

Factory Reset Isn't Enough to Ensure Vehicle Data Privacy

The Hidden Liability Sitting on Your Lot

by SHERRYL NENS, Head of U.S. Dealer Sales, Privacy4Cars

That pre-owned car may look ready to sell — detailed, factory reset, and priced to move — but a factory reset doesn't solve the bigger risk.

Even if personal data is cleared from infotainment, the prior owner still has remote access through a connected car app. With a connection remaining active, a previous owner could potentially track the car's location, remotely open the doors, or even drive away with the vehicle long after it's been traded in.

This is the hidden liability dealers miss. Vehicle privacy is not just deleting saved addresses and call logs. It's also ensuring the prior owner's digital connection has been severed. Relying on a factory reset alone is not enough.

CONNECTED VEHICLE DATA = CONSUMER DATA

Most customers will never ask whether their data was removed. They assume the dealership handles it for them when they hand over the keys. If a customer later discovers their personal information or app access is still tied to the vehicle, the issue becomes a question of responsibility.

Would you rather explain why the data was not deleted, or show proof that it was? In today's litigious environment — proof matters.

Vehicle data privacy is no longer a future concern. Regulators are already acting. The FTC's recent action against General Motors over the collection and sale of driver location and driving behavior data put the industry on notice — connected vehicle data is consumer data. California has also made vehicle privacy a priority by reviewing how OEMs collect and share data, taking enforcement action involving Honda, Ford, and General Motors.

New Jersey has taken it even further. The New Jersey Motor Vehicle Data Deletion Act requires dealers to offer in-vehicle data deletion services, recognizing the risk of personal information remaining in vehicles traded in, returned, or resold. New Jersey's "Used Car Buyers' Bill of Rights" reinforces the expectation that consumers receive clear and accurate information.

For dealers, the message is clear: **Vehicle data privacy is no longer optional** and more compliance enforcement actions are expected.

VEHICLE DATA RISKS DEALERS FACE

- 1. Unclear Vehicle Data Disclosures:** A vehicle can involve multiple privacy documents and connected services that are difficult for staff to explain. By embedding a vehicle privacy disclosure directly on VDP pages, dealers can proactively inform buyers in plain language before the sale.
- 2. Personal Data Left Undeleted on the Vehicle:** Over 80% of resold vehicles still contain the previous owner's personal data. Without a documented deletion process, dealers risk violating New Jersey statute.
- 3. Remaining Prior Driver Remote Access:** Handing over the keys does not disconnect the prior owner. Manufacturer apps may still allow a previous driver to track location, unlock doors, or start the engine, creating safety and liability exposure.

NEXT STEPS DEALERS CAN TAKE

Build vehicle data privacy into the intake process for every trade-in and lease return. Dealers should standardize disclosures, delete stored personal information, disconnect prior app access, and keep a record before the vehicle reaches the sales floor. The record demonstrates that the dealership followed a consistent process if a complaint, regulatory inquiry, or future lawsuit arises.

Privacy4Cars® supports this process with Vehicle Privacy Report™ for vehicle-specific disclosures, AutoCleared™ for certified data deletion, and DisconnectedCar™ to help sever prior owners' remote digital access. **nj car**

For more information, please visit our website at privacy4cars.com or contact us at (949) 230-0713 | sherryl@privacy4cars.com.

