ADCO
ASSOCIATION
OF DEALERSHIP
COMPLIANCE OFFICERS

How to Safeguard Personal Information Stored in Vehicles

Dealership guidelines on how to apply FTC's updated Rule to NPI captured and stored by vehicles

Andrea Amico, Founder and CEO, Privacy4Cars

June 22nd, 2022

Presenter

- Andrea Amico is the founder and CEO of Privacy4Cars, the first tech company focused on identifying and solving the data privacy and security issues created by vehicle data
- Privacy4Cars' patented vehicle Personal Information deletion platform is adopted as the compliance best practice by OEM captives, national, regional, and local auto finance companies, fleets and fleet management companies, and dealerships
- Co-chairs the compliance and education committee at the International Automotive Remarketing Alliance
- Discovered and ethically disclosed multiple vehicle vulnerabilities to tens of automakers and other companies in the automotive ecosystem
- Former engineering ethics adjunct professor, president of a large auto logistics business, managing director of strategic initiatives at NBC Universal, manager at McKinsey&Co.
- Lives in Atlanta, has a MBA from Columbia University, a Master in mechanical and industrial engineering for Italy and Sweden.

Panelist

- Randy Henrick is an experienced auto dealer compliance and consumer credit attorney and consultant. He was the regulatory and compliance attorney for Dealertrack, Inc. for 12 years and authored all of the Dealertrack's Compliance Guides. Randy also was the thought leader for Dealertrack's Compliance product.

- Randy has over 30 years experience in consumer credit and compliance. Prior to Dealertrack, Randy worked for GE Capital, Citibank, MasterCard International, and Fleet Boston. Randy does dealer consulting to provide assistance with regulatory and compliance issues ranging from advertising and policy reviews to webinar-based training on sales, F & I, privacy, data security, and other topics.

- Randy writes monthly articles in Subprime Auto Finance News covering an array of legal, regulatory and compliance best practices for vehicle dealers. He has spoken at four NADA conventions and three NIADA conventions. Randy has worked with NADA on training and publications as well. Randy wrote the NADA Management Series “A Dealer Guide to Federal Truth in Lending Requirements” (2018).

Disclaimer

The information in this webinar presentation is provided for general informational purposes only and may not reflect the current law in your jurisdiction. Nothing in this presentation should be construed as legal advice from the Association of Dealership Compliance Officers or the individual presenter, nor is it intended to be a substitute for legal counsel on any subject matter. The views and opinions in the presentation are those of the presenter and do not necessarily represent official policy or position of the Association of Dealership Compliance Officer or its members or advisors.

No attendee of this presentation should act or refrain from acting on the basis of any information included in this presentation without seeking the appropriate legal or other professional advice on the particular facts and circumstances at issue from a lawyer licensed in the attendee's state, country or other appropriate licensing jurisdiction.

New Safeguards Rule

- FTC exercised its rulemaking authority, new Rule comes into effect on December 9th 2022
- Specifically written in response to growing collection of electronic data about consumers and rising rate of data breaches
- Three main areas of change:
  - Personal Information is very broadly defined (not just SSN or credit info)
  - It applies no longer just to financial institutions (incl. dealerships), but also marketplaces and suppliers to regulated entities
  - Abandon “Reasonable Security” standard for a prescriptive list of requirements

3/29/22, 1:00 AM

FTC Strengthens Security Safeguards for Consumer Financial Information Following Widespread Data Breaches | Federal Trade Commission

FEDERAL TRADE COMMISSION
PROTECTING AMERICA'S CONSUMERS

For Release

FTC Strengthens Security Safeguards for Consumer Financial Information Following Widespread Data Breaches

Agency updates Safeguards Rule to better protect the American public from breaches and cyberattacks that lead to identity theft and other financial losses

October 27, 2021
Tags: Consumer Protection | Bureau of Consumer Protection | Finance | Privacy and Security | Consumer Privacy | Data Security | Gramm-Leach-Bliley Act

The Federal Trade Commission today announced a newly updated rule that strengthens the data security safeguards that financial institutions are required to put in place to protect their customers' financial information. In recent years, widespread data breaches and cyberattacks have resulted in significant harms to consumers, including monetary loss, identity theft, and other forms of financial distress. The FTC's updated Safeguards Rule requires non-banking financial institutions, such as mortgage brokers, motor vehicle dealers, and payday lenders, to develop, implement, and maintain a comprehensive security system to keep their customers' information safe.

