Your Chinese-made Children's Monitor Is Spying on Your Family

By R. Russell Walker

June 2026

Rainey Center

Right now, in nurseries and bedrooms across America, a camera is watching your child sleep.

You put it there. You paid for it. You trusted it. And there is a growing body of legal evidence suggesting that someone else is watching too—someone in Beijing who has no business being in your child's room, but who has built a legal, technical, and commercial infrastructure specifically designed to make sure they can be.

This isn't a spy thriller. It's a Tuesday night in an American home. And the device you bought at Costco to keep your baby safe may be the most intimate surveillance tool the Chinese Communist Party has ever deployed.

The Monitor Knows Everything

Think about what your baby monitor actually captures. It sees your child's face. It records your child's first words. It picks up your conversations with your spouse after a hard day, your arguments, your worries, your most unguarded moments. It knows when you're home and when you're not. It maps your sleep schedule, your daily routine, the layout of your most private spaces. It listens, without pause, to the heartbeat of your family's life.

Now consider who else might be listening.

Missouri AG Catherine Hanaway's lawsuit against Lorex, one of the country's leading baby monitor manufacturers, alleges that the company's firmware routes directly back to servers controlled by Dahua, its Chinese parent company.[1] Dahua was designated a Chinese Military Company by the Pentagon in 2022.[2] Texas AG Ken Paxton's lawsuit against TP-Link makes parallel allegations about home routers, alleging the company's firmware phones home to Chinese-controlled servers.[3] Independent researchers who analyzed Lorex firmware found it connecting to Dahua-controlled domains—not occasionally, not accidentally, but systematically.[4]

Your baby monitor is not just a camera. According to these lawsuits, it is a live feed into a data pipeline that runs straight to a company the U.S. government has identified as a threat to national security. The nursery you painted, the crib you assembled, the monitor you positioned just so—all of it potentially visible to people you will never meet, in a country whose government has enshrined in law its right to access exactly this kind of data.

1 Missouri Attorney General's Office, Press Release: Missouri Attorney General Hanaway Sues Baby Monitor Manufacturer for Concealing Links to Chinese Military, June 15, 2026. ago.mo.gov

2 Washington Examiner, Missouri sues baby monitor maker for hiding ties to Chinese military, June 15, 2026. The Pentagon designated Zhejiang Dahua Technology a Chinese Military Company in 2022 under Section 1260H of the National Defense Authorization Act.

3 Texas Attorney General's Office, Press Release: Attorney General Paxton Sues TP-Link for Allowing the CCP to Access Americans' Devices, February 17, 2026. texasattorneygeneral.gov

4 ClassAction.org, Lorex Home Security Cameras Made With Tech From Banned Chinese Company, Class Action Lawsuit Alleges, January 22, 2026; Nebraska Public Media, Nebraska AG Files Lawsuit, Offers Warning About Lorex Home Security Cameras, September 23, 2025. Nebraska AG Mike Hilgers stated: "The firmware of these particular products are still made by Dahua. They're still connected to Dahua."

The Law That Makes It Legal—In China

Here is the fact that every parent buying a baby monitor needs to understand: under Chinese law, no Chinese company can say no to Beijing.

China's 2017 National Intelligence Law makes that explicit. Article 7 states: *"All organizations and citizens shall support, assist, and cooperate with national intelligence efforts in accordance with law."*[5] There are no exceptions for private companies. No

5 People's Republic of China, National Intelligence Law of the People's Republic of China, Article 7, enacted June 28, 2017 (amended 2018). Full English translation available at chinalawtranslate.com

carve-outs for consumer electronics manufacturers. No opt-outs for firms that prefer to market themselves as trustworthy, family-friendly brands in Western stores.

The U.S. Department of Homeland Security has formally recognized this threat, stating in its own advisory that Article 7 *"compels all PRC firms and entities to support, assist, and cooperate with the PRC intelligence services, creating a legal obligation for those entities to turn over data collected abroad and domestically to the PRC."*[6]

Any organization. Any citizen. Support, assist, and cooperate.

