November 7, 2018

Submitted via email at privacyrfc2018@ntia.doc.gov

National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Avenue NW, Room 4725
Attn: Privacy RFC
Washington, DC 20230.

Re: Developing the Administration's Approach to Consumer Privacy, Docket No. 180821780-8780-01.

The National Automobile Dealers Association ("NADA") submits the following comments to the U.S. Department of Commerce, National Telecommunications and Information Administration ("Department" or "NTIA"), regarding the notice and request for public comment ("Notice") on ways to advance consumer privacy while protecting prosperity and innovation.

NADA represents over 16,000 franchised dealers in all 50 states who market and sell new and used cars and trucks, and engage in service, repair, and parts sales to consumers and others. Our members collectively employ over 1 million people nationwide. Most of our members are small businesses as defined by the Small Business Administration. In the course of their operations, NADA members routinely gather and maintain consumer information and take numerous steps to ensure that data is protected from both a process and technology perspective.

In addition, as "financial institutions" under the Gramm Leach Bliley ("GLB") Act, automobile dealers have many years of experience with certain core privacy and data security concepts and implementation of those concepts in practice. And as automotive retailers, dealers

May 1, 2017

Filed Electronically at https://ftcpublic.commentworks.com/ftc/connectedcarsworkshop

Office of the Secretary
Federal Trade Commission
Suite CC-5610 (Annex A)
600 Pennsylvania Avenue, NW
Washington, DC 20580

Re: Connected Cars Workshop P175403

Dear Secretary:

The National Automobile Dealers Association ("NADA") [1] submits the following comments in response to the Notice seeking comments on the FTC/NHTSA Connected Cars Workshop ("Workshop") that the Federal Trade Commission ("FTC" or "Commission") published in connection with the above captioned matter.[2]

In a modern car, there is no key, you press a button and you watch an operating system load, and you watch it connect to your devices and the internet. Today's vehicles are not simply a connected computer, but a connected network.[3] Computers control your steering, brakes, and other systems. Indeed, virtually every aspect of your car has some sort of software exposure. These software systems gather, create, store, and transmit data about the vehicle, the driver, its occupants, and its surroundings in ways that consumers generally do not yet understand, and in many ways they do not expect. Currently (or soon to be) available sensors gather data about the

[1] NADA represents over 16,000 franchised dealers in all 50 states who (i) sell new and used cars and trucks; (ii) extend vehicle financing and leases to consumers that routinely are assigned to third-party finance sources; and (iii) engage in service, repair, and parts sales. Our members collectively employ over 1 million people nationwide. Most of our members are small businesses as defined by the Small Business Administration.

[2] Available at https://www.ftc.gov/system/files/attachments/press-releases/ftc-nhtsa-conduct-workshop-june-28-privacy-security-issues-related-connected-automated-vehicles/notice_connected_cars_workshop_with_nhtsa_1.pdf

[3] The average modern vehicle contains dozens of individual computers.

location and speed of a vehicle, as well as biometric (e.g., facial recognition, fingerprint, and other physical) and health related data (e.g., heart rate, breathing) about the driver and the passengers. In addition, there are (or soon will be) microphones and cameras that can record conversations and video within the vehicle cabin, sensors recording driver behavior data (e.g., the way in which the driver operates the vehicle, whether they are looking at the road, etc.), weather sensors, road condition sensors, light detection and ranging (LIDAR) sensors, cameras recording pedestrians and other information outside the automobile, and many more. And as the Notice states, such data gathering and connected systems are vast in scale and "will only become more complex in the future, with increased functionality," as vehicles connect beyond the internet ("connected vehicles"), to each other ("V2V"), the infrastructure ("V2I"), and ultimately to numerous other entities and outlets ("V2E").

NADA agrees that the overall promise of connected vehicles is to help consumers, add to in-vehicle entertainment options, increase convenience, and promote safety. However, we also agree that these same technologies must be carefully considered, and that addressing three broad areas of potential concern are fundamental, and must be thoughtfully and completely addressed *before* many of these technologies are deployed – (1) privacy, (2) cybersecurity, and (3) consumer education and choice. In each of these areas, NADA dealer members play and will continue to play a central role.

