooperate with national intelligence, public security, and state security authorities. Those statutes require organizations and individuals to maintain secrecy regarding that cooperation.

64. These obligations are not limited to state-owned enterprises or government agencies. They apply to any organization or citizen subject to PRC jurisdiction, including private companies engaged in technology development, software services, data processing, and network operations.

65. The National Intelligence Law ("NIL") of the PRC requires organizations and individuals to support, assist, and cooperate with state intelligence work in accordance with law, and to protect the secrecy of national intelligence work in their possession.⁵⁴

66. The NIL further authorizes intelligence agencies to require organizations and individuals to provide assistance, facilities, technical support, and access to relevant information in furtherance of intelligence work.⁵⁵

67. Legal and academic commentary has observed that these obligations are not

⁵⁴ *National Intelligence Law of the People's Republic of China*, art. 7 (adopted June 27, 2017), English translation published by China Law Translate, <https://www.chinalawtranslate.com/en/what-the-national-intelligence-law-says-and-why-it-doesnt-matter/> (last visited Jan. 6, 2026).

⁵⁵ *Id.* arts. 10, 14.

meaningfully constrained by independent judicial oversight or adversarial process, and that secrecy provisions restrict disclosure of cooperation with intelligence authorities.⁵⁶

ii. *Cybersecurity and Data Governance Laws Relevant to State Access and Control*

68. The intelligence cooperation requirements described above operate within a broader statutory framework governing cybersecurity and data governance in the PRC, which prioritizes national security and state oversight of information systems and data flows.

69. The Cybersecurity Law of the PRC governs network operators and information systems. The law identifies national security, social order, and public interests as regulatory objectives.⁵⁷

70. The Cybersecurity Law requires network operators to submit to government supervision and inspection. It also requires network operators to provide technical support and assistance to public security and national security authorities and to comply with state security standards.⁵⁸

71. In 2021, PRC enacted the Data Security Law (“DSL”). The law regulates data processing activities through data categorization tied to national security and through restrictions on data handling, storage, and transfer.⁵⁹

72. The DSL establishes categories of data, including “important data” and “core national data.” It provides for enhanced regulatory oversight and state control when those

⁵⁶ See Rogier Creemers, *What the National Intelligence Law Says and Why It Doesn't Matter*, China Law Translate (2017), <https://www.chinalawtranslate.com/en/what-the-national-intelligence-law-says-and-why-it-doesnt-matter/>

⁵⁷ *Cybersecurity Law of the People's Republic of China* (adopted Nov. 7, 2016), English translation published by China Copyright and Media, <https://chinacopyrightandmedia.wordpress.com/2016/11/07/cybersecurity-law-of-the-peoples-republic-of-china/> (last visited Jan. 6, 2026).

⁵⁸ *Cybersecurity Law of the People's Republic of China*, arts. 21, 28, China Copyright and Media, *supra*.

⁵⁹ *Data Security Law of the People's Republic of China* (adopted June 10, 2021), English translation published by DigiChina, Stanford University, <https://digichina.stanford.edu/work/translation-data-security-law-of-the-peoples-republic-of-china/> (last visited Jan. 6, 2026).

categories are involved.⁶⁰

73. The Personal Information Protection Law of the PRC regulates personal information processing. The law provides exceptions for national security, public security, and state interests.⁶¹

iii. Reasonable Basis for Plaintiffs' Belief Regarding Potential Access or Cooperation

74. Plaintiffs do not allege specific instances of disclosed user data to PRC authorities. The existence and scope of any such cooperation may be subject to statutory secrecy obligations under PRC law.

75. Plaintiffs allege that enacted statutes, mandatory regulatory regimes, and documented technical control mechanisms governing network-connected surveillance products provide a reasonable and fact-based basis for concern regarding potential data or system access by entities subject to PRC jurisdiction, facts material to their purchasing decisions.

76. U.S. congressional and executive branch reporting has repeatedly stated that PRC intelligence, cybersecurity, and data security laws must be considered together. That reporting identifies legal authority permitting Chinese officials to require access, assistance, or technical cooperation from companies operating within China or otherwise subject to Chinese law.⁶²

77. Government reporting has also documented regulatory requirements mandating the reporting of software vulnerabilities and technical flaws to state authorities. Those materials

⁶⁰ Data Security Law of the People's Republic of China, arts. 21–24, DigiChina, *supra*.

⁶¹ *Personal Information Protection Law of the People's Republic of China* (adopted Aug. 20, 2021), English translation published by DigiChina, <https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/> (last visited Jan. 6, 2026).

⁶² See *U.S.–China Economic and Security Review Commission, China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States*, Chapter 3, Section 2 (Nov. 2022), HYPERLINK "https://www.uscc.gov/sites/default/files/2022-11/Chapter_3_Section_2--Chinas_Cyber_Capabilities.pdf"https://www.uscc.gov/sites/default/files/2022-11/Chapter_3_Section_2--Chinas_Cyber_Capabilities.pdf (last visited Jan. 6, 2026).

explain that reported information may be shared across public security and state security institutions.⁶³

78. These obligations are not limited by the geographic location of data and may apply based on corporate jurisdiction, control, or technical capability.⁶⁴

iv. Application to Network-Connected Surveillance Products and Lorex-Branded Devices

79. Network-connected surveillance products, including consumer cameras and monitoring devices, collect continuous, location-specific, and behaviorally rich data in private environments.

80. These products operate through layered technical architectures that include firmware, cloud services, software updates, analytics, and diagnostic telemetry. Manufacturers often retain centralized control over these functions even when data is stored on geographically distributed servers.

81. Firmware update mechanisms allow remote code execution on deployed devices and operate independently of user-facing privacy controls.⁶⁵

82. Where system development, maintenance, vulnerability handling, or update infrastructure involves entities subject to PRC law, those entities may be subject to legal obligations to provide assistance, access, or technical cooperation to PRC authorities.

83. Statements that data are encrypted or stored outside of China do not address

⁶³ See Dakota Cary & Kristin Del Rosso, *Sleight of Hand: How China Weaponizes Software Vulnerabilities*, Atlantic Council Global China Hub (Sept. 6, 2023), <https://www.atlanticcouncil.org/in-depth-research-reports/report/sleight-of-hand-how-china-weaponizes-software-vulnerability/> (last visited Jan. 6, 2026).

⁶⁴ See Lawfare, *Beijing's New National Intelligence Law: Defense and Offense*, <https://www.lawfaremedia.org/article/beijings-new-national-intelligence-law-defense-offense> (last visited Jan. 6, 2026).

⁶⁵ See Department of Homeland Security, Cybersecurity and Infrastructure Security Agency, *Securing Software Supply Chains*, <https://www.cisa.gov/software-supply-chain-security>; see also Bruce Schneier, Software Updates and Security, https://www.schneier.com/blog/archives/2019/09/software_upda.html (last visited Jan. 6, 2026).

whether entities subject to PRC law retain technical or legal ability to access systems, encryption keys, metadata, telemetry, or update channels.⁶⁶

84. Despite these restrictions, vulnerabilities, and undisclosed technical relationships, Lorex marketed and sold its Camera Products as private and secure through its own website and through major national retailers. Those representations were consistent across platforms and reinforced through product placement, imagery, and branding.

II. Lorex Markets and Sells Its Products Through Major Retailers While Making Misleading Privacy Representations

A. Representations on Lorex’s Own Webpages

85. Lorex operates and owns the retail website Lorex.com, through which it sells Lorex-branded products. The website contains numerous misleading representations concerning the nature of those products. On Lorex’s website, within a webpage describing the security of its products, it assures consumers that Lorex is “committed to protecting the integrity, privacy, and security of . . . customers’ information” and that “take[s] every step to ensure [consumer's] security.”⁶⁷

⁶⁶ See *National Institute of Standards and Technology, Key Management Guidelines*, NIST SP 800-57, HYPERLINK "<https://csrc.nist.gov/publications/detail/sp/800-57-part-1/rev-5/final>"<https://csrc.nist.gov/publications/detail/sp/800-57-part-1/rev-5/final> (last visited Jan. 6, 2026).

⁶⁷Lorex marketing materials archived at <https://perma.cc/79L4-78D3> (showing representations regarding privacy and security of Lorex cameras) (last visited Jan. 6, 2026).

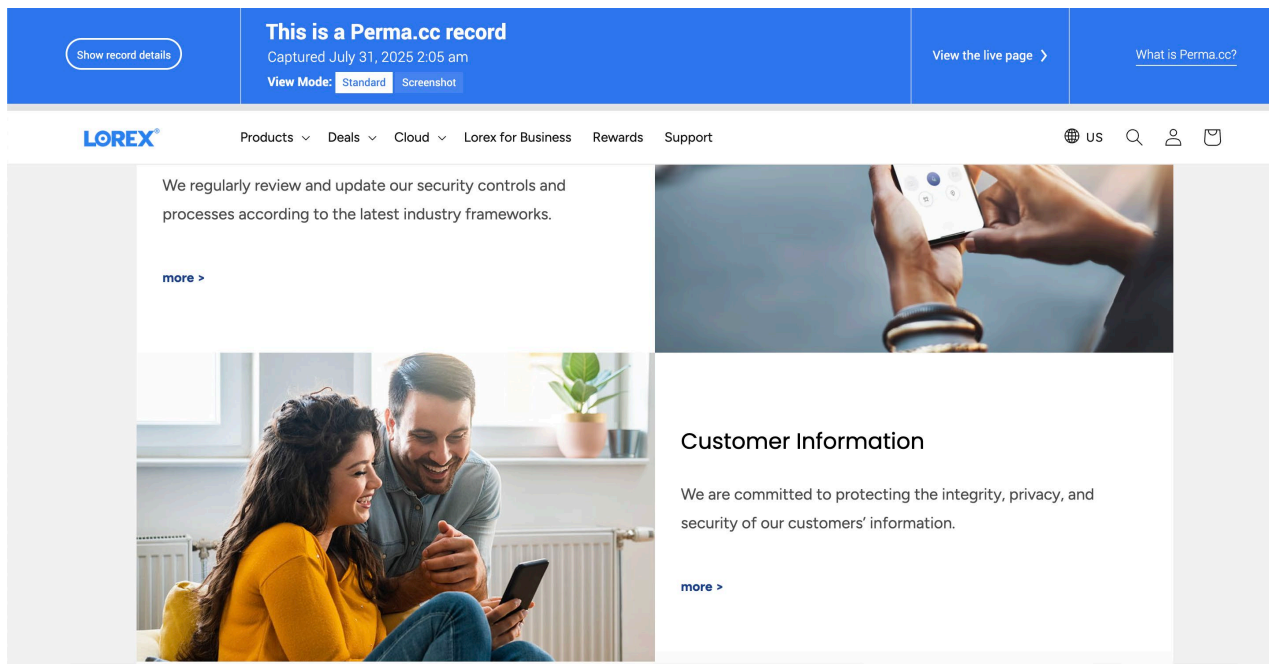
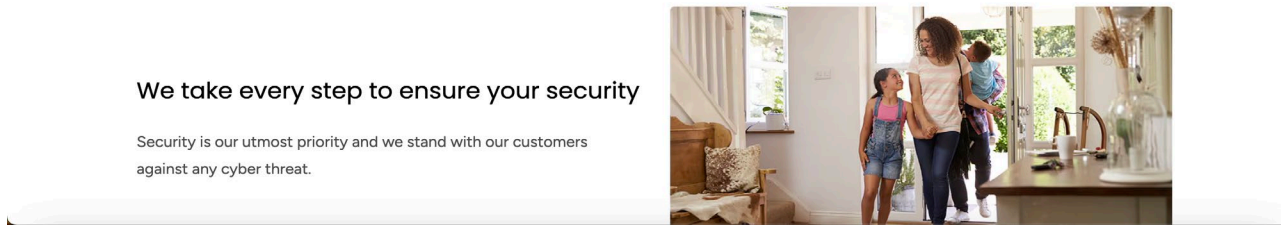
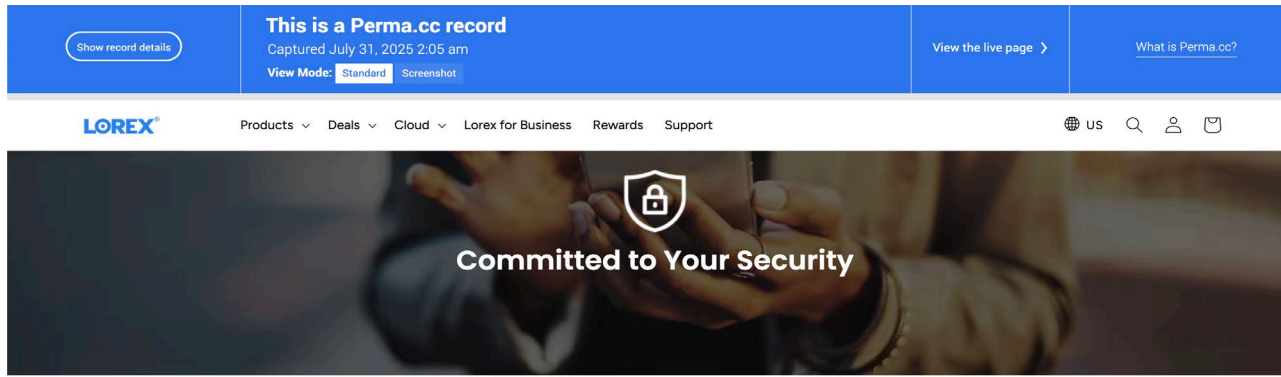


