LEXOLOGY

State AGs zero in on China-linked data flows

Updated as of: **02 March 2026**

Victoria Hudgins

LEXOLOGY PRO

A trend of states invoking national security in consumer protection enforcement may test their authority as they target China-linked companies' handling of personal data.

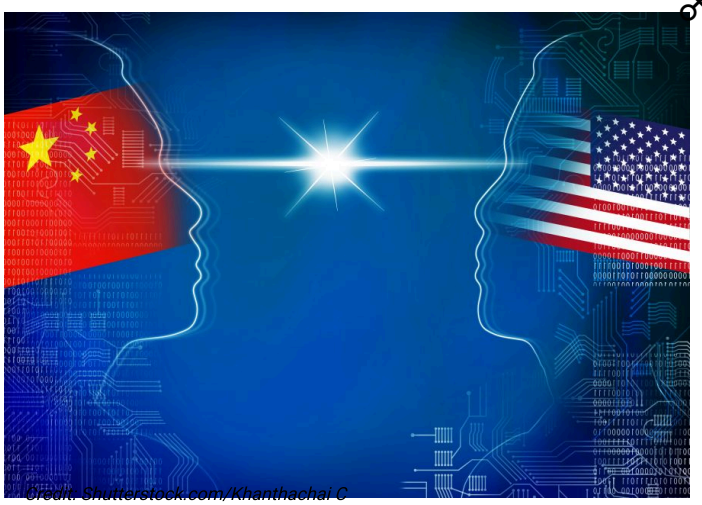
Key takeaways

- State attorneys general are increasingly using their unfair or deceptive acts or practices laws to bring claims against China-linked companies' data practices.
- States favour these laws because cases brought under them are easier to prove than under data privacy laws.
- This enforcement strategy risks constitutional challenges, as courts may view state actions tied to foreign adversaries as encroaching on federal authority.

Last month, the Texas Attorney General's Office filed a flurry of lawsuits in Texas state courts against companies with ties to China. The lawsuits alleged that the companies have misrepresented the security of US users' personal data that they collect, in violation of Texas' unfair or deceptive acts or practices (UDAP) law.

Texas claimed those companies are based in or owned by a parent company subject to China's national laws, which may require companies to provide personal data and state intelligence to the Chinese government.

In a statement, a T-P Link spokesperson said that Texas' claims are "without merit and will be proven false." Clothing retailer Shein also refuted Texas' accusations and said it will fight those claims, according to a statement provided to Lexology PRO.



Credit: Shutterstock.com/Khanthachai C

Anzu Robotics, Lorex Technology and Temu didn't respond to Lexology PRO's requests for comment.

Enforcement takes a partisan shift

Quinn Emanuel Urquhart & Sullivan partner Manisha Sheth said that Texas' lawsuits are an acceleration of a common legal theory used by state attorneys general, under which states challenge companies' privacy policies or marketing claims about data security.

In 2022, for instance, Google agreed to pay US$391.5 million to end 40 states' claims that its location data collection practices violated their consumer protection laws.

However, Texas and other Republican-led states are now targeting companies that are subject to Chinese law.

For example, the Nebraska Attorney General's Office in 2025 alleged that Lorex and ADI Global Distribution failed to disclose to consumers that their personal data might be shared to the Chinese government. Arkansas filed a similar lawsuit against Temu in 2024.

The Florida Attorney General's Office may also join this enforcement trend. In February 2026, Florida announced it launched the Consumer Harm from International Nefarious Actors Prevention Unit to tackle the threats posed by the Chinese government and other foreign adversaries to Floridian consumers, data privacy and economic security.

Are state data privacy law claims next?

Those lawsuits, so far, have alleged violations of states' UDAP laws. Texas' and Nebraska's recent lawsuits regarding China-linked companies' data protection laws don't allege violations of their enacted omnibus data privacy laws.