1. Privacy.

Much of the data gathered by this array of sensors is personal and highly sensitive. It is also valuable, and thus there will a tremendous push for access (along with a tremendous incentive to share). Standing alone, the existence of this data in the vehicle presents substantial privacy challenges. However, once that automobile is connected to the internet, the concerns multiply exponentially because that data becomes exposed. Dealers believe that this data should largely be treated as highly sensitive and personal and therefore automobile consumers should be provided transparency and choice with respect to the gathering and use of that data. The FTC and other regulators, along with industry participants, should work to ensure that consumers (a) fully understand the data that is being collected by the automobile, and any devices connected to the automobile, and (b) have control over what data is gathered and whether and how it is shared. Such protection would allow consumers to make informed choices whether the sharing of this data is worth the convenience or product functionality that is offered in exchange for the data. If not,

consumers will not only be deprived of the value of this highly sensitive data, but consumer acceptance of these new technologies will be suppressed, and the safety and convenience promises of these new technologies will not be fulfilled.

We do not believe that consumers currently understand what data is collected in and through their vehicles today – and the problem is likely to get much worse. Dealers routinely get questions from consumers about what data is collected and stored in their vehicles, and in many cases, even the dealer is unable to determine with any accuracy what data a vehicle is collecting or has collected (much less what data is being collected by phones or other devices plugged into the vehicle's USB port, or aftermarket dongles or other devices plugged into the vehicles OBD-II port). That is because there is often no public disclosure of such information, and no standardized method for doing so.

In our view, manufacturers and any third party collecting data in or through a connected automobile should make all relevant information about data collection publicly available (e.g., via website). This should include not only what data is collected, but also: (a) the means by which it is collected (sensors, microphones, cameras, etc.); (b) whether that data is necessary for any vehicle safety feature; (c) how a consumer can turn off or deactivate that data collection; (d) whether that information is shared with any unaffiliated third party, and; (e) how a consumer can opt-out of such sharing.

The last point is particularly important from a privacy perspective because many of these data collection devices will need to be operative in order for certain safety or convenience features of the vehicle to operate properly. Consumers should not be required to choose between privacy and safety- that is, they should not have to choose between allowing personal data to be shared or turning off the sensor altogether. There should be an option, where possible, for a consumer to allow a sensor to operate but limit the sharing of the data collected.

One other issue that the FTC and NHTSA should consider is how to protect the privacy of consumers who do not own the vehicle. This would include passengers in privately owned vehicles, as well as passengers in ride-sharing, taxi, rental, or related services. Such passengers are even less likely to be aware of the data being collected about them in the vehicle, and should not forfeit their own privacy rights simply by riding in a vehicle they do not own.

In addition, we note that the much of the current debate focuses almost exclusively on the vehicle manufacturers and their privacy obligations. However, the manufacturers (and their dealers) are the entities most likely to have legitimate needs for consumer vehicle data in order to improve the safety, efficiency and security of the vehicles they manufacture, and to securely service and maintain those vehicles. At the same time, they also have the greatest incentive to protect that data. In our view, it is more likely that non-manufacturer entities with access to customer data[4] (legitimate or otherwise) present a far more substantial privacy threat than the manufacturers themselves.[5] There are many entities who are seeking access to personal data from connected vehicles, and many more to come. While a certain focus on automobile manufacturers is appropriate, we would urge the FTC and NHTSA to also provide the strongest possible protections by focusing more specifically on third parties with access to that sensitive data. This should include tools for consumers and manufacturers to enforce privacy protections and obligations against third parties, as well as penalties against third parties who seek to access such data without the consumer's knowledge or express permission.

