Complying with FTC's Updated Safeguards Rule

Deleting Consumer PI Stored in Vehicles: Dealership Guidelines

JUNE 2022

PRIVACY4CARS

Privacy4Cars.com

Executive Summary

Due to widespread data breaches over the last few years, the Federal Trade Commission updated the Safeguards Rule in October 2021. Motor vehicle dealers were one of the groups specifically targeted with this rule change, and are now **required to develop, implement, and maintain a comprehensive system to safeguard consumers' Nonpublic Personal Information (NPI, or PI) they come into possession of**. If you are an auto dealer, you now have a much greater responsibility in protecting or disposing of the PI of consumers, - regardless of how you came into its possession - and must have "administrative, technical, and physical safeguards" in place to both prevent PI from being disclosed to unauthorized third parties and prove that you are handling PI properly through a detailed audit trail.

This white paper provides a detailed analysis of the Rule update and its effect on auto dealerships, and **specifically focuses on how to safeguard the PI (including sensitive geolocation and phone data) that is frequently stored in vehicles dealerships own, including lease returns, loaners, trades, etc.** While this whitepaper does not constitute legal advice, dealerships can find valuable insights to design, implement, and augment their own compliance program. The appendices include:

A. Sample language for a Safeguards program that dealers can use to engage with legal,
B. A strawman of what vehicle data deletion recordkeeping dealerships should consider
C. A sample consumer notice concerning vehicle data

About the Author

This material was prepared by Privacy4Cars in consultation with Randy Henrick, an auto industry compliance consultant with 30 years of experience. Randy is on the board of the Association of Dealer Compliance Officers. He previously worked for DealerTrack where he wrote DealerTrack's compliance guides. Randy also authored NADA's guide to fair lending.

About Privacy4Cars

Privacy4Cars is the first and only technology company focused on identifying and resolving data privacy issues across the automotive ecosystem through a combination of software and services.

Privacy4Cars' rigorous, patented process to delete personal information cars store is designed to reduce risk and is valued by consumers. Privacy4Cars' core PI deletion software has rapidly established itself as a best practice and a standard in the wholesale industry: vehicle manufacturer captives, auto finance companies large and small, fleets and fleet management companies, and dealerships all rely on Privacy4Cars for their compliance with hundreds of state laws and federal regulations.

Given the rising regulatory pressure, scrutiny on safeguarding consumers' personal information, and a growing number of expensive litigation (and settlements) specifically targeting companies accused of not safeguarding consumer personal information collected by vehicles, Privacy4Cars is now offering to dealerships its leading solution to delete Personal Information including phone numbers, call logs, text messages, garage door codes, and more that would otherwise remain stored in modern vehicles' systems after a handoff.

Privacy4Cars offers:

Process

A process that is simple, fast, and intuitive that delivers superior results and that your personnel will love

Procedure

A written procedure for every VIN with detailed deletion records generated by design that are trusted by some of the biggest names in automotive to meet compliance requirements

Proof

Deletion certificates that you can share with your customers to show how you care for their privacy and data security

And…the ability to offer **value-added services**
(such as our "Trade-In Peace Of Mind" offering)

To get in touch with us or schedule a demo please visit Privacy4Cars.com/contact-us

Introduction: PI stored in vehicles and the Updated Safeguards Rule

Privacy Policies of vehicle manufacturers reveal that many vehicles today can collect, store, and transmit various categories of data that fall within the definition of "Nonpublic Personal Information" ("NPI" or "PI") within the meaning of the FTC Safeguards Rule. Examples include, but are not limited to, PI about:

- Individuals or their connected devices' identifiers (including name, address, unique device identifier, IP address, email address, telephone number, gender, date of birth, marital status, and even Social Security Numbers)
- Geolocation data (including home and work address, and other locations that may associate a user with certain protected categories such as race, religion, gender, sexual orientation, and medical conditions)
- Financial and payment information (including transaction history, credit, credit card number, CVV code and expiration date)
- Biometrics, audio, and video information (including weight, voice recordings, video footage, metadata and inferences from recordings, voiceprints, facial recognition, eye scans, and gestures)
- Driver behavior information (including driving style and risk scoring, profiling from the interaction with on-board infotainment, smartphone data, and connected services, physiological or biological characteristics, and medical information)

Personal information concerning the drivers, occupants, and their personal devices ("vehicle data") is collected when vehicle occupants connect their smartphones via a wired (USB) or wireless (Bluetooth, WiFi) connection. Data is also collected directly by the vehicles through their sensors. Further nonpublic personal information is collected, generated, recorded, or stored by vehicles if consumers subscribe to or register for vehicle technologies or services. Increasingly, vehicles are equipped with native data connectivity such as embedded SIM cards that enable the vehicle to collect and transmit vehicle data to the OEM and various third parties. Finally, vehicle data, including nonpublic personal information, may be accessed in service bays through wired (e.g., the OBD-II port) or wireless connections, and also in this case transmitted to OEMs, dealerships, and third parties.