Figure 9 &10: Lorex representing that “security is our utmost priority” and that it is “committed to protecting the integrity, privacy, and security of our customers’ information”

86. On its Privacy Commitment page, Lorex states: “consumer’s privacy is [Lorex’s] top priority. That’s why [it] provide[s] [consumers] with the tools to manage [their] own devices and storage. [Lorex] is committed to taking every step possible to ensure [consumer’s] recordings

remain private.”⁶⁸

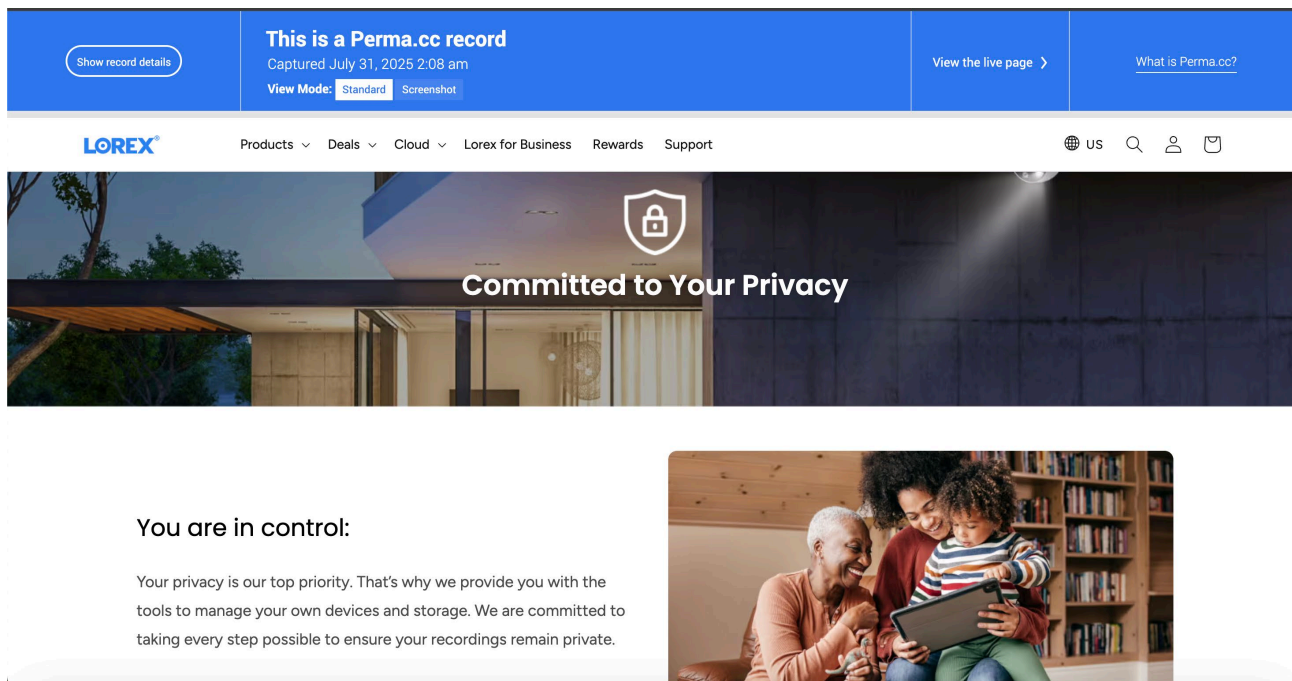


Figure 11: Lorex representing that “Privacy is our top priority”

87. On Lorex’s FAQ webpage, the question “Are Lorex wireless cameras secure?” is posted to which Lorex begins its answer with “Yes.”⁶⁹

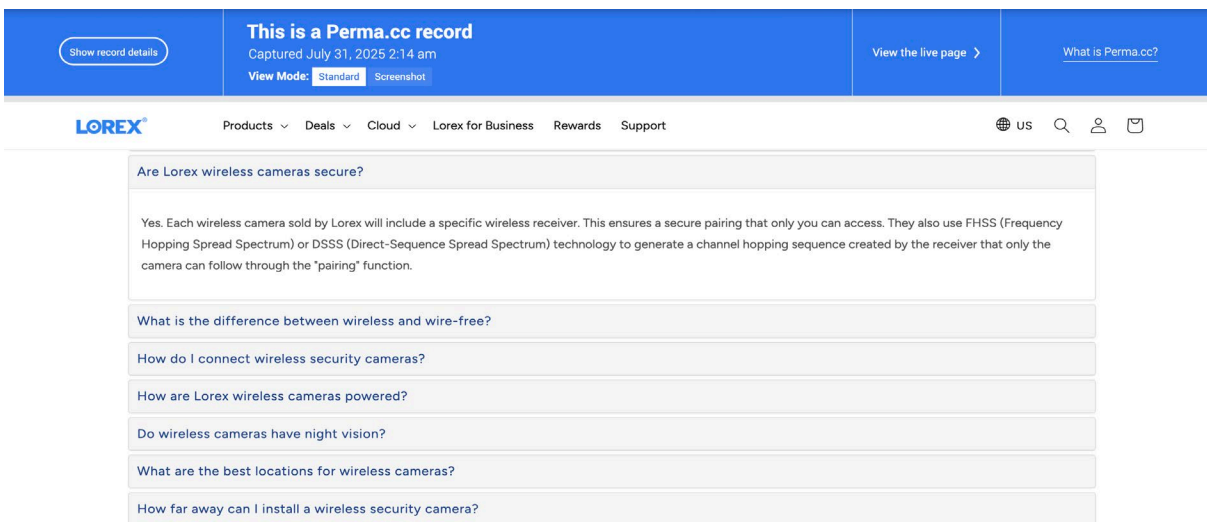


Figure 12: Lorex representing on its FAQ page that its wireless cameras are secure

⁶⁸ Lorex marketing materials archived at <https://perma.cc/79L4-78D3> (showing representations regarding privacy and security of Lorex cameras) (last visited Jan. 6, 2026).

⁶⁹ See, LOREX, <https://perma.cc/HS6B-2VJC> (last visited Jan. 6, 2026).

B. Misleading Privacy Representations on Costco’s Webpages Promoting Lorex Products

88. Costco is one of Lorex’s primary retail partners for the sale of Lorex products.

89. Lorex’s website states that “[f]or over a decade, Costco has carried a wide variety of Lorex products, including security cameras and systems.”⁷⁰

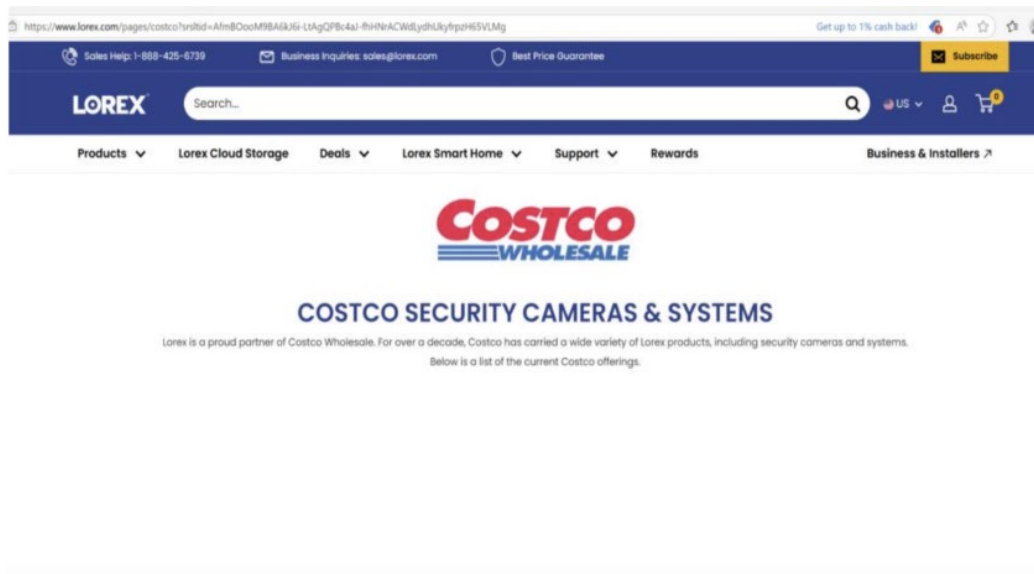


Figure 13: Costco webpage saying that “Lorex is a proud partner of Costco Wholesale”.

90. According to a report by TechCrunch, in October 2023 the co-chairs of the CECC⁷¹ Representative Christopher Smith and Senator Jeff Merkley, sent a letter to Costco.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

⁷⁰ See Lorex, <https://perma.cc/GEZ4-DCPT> (last visited Jan. 6, 2026).

⁷¹ U.S. Congressional–Executive Commission on China (CECC), <https://www.cecc.gov/> (last visited Nov. 7, 2025).

⁷² *One Hundred Eighteenth Congress Representative Christopher H. Smith, Chair & Representative Jeff Merkley, CoChair, Letter to Costco Wholesale Corp.*, CECC (last visited Jan. 6, 2026); see also Zack Whittaker, *Lawmakers say Costco’s decision to continue selling banned China surveillance tech is ‘puzzling’*, TECHCRUNCH (last visited Jan. 6, 2026).

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 explanation of who was responsible for this mistake or why the Lorex name stayed on Dahua equipment.”⁷³

C. Privacy Representations Concerning Lorex Products Sold Through Costco

91. Notwithstanding the prior history associated with Lorex products, the Costco online website continues to feature Lorex products in proximity to other major consumer security brands, including Ring, Arlo, and Blink.⁷⁴

⁷³*Id.*, at page 2.