It is not only commercial interests that are seeking access to this data. Policymakers must also address the sharing of personal data from the vehicle with governmental entities. There may likely be benefits to sharing such information, in certain limited circumstances, with law enforcement, local transportation authorities, or federal regulators, but the benefits of such sharing could be outweighed by the chill to consumer demand and appetite for connected vehicles if such sharing is not tightly and reasonably controlled. We would urge that any such sharing be done in accordance with the best practices of "Minimization, De-Identification and Retention." In other words, governmental entities should only collect the data they absolutely need, retain the minimum amount of data required to achieve safety purposes, do so in an aggregate anonymized fashion to the extent possible, and in no event, collect or require any personal information. These efforts must also be completely transparent to the consumer so that they have a clear understanding of what information is being so recorded and shared.

---

[4] This could include a phone or other device that is connected to the vehicle, an app that resides on that device (or within the vehicle's software), a third-party aftermarket product that can plug into vehicle diagnostic systems, or a third party outside of the vehicle seeking to remotely access vehicle data.

[5] That is because they will have all the incentive to use or abuse such information, with none of the accountability that the manufacturers or dealers will have/ Indeed, if there is one issue that has become clear over the last several years, it is that it is often service providers or other third party actors that present the most acute weaknesses in a cybersecurity or privacy regime.

2. Cybersecurity Issues

Cybersecurity is of immeasurable importance in a connected vehicle – especially with the increasing autonomy features available in today's vehicles (and the potential for full autonomy in the coming years). The consequences of failure to protect access to this information and these systems are potentially disastrous, not only from a privacy perspective, but from a safety perspective as well.[6] It is indisputable that adding software to something makes is weaker from a cybersecurity standpoint, and connectivity makes it exposed. The reality is that no system is secure, and experience has shown that, unfortunately, the failure rate is 100%. In other words, it is not whether a problem will occur, but when. As automobile manufacturers incorporate more advanced technologies into their automobiles, dealers believe that great care is needed to ensure that security comes first, even if it means that certain features, attributes, or systems must be limited or delayed, or that other competing interests must be overridden. This will require, in our view, adherence to certain principles, including:

- Security must be a nonnegotiable fundamental against which convenience, efficiency, and consumer demand must be measured.
- Systems must be designed to allow flexibility, but third party access must be limited to ensure security.
- Intensive training and education must be built into all levels of vehicle design, sales and operation.
- Security and privacy of the consumer and vehicle data must be optimized by ensuring that the entire vehicle ownership ecosystem - vehicle, dealership, and infrastructure - is secure.

Manufacturers can produce a secure vehicle, but if that vehicle cannot be sold or serviced securely, or if remote access is allowed to critical software, that security becomes meaningless. Similarly, the manufacturers and their dealers can protect sensitive consumer data, and honor their promises, but if a third party is able to access that same data, those privacy promises could also become meaningless

[6] We agree that "[p]rotecting the security of these vehicle technologies is crucial to maintaining adequate privacy and safety protections." Notice at 1.

Dealers believe strongly that efforts such as that of this Workshop must include a broad view of the vehicle lifecycle, and that unless the entire vehicle ecosystem is secure, great risks will remain. That ecosystem includes not only the vehicle itself - both new and used - but also the infrastructure and dealer service systems. NADA has been working closely with our manufacturer partners to ensure that dealers are prepared to meet these tremendous challenges. We have been and will continue to work diligently to help ensure that dealers have the training, tools, and equipment needed to perform this increasingly complex service work in a secure manner. We have also been working closely with manufacturers, technology vendors, and others to help establish the secure and compliant systems required to protect vehicles, dealer networks, and consumers from harm. NADA will continue to work both on an industry-wide basis to ensure that our dealers meet the high standards of professionalism and expertise that will be required, and to ensure that customer convenience is maximized without sacrificing the safety and security of the vehicle

In sum, we would urge the FTC and NHTSA to take a broad, holistic approach to vehicle security and privacy, and when the choice is presented between faster implementation of connected features and functionality and safer, more secure implementation of that functionality to err on the side of caution.