"Financial institutions and other entities that collect sensitive consumer data have a responsibility to protect it," said Samuel Levine, Director of the FTC's Bureau of Consumer Protection. "The updates adopted by the Commission to the Safeguards Rule detail common-sense steps that these institutions must implement to protect consumer data from cyberattacks and other threats."

The changes adopted by the Commission to the Safeguards Rule include more specific criteria for what safeguards financial institutions must implement as part of their information security program such as limiting who can access consumer data and using encryption to secure the data. Under the updated Safeguards Rule, institutions must also explain their information sharing practices, specifically the administrative, technical, and physical safeguards the financial institutions use to access, collect, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle customers' secure information. In addition, financial institutions will be required to designate a single qualified individual to oversee their information security program and report periodically to an organization's board of directors, or a senior officer in charge of information security.

The Safeguards Rule was mandated by Congress under the 1999 Gramm-Leach-Bliley Act. Today's updates are the result of years of public input. In 2019, the FTC sought comment on proposed changes to the Safeguards Rule and, in 2020 held a public workshop on the Safeguards Rule.

In addition to the updates, the FTC is seeking comment on whether to make an additional change to the Safeguards Rule to require financial institutions to report certain data breaches and other security events to the Commission. The FTC is issuing a supplemental notice of proposed rulemaking, which will be published in the Federal Register shortly. The public will have 60 days after the notice is published in the Federal Register to submit a comment.

Today, the FTC also announced it adopted largely technical changes to its authority under a separate Gramm-Leach Bliley Act rule, which requires financial institutions to inform customers about their information-sharing practices and allow customers to opt out of having their information shared with certain third parties. These changes align the rule with changes made under the 2010 Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank). Under Dodd-Frank, Congress narrowed the FTC's jurisdiction under that rule to only apply to motor vehicle dealers.

The Commission voted 5-0 to publish the final revisions to update the FTC's jurisdiction under Dodd-

https://www.ftc.gov/news-events/press-releases/2021/10/ftc-strengthens-security-safeguards-consumer-financial-information-0