⁷⁴ *Costco Security & Surveillance Page*, Costco, <https://www.costco.com/security-surveillance.html> (last visited Jan. 6, 2026).

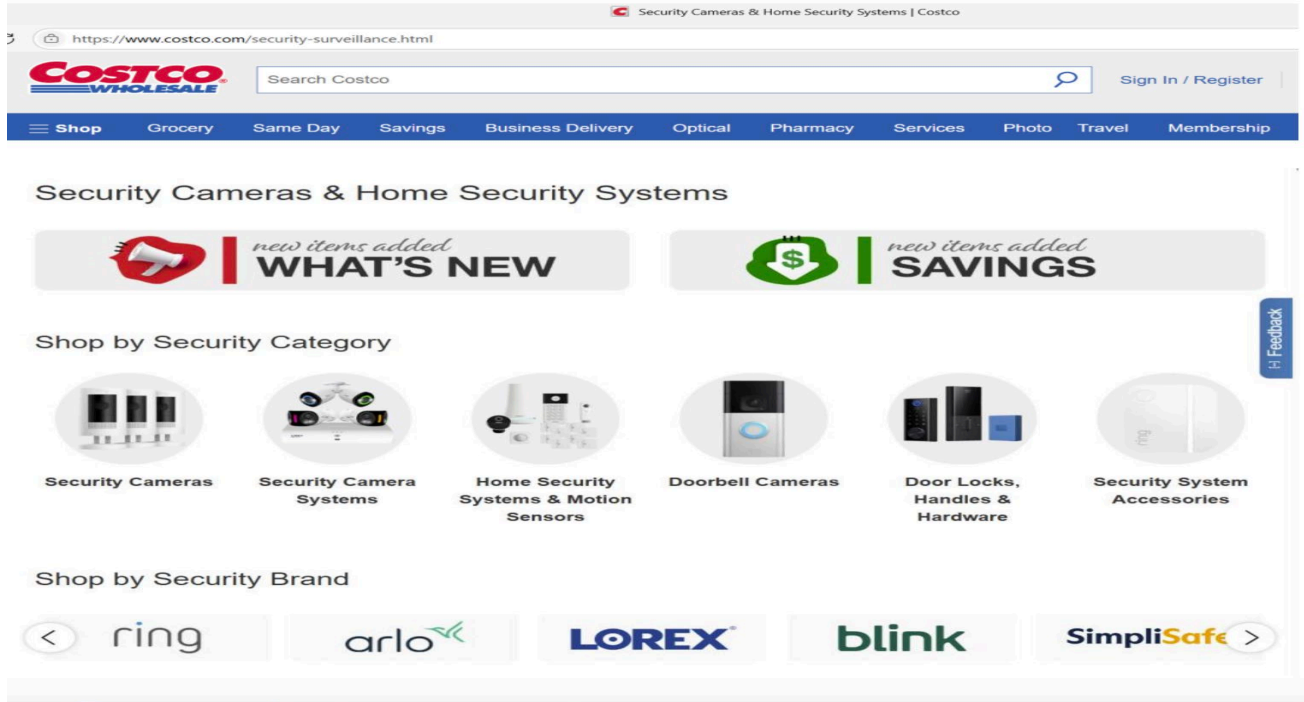


Figure 14: Costco webpage selling security cameras including Lorex

92. Costco highlights the Lorex brand in particular.

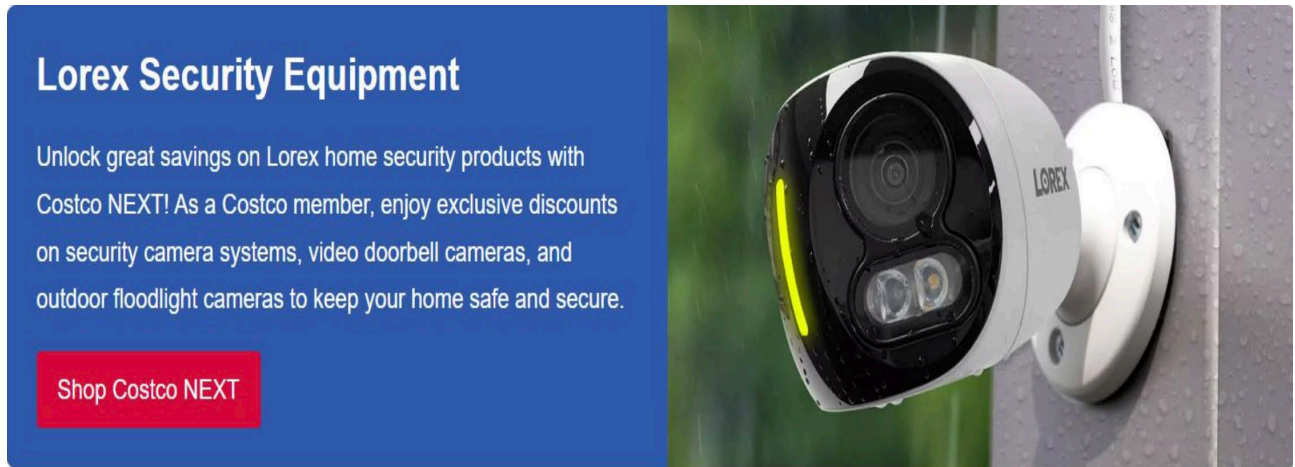


Figure 15: Costco selling Lorex security Cameras

93. As of December 3, 2025, Costco's website listed four Lorex products: the \$750 Lorex Fusion Network Video Recorder (NVR) with Two 4K 180° Panoramic Lens and Two 4K Bullet Cameras; the \$150 Lorex 2K Dual Lens Indoor Pan-tilt Wi-Fi Security Camera, 2-pack; the \$900 Lorex Classic 2TB NVR w/ 6x 4K+ Turret Cameras & 2x Dual Lens 4K Cameras, the \$130

Lorex Connect 2K Floodlight Wi-Fi Security Camera, 2-pack; and a Lorex kit where Costco members can receive exclusive value on a security equipment system from Lorex.⁷⁵

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

Online Only

\$129.99
\$129.99 After \$50 OFF
Lorex Connect 2K Floodlight Wi-Fi Security Camera, 2-pack
★☆☆☆☆ (1)
📦 Delivery Available

Compare

Select Options

Online Only

\$899.99
Lorex Classic 2TB NVR w/ 6x 4K+ Turret Cameras & 2x Dual Lens 4K Cameras
★★★★☆ (12)
📦 Delivery Out of Stock

Compare

See Details

Online Only

\$149.99
Lorex 2K Dual Lens Indoor Pan-tilt Wi-Fi Security Camera, 2-pack
★★★★☆ (17)
📦 Delivery Available

Compare

Add to Cart

Online Only

\$749.99
Lorex Fusion NVR with Two 4K 180° Panoramic Lens and Two 4K Bullet Cameras
★★★★☆ (66)
📦 Delivery Available

Compare

Add to Cart

Figure 16: Variety of Lorex Cameras sold on Costco

⁷⁵ Costco — Security & Surveillance (search: “Lorex”), Costco, <https://www.costco.com/security-surveillance.html?keyword=Lorex> (last visited Jan. 6, 2026).

94. The design of the Lorex 2K Dual Lens Indoor camera closely resembles Dahua’s “H5D-5F” and “H3D-3F” models.⁷⁶



Figure 17: Deceptively similar model of Dahua

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



Figure 18: Costco page representing that Lorex cameras are private by design

96. Lorex further represents that its cameras are appropriate for placement in highly sensitive areas of the home, including children’s bedrooms.⁷⁸

⁷⁶ Lorex Marketing Archive, <https://perma.cc/6QJ7-VSPC> (last visited Nov. 7, 2025); Lorex Promotional Archive, <https://perma.cc/EW9Y-K9ZW> (last visited Jan. 6, 2026).

⁷⁷ Costco — Security & Surveillance (search: “Lorex”), Costco, <https://www.costco.com/security-surveillance.html?keyword=Lorex> ; (last visited Nov. 7, 2025). *Under Product Details, scroll down to the picture of the Lorex Video Vault.*

⁷⁸ Lorex 2K Dual Lens Indoor Pan-Tilt Wi-Fi Security Camera (2-Pack), Costco, <https://www.costco.com/lorex-2k->

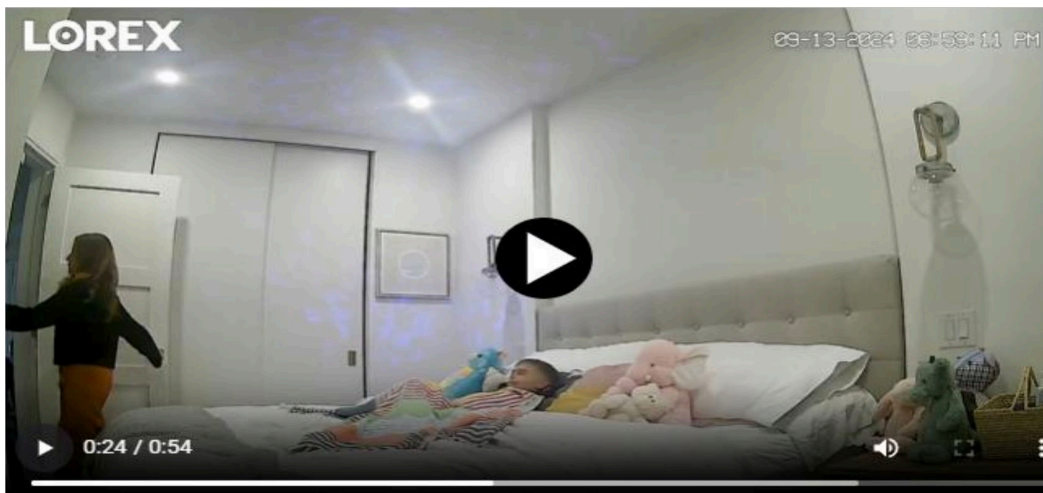


Figure 19: Lorex representing, on Costco, that its cameras are safe to use in a children's bedroom

97. 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.”⁷⁹

98. A product specification contains a similar disclaimer.⁸⁰

99. By including this disclaimer, Lorex and/or Costco demonstrate actual knowledge of security issues, yet fail to explain the significance or implications of the disclaimer to consumers.

100. Placement of Lorex products alongside trusted consumer brands and imagery depicting use in children's bedrooms reinforces consumer expectations of heightened privacy and security, particularly when offered through a retailer known for vetting product safety.

101. A reasonable consumer would understand the disclaimer as representing that Lorex cameras are suitable for household and business use.

[dual-lens-indoor-pan-tilt-wi-fi-security-camera-2-pack.product.4000384381.html](https://www.costco.com/lorex-fusion-nvr-with-two-4k-180-panoramic-lens-and-two-4kbullet-cameras.product.4000384381.html) (last visited Nov. 7, 2025). Click on “View More” under Product Details, and view first video.

⁷⁹ Lorex Fusion NVR With Two 4K 180° Panoramic Lenses and Two 4K Bullet Cameras, Costco, <https://www.costco.com/lorex-fusion-nvr-with-two-4k-180-panoramic-lens-and-two-4kbullet-cameras.product.4000272398.html>; (Emphasis added) (last visited Nov. 7, 2025).