a. Used Car Purchasers /Marketplace

As you proceed in your efforts, we urge you to consider the effects of the changes in the vehicles of tomorrow on the used vehicle market. Cars are unlike other "connected" devices for a number of reasons, one of which is that they generally have multiple owners. In fact, millions more used cars are sold in this country each year than new. A subsequent purchaser of a vehicle needs to be as assured as an original purchaser regarding the safety, privacy, and security protections provided. This will likely mean a far greater degree of interaction and obligation between used vehicle purchasers and manufacturers (and others) than ever before, and is another area where dealers role will play a key role. As automobiles become more and more computerized, issues such as software licenses, support for older technology, transferability of privacy obligations to subsequent owners, and ensuring that used vehicle owner privacy preferences are honored will need to be addressed. Any lack of confidence in the safety, security, or privacy of that vehicle could create havoc in the used car market, with the bulk of the harm falling on unsuspecting consumers who purchase those vehicles.

3. Consumer Education and Choice

For over 100 years, automobile dealers have directly served the needs of new and used vehicle consumers through the sales and service of automobiles. Dealers' entire business model is built around serving those consumers, and building "customers for life." In furtherance of that goal, dealers have historically played a central role in educating consumers on the features, capabilities, and operation of the automobiles they sell and service, and that mission will not change. Dealers also provide an array of notices and other materials to consumers addressing issues such as vehicle financing, and the effect of a consumer's credit status on the cost and availability of credit. In addition, as "financial institutions" under the Gramm Leach Bliley ("GLB") Act, automobile dealers have many years of experience in both safeguarding sensitive consumer data, and notifying consumers about the collection and sharing of certain types of sensitive consumer data.

In recent years, as cars have become increasingly complicated, dealers' educational efforts with respect to advanced safety features on modern vehicles have also increased,[7] as have consumer questions about the types of data collected and stored in vehicles.[8] For example, dealers routinely face questions about how to remove personal data from a used vehicle that a consumer is trading in. To aid dealers in their efforts to keep consumers informed, NADA, working in conjunction with the Future of Privacy Forum, produced a consumer education pamphlet "Personal Data In Your Car," a copy of which is attached at Exhibit A. That pamphlet details the types of data that may be stored in today's vehicles, and provides advice to consumers to protect and remove that data when trading in a vehicle. It is yet another example of the interface between dealers and consumers with respect to this issue.

Consumers look to dealers for information about their vehicles, and we believe that dealers will continue to be best suited to provide consumers with such information, including the types of data that a vehicle collects, why it collects that data, and what choices they have with respect to

[7] NADA and its dealers have also taken steps to work with groups such as the National Safety Council on consumer education through efforts such as www.mycardoeswhat.com to help consumers understand these important safety features.

[8] NADA believes that a clear and relatively simple method should exist that would allow consumers to delete all personal information from a vehicle anytime they wish to do so. There are broader questions about the use and storage of much of that data outside the vehicle, but with respect to the vehicle itself, consumers and dealers would benefit from a fairly simple "reset button" that would allow a consumer who trades in (or returns a lease vehicle) to delete all personal information from that vehicle.

that data collection and sharing. We believe that most consumers will want to make informed choices about data collection and sharing, and that dealers are best suited to help consumers understand the choices that will be available to them.

4. Conclusion

The tremendous promise represented by the technological improvements in automobiles will not be realized if that technology is not secure, and if consumers do not have transparency and robust privacy protections as to the data collected. Dealers' central role in selling and servicing automobiles in the United States will become increasingly complex and increasingly important as the vehicles become more complex in terms of functionality as well as data collection. NADA's members have a keen interest in the issues presented in the Workshop, and would urge the FTC and NHTSA to utilize the expertise and experience of dealers as they approach these critically important issues. We respectfully request the opportunity to participate in the workshop as panelists, and to help in any other way that we can.

We appreciate the opportunity to comment on this matter. Please contact me if we can provide further information that would be useful to the Commission.

