

United States Senate

WASHINGTON, DC 20510

September 11, 2024

To whom it may concern:

We write regarding the Chinese automobile industry and the potential national security threats posed by these vehicles. The global automotive market is being flooded with Chinese-made electric vehicles (EVs). In fact, in 2023, China became the second largest exporter of vehicles in the world.¹ Given the Chinese Communist Party (CCP)'s control of industry in China, we are deeply concerned that Chinese automakers are beholden to the regime and that the technology used in Chinese-made automobiles could be leveraged by the CCP for nefarious purposes. The data security of both American citizens and the critical infrastructure of our nation must be prioritized.

It is well documented that the CCP and Chinese intelligence agencies are provided access to data stored in China or accessible by companies incorporated in China for the purpose of “national security.”² Specifically, experts have sounded the alarm regarding the control of data for connected vehicles manufactured by companies incorporated in China, particularly when it comes to the potential for unauthorized access by the CCP to vehicle systems, data collection, and surveillance capabilities embedded within the vehicle's technology.

Modern vehicles are equipped with video cameras and sensors both within and outside the vehicle that are capable of continuously monitoring the vehicle's surroundings and passengers. These sensors can collect data about road conditions, nearby vehicles, pedestrians, and individuals in the car to be used for safety and convenience applications, but—in the hands of our adversaries—they could be used to map our critical infrastructure and roads, track the movements of U.S. citizens, provide access to the electric grid, and generally surveil Americans.³ These features may foster safety, technological innovation, and convenience when they are deployed by trusted automotive partners in a secure and responsible manner. However, we do not have this same confidence in automotive manufacturers based in the People's Republic of China. Over-the-Air (OTA) update systems found in Chinese-made vehicles also raise security concerns. OTA updates—or the digital software updates intended to ensure that a vehicle runs efficiently and safely—in a Chinese-made vehicle could be vulnerable to malicious activity, opening a window for an adversary to push compromised software to Americans' vehicles.⁴ If Chinese-made EVs proliferate in the U.S., the CCP could theoretically control or disable vehicles in the United States at will.

¹ Evelyn Cheng, *China Comes just Shy of Japan as the World's Largest Car Exporter*, CNBC (Jan. 31, 2024) <https://www.cnbc.com/2024/01/31/china-comes-just-shy-of-japan-as-the-worlds-largest-car-exporter.html>.

² U.S. DEP'T OF HOMELAND SECURITY, *DATA SECURITY BUSINESS ADVISORY: RISKS AND CONSIDERATIONS FOR BUSINESSES USING DATA SERVICES AND EQUIPMENT FROM FIRMS LINKED TO THE PEOPLE'S REPUBLIC OF CHINA* (2020), https://www.dhs.gov/sites/default/files/publications/20_1222_data-security-business-advisory.pdf.

³ David Shepardson, *US to Probe if Chinese Cars Pose National Data Security Risks*, REUTERS (March 1, 2024) <https://www.reuters.com/business/autos-transportation/us-says-investigate-national-security-data-risks-chinese-vehicles>.

⁴ U.S. DEP'T OF TRANSPORTATION, *DOT HS 812 807, CYBERSECURITY OF FIRMWARE UPDATES* (2020), https://www.nhtsa.gov/sites/nhtsa.gov/files/documents/cybersecurity_of_firmware_updates_oct2020.pdf.

The CCP has made clear that they intend to make the 21st century a “Chinese Century,” with domination of the global automotive market being a key piece of their strategy. The United States has a responsibility—for the sake of the next generation of Americans and the world at large—to ensure that does not become a reality. We recognize the Department of Commerce’s recent advance notice of proposed rulemaking seeking public comment on the national security threat posed by foreign adversary involvement, particularly Chinese government involvement, in the connected vehicle supply chain.

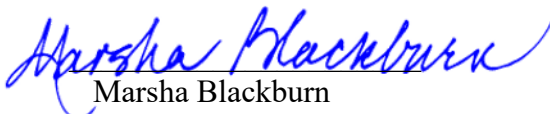
As the potential national security threat posed by connected vehicles becomes more acute, we believe you must make clear the depth and nature of your ties to the CCP, as well as your future plans to potentially import vehicles into the U.S. market.

With that in mind, we request you transmit responses to the following questions to our offices by September 30, 2024:

1. Are you currently importing or selling vehicles, or do you intend to import or sell vehicles into the U.S. market in the next 5 years?
2. Please provide an organizational chart detailing your current corporate ownership structure, noting any material changes in that structure which have occurred within the last seven years.
3. Is information your company collects from vehicles or individuals subject to the People’s Republic of China National Intelligence Law, or any other law in China requiring your company to provide sensitive information to any agency or government authority in China, upon request or otherwise? If your answer is no, please explain.
4. Does your company store or transmit vehicle or consumer data using servers, satellites, or networks located in or under the jurisdiction of the People’s Republic of China?
5. If you have sold vehicles currently operating in the U.S., please state the nature of CCP access to or the total number of requests you have received from any agency or government authority in China for access to information collected from vehicles or individuals located in the United States. For each request, provide:
 - a. The date of the request;
 - b. The type of information requested, including but not limited to odometer data; LiDAR images; driving characteristics data; geolocation or other mapping-related data; camera data; microphone data; biometric data; other types of personal information, including name, VIN, address, phone number, occupation, financial information;
 - c. The number and types of vehicles or individuals subject to the request; and
 - d. Whether your company provided any notice to those individuals or vehicle owners that their information was provided to a CCP official.

6. Please outline the steps you have taken, or would take, if you learned that actors supported by or affiliated with the CCP have accessed your company's network or databases, or are using your company to spy on, surveil, or observe individuals or groups.
7. Please document all meetings, communications, or interactions you—or any other senior company executives—have had with members of the CCP relating to current or future operations in the United States.
8. Please describe Chinese-made information and communication technology and services systems that are used in vehicles you export—including software, telematics systems, advanced driver assistance systems, automated driving systems, battery management systems, and braking systems—given that these systems are at greater risk of CCP-directed monitoring, control, manipulation, or sabotage.
9. Please describe any collaboration agreements, partnerships, or other business relationships your company has with Chinese data and technology companies or cloud service providers to support the operations of, or provide products or services via, your vehicles that are exported to or made in the United States, as these relationships could provide CCP-controlled actors with technical access vectors to the vehicles or the data they gather.

Sincerely,


Marsha Blackburn
United States Senator


Gary Peters
United States Senator