

China's Tesla restrictions expose growing concern about AVs' digital privacy

Article

The news: Officials in China have banned **Tesla** vehicles from the town of Beidaihe for two months due to government meetings held there.

- Local traffic authorities in the coastal resort town announced they were prohibiting Teslas from entering the district, which is the “**site of a secretive annual summer party**” for **Beijing leadership**, starting in July, [per](#) Reuters.

- Although a specific reason wasn't provided, officials may be concerned that data collected by vehicle cameras could be used for spying purposes, [per](#) Electrek.

Other Teslas bans: Earlier this month, the EVs were prohibited from roads in Chengdu during a visit by Chinese President **Xi Jinping**.

- Last year, China's military barred Teslas from bases and housing complexes, citing security concerns over vehicle cameras.
- Tesla CEO **Elon Musk** said the cameras weren't used for spying. He subsequently moved all data generated by Teslas in China to local storage.

Promises aren't enough: Despite a reportedly positive overall relationship between Tesla and Beijing, the cameras appear to have caused a rift likely rooted in [geopolitical tension](#) between China and the US.

- Tesla was the first foreign automaker with a factory in China that didn't have a joint venture with a state-owned company.
- This means the government's problem isn't likely with Tesla as a company. It's more an issue that a US company is operating independently within its borders, with cameras that could potentially be used for surveillance.
- While many AVs rely on radar and lidar to function, Tesla's **Autopilot** uses eight cameras linked to a [neural network](#).
- The [TeslaCam](#), a built-in dashboard camera, also allows users to record what's happening ahead of them in traffic.
- Last year, Tesla released a [Sentry Mode](#) feature that monitors a vehicle's surroundings and records footage of anything close by.

The bigger data privacy picture: The problem isn't unique to Tesla's cameras. Generally, there's not much transparency about what happens to data collected by IoT devices. Although there may be privacy policies in place, they don't necessarily allow users to "see" what happens to their data.

- The concerns are justified. Even commonplace devices like [Fitbits](#) can compromise military intelligence.

- Tesla may be bullish on cameras for AV systems, but it's hardly the only automaker to deploy them. Any vehicle with such [devices linked to AI](#) could prompt privacy concerns.
- This means law enforcement, auto companies, and hackers could potentially access an array of revealing AV data.
- As IoT-equipped vehicles proliferate, more regulation and transparency are needed to ensure trust in the technology.

Go Deeper: Read our [Smart Home Forecast](#) for more on privacy and security concerns with IoT.

Actions Their Company Has Taken to Increase the Trust of Their Brand in the Face of Privacy Concerns According to US CMOs, Feb 2022

% of respondents

Promise not to sell customers' personal information

63.1%

Asked consumers to consent to your company's use of their data

58.1%

Invested in technology infrastructure to reduce the likelihood of a data breach

52.2%

Invested in increasing trust in your brand reputation

50.7%

Make our privacy policy easy to understand

50.7%

Shared privacy notices with consumers that communicate how your company will use their data

45.3%

Developed a brand privacy policy

36.5%

Source: Duke University's Fuqua School of Business, "The CMO Survey: February 2022" commissioned by Deloitte and American Marketing Association, Feb 28, 2022

273884

eMarketer | [InsiderIntelligence.com](https://www.insiderintelligence.com)