Sincerely,

Brad Miller
Director, Legal and Regulatory Affairs

EXHIBIT A – "PERSONAL DATA IN YOUR CAR"

ATTACHED UNDER SEPARATE COVER

PERSONAL DATA IN YOUR CAR

National Automobile Dealers Association and the Future of Privacy Forum

YOUR CAR AND NEW TECHNOLOGIES

Today's vehicles come with a wide array of equipment and features that rely on the collection and use of data about you and/or your vehicle to support safety, efficient performance, convenience, and entertainment.

Depending on the make and model, and the options you select, these features may include technologies like navigation, blind spot detection, automatic emergency braking, parking assist, lane departure warnings, and many others. These features also include "infotainment" features, in-car "apps," telephone and text connectivity, and even in-vehicle internet connectivity.

Many of these features depend on collecting certain data about you, your vehicle, and your driving habits in order to perform effectively. Some of this data may be collected automatically, and some you may choose to provide in order to enable certain functions. For example, in order for you to benefit from navigation and traffic services, the location of your vehicle is generally needed. Similarly, to enable easy hands-free dialing, you may choose to sync your phone address book to the vehicle.

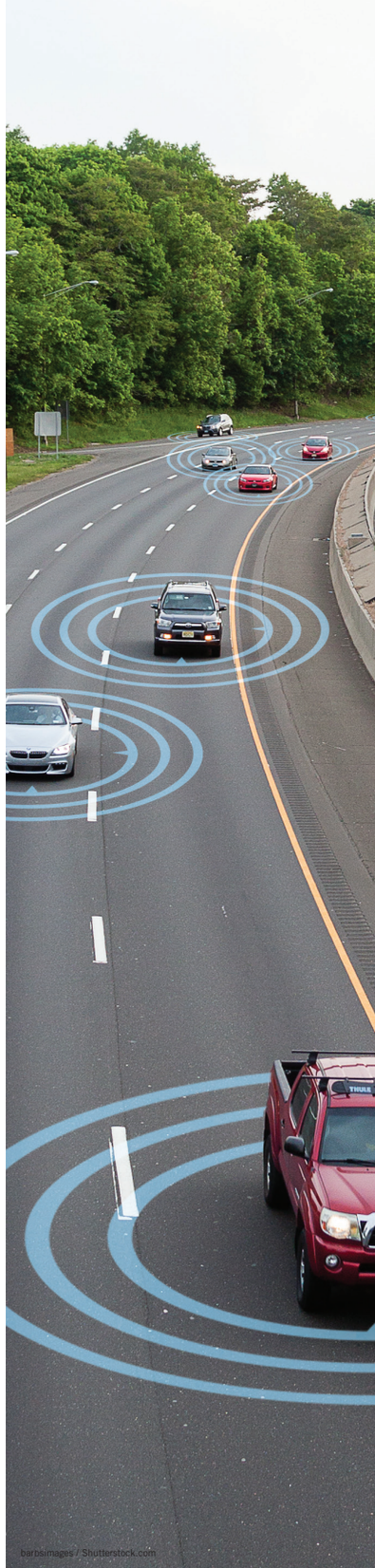
Franchised new-car dealers work hard to ensure that their customers fully understand not only the features of their new vehicles, but also the types of personal data that may be gathered or stored by or through their vehicles. Dealers are working with automobile manufacturers to ensure that consumers understand what information their vehicles collect, and how they can responsibly control that information. The list of features, and the data they utilize is changing rapidly. Check back with your manufacturer often, and for more information about many of the newer vehicle safety features visit **mycardoeswhat.org.**

This guide explains the kinds of information that may be collected by or through your car, the guidelines around how it is collected and used, and the options you may have. This guide provides a general overview; please consult your dealer and/or vehicle manufacturer for the full list of features and privacy policies integrated into your particular vehicle.

RULES ON USING DATA MY CAR COLLECTS

Your vehicle may collect and use different types of information about your driving activity for a wide range of purposes. Services that collect and share this information should be accompanied by a privacy policy that describes data collection and use. You may find these policies in your purchase agreement, your user manual, on the screen when signing up for services, or in the interface of any device or app that you connect.

