

# Electric Vehicles Pose Grave Threat to National Security

## *Savvy or unsafe?*

**2nd Lt. Ahdam A. Wilson**  
*160th Signal Brigade*

Electric vehicles pose a serious threat to national security because they maintain a full suite of cameras and sensors that are always active and record everything within their area of operation.

Other key issues include each owner's inability to control how their vehicle's data is collected, who their data is sold to, and the lack of federal regulations to govern data privacy. These issues could potentially lead to sensitive information being leaked to adversaries of the United States. Serious discussions need to take place at the highest levels of federal government on how to address the threat of electric vehicles on military bases.

Electric vehicles are revolutionizing the automotive industry. Their slick design, awe-inspiring speed, and economical pricing have given the traditional premium gasoline-powered cars a run for their money. Furthermore, as nations worldwide are eager to transition to a sustainable future, the future of electric vehicles is as bright as the North Star.

Despite their eye-catching popularity, electric cars, with their autonomous driving technologies, have one major drawback: they are a grave threat to national security, especially on military bases. Electric vehicles pose as a serious national security concern for the Department of Defense (DoD), its allies and other partner nations due to the vehicles' always-on surveillance, vulnerability to hacking, and lack of stringent privacy regulations.

### **Always On**

Electric cars have become synonymous with autonomous driving. The algorithm that powers this type of driving requires data collected from millions of vehicles to learn and adapt to the dynamic conditions of the road. Each automobile is fitted with a full suite of cameras and sensors that collect and record 360 degrees around the vehicle. A vehicle's cameras and sensors record every time the car is turned on. Tesla vehicles also have what the manufacturer calls Sentry Mode, which records when the car's sensors detect an attempted break in while the vehicle is in park (Jones, 2023).

*Figure 1* depicts Tesla's flagship vehicle, the Model S Plaid. Oftentimes there is not a viable option for a non-technologically savvy individual to turn the cameras off without seriously damaging

the functionality of the vehicle or voiding the car's warranty. Furthermore, the data the vehicle collects is often sold to third parties for a profit. Allowing electric vehicles on military bases is synonymous with allowing influencers to live stream in sensitive areas in which the owner has no control over where the data will go nor how it will be used.

### **Vulnerabilities**

Electric vehicles are vulnerable to hacking. This is proven true in numerous manufacturer-authorized hacking events such as Pwn2Own (Nelson, 2024), where teams of elite white hat hackers are authorized to break into car manufacturer's vehicles for a monetary reward. If a small team of elite hackers can remote into electric vehicles, imagine what a nation-state with trained black hat hackers and a sufficient budget could accomplish.

In an adversary-targeted attack, an electric vehicle's camera and sensor data could become a high-valued target, especially if the vehicle is known to frequent a military base or sensitive areas that interests an enemy. With sufficient time, resources, and persistence, a team of nation-state hackers might remotely obtain access and control of an electric vehicle, drive around an area of interest, and collect the intelligence with the car's high-definition cameras. Due to its popularity and controversy, electric vehicle manufacturers go to great lengths to ensure their vehicles are secure from a cybersecurity perspective. However, no company has an unlimited budget, and every company must balance between security, operations, and profitability.

### **Lack of Privacy Laws**

Car manufacturers are known for collecting and selling consumer's personal information to third parties for a profit (Bajak, 2023). The State of Texas sued General Motors for allegedly collecting and selling consumer's driving data without authorization (Stempel, 2024).

Other manufacturers, such as Toyota, have also been accused of illegally



*Figure 1: Tesla's flagship, the Model S Plaid*

collecting and selling data to third-party vendors. Vehicle manufacturers selling owner's driving data to third parties introduces a grave concern for electric vehicles that frequently visit military bases or other sensitive areas. A foreign adversary can purchase large amounts of vehicle data from car manufacturers using shell companies to not arouse suspicion and gather intelligence from the information they acquired. The federal government must update data privacy laws to protect consumer's private data, and the DoD must enact policies and procedures to ensure its facilities are secure from the proliferation of smartphones on wheels.

### **Solution**

The European Union's General Data Protection Regulation and the California Consumer Privacy Act are a good start for data privacy laws. However, it is time for the United States federal government to update its data privacy regulations to meet the conditions of the digital age and the increased expansion of the Internet of Things.

Banning a technology or a product is not always the answer, but DoD must enact measures to ensure

the sensitive areas of a military base are protected. This could mean restricting electric vehicle access to the less sensitive areas of a post only. Other measures can include finding ways and requiring the car owners to cover up the cameras when the vehicle is on a military post. User training can also play a big part in alleviating the dangers of electric vehicles. Users must understand the implications of electric vehicles. The data is collected from users, and they have no control over how it is used or where it is disseminated.

### **Conclusion**

Electric vehicles can pose a serious national security risk due to the always-on and continuously recording suite of cameras and sensors. Malicious actors can exploit the lack of sufficient data privacy laws and cybersecurity vulnerabilities in electric vehicles as an intelligence-gathering tool on military bases and other sensitive areas. The soaring popularity of electric cars only exasperates the problem. The solution requires a multi-pronged approach from the federal government and user training at the operator level.

## *References*

Bajak, F. (2023, September 6). Wiretap on wheels: How your car is collecting and selling your personal data. Los Angeles Times. <https://www.latimes.com/business/story/2023-09-06/carmakers-privacy-data-collection-drivers>

Jones, P. (2023, October 19). *When do Tesla cameras record? (10 common questions)*. Motors & Wheels. <https://motorandwheels.com/when-do-tesla-cameras-record/>

Nelson, N. (2024, January 25). Pwn2Own 2024: Tesla hacks, dozens of zero-day in electrical vehicles. Dark Reading. <https://www.darkreading.com/ics-ot-security/pwn2own-2024-teslas-hacked-dozens-new-zero-days-evs>

Stempel, J. (2024, August 14). Texas sues GM for allegedly violating drivers' privacy. Reuters. <https://www.reuters.com/legal/texas-sues-general-motors-allegedly-collecting-selling-drivers-private-data-2024-08-13/>