Except for a narrow subset of information (e.g., for service, maintenance, recall, and warranty purposes) and in specific circumstances, a dealer may not want to collect, use, or share this vehicle data. However, by taking financial and physical ownership or control of the assets, the data stored in vehicles is nevertheless owned by the dealer.

The recent October 2021 FTC revision of the Safeguards Rule focuses on electronic nonpublic personal information a dealer may be in possession of, and requires "administrative, technical, and physical safeguards" to be in place to prevent the wrongful use or disclosure such nonpublic personal information. Given much (if not all) of the nonpublic personal information stored in vehicles can be viewed or extracted by dealership personnel or consumers having access to a vehicle, dealers wanting to comply with the updated Safeguards Rule should:

A. Properly disclose to consumers that vehicles may collect, store, and transmit various

categories of data, including data that falls within the definition of "nonpublic personal information"

B. Systematically delete or clear personal information stored in vehicles in their possession

Vehicle data disclosure

Based on the previous considerations, a dealer's Safeguards information security program should address vehicle data, and the portion of vehicle data that constitutes nonpublic personal information under the FTC Safeguards Rule should be protected. There are three separate cases, and dealers should consequently consider making three separate disclosures:

1. **A general disclosure on vehicle data collection capability and transmission and sharing with the OEM and their third parties (excluding the dealership).** Dealers should consider disclosing that vehicles may be able to collect, store, and share data that may fall under the definition of nonpublic personal information. Dealers should refer consumers to the OEM's privacy policy but you may consider disclosing at least some categories, e.g. owner's identity, geolocation, biometrics, and driver behavior information (those are the four "sensitive" categories of information the Auto Alliance and Global manufacturers decided to disclose in their "consumer privacy protection principles" letter to the FTC in November 2014.) If you are a franchised dealer, you may also consider including a link to your brand's privacy policy. Lastly, you may point out that the OEM and their third parties should be the entities in charge of safeguarding the data they obtain directly via the telematics (the cellular connection native to the vehicle itself) and other wireless or wired connections, or indirectly through a data sharing agreement.

2. **A disclosure for the data your dealership may share with the OEM, and the OEM may share with your dealership.** If you are a franchised dealer, you are likely to have a data sharing agreement with the OEM. In that case, you should consider reviewing that data agreement with your attorneys to decide what and how to disclose to consumers. Since each OEM agreement is different and state laws on data protection are different, your state dealer association may provide some guidance.

3. **A disclosure for the data captured and stored in the vehicle itself.** You may consider disclosing what reasonable technical, administrative, and physical safeguards you have in place, as required by the FTC. The only way to effectively safeguard the nonpublic personal information stored locally in a vehicle is by deleting it after each customer use of a vehicle owned by the dealership or upon request by a customer for their vehicle.

Vehicle data deletion

For all the vehicles that a dealership owns or acquires, the Safeguards Program should have a documented process and a record-keeping system covering the following:

1. **Trade-ins and Lease returns:**

   Vehicle data deletion should occur at the point of acquisition and prior to offering the vehicle for sale (e.g., during the make-ready process)

2. **Vehicles purchased at auctions:**

   Unless the buying dealer has evidence that vehicle data was deleted by the auction, vehicle data deletion should occur after taking physical possession of the asset and prior to offering the vehicle for sale (e.g., during the make-ready process)

3. **Repossessed vehicles:**

   Unless the repossessing dealer has evidence that vehicle data was deleted by the recovery agent, vehicle data deletion should occur after taking physical possession of the asset and prior to offering the vehicle for sale (e.g., during the make-ready process)

4. **Vehicles destined to wholesale:**

   For physical auctions, the dealer should delete vehicle data prior to shipping the vehicle to the auction or cause it to be deleted at the auction. For online auctions, the dealer should delete vehicle data either prior to or during the listing process and in either case prior to shipping the vehicle to the buying entity

5. **Test Drives, employee vehicle use, and loaners:**

   Vehicle data should be deleted as part of the vehicle return process prior to the vehicle being made ready to another customer.

Dealers may take temporary custody of **vehicles for service or warranty work**. The terms of servicing or warranty agreements should state that a dealer does not take possession, custody, or control of vehicle data except as necessary to perform the work and that it does not authorize any person to access or use any vehicle data while the vehicle is in the dealer's possession, custody, or control. The terms should indicate that the dealer will not delete any vehicle data unless specifically requested by the customer to do so at the time of service.

