State AGs May Extend Their Reach To Nat'l Security Concerns

By **Joshua Turner, Sara Baxenberg and Joel Nolette** (November 24, 2025)

Joshua Turner

Sara Baxenberg

Joel Nolette

On Oct. 29, the Texas Attorney General announced that he had opened an investigation into the domestic home security camera manufacturer Lorex Corp. for potentially violating state data privacy law.

The alleged violation stemmed from Lorex's use of components supplied by a Chinese company, Zhejiang Dahua Technology Co., that is affiliated with the Chinese Communist Party, and the video surveillance and telecommunications equipment of which is restricted in the U.S. by the Federal Communications Commission.

If ultimately successful, the state's legal theory would restrict companies' abilities to build and sell communications technologies in Texas far more than the FCC regime that inspired the investigation.

This investigation is the latest in a recent uptick of actions taken by state attorneys general using state consumer protection laws prohibiting unfair and deceptive acts and practices, or UDAP, against companies because of their affiliations with entities headquartered in or otherwise associated with foreign adversary nations.

States and the Federal Trade Commission routinely apply UDAP laws to bring enforcement actions against companies that engage in undisclosed transfers of consumer data, fail to take commercially reasonable data security measures, or make material misrepresentations about their data privacy or security practices.

But these recent actions are unusual in their explicit acknowledgment that they are driven by national security and trade policy concerns.

Federal agencies like the FCC and the U.S. Department of Commerce already heavily regulate this arena. But those regulations have not occupied the field, and state officials are increasingly looking to use broadly worded state UDAP statutes to address national security concerns on their own — sometimes, as with the Lorex investigation, even more aggressively than the federal government.

While such actions are in tension with public remarks by FTC Chairman Andrew Ferguson urging that "the broad scope of consumer protection laws" should not be used to "solve larger social, economic or political issues facing our respective nations," state officials have wide latitude in applying these state laws.[1]

Companies with foreign supply-chain risk exposure need a comprehensive risk-management strategy that accounts for this emerging enforcement trend in the states.

Starting in 2019, Congress directed federal agencies, including the FCC, to restrict the use of certain video surveillance and telecommunications equipment produced by several entities, including Dahua, with affiliations to foreign adversary nations — mainly China.[2]

In short order, Dahua was added to the Commerce Department's Entity List, resulting in export controls against the company, and federal contractors were barred from using the relevant Dahua equipment.

The next year, Congress required the FCC to create and maintain a "covered list" to identify equipment and services that were deemed by appropriate federal agencies and interagency bodies to pose an unacceptable national security risk.[3]

In its current form, the FCC's covered list includes equipment produced by several entities, including Dahua.[4] The covered list initially just restricted the equipment and services eligible for use with Universal Service Fund disbursements, but the FCC has in the years since expanded the way in which the list is used.

Because of its inclusion on the covered list, Dahua now also cannot obtain any new FCC authorizations for the named equipment — a necessary precursor for the import, marketing, sale or use of radiofrequency-emitting equipment in the U.S.

Although the FCC authorizations that Dahua received before the 2023 rule changes are still in effect, the FCC may in the future elect to revoke those authorizations, or limit the import or marketing of the equipment.

The FCC continues to be active in this space. Most recently, on Oct. 29, the commission issued an order clarifying its position that "produced by" should be interpreted broadly to include not only equipment wholly manufactured by a covered entity but also equipment that a covered entity had a substantial hand in developing or producing.

The order also clarifies that modular transmitters can be covered equipment, and so products by noncovered entities that incorporate those transmitters as components are themselves covered and ineligible for FCC authorization.[5] And it tees up for comment further potential restrictions on other component parts, beyond modular transmitters.

Though extensive, this federal regulatory scheme does not comprehensively ban equipment produced by covered list entities. For Dahua and certain other manufacturers, the telecommunications and video surveillance equipment they produce is covered only when used for specified purposes — in particular, "public safety, security of government facilities, physical security surveillance of critical infrastructure, and other national security purposes."

Thus, many consumer products are not encompassed by this regulatory regime at all, even if those products are manufactured, in whole or in part, by covered entities.