1/2

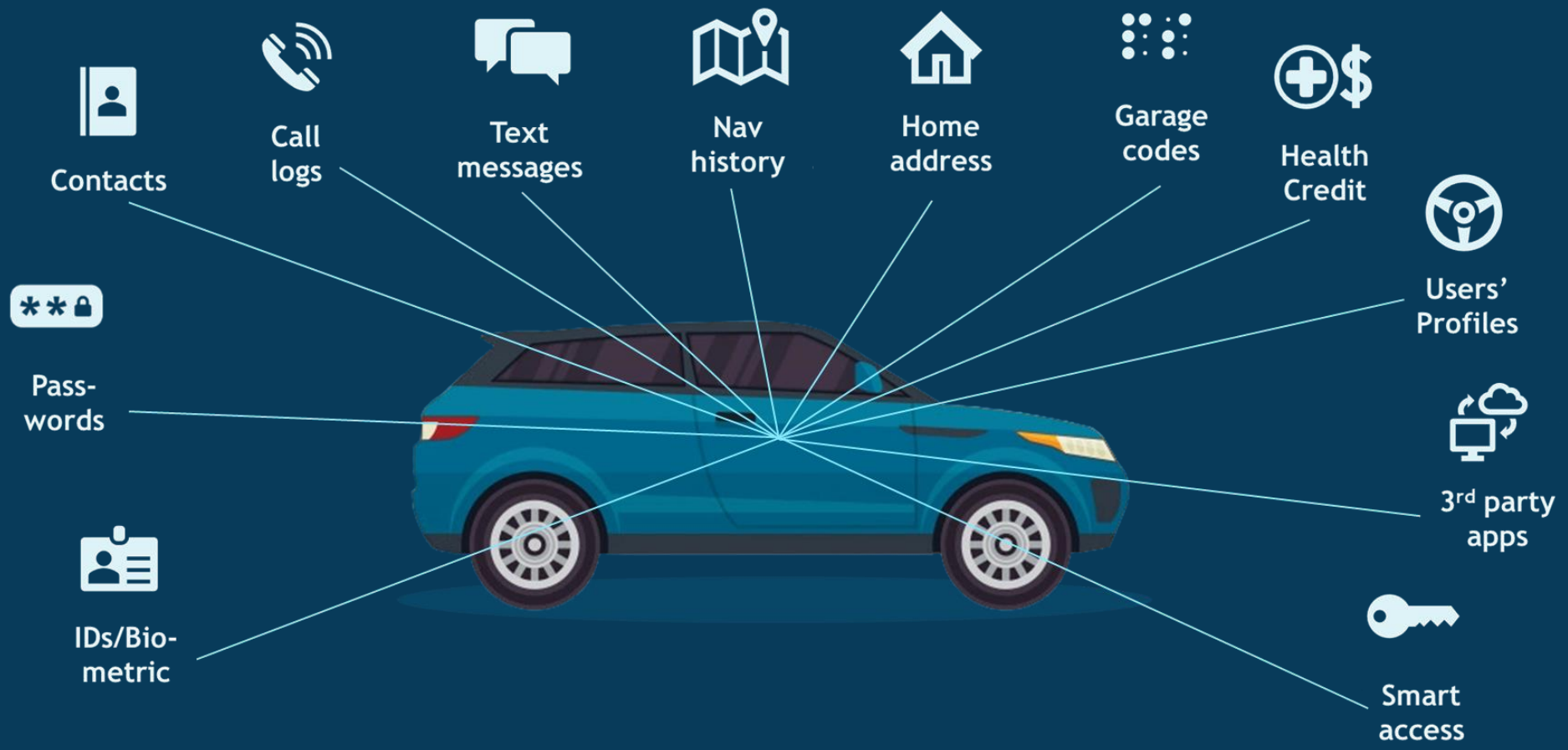
NADA

New Requirements

Qualified Employee	Written Risk Assessment	Access Controls	Data and Systems Inventory
Data Encryption	Secure Development Practices	Multi-Factor Authentication	Systems Monitoring and Logging
Secure Data Disposal Procedures	Change Management Procedures	Unauthorized Activity Monitoring	Intrusion Detection/ Vulnerability Testing
Overseeing/Monitoring Service Providers	Written Incident Response Plan	Annual Reporting to Board	

#NADASHOW

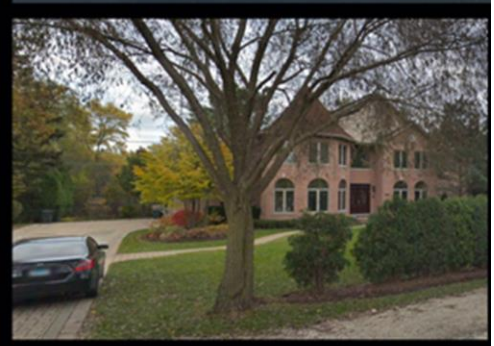
Vehicles are Unencrypted Databases of Personal Information

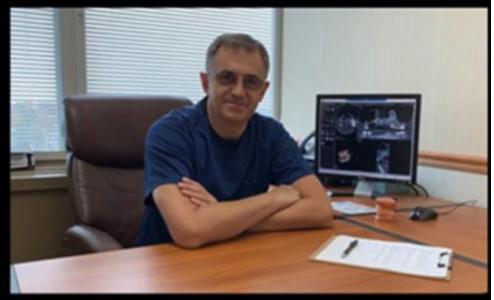


Real Example: A Luxury Vehicle For Sale

- Shot a 30-second video during a test drive
- Fully reidentified previous owner, wife, and son (a minor)
- Have received multiple reports from new owners of vehicles previously owned by celebrities, wealthy individuals, politicians
- **Whose reputation and liability is at risk?**

- Vehicle formerly owned by Vladimir [redacted] (54, dentist, owns [redacted] of Chicago)
  - Living with wife Victoria (51) at [redacted] Glenview IL: $1m single home, 5BR, 4 BA, 3 car garage (have codes)
  - His email is d[redacted]a2@gmail.com
  - Have 4 mobiles and 3 landlines for the family
  - He sees a nutritionist (Dawn [redacted], RD) and goes to an exercise coach and to LA Fitness (but stops at Starbucks before or after the gym)
  - Had a recent visit at [redacted] Retinal Consultants (5600 W[redacted]gs)
- Son is a senior at New [redacted] High School
  - He is a competitive swimmer (recent competitions include [redacted] Hills High School, at [redacted] Green Center, at [redacted] High School, at [redacted] Catholic High School)
  - He is taking safe driving lessons at [redacted] School of Driving
  - He is getting SAT support at two different [redacted] Tutoring Centers ([redacted] Avenue, Highland Park and at [redacted] ve, Northfield) – mother unhappy with service
  - He has been with his dad to college campuses, including Northwestern University (where is father is an alumnus) and Indiana University Bloomington
- Wife
  - Victoria likes shopping at unusual clothing stores: Squasht Boutique, Chloe's Boutique, Moda Too, and to the home of designer Olivia Joffrey
  - Likely remodeling the house: recently visited an architect, an interior design group, and a furniture store. Shopped at BBQ store.
- Have addresses of 5 friends