Lawyers told Lexology PRO that states are likely bringing these claims under their UDAP laws as there's established case law under those measures.

"It's an easier claim to make, UDAP is easier to prove," said Patterson Belknap Webb & Tyler of counsel and former New Jersey Attorney General Peter Harvey.

"It's interpreted to have a broader application and substantial penalties. It also has some litigation advantages. The AG does not have to show actual loss. For certain types of relief, the AG can base a claim on potential harm," Harvey said.

Under states' UDAP laws, the state attorney general also doesn't need to prove that a consumer relied on the company's representation, Harvey added.

In addition to obtaining financial penalties, Sheth noted that UDAP claims regarding companies' data practices may also tell a more compelling narrative to the public.

"I think it tells a better story. The [Texas] Data Privacy and Security Act law is only a technical violation. OK, you didn't respond to a privacy notice, you didn't make certain disclosures, you didn't offer a consumer an opt-out right. In contrast, the [Texas] Deceptive Trade Practices Act cases tell a more, I think, interesting-to-a-jury narrative because it's fraud and deception. You misled consumers. That has a little more appeal to the public because a lot of these AGs are elected officials. That will generate more interest than a technical violation," she said.

Do states have the authority to bring these claims?

As states step into the potential national security risks created by data transfers, they may run into pre-emption challenges.

For example, Montana enacted legislation banning TikTok's usage in its state to avoid users' data potentially being accessed by the Chinese government. Federal courts ruled that the law was unconstitutional, in part, because Montana didn't have authority over foreign affairs. The parties jointly dismissed the lawsuit in February 2026 after TikTok divested its majority China-based ownership.

Courts may also find Texas' recent lawsuits overstep its authority as foreign relations policy power is generally given to the US president, said UC Berkeley School of Law professor Paul Schwartz.

"The federalism argument is that this is a power reserved to the states," said Schwartz. "While . . . there's a state role in protecting consumers from unfair trade practices, it does seem that raises very strong foreign-relations issues."

UDAP data best practices

With some states testing their UDAP laws against potential national security risks, companies should adopt best practices to reduce the likelihood of similar lawsuits.

Companies that are listed on Texas' prohibited technologies list, Florida's banned software list and the US Department of Defense's list of Chinese military companies will likely be scrutinised by Republican state attorneys general, Sheth said. Companies using technologies from those listed companies will also likely face state regulatory scrutiny, she added.

Disclosures

To weather those potential investigations, Sheth said disclosures are key. For example, a company shouldn't say it doesn't share data with any government when they do.

"It's really making sure your disclosures are accurate," she said.

Data mapping

Morrison Foerster partner Kaylee Cox Bankston said this enforcement trend should prompt companies to review and understand their external and internal data practices.

"I think these broader trends serve as a good reminder for companies to take a fresh look at their data processing practices," said Bankston. "That includes the sources of information they are collecting data from, the third party they are disclosing data to and really getting their arms around the data mapping in their company."

Potentially obtaining consent

Companies should also consider obtaining consent before collecting personal data, Harvey added.

"You also have to determine whether you should seek a consumer's consent and invite that consumer to agree to the terms and consent to certain types of use of data. See, if the consumer has knowledge and they give consent there's no issue. None. But if the consumer doesn't know and the consumer didn't give you permission to share, then you have an issue," he said.

Resources

Daily newsfeed | Panoramic | Research hubs | Learn | In-depth | Lexy: AI search | Scanner | Contracts & clauses

Lexology Index

Find an expert | Reports | Research methodology | Submissions | FAQ | Instruct Counsel | Client Choice 2025

More

About us | Legal Influencers | Firms | Blog | Events | Popular | Lexology Academic | Lexology Talent Management

Legal

Terms of use | Cookies | Disclaimer | Privacy policy

Contact

Help centre | Contact | RSS feeds | Submissions

Login | Register

Search Lexology

Follow on X | Follow on LinkedIn