⁸⁰ Lorex Product Specification Sheet, <https://content.syndigo.com/asset/d3521e89-58ea-45f9-9487-b29806458c86/original.pdf>; (last visited Jan. 6, 2026).

D. Other Retailer Websites Make Similar Misleading Representations Regarding Privacy

102. Best Buy offers multiple Lorex products on its website,⁸¹ including the Lorex 2K Dual Lens Indoor Pan-Tilt Wi-Fi Security Camera – White and the Lorex 2K Wi-Fi Smart Lightbulb Camera.⁸²

i. Best Buy

103. 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.⁸³

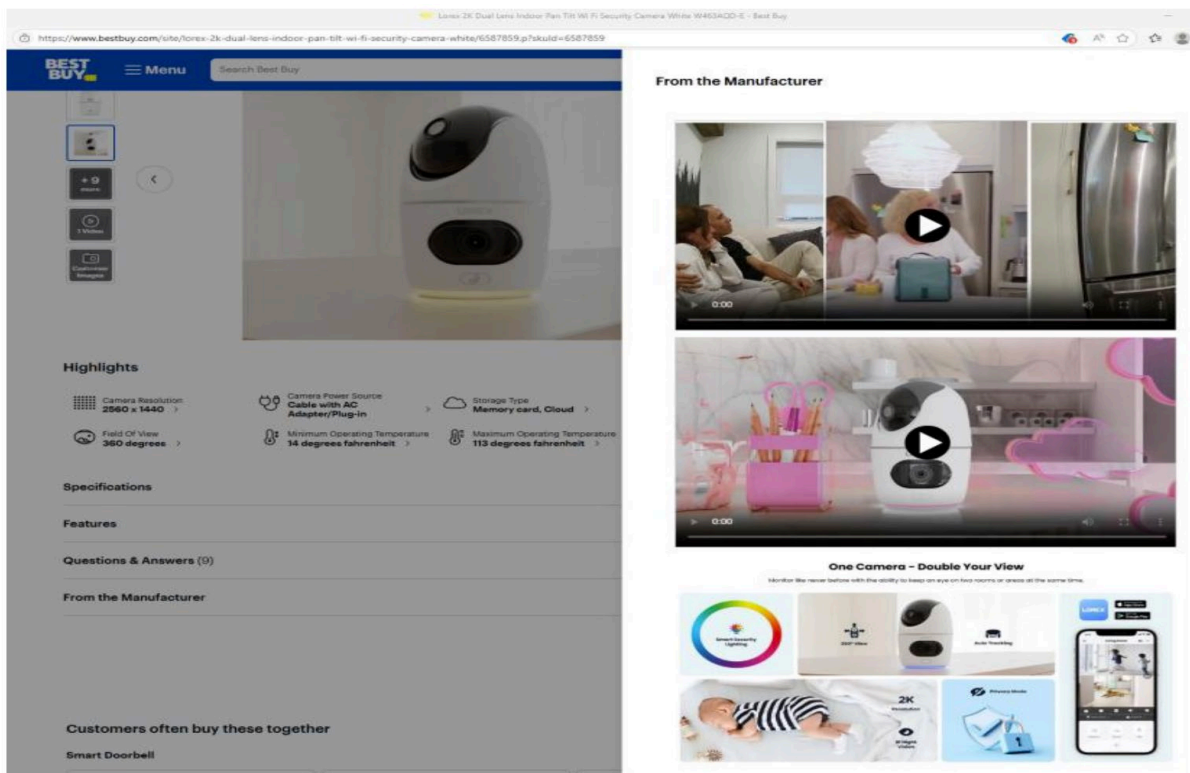


Figure 20: “Best Buy” selling Lorex Cameras

⁸¹ <https://www.bestbuy.com/site/searchpage.jsp?id=pcat17071&st=lorex+camera>

⁸² Lorex Security Cameras — Best Buy, BestBuy.com, <https://www.bestbuy.com/site/shop/lorex-security-cameras> (last visited Jan. 6, 2026).

⁸³ Lorex 2K Dual Lens Indoor Pan-Tilt Wi-Fi Security Camera – White, BestBuy.com, <https://www.bestbuy.com/site/lorex-2k-dual-lens-indoor-pan-tilt-wi-fi-security-camera-white/6587859.p?skuId=6587859> (last visited Nov. 7, 2025).

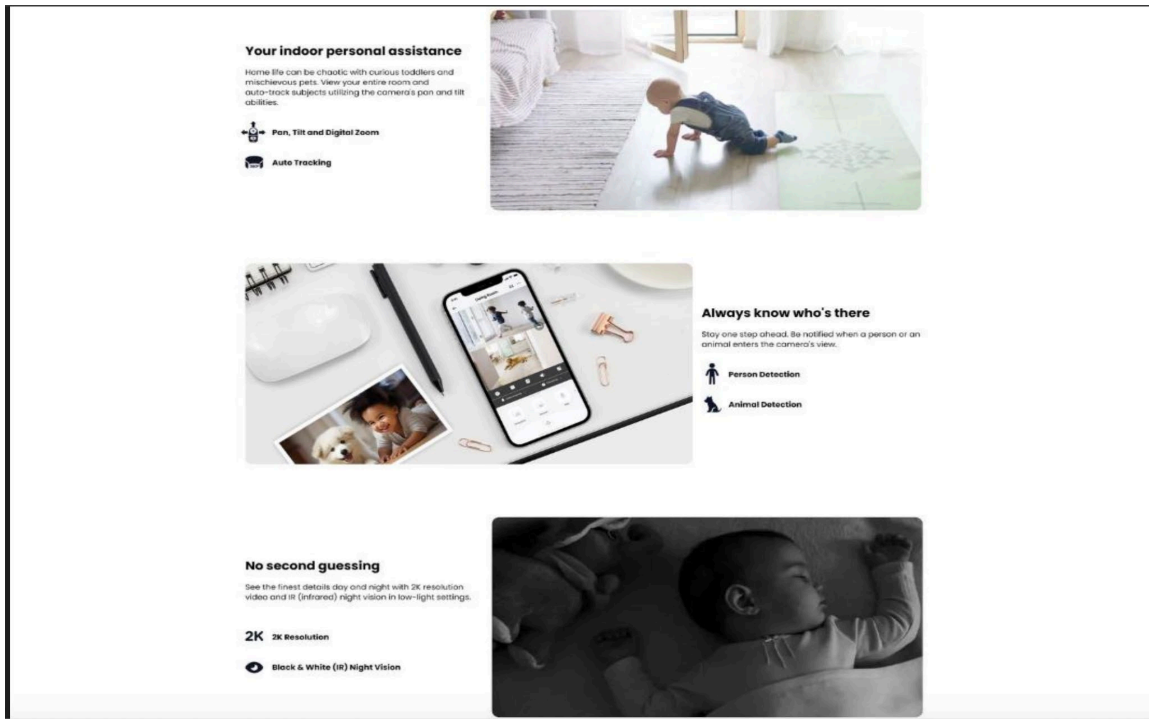


Figure 21: Best Buy representing that Lorex is protecting children's privacy

104. The first video appearing under the "From the Manufacturer" tab depicts the camera being used in a child's bedroom:

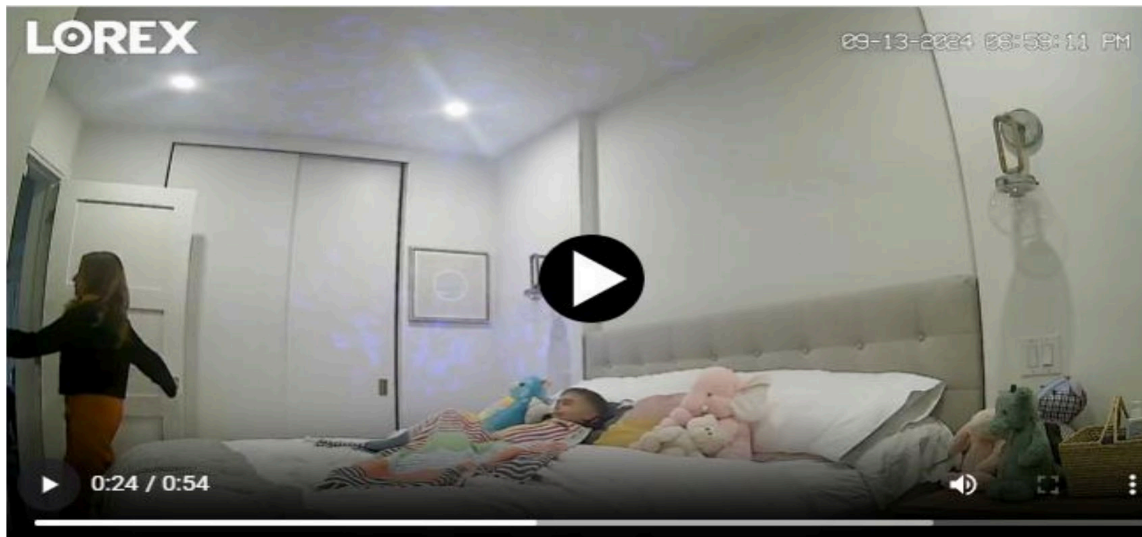


Figure 22: Lorex on Best Buy representing that its cameras are safe to use in kids bedroom

105. This type of deployment would raise heightened privacy concerns for a reasonable consumer.

106. The “From the Manufacturer” tab also states “Private by design,” including a bullet that lists “Enhanced Privacy features.”⁸⁴



Figure 23: Best Buy page representing that Lorex cameras are private by design

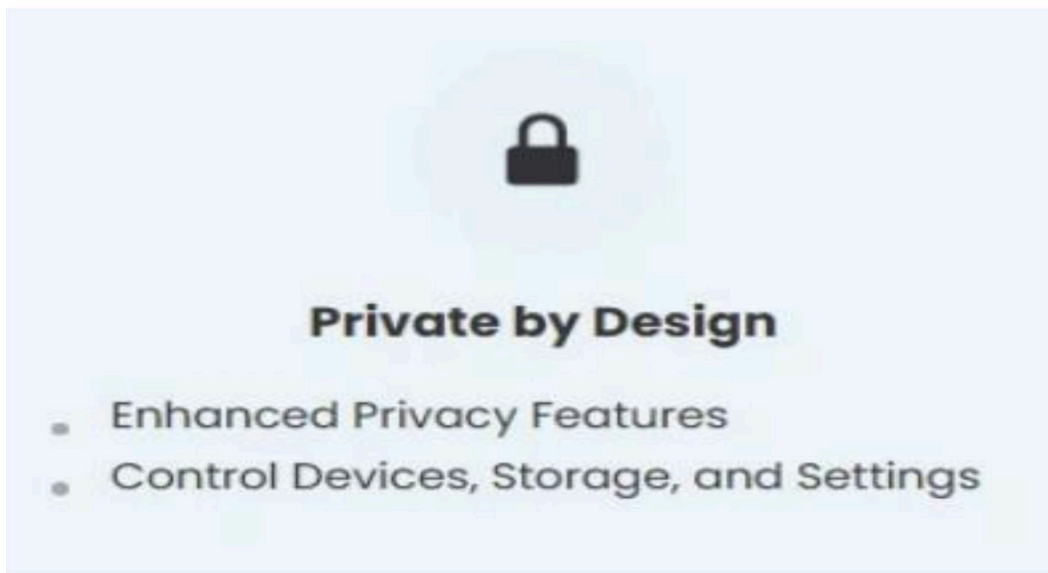


Figure 24: Lorex claims that its camera has enhanced security features

107. 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.”⁸⁵

⁸⁴ Click on From the Manufacturer and scroll down to the bottom.