And, as noted above, the covered list is at least currently only prospective in nature. The addition of an entity to the covered list does not retroactively affect preexisting equipment authorizations that allow the equipment to be sold into the U.S. market, though this is an area where the FCC has reserved its authority to take action in the future.

But particularly in the past year, some state attorneys general have decided not to wait for further federal government action and have turned to broad state consumer protection and trade practices statutes to expand on this federal regulatory scheme. These efforts target companies based on connections to Chinese products or manufacturers, even where the companies and their products appear to comply with current federal national security and supply chain laws.

For instance, in June 2025, Florida Attorney General James Uthmeier announced an investigation into Florida-based Epsimed concerning its relabeling and reselling of medical patient monitors manufactured by Contec Medical Systems, a Chinese medical device company.[6]

In his announcement, Uthmeier alleged that Epsimed's monitors had undisclosed security vulnerabilities by which they were secretly transmitting patient data to China,[7] potentially amounting to "unconscionable acts or practices," or "unfair or deceptive acts" under Florida's Deceptive and Unfair Trade Practices Act.[8]

The federal Cybersecurity and Infrastructure Security Agency issued a fact sheet on cybersecurity vulnerabilities in Contec firmware in January 2025, and the U.S. Food and Drug Administration issued proposed mitigations, but the federal government at the time had not banned the products.[9]

Also, in September of this year, Nebraska Attorney General Mike Hilgers filed a lawsuit against Lorex Corp., the home-security cameras of which are sold in major retail stores across the state.[10]

In his complaint, Hilgers alleged Maryland-headquartered Lorex markets its cameras as secure and appropriate for use in sensitive spaces such as children's bedrooms, but that this is misleading because "Dahua's involvement" in the product "creates serious security and privacy risks."

In particular, the complaint alleged Dahua — which the complaint notes is on the FCC covered list as well as other government entity lists — supplies components for these cameras that contain security vulnerabilities allowing unauthorized remote viewing of the cameras' video and audio feeds.[11]

The complaint included claims of "unfair or deceptive acts or practices" under Nebraska's Consumer Protection Act and of "unconscionable acts or practices" under the state's Uniform Deceptive Trade Practices Act.[12]

And most recently, on Oct. 29, Texas Attorney General Ken Paxton followed suit by announcing a consumer protection investigation into Lorex for its use of Dahua components, invoking as justification the FCC's "restrictions on Dahua's products due to national security risks."[13]

As with the Nebraska complaint, the Texas investigation seeks to leverage federal concern about Dahua into areas beyond the literal federal restrictions. Dahua is on the FCC's covered list when it comes to certain public safety and national security uses, but the federal government has to date not gone so far as to identify consumer use of Dahua equipment as problematic.

These actions illustrate a growing trend of state attorneys general looking to use broadly written state laws to target conduct that may not violate federal national security regulations, but arguably still constitutes a threat.[14] And, with some of these very state officials predicting that 2025 will prove to be merely the early innings of a long-term project to protect consumers from security threats, this trend is not likely to subside any time soon.[15]

It is not clear how successful state authorities will ultimately be in using federal national security concerns as the basis for state consumer protection suits. The targeted entities will

presumably argue that it is inappropriate under state and federal law for states to involve themselves in matters of foreign policy, or to try and parlay limited federal restrictions into broader omnibus consumer protection actions, especially where those restrictions have been carefully tailored by federal officials.

Nevertheless, regulated entities with foreign supply chain risk exposure should not take for granted that federal compliance eliminates that risk. Without a comprehensive risk management strategy accounting for state-level enforcement, they may soon find themselves in the net of consumer protection laws around the country.

Joshua S. Turner and Sara M. Baxenberg are partners, and Joel S. Nolette is an associate, at Wiley Rein LLP.

Wiley partner Duane Pozza and of counsel Ian Barlow contributed to this article.

[1] Andrew Ferguson, Staying in Our Lane: Resisting the Temptation of Using Consumer Protection Law to Solve Other Problems, Sept. 27, 2024, available at: https://www.ftc.gov/system/files/ftc_gov/pdf/9.27.2024-Ferguson-ICPEN-Remarks.pdf.