PRIVACY4CARS
REPORTING
TRAINING
ABOUT US
Contact Us
HOME
PERSONAL USE
FOR BUSINESS
LEGAL RESOURCES
DATA IN CARS
NEWS
Over 4 Out Of 5 Cars Sold Last Year Contained Personal Data
Privacy4Cars enables the automotive ecosystem to delete personal information from vehicles in a fast, traceable, and cost-effective manner to reduce liability, meet regulatory requirements and improve customer satisfaction
Protect Yourself & Your Family
Protect Your Business & Customers
Car shoppers who found previous owners' PI by test driving 1 or 2 cars of their choice
12%
88%

New Requirements

State that vehicles capture PI and your policy on how to protect against risk of exposure to employees and other consumers

Responsible for all PI (incl. in-vehicle)

Qualified Employee	Written Risk Assessment	Access Controls	Data and Systems Inventory
Data Encryption	Secure Development Practices	Multi-Factor Authentication	Systems Monitoring and Logging
Secure Data Disposal Procedures	Change Management Procedures	Unauthorized Activity Monitoring	Intrusion Detection/ Vulnerability Testing
Overseeing/Monitoring Service Providers	Written Incident Response Plan	Annual Reporting to Board	

Consumer Disclosures On Vehicle Data

There are three separate cases where nonpublic personal information under the FTC Safeguards Rule should be protected:

1. **A general disclosure on vehicle data collection capability and transmission and sharing with the OEM and their third parties (excluding the dealership)**
   - Vehicles may be able to collect, store, and share data that may fall under the definition of NPI
   - Refer consumers to the OEM's privacy policy; franchised dealers may link to it
   - Consider disclosing at least owner's identity, geolocation, biometrics, and driver behavior information

2. **A disclosure for the data your dealership may share with the OEM, and the OEM may share with your dealership**
   - For franchised dealers only. Consider reviewing your OEM data agreement with your attorneys (each OEM agreement is different and state laws on data protection are different)
   - Consider contacting your state dealer association may provide some guidance.

3. **A disclosure for the data captured and stored in the vehicle itself**
   - *More on this…*

New Requirements

State that vehicles capture PI and your policy on how to protect against risk of exposure to employees and other consumers

Responsible for all PI (incl. in-vehicle)

Qualified Employee	Written Risk Assessment	Access Controls **Not Possible**	Data and Systems Inventory
Data Encryption **Not Possible**	Secure Development Practices **Not Possible**	Multi-Factor Authentication **Not Possible**	Systems Monitoring and Logging
Secure Data Disposal Procedures	Change Management Procedures **Not Possible**	Unauthorized Activity Monitoring **Not Possible**	Intrusion Detection/ Vulnerability Testing **Not Possible**
Overseeing/Monitoring Service Providers	Written Incident Response Plan	Annual Reporting to Board	

#NADASHOW

New Requirements

State that vehicles capture PI and your policy on how to protect against risk of exposure to employees and other consumers

Responsible for all PI (incl. in-vehicle)

Need detailed metrics and logs for day-to-day management of the program as well as for annual reporting to board/principle

Only solution: clear PI from vehicles for sale, lease returns, trade-ins, loaners

Includes OEMs and 3rd parties

Qualified Employee	Written Risk Assessment	Access Controls	Data and Systems Inventory
		Not Possible	
Data Encryption	Secure Development Practices	Multi-Factor Authentication	Systems Monitoring and Logging
Not Possible	Not Possible	Not Possible	
Secure Data Disposal Procedures	Change Management Procedures	Unauthorized Activity Monitoring	Intrusion Detection/ Vulnerability Testing
	Not Possible	Not Possible	Not Possible
Overseeing/Monitoring Service Providers	Written Incident Response Plan	Annual Reporting to Board	