⁸⁵ Lorex Product Specification Sheet, (last visited Jan. 6, 2026).

108. The Lorex lightbulb camera page contains similar representations regarding Private by Design.⁸⁶

ii. Kohl's

109. Kohl's appears to contain a large number of Lorex products for sale.⁸⁷ This includes the Lorex 2K Dual Lens Indoor PanTilt Wi-Fi Security Camera.⁸⁸

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



Figure 25: Kohl's webpage selling Lorex Cameras

111. The page shows the camera installed in children's rooms, including one labeled "Privacy Mode."

112. Kohl's also lists the Lorex 2K Indoor Wi-Fi Security Camera.⁸⁹

113. That product listing states: "Keep your footage private and secure with built-in local

⁸⁶ Lorex 2K Wi-Fi Smart Lightbulb Camera – White, BestBuy.com, <https://www.bestbuy.com/site/lorex-2k-wi-fi-smart-lightbulb-camerawhite/6614839.p?skuId=6614839> (last visited Jan. 6, 2026). (Click "From the Manufacturer" and scroll down.)

⁸⁷ Lorex Brand Storefront, Kohl's, <https://www.kohls.com/catalog/lorex.jsp?CN=Brand:Lorex> (last visited Jan. 6, 2026).

⁸⁸ Lorex 2K Dual-Lens Indoor Pan-Tilt Wi-Fi Security Camera, Kohl's, <https://www.kohls.com/product/prd-7462714/lorex-2k-dual-lens-indoor-pan-tilt-wi-fi-security-camera.jsp> (last visited Jan. 6, 2026).

⁸⁹ Lorex 2K Indoor Wi-Fi Security Camera, Kohl's, <https://www.kohls.com/product/prd-6378004/lorex-2k-indoor-wi-fi-security-camera.jsp> (last visited Jan. 6, 2026).

storage.”⁹⁰

iii. Office Depot

114. The Office Depot website includes listings for multiple Lorex camera products.⁹¹

115. 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.”⁹²

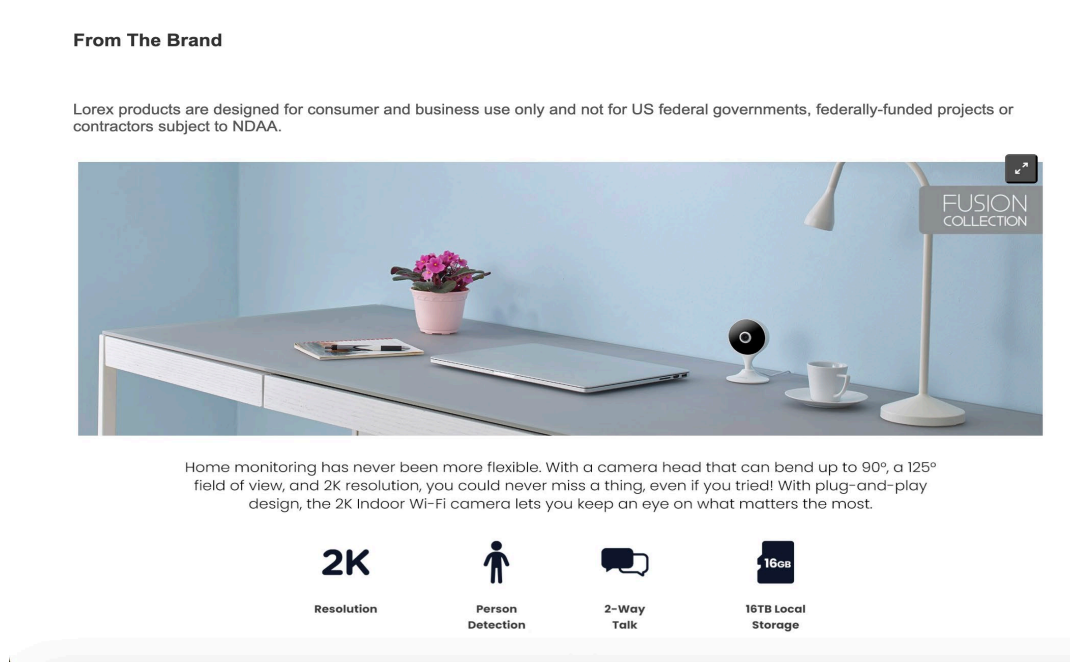


Figure 26: Disclaimer on the website of Office Depot saying “Lorex products are designed for consumer and business use only and not for US federal governments, federally-funded projects or contractors subject to NDAA.”

116. The page also contains the statements: “Keep your security footage where it belongs. Private, at home, and in your control” and “Private by Design.”⁹³

⁹⁰ *Id.* Click on “more” under product details.

⁹¹ *Lorex Security Cameras — Office Depot Security Camera Category*, OfficeDepot.com, <https://www.officedepot.com/b/security-cameras/Brand--Lorex/N-509546> (last visited Jan. 6, 2026).

⁹² *Lorex 2K QHD Indoor Wi-Fi Camera*, OfficeDepot.com, <https://www.officedepot.com/a/products/7842911/Lorex-2K-QHD-Indoor-Wi-Fi/#MoreInfo> (last visited Jan. 6, 2026).

⁹³ *Id.*

iv. Amazon

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

118. 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 View – Free 16GB Micro SD identifies the seller as “Lorex Technology Inc.”⁹⁴

119. 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).”

120. 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.”

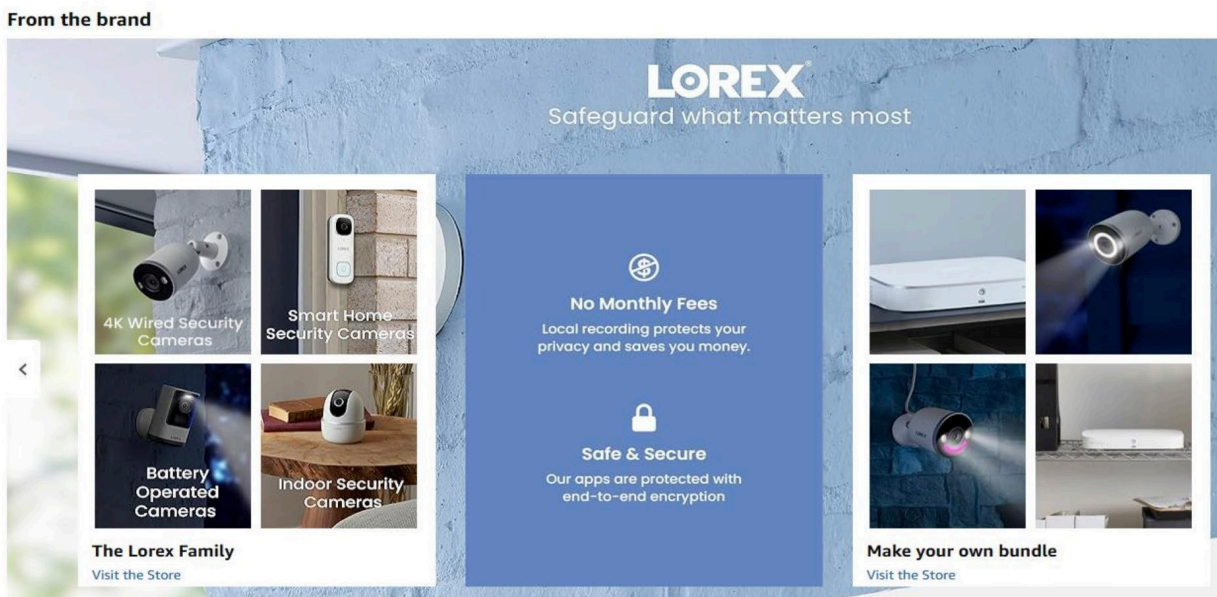


Figure 27: Amazon selling Lorex cameras with the statement “Safe and Secure”

121. The Lorex store on Amazon.com contains additional representations about privacy.⁹⁵

⁹⁴ Lorex Security & Detection Two-Way Control Camera, Amazon.com, https://www.amazon.com/Lorex-Security-Detection-Two-Way-Control/dp/B0CPT61DMG?ref=ast_sto_dp (last visited Jan. 6, 2026).

⁹⁵ Lorex Storefront, Amazon.com, <https://www.amazon.com/stores/Lorex/page/E7453005-0B96-4A82-8188-A18E40241FDB> (last visited Jan. 6, 2026).

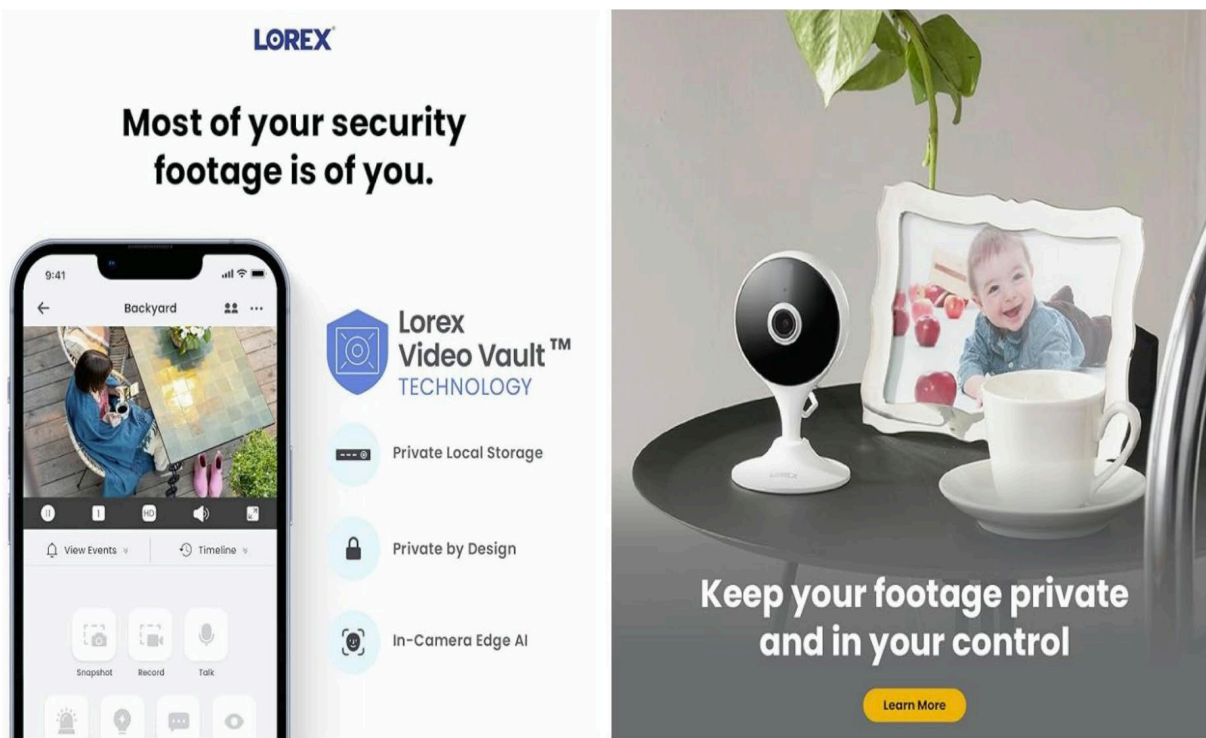


Figure 28: Lorex represented on Amazon that its cameras are private by design

122. The Amazon website offers the same 2K Indoor Wi-Fi Security Camera that researchers determined contains firmware associated with Dahua.

