



The Hidden Dangers of In-Car Tech to Consumer Privacy

July 7th, 2021 | and [Eric L. Johnson](#)

This article appeared in *Spot Delivery*®. Reprinted with express permission from CounselorLibrary.com.

When you start your car, a notice may pop up on the car's onboard navigation computer screen. The notice may ask you to agree to provide certain information to the car's manufacturer regarding the car's performance and information about you and your driving history. This notice asks you to agree or decline to provide that information to the manufacturer. What you may not see, and what you may not provide specific consent for, is a treasure trove of personal information that a car may capture about you, your contacts, and your car's location.

For example, whenever you connect your cell phone to a car's infotainment center, you are giving that car access to such things as your personal and business contacts, call logs, text messages, navigation history, home and work addresses, garage codes, passwords, IDs, health and other biometric information, credit information, user profiles, and third-party apps.

Hidden within most of the cars sitting on your lot are potential claims for breach of a consumer's privacy. There are already class action cases in play where the plaintiffs have argued that rental car companies captured their personal information without their consent and breached their constitutional right to privacy when the companies allegedly failed to delete that information when the rental cars were returned. The plaintiffs also argued that the companies committed unfair business acts by not having "responsible policies and procedures" regarding the deletion of personal information and by engaging in conduct that is "immoral, unethical, oppressive, unscrupulous, or substantially injurious."

This recent litigation highlights the privacy risks to all vehicle dealerships that acquire, sell, and finance used vehicles that may have captured consumers' personal information. In addition, this practice has drawn interest from the Federal Trade Commission, which has indicated that it is looking into the collection and storage of vehicle data. A used car dealer is particularly at risk of a federal or state law claim if it is passing along unprotected, unredacted, unencrypted consumer data in a vehicle that it sells.

Some state laws and regulations come with statutory penalties in the \$500-\$7,500 range per VIN, and many of these laws and regulations come with a private right of action. Attorneys' fees and costs could be awarded to the victor, too. State privacy laws, such as the California Consumer Privacy Act and the new Virginia Consumer Data Privacy Act, state unfair and deceptive acts and practices laws, state data security laws, and other state laws could be impacted. Federal laws may also apply, with civil penalties for a UDAP violation now at over \$43,792 per occurrence.

Some questions to ask yourself:

- Do you operate any dealerships in a “handsfree” or “no-text-and-drive” state?
- Do you have a vehicle loaner, rental, or carsharing program?
- Do you serve customers with sensitive information/special privacy considerations, such as customers in the government, military, or law enforcement or who otherwise have security clearance? What about high net worth individuals, C-level executives, those who work in HR, IT, or security departments? What about customers who may have been victims of a crime or harassment or who are in a protected class?
- Do you sell (and upsell) vehicles with telematics/connected services?
- Have you sold or will you sell at least one vehicle to one California resident in 2021?
- Are you sure that no employees/contractors would help themselves to the personal information captured by a vehicle?
- Do you have a policy on how to handle personal information that may be stored or processed by vehicles’ systems?

Here are some basic first steps you may take to address these issues:

- Know what personal information is collected by the vehicles you buy and sell. To make this determination, consider performing an audit of your vehicles;
- Have a written policy addressing the collection, retention, and/or deletion of captured vehicle data;
- Disclose to the consumer what information you collect and for what purpose and then honor that disclosure;
- Only keep the information for as long as it is needed, and remember record retention requirements;
- Consider differentiating between information left in a vehicle vs. information that may have been downloaded (e.g., at the service center) to serve the customer;
- Consider differentiating between different vehicle types (e.g., lease returns you will not keep vs. trade-ins);
- Revise your legal documents accordingly (e.g., sale or lease contracts, agreements with OEMs and other third parties, etc.); and
- Prepare for a potential bad headline or lawsuit by engaging in public relations and contingency planning.

Remember that you don’t have to go at this alone. Consider getting external advice from a service provider that has the expertise and specialized tools to “wipe” the data from the cars you buy for inventory, sell, and lease. There are ways to turn the deletion of customer data into a competitive advantage. For instance, privacy is a top-of-mind consumer issue, so being upfront and visibly implementing a deletion policy can be a reputation builder and source of differentiation. Keep an eye on legislative changes at the federal and state levels. Finally, don’t forget about those pesky federal regulators like the FTC and the Consumer Financial Protection Bureau because they could be looking at you!

CounselorLibrary LLC and Hudson Cook LLP are affiliated companies with common ownership. CounselorLibrary LLC does not provide legal services, representation or advice. It is not necessary for you to use the legal services of Hudson Cook in order to be a customer of CounselorLibrary, and vice versa.