Data disposal minimizes need for an IRP

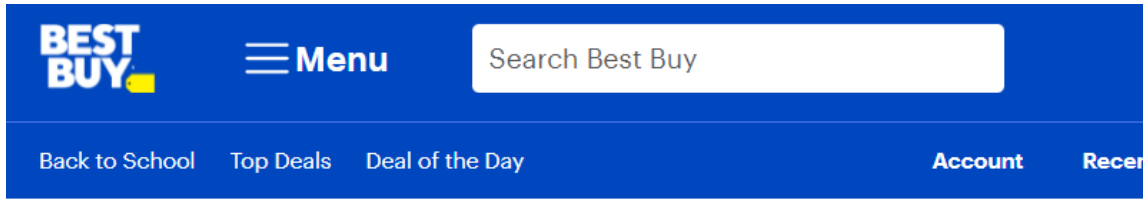
#NADASHOW

Disclosure, Policy, and Process to Protect In-Vehicle PI

1. **A disclosure and Policy for the data captured and stored in the vehicle itself**
   - Delete PI stored in vehicles prior to next handoff is the only reasonable technical, administrative, and physical safeguards you can have in place (as required by the FTC)
   - Need to cover (1) trade-in & lease returns, (2) wholesale purchases, (3) repos, (4) vehicles desined to wholesale, and (5) test drives, employee vehicle use, loaners
   - Disclaimer for warranty or service work

2. **Have "administrative, technical, and physical measures" to delete consumer PI from all vehicles prior to reintroducing them into the stream of commerce**
   - Want to do efficiently (little time and with lowest cost resources)
   - Want to do it effectively (little percentage of defects)
   - Want to do it in a auditable manner (need detailed records)
   - Want to do it in a way that communicates value to your customers

Established Best Practice For Computers and Smartphones

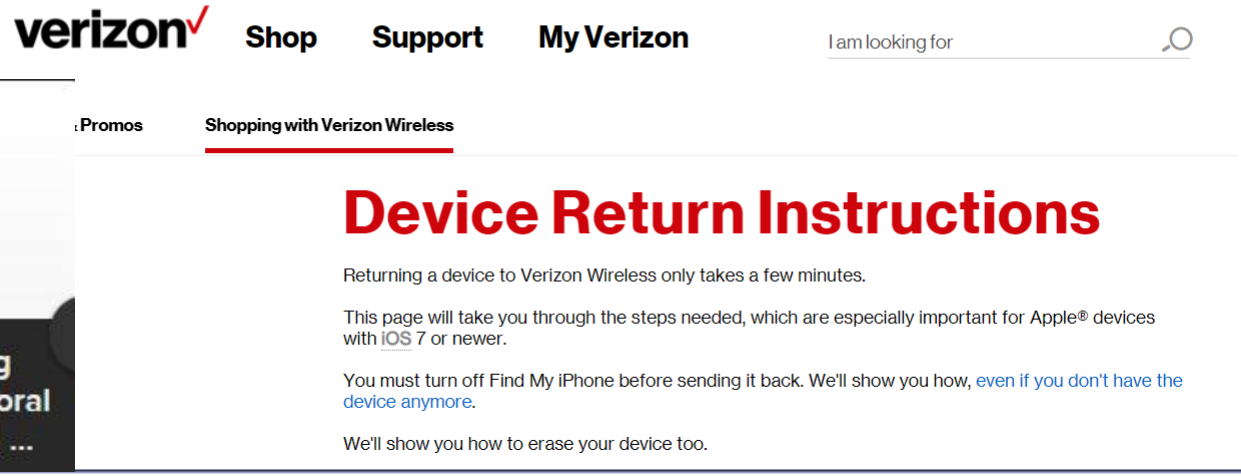


Best Buy › Customer Service › Help › Privacy Policy

How Best Buy interacts with your devices.

We know you entrust us with your confidential and personal information when you use Best Buy to provide service and support on your device. And while you should always remove your data from any device you choose to dispose of, we also work to protect your confidential and personal information through appropriate handling, safe storage, and high standards for wiping your data. We know that, as our customer, you expect us to safeguard your data at all times and in all of these situations.