TOLLING ALLEGATIONS

123. Any applicable statute of limitations should be tolled by the Discovery Rule.

124. Here, Plaintiffs and other Class Members reasonably relied on Lorex's representations regarding the fact that its Camera Products store all information locally, do not share such information with Lorex, and were encrypted.

125. It was not until September 23, 2025, when the Nebraska Attorney General publicly filed a complaint alleging that Lorex Camera Products transmitted data to Lorex servers and that video feeds were not encrypted, that Plaintiffs and other Class Members learned that these representations were false. Consumers exercising reasonable diligence could not have discovered the false and misleading nature of Lorex's representations earlier.

CLASS ACTION ALLEGATIONS

126. Plaintiffs bring this action individually and as representatives of all those similarly situated pursuant to Rule 23 of the Federal Rules of Civil Procedure, on behalf of the below-defined classes:

National Class: All persons in the United States who purchased the Camera Products for personal or household use, and not for resale, during the applicable statute of limitations.

Illinois Class: All persons in the State of Illinois who purchased the Camera Products during the applicable statute of limitations.

California Class: All persons in California who purchased the Camera Products for personal or household use, and not for resale, during the applicable statute of limitations period.

New York Class: All persons in New York State who purchased the Camera Products for personal or household use, and not for resale, during the applicable statute of limitations period.

127. The following are excluded from the classes: (1) government entities; (2) any Judge presiding over this action and members of his or her family; (3) Defendants, Defendants' subsidiaries, parents, successors, predecessors, and any entity in which a Defendant or its parent has a controlling interest (as well as current or former employees, officers, and directors); (4) persons who properly execute and file a timely request for exclusion from the Class; (5) persons whose claims in this matter have been finally adjudicated on the merits or otherwise released; (6) Plaintiffs' counsel and Defendants' counsel; and (7) the legal representatives, successors, and assigns of any such excluded persons.

128. The classes described in this complaint may be jointly referred to as the "Class" or "Classes" and members of the proposed classes may be jointly referred to as "Class Members." Plaintiffs reserve the right to amend or modify the Class definitions with greater specificity, further division into subclasses, or with limitation to particular issues as discovery and

the orders of this Court warrant. In addition, the Court can define the Classes and create additional subclasses as may be necessary or desirable to adjudicate common issues and claims of the Class Members if, based on discovery of additional facts, the need arises.

129. Pursuant to Rule 23(b)(2) of the Federal Rules of Civil Procedure, Defendants have acted or refused to act on grounds generally applicable to the Classes, thereby making final injunctive relief or corresponding declaratory relief and damages appropriate with respect to the Classes as a whole. Defendants continue to falsely market their cameras, where users can “Keep your recordings private and in your control,” continue to misrepresent that they apply facial recognition technology to images captured by the cameras, and continue to apply facial recognition technology to images captured by the cameras without users’ knowledge or consent.

130. Certification of Plaintiffs’ claims for class-wide treatment is appropriate because Plaintiffs can prove the elements of their claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

131. The members of the Class are so numerous that individual joinder of all Class Members is impracticable. On information and belief, Class Members number in the thousands. The precise number or identification of members of the Class is presently unknown to Plaintiffs, but may be ascertained from Defendants’ books and records. Class Members may be notified of the pendency of this action by recognized, Court-approved notice dissemination methods, which may include U.S. mail, electronic mail, Internet postings, and/or published notice.

132. Common questions of law and fact exist as to all members of the Class, which predominate over any questions affecting individual members of the Class. These common questions of law or fact include, but are not limited to, the following:

- a. Whether the marketing, advertising, packaging, labeling, and other

- promotional materials for the Camera Products was deceptive;
- b. Whether Lorex's actions violate the consumer protection statutes invoked herein;
 - c. Whether Lorex unlawfully collected, transmitted, and disseminated images and/or biometric information from Plaintiffs and Class Members' Camera Products;
 - d. Whether Lorex disclosed to Plaintiffs and Class Members before they purchased Camera Products that images and/or biometric information from such cameras would be collected and transmitted by Lorex;
 - e. Whether Lorex omitted material facts with regard to the collection and transmittal of images and/or biometric information from the Camera Products;
 - f. Whether Plaintiffs and Class Members consented to the collection and transmittal of images and/or biometric information from the Camera Products;
 - g. Whether Lorex's marketing of their camera products was likely to deceive or mislead reasonable consumers;
 - h. Whether Lorex's conduct constitutes violations of the laws and statutes asserted herein;
 - i. Whether Lorex warranted that data collected by the Camera Products would be stored locally and would be encrypted;
 - j. Whether Lorex's conduct was knowing and/or negligent;
 - k. Whether Defendants were unjustly enriched at the expense of Plaintiffs and

Class Members;

- l. Whether Plaintiffs and Class Members are entitled to damages, including compensatory, exemplary, and statutory damages, and the amount of such damages;
- m. Whether Plaintiffs and the other Class Members have been injured and the proper measure of their losses as a result of those injuries;
- n. Whether Plaintiffs and the Class Members are entitled to injunctive, declaratory, or other equitable relief; and
- o. Whether, as a result of Lorex's conduct, Plaintiffs and Class Members are entitled to an award of reasonable attorneys' fees, prejudgment interest, or costs of suit.

133. Lorex engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiffs, on behalf of themselves and the other Class Members. Similar or identical statutory and common law violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quality and quantity, to the numerous common questions that dominate this action.

134. Plaintiffs' claims are typical of the claims of the other Class Members because, among other things, all such claims arise out of the same wrongful course of conduct engaged in by Lorex in violation of law as complained of herein. Further, the damages of each Class member were caused directly by Lorex's wrongful conduct in violation of the law as alleged herein.

135. Plaintiffs are adequate representatives of the Class because they are members of the Class and their interests do not conflict with the interests of the Class Members that they seek to represent. Plaintiffs have also retained counsel competent and experienced in complex

commercial and class action litigation. Plaintiffs and their counsel intend to prosecute this action vigorously for the benefit of all Class Members. Accordingly, the interests of the Class Members will be fairly and adequately protected by Plaintiffs and their counsel.

136. A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages or other financial detriment suffered by Plaintiffs and the Class Members are relatively small compared to the burden and expense that would be required to individually litigate their claims against Lorex, so it would be impracticable for Class Members to individually seek redress for Lorex's wrongful conduct. Even if Class Members could afford individual litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties, and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

CAUSES OF ACTION

COUNT I

VIOLATION OF THE ILLINOIS CONSUMER FRAUD AND DECEPTIVE TRADE PRACTICES ACT ("ICFA") 815 ILCS 505/1, ET SEQ.

**(On Behalf of Plaintiff Shah and the National Class and, alternatively, the
Illinois Class)**

137. Plaintiff Shah and the Subclass re-allege and incorporate the allegations above as if set forth herein.

138. Illinois law applies under the terms of the EULA.

139. Plaintiff Shah and the Subclass and other Class Members are persons within the context of the ICFA, 815 ILCS 505/1(c).

140. Lorex is a person within the context of the ICFA, 815 ILCS 505/1(c).

141. At all times relevant hereto, Lorex was engaged in trade or commerce as defined under the ICFA, 815 ILCS 505/1(f). 183.

142. Plaintiff Shah and the Subclass are “consumers” who purchased the Camera Products for personal, family, or household use within the meaning of the ICFA, 815 ILCS 505/1(e).

143. The ICFA prohibits engaging in any “unfair or deceptive acts or practices ... in the conduct of any trade or commerce....” ICFA, 815 ILCS 505/2.

144. The ICFA prohibits any deceptive, unlawful, unfair, or fraudulent business acts or practices including using deception, fraud, false pretenses, false promises, false fact, or the use or employment of any practice described in Section 2 of the Uniform Deceptive Trade Practices Act (“UDTPA”). 815 ILCS § 505/2. Plaintiff Shah and the Subclass reasonably relied upon Lorex’s representation that the Camera Products stored all data locally and encrypted such data.

145. Lorex’s conduct, as described herein, constitutes unfair or deceptive acts or practices in the course of trade and commerce, in violation of 815 ICFA 505/1, *et seq.*

146. Lorex violated the ICFA by representing that the Camera Products have characteristics or benefits that they do not have. 815 ILCS § 505/2; 815 ILCS § 510/2(7).

147. Lorex advertised the Camera Products with intent not to sell them as advertised, in violation of 815 ILCS § 505/2 and 815 ILCS § 510/2(9).

148. Lorex engaged in deceptive conduct, which creates a likelihood of confusion or of misunderstanding in violation of 815 ILCS § 505/2; 815 ILCS § 510/2(3).

149. Lorex engaged in misleading and deceptive advertising by representing that its Camera Products were “Private by Design,” “Safe and Secure,” and that users could “Keep your

recordings private and in your control.” Lorex intentionally advertised and labeled its Camera Products to influence consumer purchasing decisions and obtain a competitive advantage in the home security market, aware that consumers place significant weight on privacy and data protection. As a result, consumers who purchased Lorex Camera Products were uniformly exposed to these representations and reasonably believed that their recordings and personal data would remain local, private, and inaccessible to third parties.

150. Contrary to those representations, Lorex Camera Products are integrated with and depend on hardware, firmware, and backend infrastructure supplied by Dahua

151. Lorex intended that Plaintiff Shah and the Subclass would reasonably rely upon their misrepresentations, characterizations, warranties, and material misrepresentations concerning the true nature of the Camera Products.

152. Lorex’s misrepresentations, concealment, omissions, and other deceptive conduct were likely to deceive and cause misunderstanding, and/or in fact caused Plaintiff Shah and the Subclass Members to be deceived about the true nature of the Camera Products.

153. Plaintiff Shah and the Subclass have been damaged as a proximate result of Lorex’s violations of the ICFA and have suffered damages as a direct and proximate result of purchasing the Camera Products.

154. As a direct and proximate result of Lorex’s violations of the ICFA, as set forth above, Plaintiff Shah and the Subclass have suffered ascertainable loss of money caused by Lorex’s misrepresentations.

155. Had they been aware of the true nature of the Camera Products, Plaintiff Shah and the Subclass Members either would have paid less for the Camera Products or would not have purchased them at all.

156. Plaintiff Shah and the Subclass are therefore entitled to relief, including restitution, actual damages, treble damages, punitive damages, costs and attorney’s fees, under sections 815 ILCS 505/10a of the ICFA. Plaintiff Shah and the Subclass Members are also entitled to injunctive relief, seeking an order enjoining Lorex’s unfair and/or deceptive acts or practices.

COUNT II
VIOLATION OF NEW YORK DECEPTIVE ACTS AND PRACTICES,
NEW YORK GENERAL BUSINESS LAW § 349
(On Behalf of Plaintiff Hill and the New York Class)

157. Plaintiff Hill and the Subclass re-allege and incorporate the allegations above as if set forth herein.

158. New York General Business Law (“GBL”) section 349 declares unlawful “[d]eceptive acts or practices in the conduct of any business, trade or commerce or in the furnishing of any service in this state.”

159. Defendants engaged in consumer-oriented conduct by marketing, advertising, selling, and supporting their Camera Products to consumers throughout the State of New York, including through major retailers and online marketplaces.

160. Defendants violated GBL § 349 by deceptively and misleadingly misrepresenting and omitting material facts concerning the privacy, security, and data-handling practices of their Camera Products, including but not limited to representations that users could “keep recordings private and in [their] control,” that data was stored locally, and that video feeds were encrypted.