Sample language for inclusion in a Safeguards Program is attached as Exhibit A. A sample form for disclosing the existence of vehicle data to consumers is attached as Exhibit B.

Exhibit A: Sample Language for Safeguards Program Relating to Vehicle Data

Many vehicles today can collect and even transmit (through wired or wireless connections) information concerning the vehicle, its drivers, occupants, and their personal devices ("vehicle data"). This vehicle data can be collected by the vehicle through its sensors or when vehicle occupants connect a personal device such as a smartphone. While a large part of the vehicle data will consist of vehicle diagnostic code and operation material, much of this vehicle data may fall within the definition of "nonpublic personal information" within the meaning of the FTC Safeguards Rule. Accordingly, except for purposes of service, recall, or warranty work or if required by applicable law, it is the policy of this dealership to not take possession, custody, or control of vehicle data for vehicles acquired by this dealership and to reasonably attempt to clear and delete vehicle data from all vehicles in which the dealership takes an ownership interest.

Clearing will be done by attempting to systematically delete or make unavailable the vehicle data using good industry practices to do so at or about the time the dealership takes an ownership interest in the vehicle. Specifically, vehicle data deletion will be done and documented as follows unless otherwise required to perform service, recall, or warranty work or to comply with applicable law:

1. **Trade-ins and Lease returns:**

   Dealership will delete vehicle data at the point of acquisition and prior to offering the vehicle for sale (e.g., during the make-ready process)

2. **Vehicles purchased at auctions:**

   Unless our dealership has evidence that vehicle data was deleted by the auction, dealership will delete vehicle data after taking physical possession of the asset and prior to offering the vehicle for sale (e.g., during the make-ready process)

3. **Repossessed vehicles:**

   Unless this dealership has evidence that vehicle data was deleted by the recovery agent, dealership will delete vehicle data after taking physical possession of the asset and prior to offering the vehicle for sale (e.g., during the make-ready process)

4. **Vehicles destined to wholesale:**

   Dealership will delete vehicle data prior to shipping the vehicle to a physical auction or, for online auctions, delete it either prior to or during the listing process or prior to shipping the vehicle to the buyer at the auction.

5. **Test Drives, employee vehicle use, and loaners:**

   Dealership will delete vehicle data on a regular basis in between customer uses, and in any case prior to putting the vehicle for sale

6. **Data deletion prior to delivery:**

   Dealership may further delete vehicle data at the point of delivery of a vehicle to a purchaser or lessee. This vehicle data deletion is intended to cover additional vehicle data that the vehicle may capture from test drives, employee use, or otherwise during the dealer's ownership of the vehicle if such data has not been previously deleted.

The head of the F & I Office will own the process for vehicle data deletion. Vehicle data deletion responsibilities will be delegated to a designated employee. The employee charged with deleting the data will document the date of the deletion on a form that is substantially in the form of the attached document. If the vehicle data cannot be deleted for technical or systems issues involving the vehicle, the employee will complete the form indicating the date of attempted deletion and the reasons why the data was not fully deleted. The employee must sign and date the form and file it as directed by the head of the F & I Office or their authorized deputy. The head of the F & I office must have technical, administrative, and physical systems in place to monitor the data deletion activity and verify the completion of the form for each vehicle in which the dealership takes an ownership interest. The completed forms and any underlying records will be maintained by the head of the F & I Office and are subject to audit.

The dealership acknowledges that it may take temporary custody of vehicles with vehicle data for purposes of servicing, recall, or warranty work. With respect to nonpublic personal information, it is the policy of this dealership not to access, disclose, or use the vehicle data in such vehicles at any time except as and to the extent necessary to perform the service, recall, or warranty work. The following language will be added to all servicing and warranty repair orders:

“Customer acknowledges that the subject vehicle may contain data concerning the customer or its use of the vehicle in an embedded form. This data may be acquired natively by the vehicle or by synchronizing with the customer’s or another person’s devices such as smartphones.

Dealer takes no interest in the vehicle data, and it is the policy of this dealership not to access, use, or disclose the data to any person, except as necessary to perform service, recall, or warranty work or as required by the OEM or authorized by the customer. Access by the vehicle’s OEM or other parties may have been previously authorized by the customer. Except as necessary to perform the service, recall, or warranty work or comply with provisions of law, Dealer will take no action with respect to the vehicle data unless the customer instructs the dealer in a written document to delete any data and then only if the dealer agrees in writing to do so. Dealer has no liability to customer for any matter, cause, or thing relating to vehicle data. If a customer instructs the dealer in writing to delete any data, dealer does so at customer’s sole risk.”