NIST 800-88 Rev 1 mandates data clearing as a minimum reasonable standard



Two Approaches to Deleting In-Vehicle PI

Tell to delete:

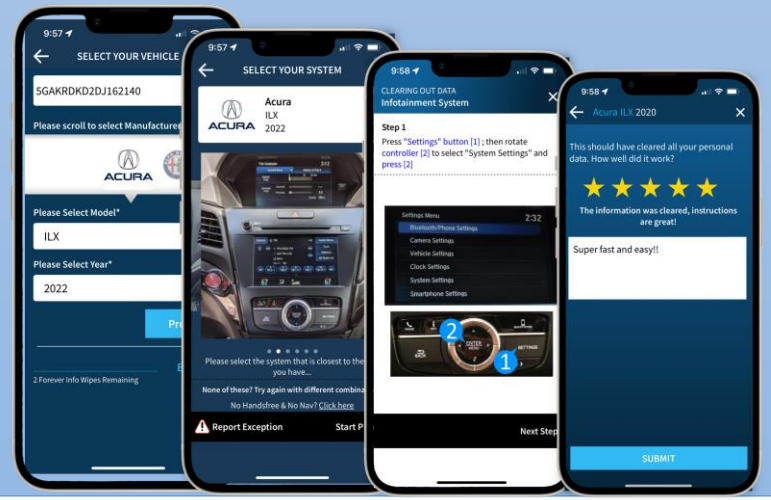
- Rely on user knowledge
- Record-keeping is inefficient or ineffective
- Typical audit shows **30-70% of vehicle still contain PI after processing**

Give a tool to delete:

- Almost foolproof
- Records by design and by default
- Can be embedded in you own apps
- Offer value-add privacy services

01 Scan VIN
02 Match Infotainment System
03 Follow Deletion Steps
04 Send Feedback

US PATENT #
US11157648B1
US11113415B1
US11256827B1



What Car Shoppers Say When They Find Personal Data In Cars

Seeing the last owners home address and routine navigational routes scared me and really made me realize there is a problem.

This is a brand I would have usually been interested in purchasing. However, I am not confident in the salesperson answers to evidence that was seen in the brand vehicles navigation system left by the last owner.

Based on the salesperson answers about privacy, they won't keep me from returning one way or another.

My private information is available for anyone to see and copy.

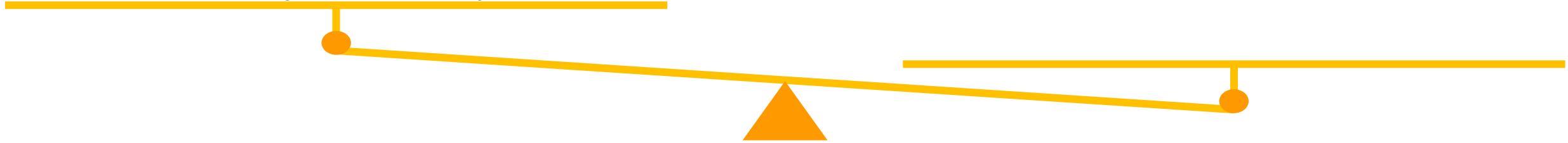
Why would I give away my personal information? I don't even answer the phone from a number I don't know. I value my privacy.

It seems very important that the privacy is protected both in the computer in the car and from the computer in the dealership

Compliance to Unlock Value For Your Dealership

- Legal exposure
  - Safeguards Rule
  - Over 200 state laws https://privacy4cars.com/legal-resources/laws-by-geography/
  - Growing list of lawsuits
- Reputation exposure
  - 86% of vehicle owners are concerned
  - The more they learn, the more are concerned
  - 41% is less likely to buy from same dealer/OEM
  - 12% believe they are owed compensation

- Barrier against competitors who do not protect PI
  - Dealership Net Promoter Score of 44 (very high) for dealerships who tell consumers they delete data (and consumer does not find data) vs. NPS of -11 (extremely low) when consumers find PI
- Opportunity for new services
  - 87% of vehicle owners are willing to pay for a certificate attesting PI is deleted and protected
  - 87% of vehicle owners are willing to purchase monthly coverage to protect vehicle data



Resources Available To You

- Whitepaper can be downloaded at https://privacy4cars.com/dealers/
- Includes sample language you can review with your legal counsel
  - A. Sample language for a Safeguards program
  - 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.

- Additional resources on the Privacy4Cars Website
- Contact us at info@privacy4cars.com

Thank You For Your Time