161. Defendants’ misrepresentations and omissions, including affirmative statements, half-truths, and active concealment, falsely conveyed that the Camera Products were private-by-design, secure, and suitable for use in sensitive locations, when in fact Lorex collected, transmitted, and/or permitted access to images, video feeds, and related data without adequate disclosure, consent, or safeguards.

162. Defendants' deceptive conduct was directed at the consuming public at large, as it was uniform, repeated, and disseminated through marketing materials, retail listings, packaging, and online content, and was capable of deceiving reasonable consumers.

163. The facts misrepresented and concealed by Defendants were material. The Plaintiff and New York Subclass, acting reasonably, would have considered such information important in deciding whether to purchase the Camera Products and how to deploy them within their homes. Had they known the true nature of Lorex's data-collection, transmission, and security practices, they would not have purchased the Camera Products or would have paid substantially less.

164. Defendants charged, and the Plaintiff and New York Subclass paid, a price premium for the Camera Products based on Lorex's representations regarding privacy, security, and user control, despite the availability of comparable, lower-priced alternatives.

165. Defendants possessed exclusive knowledge of the material facts relating to the Camera Products' backend data practices, system architecture, and security risks, and failed to disclose such information to consumers.

166. Defendants have engaged and continue to engage in deceptive conduct in violation of GBL section 349.

167. As a direct and proximate result of Defendants' deceptive conduct, the Plaintiff and New York Subclass suffered actual injury, including overpayment, loss of the benefit of the bargain, and purchase of products that were worth less than represented.

168. Defendants intended that the Plaintiff and New York Subclass rely on their misrepresentations and omissions regarding the privacy, security, and data-handling capabilities of the Camera Products, and they reasonably did so.

169. GBL § 349 applies to the Plaintiff and New York Subclass because New York has a strong interest in regulating deceptive business practices affecting its residents. Lorex conducts substantial business directed toward New York consumers, and its challenged conduct caused injury within the state.

170. Defendants' conduct has caused and continues to cause immediate and irreparable harm to the New York Plaintiffs and New York Subclass and will continue to deceive consumers unless enjoined by this Court.

171. Unless Defendants are enjoined from continuing their deceptive acts and practices, the New York Plaintiffs, the New York Subclass, and the public will continue to suffer harm.

172. Pursuant to GBL sections 349(h) and 350-e, Plaintiff Hill and New York Subclass seek injunctive relief, declaratory relief, full refund, compensatory and punitive damages, actual damages or \$50 (whichever is greater), statutory and treble damages, and attorneys' fees.

COUNT III
VIOLATION OF NEW YORK DECEPTIVE ACTS AND PRACTICES,
NEW YORK GENERAL BUSINESS LAW § 350
(On Behalf of Plaintiff Hill and the New York Class)

173. Plaintiff Hill and the Subclass re-allege and incorporate the allegations above as if set forth herein.

174. GBL section 350 prohibits false advertising in the conduct of any business, trade, or commerce.

175. Pursuant to GBL section 350, false advertising is defined as “advertising, including labeling, or a commodity... if such advertising is misleading in a material respect. ... [considering] representations made by statement, word [or] design [and] the extent to which the advertising fails to reveal facts material in the light of such representations.”

176. Defendants knew or should have known that their Camera Products did not possess the privacy, security, and data-protection features advertised to consumers, including representations that users could “keep recordings private and in [their] control,” that recordings were stored locally, and that video feeds were encrypted.

177. Defendants affirmatively misrepresented, actively concealed, and failed to disclose material facts regarding the collection, transmission, storage, and security of images, video feeds, and related data generated by the Camera Products, including that such data could be transmitted to or accessed by Lorex or third parties without adequate disclosure or consumer consent.

178. The facts misrepresented and omitted by Defendants were material. The Plaintiff, the New York Subclass, and reasonable consumers would have considered such information important when deciding whether to purchase the Camera Products and how to deploy them within their homes, including in sensitive locations. Had they known the true nature of Lorex’s data-handling and security practices, they would not have purchased the Camera Products or would not have paid a premium price.

179. Defendants charged, and the Plaintiff and New York Subclass paid, a premium price for the Camera Products based on Lorex’s advertising and promotional claims regarding privacy, security, and user control, despite the availability of comparable, lower-priced alternatives that did not make such representations.

180. As a direct and proximate result of Defendants’ false advertising, the Plaintiff and New York Subclass suffered actual damages, including overpayment and the purchase of products that were worth less than represented and that they would not have purchased at all had they known the truth.

181. Defendants' violations of GBL § 350 caused and continue to cause harm to the Plaintiff and the New York Subclass, and such harm will continue unless Lorex is enjoined from continuing to falsely advertise the privacy, security, and data-protection features of its Camera Products.

182. Defendants' false advertising has also injured the public at large in New York, as consumers were exposed to and relied upon Lorex's advertising while unaware of material omissions regarding the collection, transmission, and security of their images and video data. These omissions deprived consumers of the ability to make informed purchasing decisions and created a false impression that the Camera Products were private, secure, and suitable for use in sensitive environments.

183. Defendants' conduct thus caused real-world harm and poses an ongoing risk of further injury if not enjoined.

184. Pursuant to GBL section 350-e, the Plaintiff and New York Subclass seek injunctive relief, declaratory relief, full refund, actual and punitive damages or \$500 (whichever is greater), statutory damages of three times the actual damages (up to \$10,000), and attorneys' fees.

COUNT IV
VIOLATION OF CALIFORNIA'S FALSE ADVERTISING LAW
CAL. BUS. & PROF. CODE §§ 17500, ET SEQ.
(On behalf of Plaintiff Portman and the California Subclass)

185. Plaintiff Portman and the Subclass incorporate by reference each preceding and succeeding paragraph as though fully set forth at length herein.

186. Defendants' conduct as alleged herein violates California's False Advertising Law ("FAL"), Cal. Bus. & Prof. Code §§ 17500, et seq., which makes it unlawful for a business to make, disseminate, or cause to be made or disseminated to the public "any statement, concerning...personal property...which is untrue or misleading, and which is known, or which by

the exercise of reasonable care should be known, to be untrue or misleading.” Cal. Bus. & Prof. Code § 17500.

187. The Camera Products at issue are “personal property” within the meaning of the FAL.

188. The Camera Products’ packaging emphasized that the Camera Products were private and secure

189. Any express or implied representation, material omission of information, or failure to correct a past material misrepresentation or omission regarding the privacy of the Camera Products is a “statement[] concerning personal property” within the meaning of the FAL.

190. Defendants violated the FAL by making, disseminating, and causing to be made or disseminated to the public statements about the privacy of the Camera Products that were “untrue or misleading” within the meaning of the FAL.

191. Defendants failed to disclose accurate information regarding the Camera Products generally. Defendants made, disseminated, or caused to be made or disseminated untrue or misleading public statements about the Camera Products in numerous forums, including but not limited to Defendants’ website. Defendants falsely stated that there were robust privacy mechanisms built into the Camera Products, when in fact they omitted the known risk.

192. Defendants knew, or by the exercise of reasonable care, should have known that each of those statements was untrue, misleading, and likely to deceive the public at or near the time it was made or disseminated, and at all times thereafter.

193. Defendants’ marketing materials fail to disclose details of the Camera Products and that their advertising communicated falsehoods, including that consumers would be safe.

194. As a result of Defendants’ FAL violations and the harm caused thereby, Plaintiff

Portman and Subclass Members are entitled to and seek (a) injunctive relief to protect the consuming public by prohibiting Defendants from engaging in its past and ongoing acts, omissions, and conduct that violate the FAL; (b) restitution of the full value of all monies and other consideration that Plaintiff and Class Members paid Defendants for the purchase of the Camera Products, including any reduced value of Plaintiff Portman's and Subclass Members' cameras, and disgorgement of the profits Defendants derived from its wrongful conduct; and (c) an award of reasonable attorneys' fees under Cal. Code Civ. Proc. § 1021.5.

COUNT V
VIOLATION OF CALIFORNIA'S CONSUMER LEGAL REMEDIES ACT CAL. BUS. &
PROF. CODE §§ 1750, ET SEQ.
(On behalf of Plaintiff Portman and the California Subclass)

195. Plaintiff Portman repeats, re-alleges, and incorporates each and every factual allegation contained in all previous paragraphs as if fully set forth herein.

196. California's Consumer Legal Remedies Act ("CLRA") prohibits "unfair methods of competition and unfair or deceptive acts or practices" in connection with the sale or lease of goods. Cal. Civ. Code § 1770.

197. The CLRA is to be liberally construed and applied to protect consumers against unfair and deceptive business practices. Cal. Civ. Code § 1760.

198. Plaintiff, and each California Subclass member, is a "consumer," as defined in Cal. Civ. Code § 1761(d).

199. The Camera Products are a "good[]," as defined in Cal. Civ. Code § 1761(a).

200. Defendants are "persons" as defined in Cal. Civ. Code § 1761(c).

201. Plaintiff Portman and each proposed Subclass member's purchase of Defendants' Camera Products constituted a "transaction" as defined in Cal. Civ. Code § 1761(e).

202. Defendants' actions were unfair, unlawful, and deceptive under the CLRA.

Defendants made false representations about the Camera Products. Defendant falsely represented that the Camera Products met specific safety standards, while the Camera Products did not meet these standards and did not contain the advertised safety. Cal. Civ. Code § 1770(a)(7).

203. Defendants' actions were unfair, unlawful, and deceptive under the CLRA as Defendants fraudulently advertised their Camera Products and falsely advertised that the Camera Products would contain certain qualities but sold consumers the Camera Products that were different than what was advertised. Cal. Civ. Code § 1770(a)(9).

204. Defendants' actions were unfair, unlawful, and deceptive under the CLRA as Defendants promised that Plaintiff and the California Subclass Members that the Camera Products were private. Cal. Civ. Code § 1770(a)(7).

205. Defendants' actions were unfair, unlawful, and deceptive under the CLRA as Defendants inserted untrue statements about safety on its website. Cal. Civ. Code § 1770(a)(14).

206. Defendants deceived Plaintiff Portman and the California Subclass by representing that their Camera Product and services have certain characteristics, benefits, and qualities, which they do not have. In doing so, Defendants intentionally misrepresented and concealed material facts from Plaintiff Portman and the California Subclass. Defendants falsely advertised that their Camera Products had higher quality standards than those that were ultimately delivered. These misrepresentations and concealments were committed with the intention of deceiving Plaintiff Portman and the California Subclass and depriving them of their legal rights and money.

207. Defendants' claims about their products have led and continue to lead consumers to reasonably believe that Defendants' Camera Products were private.

208. Plaintiff and the California Subclass have suffered injury-in-fact as a result of and in reliance upon Defendants' false representations and have lost money as a result of Defendants'

unfair, and unlawful conduct. Plaintiff and the California Subclass would not have bought Defendants' Camera Products, or would have paid significantly less for them, had they known that they would receive a product that was not secure.

209. Defendants' actions as described herein were done with conscious disregard for Plaintiff Portman and the rights of California Subclass Members, and Defendants intentionally represented that the Camera Product or services have approval, characteristics, uses, benefits, or quantities which they do not have.

210. Plaintiff and California Subclass Members seek all monetary and nonmonetary relief allowed by law, including restitution, reasonable attorneys' fees and costs under California Code of Civil Procedures § 1021.5, and injunctive relief under the CLRA pursuant to Cal. Civ. Code § 1782(d) and other appropriate equitable relief.

