UC San Diego
SCHOOL OF GLOBAL POLICY AND STRATEGY
21st Century China Center

POWER TRANSFORMATION LAB

Future of U.S.-China Energy Relations Policy Brief Series

MANAGING DATA SECURITY IN FOREIGN DIRECT INVESTMENT FLOWS FOR ELECTRIC VEHICLES

PETER COWHEY

Nov. 2025

GPS

The shift towards electric vehicles (EVs) presents unique challenges related to data security and cybersecurity. Drawing on the Tesla-China case and the TikTok negotiations, this memo explores how foreign direct investment in EVs can be structured to address national security concerns while maintaining beneficial interdependence in green supply chains.

Context

The four challenges to maintaining an interdependent green supply chain are well known, which include national security, competition in industrial policy, supply chain fragility, and protectionism. The first three challenges may not be fully resolved but they can be made more tractable by shifting global supply chain flows more through the vehicle of foreign direct investment (FDI). However, despite its benefits in terms of importing advanced technology and fostering knowledge and skills spillovers, FDI in electric vehicles (EVs) and EV batteries entail some new concerns. In contrast to earlier phases of automobile competition and localization, the EV sector must address distinct challenges related to data security and cybersecurity. EVs share more similarities with information technology than traditional manufacturing and require careful management for safe interdependence.

Analysis

Data issues matter greatly because so much of the value added and competitive advantage in both manufactured goods and services rest on continuous data flow. EVs are smart vehicles, massively networked both for their everyday operations and for continuous improvement in safety; reliability; and performance, navigation and guidance systems. EVs are all on an evolutionary path with a goal for semi or full autonomous driving, making the previous networked capabilities of particular importance.

Even as data, software, and complex information technology systems operate pervasively and frequently on cross-border systems (because variations in national driving conditions open opportunities for AI learning), the concerns about every imaginable aspect of data security become more sensitive issues.

A particular political issue of deep resonance to many is data sovereignty: who gets to control data on what terms. For the issue of sovereignty to be addressed, issues and their solutions must be carefully broken down in order to improve the potential for productive and safe interdependence.

It is likely that some green technology will not be open to cross-border investment between the U.S. and China. The classic example in green technology is the new generation of sophisticated electric grid control systems that open the way to major cybersecurity risks. In contrast, some green products and technology pose potential data/cybersecurity risks, but risk mitigation by restricting cross-border data flows and imposing certain software restrictions may suffice to let EV FDI operations succeed. This risk mitigation would entail some combination of local data storage and management of particularly sensitive data by a commercial intermediary trusted by the host government.

The Tesla Bargain in China

Tesla has struggled with Chinese government concerns over its accumulation and use of data, with possible security implications, for several

years. The deal that evolved deserves careful attention for its possibility to serve as a model. [1] In May 2021, Tesla took a first step to respond to data sovereignty issues when it announced that it was building its own data center in China to demonstrate that it would comply with regulations requiring local data storage. Nonetheless, even after that measure,

Tesla vehicles were restricted from entering military bases or other sensitive government locations out of security and consumer privacy concerns.

In late April 2024, Elon Musk met with Premier Li Qiang, an early champion of Tesla FDI in China, to strike a deal. To resolve the government's worries, data security tests examined how Tesla vehicles collected sensitive personal information and the ease with which a consumer could stop this data collection.[2] Among the specific guarantees were that Tesla would anonymize data from auto sensors that observed license plates or faces.

The agreement created a financial incentive for Tesla to adopt the use of Baidu mapping software in its vehicles, thereby assuring Chinese regulators that the vehicle data would not only stay in China but it would be using a complex software system that fit the country's security guidelines. The financial incentive for Tesla was straightforward. Until that point, it had to rely on its cars' camera systems and lower quality mapping data to guide its smart vehicles. Baidu is one of 20 Chinese firms permitted by the government to use higher resolution mapping data for commercial purposes. Tesla's adoption of the Baidu system boosted Baidu as a world player in that space. In turn, the higher quality mapping data let Tesla win government approval to activate its supervised full self-driving system. This system is offered as a $99/month upgrade option on a Tesla, a major boost for their profit margins just as Tesla had to lower prices in the face of much stronger competition. It also meant that BYD, its biggest competitor, and Nio could not pull ahead on self-driving options.

The high level of political engagement in this negotiation also suggested that it represented what Chinese EV vehicles might offer when seeking entry into the OECD countries. One could imagine BYD, for example, bidding to open manufacturing facilities in OECD countries and then offering to use OECD sourced systems for mapping data and localized data storage and computing facilities in OECD countries. The credibility of data protection would be further enhanced if, as some think feasible, it proves possible to tag data sufficiently to allow tracing any movement outside of U.S. boundaries.