[2] John S. McCain National Defense Authorization Act for Fiscal Year 2019, Pub. L. No. 115-232, § 889(a), (f)(3)(B), 132 Stat. 1636, 1917-19 (2018).

[3] Secure and Trusted Communications Networks Act, Pub. L. No. 116-124, § 2, 134 Stat. 158, 158 (2020).

[4] FCC, List of Equipment and Services Covered by Section 2 of The Secure Networks Act (last updated July 23, 2025), https://www.fcc.gov/supplychain/coveredlist.

[5] Protecting Against National Security Threats to the Communications Supply Chain Through the Equipment Authorization Program, ET Docket No. 21-232, FCC 25-71, ¶¶ 20, 53 (Oct. 29, 2025), https://docs.fcc.gov/public/attachments/FCC-25-71A1.pdf.

[6] Press Release, Attorney General James Uthmeier Issues Subpoenas to Companies Selling Medical Devices Sending Patient Data to Communist China, Fla. Att'y Gen. (June 16, 2025), https://tinyurl.com/yke7sz7h.

[7] See id.

[8] Fla. Stat. § 501.204.

[9] Alert, CISA Releases Fact Sheet Detailing Embedded Backdoor Function of Contec CMS8000 Firmware, CISA (Jan. 30, 2025), https://www.cisa.gov/news-events/alerts/2025/01/30/cisa-releases-fact-sheet-detailing-embedded-backdoor-function-contec-cms8000-firmware. Subsequently, the FDA has taken steps to prohibit importation of Contec's devices. See Warning Letter, Contec Medical Sys. Co., FDA (Oct. 2, 2025), https://www.fda.gov/inspections-compliance-enforcement-and-criminal-

investigations/warning-letters/contec-medical-systems-co-ltd-717941-10022025 ("FDA is taking steps to refuse entry of these devices into the United States.").

[10] See generally Complaint, State ex rel. Hilgers v. Lorex Corp., No. CI250003315 (Neb. Dist. Ct. Sept. 23, 2025), https://tinyurl.com/26p6hz7f.

[11] Id. ¶¶1-27, 47-48.

[12] Id. ¶¶109-28.

[13] Press Release, Attorney General Ken Paxton Investigates Security Camera Company for Potential Ties to the Chinese Communist Party, Tex. Att'y Gen. (Oct. 29, 2025), https://tinyurl.com/mwdem59w.

[14] See, e.g., Press Release, Attorney General Ken Paxton Investigates Whether Major Tech Company Is Allowing the Chinese Government to Abuse Texans' Consumer Data, Tex. Att'y Gen. (Oct. 6, 2025), https://tinyurl.com/4r8bfh6c (announcing an investigation into TP-Link Systems Inc., for potentially violating Texas data-privacy laws by providing the Chinese government with "back doors" into TP Link's internet-networking equipment to permit access to consumers' network traffic); Complaint, State ex rel. Hilgers v. PDD Holdings Inc., No. CI250002002 (Neb. Dist. Ct. June 11, 2025), https://tinyurl.com/27jnf3xe (asserting state consumer-protection and deceptive-trade-practices claims against the companies that own and operate the Temu online shopping app for allowing surreptitious third-party access to users' cell-phone data); Complaint, Commonwealth ex rel. Coleman v. PDD Holdings Inc., No. 25-CI-00232 (Ky. Cir. Ct. July 17, 2025), https://tinyurl.com/4hdnfaca (asserting similar claims against Temu under Kentucky's Consumer Protection Act); Complaint, State ex rel. Griffin v. PDD Holdings Inc., No. 12CV-24-149 (Ark. Cir. Ct. June 25, 2024), https://tinyurl.com/335v5cdc (bringing similar claims against Temu under Arkansas's Deceptive Trade Practices Act and Personal Information Protection Act).

[15] See Federalist Soc'y, Discussion on the Future of State AG's Consumer Lawsuits Against Chinese Companies, at 53:15-53:20 (Oct. 29, 2025), https://www.youtube.com/watch?v=ZLe8rAAurJs.