The head of the F & I office will make reports to the Qualified Individual in charge of the dealership’s Safeguards Information Security Program concerning compliance with these procedures along with recommending any changes. Such reports will be made not less often than annually in connection with the dealership’s review of its Safeguards Information Security Program.

Exhibit B: Strawman of Vehicle Data Deletion Recordkeeping

Vehicle Year and Make:

_____

Vehicle Model:

_____

VIN:

_____

Date Acquired:

_____

Date of Initial Data Deletion:

_____

Dates of Further Data Deletions:

_____

Reasons Why Data Could Not Be Fully Deleted (if applicable):

_____

This document certifies that on the subject dates listed above the individual/entity signing this form took industry-appropriate measures to make the personal information stored in the vehicle unavailable by deleting it. Any reasons that may have prevented the individual/entity from deleting the vehicle data are noted. The signing/processing individual has not accessed, transmitted, or communicated the personal data to any person except as may be necessary to perform the data deletion or if otherwise required by law.

_____ _____

Name of Person/Entity Certifying Date of Certification

Exhibit C: Sample Consumer Notice Concerning Vehicle Data

Today's vehicles have electronic systems and processes designed to collect data concerning the use of the vehicle. For example, vehicle telematics is data transmitted from the vehicle to the automaker or OEM through embedded communications systems in the car. Much of this data is diagnostic helping to provide information for the servicing of the vehicle or to identify problems.

In addition to its native data collection and transmission capabilities, many vehicles have systems that capture data from devices that are synced or attached to the vehicle. Examples are a smartphone or data from an insurance company's transponder that measures safe driving behavior. Other applications like a GPS system and other sensors may also generate data that is captured by the vehicle. Some of this data may relate to the users of the vehicle and the persons whose devices are synced.

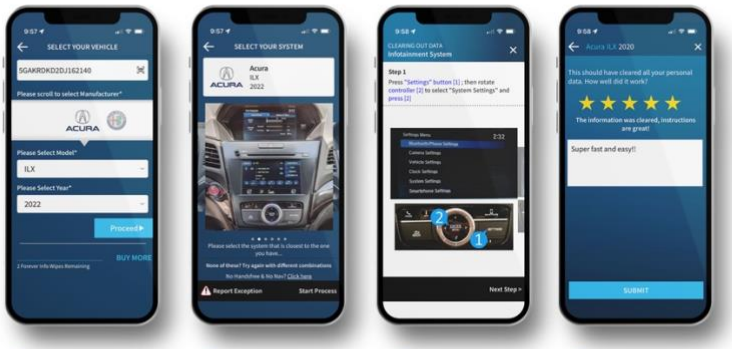
The vehicle manufacturer's privacy policy available on its website may provide more information about vehicle data that is captured directly by the vehicle, from synced devices, or as a result of applications that are linked to the vehicle. You should review their privacy policy to learn both what information is collected and what the manufacturer and its service providers do with the data.

This dealership does not collect or store any data from a vehicle except as necessary to perform service, recall, or warranty work. Use of this data is limited to the purpose for which it is collected. We may also collect a vehicle's data if we are required by law to do so such as if we are subpoenaed.

You have the right to delete data collected by the vehicle. The manufacturer's privacy policy may tell you how to delete data or you can use a commercially available solution to do so.

SELL CARS, NOT YOUR CUSTOMERS' PERSONAL INFORMATION (PI)

The ONLY PATENTED Vehicle Personal Info Clearing Process



- A VIN-specific written standard procedure
- Fast and intuitive (<1.5 min average)
- Anybody can do it
- Proven, superior deletion rates vs. relying on internal "experts"
- Detailed audit trail to prove compliance with federal and state laws on data security, disposal, and privacy

Step 01 › Scan VIN

Step 02 › Select systems to delete

Step 03 › Follow deletion steps

Step 04 Send feedback

Shareable Certificates of Deletion

- A Certificate with deletion details for every VIN
- Share it electronically or print it for your customers
- Show you care: co-branded with your dealership logo
- Backed by Privacy4Cars' $3,000,000 warranty
- Offers opportunities for additional premium services

Uncontested vehicle privacy leader as featured on:

The Washington Post · VICE · The National Law Review · abc News · Car and Driver · UCN · Los Angeles Times · FOX · NBC News · Automotive Compliance Professional · CBS

Schedule a Quick Demo Today!

Privacy4Cars.com/Contact-Us Sales@Privacy4Cars.com

(833) PRI-4CAR (833) 774-4227