This approach still may not satisfy American critics of personal data protection and security issues involving Chinese products. Indeed, the Biden Administration's closing months included a new rule on the movement of personal data of U.S. citizens to locations outside America that would prove quite restrictive regarding China. The U.S. Congress has also voted overwhelmingly to force Chinese controlled TikTok out of the country over data security concerns. Still, given that the Trump Administration has been open to rethinking the banning of TikTok from the United States points to some potential flexibility on the issue of data sovereignty.

Recommendations

The discussion about the future of TikTok in the U.S. is a reasonable proxy for how the Trump administration could address the same security and privacy issues for EVs resolved by Tesla's China negotiations. In regard to TikTok, critics claimed it would collect extensive information on U.S. users (including U.S. military personnel) and share it with the Chinese government for possible blackmail, collection of sensitive geolocational data, and political propaganda. These accusations

led to a Congressional bipartisan act to set a deadline for either TikTok to be banned in the U.S. or sold to U.S. owners.

TikTok waged a skilled political and legal court campaign to delay the ban while searching for new allies. Its popularity among younger cohorts eventually caught the notice of the Trump political apparatus. Then, in a move reminiscent of Tesla in China, TikTok agreed with Oracle, controlled by a Trump supporter (Larry Ellison), to store all of its U.S. data in America.

The Trump Administration then repeatedly extended the deadline for TikTok to reach an acceptable deal on ownership and control of its U.S. operations. A U.S./global consortium of investors proposed a deal where the algorithm will be retrained under U.S. oversight, Americans will hold most board seats (with ByteDance retaining under 20%), and algorithmic control will rest with the new joint venture. However, ByteDance retains intellectual property ownership of the code globally; the U.S. subsidiary operates under a license for the code. In September 2025, Trump signed an Executive Order giving its approval to the deal. But the Chinese government must approve the export of this intellectual property and this remained as unfinished business even after the meeting of Presidents Trump and Xi in Korea.

The TikTok tale shows how the collection of some forms of U.S. personal and geolocational data could prove acceptable to the Trump administration if China had manufacturing plants for technology like EVs and batteries in the U.S. The formula might be:

1. Production of Chinese EVs or batteries in the U.S. in joint ventures with majority U.S. ownership and requirements for high levels of local value added in production;
2. Some requirements for technology transfer to U.S. partners and suppliers;
3. Potential bans on use of such vehicles by employees of the U.S. Government and some restrictions on where they could be used;
4. Data controls resembling those for Tesla and TikTok. This might include using U.S. information technology for all data handling and an American GPS software system to address geolocational questions.
5. This approach might be more economically attractive for Chinese parts producers than for EV manufacturers. It is hard to know without better defined specifics, but some set of policy parameters could be tested by specific business models. Some auto industry experts argue Chinese firms could profitably export EVs to the U.S. even if the U.S. imposed tariffs of 50%. If this is correct, it suggests that Chinese producers could afford considerable compliance costs involving U.S. cybersecurity rules and still succeed in the American market.

---

[1] Sources for this account include: Tesla and Baidu Partner for Self-Driving Cars in China - EFE Noticias; As Musk Visits China, Tesla Wins Key Data Security Clearance - Bloomberg Tesla Wins Data-Security Clearance in China - MarketWatch Tesla says it has established a data center in China - DCD (datacenterdynamics.com) Elon Musk Reaches Deals in China on Self-Driving Teslas - The New York Times (nytimes.com)

[2] As Musk Visits China, Tesla Wins Key Data Security Clearance - Bloomberg

About the Author

Peter F. Cowhey is Dean Emeritus and Qualcomm Chair Emeritus of the UC San Diego School of Global Policy and Strategy. His research focuses on international political economy, telecommunications policy, and technology governance. He has extensive experience in policy analysis and has served in various advisory roles on technology and trade policy issues.

21st Century China Center

Through cutting-edge research and collaboration between expert scholars, UC San Diego's School of Global Policy and Strategy's 21st Century China Center is driving innovative policy solutions on a global scale. Its mission is to produce and disseminate impactful, evidence-based research about China and to enhance U.S.-China mutual understanding by advancing scholarly collaboration, convening policy discussions, and actively communicating with policymakers and the general public in both countries. Learn more at china.ucsd.edu.

Power Transformation Lab

The Power Transformation Lab at UC San Diego examines the engineering and institutional conditions needed to scale low-carbon energy. We work with academic, government, civil society, and industry partners to advance research and solutions focused on the power grid, including renewable energy planning, affordable and reliable low-carbon power markets, and the political economy of industrial policy and low-carbon transitions in firms. Learn more at pwrlab.org.

School of Global Policy and Strategy
University of California San Diego
9500 Gilman Drive #0519
La Jolla, CA 92093-0519

gps.ucsd.edu

UC San Diego

SCHOOL OF GLOBAL POLICY AND STRATEGY