COUNT VI
UNJUST ENRICHMENT

**(On Behalf of the National Class and, alternatively, the Illinois Class, the
New York Class, and the California Class)**

211. Plaintiffs Portman, Hill, Shah, and the Class re-allege and incorporate the allegations contained in all previous paragraphs as if fully set forth herein.

212. Plaintiffs and the other members of the Class conferred benefits on Lorex by purchasing the Camera Products.

213. Lorex has been unjustly enriched in retaining the revenues derived from the purchase of the Products by Plaintiffs and the other members of the Class.

214. Retention of those monies under these circumstances is unjust and inequitable because Lorex's labeling of the Products was misleading to consumers, which caused injuries to Plaintiffs and the other members of the Class because they would have not purchased the Camera Products if Lorex had disclosed that the Camera Products were not secure.

215. Because Lorex's retention of the non-gratuitous benefits conferred on them by Plaintiffs and the other members of the Class is unjust and inequitable, Lorex must pay restitution to Plaintiffs and the other members of the Class for their unjust enrichment, as ordered by the Court.

COUNT VII
BREACH OF IMPLIED WARRANTY
(On Behalf of Plaintiffs and All Class Members)

216. Plaintiffs repeat and reallege each and every allegation contained in the foregoing paragraphs as if fully set forth herein.

217. Defendants manufactured, marketed, labeled, distributed, and sold the Camera Product, as part of its overall business.

218. The Camera Product is considered a "good" under the relevant laws.

219. For goods to be merchantable under U.C.C. § 2-314, they must (a) pass without objection in the trade under the contract description; (b) in the case of fungible goods, are of fair average quality within the description; (c) are fit for the ordinary purposes for which such goods are used; and (d) run, within the variations permitted by the agreement, of even kind, quality and quantity within each unit and among all units involved.

220. The ordinary purpose of the Camera Products includes use inside and around private residences, including bedrooms and other sensitive living spaces, in reliance on Defendants' express representations that the products were private, secure, and suitable for such use. Merchantability, therefore, required that the Camera Products operate in a manner consistent with those representations and with reasonable consumer expectations for residential security cameras marketed for privacy-sensitive environments.

221. Defendants breached the implied warranty of merchantability because, as alleged herein, the Camera Products failed to conform to their ordinary purpose and advertised

characteristics. Specifically, the products operated through undisclosed technical architectures and data practices inconsistent with Defendants' representations regarding local control, privacy, and security.

222. Defendants had notice of the breach through consumer complaints, internal testing and quality assurance processes, and publicly available reporting and regulatory scrutiny concerning the privacy and security characteristics of network-connected camera products using similar hardware, firmware, and backend infrastructure.

223. The Camera Products were not private as promised. Plaintiffs and each of the members of the Class were injured as a result. Defendants thereby breached the following state warranty laws: Alabama: Ala. Code § 7-2-314 (2024) (Implied Warranty: Merchantability; Usage of Trade); Alaska: Alaska Stat. § 45.02.314 (2024) (Implied Warranty: Merchantability; Usage of Trade); Arizona: Ariz. Rev. Stat. Ann. § 47-2314 (2024) (Implied Warranty: Merchantability; Usage of Trade); Arkansas: Ark. Code Ann. § 4-2-314 (2024) (Implied Warranty: Merchantability; Usage of Trade); California: Cal. Com. Code § 2314 (2024) (Implied Warranty: Merchantability; Usage of Trade); Colorado: Colo. Rev. Stat. § 4-2-314 (2024) (Implied Warranty: Merchantability; Usage of Trade); Connecticut: Conn. Gen. Stat. § 42a-2-314 (2024) (Implied Warranty: Merchantability; Usage of Trade); Delaware: 6 Del. C. § 2-314 (2024) (Implied Warranty: Merchantability; Usage of Trade); Florida: Fla. Stat. § 672.314 (2024) (Implied Warranty: Merchantability; Usage of Trade); Georgia: Ga. Code Ann. § 11-2-314 (2024) (Implied Warranty: Merchantability; Usage of Trade); Hawaii: HRS § 490:2-314 (2024) (Implied Warranty: Merchantability; Usage of Trade); Idaho: Idaho Code § 28-2-314 (2024) (Implied Warranty: Merchantability; Usage of Trade); Illinois: 810 ILCS 5/2-314 (2024) (Implied Warranty: Merchantability; Usage of Trade); Indiana: Burns Ind. Code Ann. § 26-1-2-314 (2024) (Implied

Warranty: Merchantability; Usage of Trade); Iowa: Iowa Code § 554.2314 (2024) (Implied
Warranty: Merchantability; Usage of Trade); Kansas: K. S. A. § 84-2-314 (2024) (Implied
Warranty: Merchantability; Usage of Trade); Kentucky: KRS § 355.2-314 (2024) (Implied
Warranty: Merchantability; Usage of Trade); Louisiana: La. C.C. Art. 2520, 2524 (2024)
(warranty against redhibitory defects; thing fit for ordinary use); Maine: 11 M.R.S. § 2-314 (2024)
(Implied Warranty: Merchantability; Usage of Trade); Maryland: Md. Commercial Law Code
Ann. § 2-314 (2024) (Implied Warranty: Merchantability; Usage of Trade); Massachusetts: ALM
GL ch. 106, § 2-314 (2024) (Implied Warranty: Merchantability; Usage of Trade); Michigan:
MCLS § 440.2314 (2024) (Implied Warranty: Merchantability; Usage of Trade); Minnesota:
Minn. Stat. § 336.2-314 (2024) (Implied Warranty: Merchantability; Usage of Trade); Mississippi:
Miss. Code Ann. § 75-2-314 (2024) (Implied Warranty: Merchantability; Usage of Trade);
Missouri: § 400.2-314 R.S.Mo. (2024) (Implied Warranty: Merchantability; Usage of Trade);
Montana: 30-2-314, MCA (2024) (Implied Warranty: Merchantability; Usage of Trade);
Nebraska: R.R.S. Neb. (U.C.C.) § 2-314 (2024) (Implied Warranty: Merchantability; Usage of
Trade); Nevada: Nev. Rev. Stat. Ann. § 104.2314 (2024) (Implied Warranty: Merchantability;
Usage of Trade); New Hampshire: RSA § 382-A:2-314 (2024) (Implied Warranty:
Merchantability; Usage of Trade); New Jersey: N.J. Stat. § 12A:2-314 (2024) (Implied Warranty:
Merchantability; Usage of Trade); New Mexico: N.M. Stat. Ann. § 55-2-314 (2024) (Implied
Warranty: Merchantability; Usage of Trade); New York: NY CLS UCC § 2-314 (McKinney 2024)
(Implied Warranty: Merchantability; Usage of Trade); North Carolina: N.C. Gen. Stat. § 25-2-314
(2024) (Implied Warranty: Merchantability; Usage of Trade); North Dakota: N.D. Cent. Code
§ 41-02-31 (2024) (Implied Warranty: Merchantability; Usage of Trade); Ohio: ORC Ann.
§ 1302.27 (2024) (Implied Warranty: Merchantability; Usage of Trade); Oklahoma: 12A Okl.

St. § 2-314 (2024) (Implied Warranty: Merchantability; Usage of Trade); Oregon: ORS § 72.3140 (2024) (Implied Warranty: Merchantability; Usage of Trade); Pennsylvania: 13 Pa. Cons. Stat. § 2314 (2024) (Implied Warranty: Merchantability; Usage of Trade); Rhode Island: R.I. Gen. Laws § 6A-2-314 (2024) (Implied Warranty: Merchantability; Usage of Trade); South Carolina: S.C. Code Ann. § 36-2-314 (2024) (Implied Warranty: Merchantability; Usage of Trade); South Dakota: S.D. Codified Laws § 57A-2-314 (2024) (Implied Warranty: Merchantability; Usage of Trade); Tennessee: Tenn. Code Ann. § 47-2-314 (2024) (Implied Warranty: Merchantability; Usage of Trade); Texas: Tex. Bus. & Com. Code Ann. § 2.314 (2024) (Implied Warranty: Merchantability; Usage of Trade); Utah: Utah Code Ann. § 70A-2-314 (2024) (Implied Warranty: Merchantability; Usage of Trade); Vermont: 9A V.S.A. § 2-314 (2024) (Implied Warranty: Merchantability; Usage of Trade); Virginia: Va. Code Ann. § 8.2-314 (2024) (Implied Warranty: Merchantability; Usage of Trade); Washington: Rev. Code Wash. (ARCW) § 62A.2-314 (2024) (Implied Warranty: Merchantability; Usage of Trade); West Virginia: W. Va. Code § 46-2-314 (2024) (Implied Warranty: Merchantability; Usage of Trade); Wisconsin: Wis. Stat. § 402.314 (2024) (Implied Warranty: Merchantability; Usage of Trade); Wyoming: Wyo. Stat. § 34.1-2-314 (2024) (Implied Warranty: Merchantability; Usage of Trade); and District of Columbia: D.C. Code § 28:2-314 (2024) (Implied Warranty: Merchantability; Usage of Trade).

224. Defendants' breach of the implied warranty of merchantability was uniform across jurisdictions. Defendants designed, manufactured, and distributed the Camera Products according to common specifications. They marketed the products using materially identical representations concerning privacy, security, and suitability for residential use. The defects alleged herein arise from the same course of conduct and affect all purchasers in the same manner, regardless of the state in which the purchase occurred.

225. As a direct and proximate result of Defendants' breach of the implied warranty, Plaintiffs and Class Members were damaged in the amount of the price they paid for the Camera Products.

REQUEST FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of the Class Members, pray for judgment and relief against Lorex as follows:

1. For an order declaring: (i) this is a class action pursuant to Rule 23 of the Federal Rules of Civil Procedure on behalf of the proposed Class described herein; and (ii) appointing Plaintiffs to serve as representative for the Class and Plaintiffs' counsel to serve as Class Counsel;
2. For an order enjoining Lorex from continuing to engage in the unlawful conduct set forth herein;
3. For an order awarding restitution of the monies Lorex wrongfully acquired by its illegal and deceptive conduct;
4. For an order requiring disgorgement of the monies Lorex wrongfully acquired by its illegal and deceptive conduct;
5. For compensatory and punitive damages, including actual and statutory damages, arising from Lorex's wrongful conduct and illegal conduct;
6. For an award of reasonable attorneys' fees and costs and expenses incurred in the course of prosecuting this action; and
7. For such other and further relief as the Court deems just and proper.

JURY DEMAND

Pursuant to Federal Rule of Civil Procedure 38(b), Plaintiffs demand a trial by jury of all claims in this complaint so triable.

Respectfully submitted,

Dated: January 16, 2026

LEVI & KORSINSKY, LLP

By: /s/ Mark S. Reich
Mark S. Reich (MR-4166)
Michael N. Pollack (6173272)
Gary Ishimoto*
33 Whitehall Street, 27th Floor
New York, NY 10004
Telephone: 212-363-7500
Facsimile: 212-363-7171
Email: mreich@zlk.com
Email: mpollack@zlk.com
Email: gishimoto@zlk.com

Counsel for Plaintiffs

**Pro Hac Vice Forthcoming*

ClassAction.org

This complaint is part of ClassAction.org's searchable class action lawsuit database and can be found in this post: [Lorex Home Security Cameras Made With Tech From Banned Chinese Company, Class Action Lawsuit Alleges](#)