That means Lorex, despite its North American branding and its reassuring privacy promises, carries legal obligations through its ties to Dahua that run directly to Chinese state intelligence.[7] It means the company that made the device watching your child breathe tonight is legally compelled to hand over whatever Beijing asks for. The soft glow of that monitor on your nursery wall is, under Article 7, a window that opens both ways.

This is not a hypothetical. It is the law of the People's Republic of China, enacted June 28, 2017, actively enforced, and never repealed.[8]

6 U.S. Department of Homeland Security, Data Security Business Advisory, December 2020. dhs.gov

7 Fox4KC / Missouri AG Office, Missouri Attorney General Sues Baby Monitor Company Over Alleged Ties to China, June 2026.

8 National People's Congress of the PRC, National Intelligence Law, enacted June 27, 2017, effective June 28, 2017.

The Backdoor in the Nursery

The legal obligation is one thing. The technical mechanism is another and it is equally deliberate.

Georgetown University's Security Studies Review documented that in a five-year period, there were at least a half dozen confirmed cases of pre-installed malware appearing on electronics manufactured in China, creating backdoors that collected sensitive information without users' knowledge

or consent.[9] Chinese state-sponsored hacking groups have gone further, embedding malicious firmware implants directly into consumer networking equipment. Check Point Research documented exactly this in 2023, when a Chinese APT group dubbed "Camaro Dragon" deployed a custom firmware backdoor—dubbed "Horse Shell"—specifically engineered for TP-Link routers, using it to conduct cyberattacks against government targets.[10] Congress cited this research directly in its bipartisan letter to the Commerce Department demanding action.[11]

More recently, Google's Mandiant division documented a China-linked hacking campaign deploying "Brickstorm" malware on edge devices and network infrastructure across the United States, with victims taking an average of 393 days to even detect the intrusion, nearly thirteen months of invisible access.[12] CISA confirmed the campaign in December 2025.[13]

Your baby monitor records your child. The firmware sends that data home. The backdoor keeps the door open. And somewhere in a data center you will never see, recordings of your child's face, your child's voice, and your family's most intimate hours sit on servers that Chinese intelligence services can access whenever they choose.

Lorex markets its cameras as "private by design."[14] Private for whom, exactly?

---

9 Georgetown Security Studies Review, Flawed by Design: Electronics with Pre-Installed Malware, May 23, 2018. georgetownsecuritystudiesreview.org ("In the past five years, there have been at least a half dozen cases of pre-installed malware appearing on electronics built in China.")

10 Check Point Research, Malware in the Wild: Horse Shell—A New TP-Link Firmware Implant Used by Chinese State-Sponsored APT Group "Camaro Dragon", May 2023.

11 House Select Committee on the CCP, Bipartisan Letter to Secretary of Commerce Gina Raimondo, August 13, 2024. chinaselectcommittee.house.gov

12 Google Mandiant / Cybersecurity Dive, China-linked groups are using stealthy malware to hack software suppliers, September 24, 2025. cybersecuritydive.com

13 CISA / The Hacker News, CISA Reports PRC Hackers Using BRICKSTORM for Long-Term Access in U.S. Systems, December 4, 2025. thehackernews.com

14 Missouri AG Office, op. cit. ("Lorex tells families its video cameras are 'private by design' while concealing ties to a Chinese military company.")

The Bigger Picture: Your Child's Voice Is AI Training Data

Large language models, the AI systems powering the next generation of technology, are only as capable as the data they're trained on. Chinese AI developers are in a global race to accumulate more of it: more voices, more faces, more behavioral patterns, more of the raw human data that teaches machines to think.

Your baby monitor is a perfect collection device. It captures voice. It captures faces. It captures the ambient patterns of human life in its most unguarded setting. Multiplied across millions of American homes, data flowing from Chinese-linked baby monitors represents an extraordinary training dataset, one that American parents funded, American retailers distributed, and American families delivered directly into the hands of Chinese AI developers explicitly racing to surpass American capabilities.

