Cooley

Florida Attorney General Launches 'CHINA Prevention Unit' Targeting Foreign Adversary Data Sharing

February 13, 2026

On February 5, 2026, Florida Attorney General James Uthmeier announced the creation of a dedicated "Consumer Harm from International Nefarious Actors" (CHINA) Prevention Unit within the Florida Office of the Attorney General.

While the acronym is pointed, the CHINA Prevention Unit's mandate is broad: to investigate and prosecute foreign corporations – specifically, those with ties to "foreign adversaries," like China, that collect sensitive data from Floridians. This development marks a growing trend in state-level enforcement, moving beyond traditional consumer protection into the realms of national security and data sovereignty.

What the CHINA Prevention Unit is designed to do

Housed within the Florida Office of the Attorney General, the CHINA Prevention Unit is tasked with leveraging the Florida Deceptive and Unfair Trade Practices Act and state privacy laws to target companies whose data practices may expose Florida residents to foreign exploitation. The CHINA Prevention Unit is framed as both preventative and enforcement-oriented, with an emphasis on demanding "transparency from companies operating in Florida" with ownership or ties to China and other countries of concern.

The attorney general has already signaled his enforcement priorities by taking several immediate actions:

- **Subpoenas issued:** The CHINA Prevention Unit apparently issued subpoenas to several companies that the attorney general suspects have relationships with China.
- **Healthcare audits:** The CHINA Prevention Unit is apparently sending formal letters to several medical device manufacturers demanding audits to identify ties to China and verify whether sensitive biometric or patient data is being transmitted to foreign servers.
- **Technology scrutiny:** The CHINA Prevention Unit's work will build on previous investigations by the attorney general into foreign router manufacturers and security camera companies regarding backdoors and supply chain vulnerabilities.

These actions demonstrate that the CHINA Prevention Unit is leveraging a cacophony of state laws (e.g., consumer protection, privacy, sectoral rules and public contracting) to further its transparency and remediation goals. They also clearly signal aggressive enforcement into the data collection, processing and disclosure practices of companies with ties to China and other foreign adversaries to the state of Florida.

Key takeaways for businesses operating in Florida

- **Healthcare and biometrics are ground zero**. The attorney general has explicitly stated that healthcare is the "primary industry" of concern, "with personal health data, the most sensitive of human data, being shared with an enemy that wants to do us harm." If your organization manufactures, distributes or utilizes internet-connected medical devices, diagnostic equipment or health-tech platforms with any component of Chinese ownership or manufacturing, you may be in the attorney general's crosshairs.
- **Enforcement over legislation**. Historically, protection of national security has been the remit of the US federal government. Florida's attorney general is clearly not waiting for new federal laws. By "repurposing" existing resources, the attorney general is using broad consumer protection statutes to conduct what are essentially national security audits. Thus, many businesses may find themselves receiving "investigative subpoenas" even in the absence of a specific data breach or security incident, as the CHINA Prevention Unit's focus is on prevention.

- **Transparency is now a legal risk**. The CHINA Prevention Unit is focusing on deceptive trade practices. If a company's privacy policy or marketing materials fail to clearly disclose that data may be accessible by foreign entities or stored on foreign servers, the attorney general may view this as a deceptive or fraudulent omission. Admittedly, Florida would not be the first government agency to take this position, but businesses operating in Florida may want to consider being more transparent about any data storage outside of the US, as well as the extent of any relationships between the business and "foreign adversaries."

Considerations for businesses operating in Florida

- **Audit supply chain and international data flows**. Map the data journey of your products. Do your devices or software platforms communicate with servers in "countries of concern"? Of particular note, you may want to identify any Chinese-manufactured components in your IT or medical infrastructure.
- **Review privacy disclosures**. Consider whether your privacy notices and other public disclosures should be explicit about international data transfers. Boilerplate language may no longer be sufficient to ward off state-level scrutiny in Florida.
- **Assess Medicaid/public funding risks**. There are calls encouraging legislative momentum to condition state funding and Medicaid reimbursements on the use of "non-China-linked" equipment. Entities relying on state contracts should begin evaluating alternative domestic or "friendly-nation" technology providers.
- **Federal government enforcement**. The Florida attorney general's focus on China and foreign adversaries aligns with recent federal government activity. For example, this week, the US Federal Trade Commission announced it had sent letters to 13 data brokers warning them against selling, releasing, disclosing or providing access to personally identifiable sensitive data about Americans to any foreign adversary. Earlier this year, the US Department of Justice promulgated the Data Security Program, a similar federal regulatory framework that restricts or prohibits certain categories of transactions between US persons and "countries of concern" that include bulk sensitive US personal data, such as geolocation data and biometric data.

Conclusion

Florida's move represents a "new front" in the regulatory enforcement landscape. What was once a matter of federal trade policy has now become a local enforcement priority.

If you have questions about how these new enforcement priorities affect your compliance posture, or if you have received an inquiry or investigative demand from the Florida attorney general's office, please contact our cyber/data/privacy team.

Key Contacts

Travis LeBlanc Washington, DC	tleblanc@cooley.com +1 202 728 7018

Zhijing Yu Singapore	zyu@cooley.com +65 6962 7527
Richard Koch Washington, DC	rkoch@cooley.com +1 202 776 2323