Beijing has formally declared AI supremacy a national strategic priority.[15] And unlike American companies, which must navigate privacy laws and data ethics debates, Chinese AI developers operate under the PRC's Cybersecurity Law, which requires firms to store data locally and provide authorities access upon request, with no meaningful constraint on how that data, including data harvested from American homes, may subsequently be used.[16]

This is unrestricted warfare as described by PLA colonels Qiao Liang and Wang Xiangsui in their 1999 strategic manifesto published by the People's Liberation Army Literature and Arts Publishing House: not tanks and missiles, but technology, law, and commerce working in concert to extract strategic advantage from an adversary who doesn't realize the battle is happening.[17] Your nursery is a battlefield. Your child's voice is a resource. And the extraction has been underway for years.

15 China's State Council, New Generation Artificial Intelligence Development Plan, July 2017. Beijing formally declared the goal of becoming the world's primary AI innovation center by 2030.

16 People's Republic of China, Cybersecurity Law, effective June 1, 2017; Georgetown Security Studies Review, op. cit.

17 Qiao Liang and Wang Xiangsui, Unrestricted Warfare (Beijing: PLA Literature and Arts Publishing House, February 1999). Translated by the Foreign Broadcast Information Service (FBIS). Available at archive.org

What Congress Must Do—Now

The lawsuits from Texas and Missouri are necessary. They are not sufficient.

Congress must pass an immediate, comprehensive ban prohibiting American citizen data, especially data captured in private homes, from being stored in Chinese data centers or on servers accessible to Chinese state entities. Not a disclosure requirement. Not a voluntary framework. A hard ban, with criminal penalties for executives who route around it and supply chain verification requirements that go beyond assembly locations to the origin of every component and every line of code.

The FCC must remove Chinese-linked consumer devices from American shelves, not just from federal procurement lists. The FCC itself acknowledged in a March 2026 national security determination that foreign-produced routers *"present additional and unacceptable risks to Americans"* and were *"directly implicated in the Volt, Flax, and Salt Typhoon cyberattacks which targeted critical American communications, energy, transportation, and water infrastructure."*[18] A backdoored baby monitor in a government office and a backdoored baby monitor in a nursery are the same threat.

Every Chinese-linked company selling connected devices in the United States must submit to mandatory, independent firmware audits before their products touch American home networks. If they refuse, they don't sell here.

And Congress must formally reckon with what China's 2017

18 Federal Communications Commission, National Security Determination on the Threat Posed by Foreign-Produced Routers, March 2026. fcc.gov

National Intelligence Law actually means: that under Article 7, no Chinese-linked company is truly a private company. Every one of them is a potential instrument of Chinese state intelligence. American law needs to treat them accordingly, not product by product, lawsuit by lawsuit, but with a comprehensive legal framework that matches the scope of the threat.

TP-Link controls roughly 65 percent of the American consumer router market.[19] Lorex cameras are sold at Costco, Best Buy, Amazon, Staples, and Office Depot.[20] These are not fringe products. They are in the majority of American homes, in the most intimate rooms, capturing the most private moments of American family life.

The 2017 National Intelligence Law is not a secret. Article 7 is not buried in fine print. Beijing published it openly, enforces it actively, and built an entire consumer technology export strategy around the data collection infrastructure it enables. The only people who haven't fully reckoned with what it means are the American consumers buying these products, and the American lawmakers who have yet to make that reckoning their problem to solve.

Ban the data transfers. Audit the hardware. Remove the backdoors. Hold every company, and every retailer that profits from selling them, accountable for what flows through the devices they put in our homes.

The law China uses to reach into your nursery has been sitting in plain sight since 2017.

It's past time we read it—and act like we mean it.

19 Engadget / Wall Street Journal, TP-Link Routers Are Being Investigated by Several U.S. Authorities, December 18, 2024.

20 Missouri AG Office, op. cit.; Nebraska AG Office, op. cit. Lorex products are sold at Best Buy, Staples, Costco, Menards, Micro Center, Office Depot, Amazon, and directly through Lorex's website.

Rainey
Center

info@raineycenter.org
raineycenter.org