It is important to review and understand the privacy policies of the company that manufactured your vehicle, as well as any third party with access to your vehicle data (through an OBD-II "dongle," in-car "app," or otherwise). These policies serve as the main legal mechanism regulating use of your data. You may have the right to "opt-out" or request that some information not be gathered, or if gathered, not be shared. However, opting out may limit the functionality of some of the features available to you.



COMMON TYPES OF COLLECTED DATA

An overview of the types of data that may be collected by your vehicle:

Collected by Most Vehicles

Certain technologies are in most vehicles today.

- **Event Data Recorders** – EDRs have been integrated into cars since the 1990s, and are currently installed in over 90% of vehicles. EDRs record technical information about a vehicle's operation in the seconds before and after a crash. This information includes speed, accelerator and brake position, seat belt usage, and whether the airbags deployed. EDRs are intended to provide crucial information to crash investigators and others. Accessing EDR information requires access to the vehicle as well as a specific EDR reader tool, in addition to meeting any consent requirements for a given state. If equipped with an EDR, a vehicle's systems must meet certain federal requirements, and additional laws governing ownership of EDR data vary state by state. Some states require the owner's consent or a court order in order to access this information.

- **On-Board Diagnostic Information** – All vehicles manufactured after 1996 are legally required to have an On-Board Diagnostic port, or "OBD-II." The OBD-II port is generally located underneath the driver's side dashboard in your car, and the information available here can be retrieved by physically inserting a compatible device into the port. This port enables access to information that can help service technicians measure emissions, diagnose performance issues, or repair your vehicle. Owners may also choose to plug in a third-party device (or "dongle") into the OBD-II port in some vehicles to collect or share information about their vehicle with third parties of their choice (for example, with their insurance company in order to gain safe driving discounts). Accessible information may include driver behavioral information (how fast you drive, how aggressively you apply the brakes, etc.) as well as geolocation data (where you are, where you have traveled, and your speed).

New Technologies

Other newer technologies may be included or available as an option in your next car.

- **Location Information** – The location of your vehicle and your destination may be collected by your navigation and related systems in order to route you to your destination.

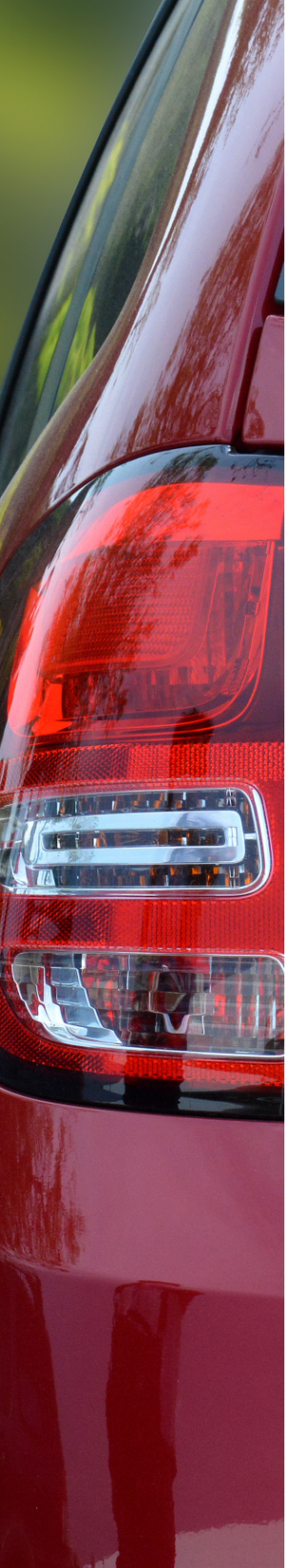
- **External Information** – Modern vehicles may contain cameras and sensors that are used to gather information about your car's immediate surroundings. These sensors can detect road or weather conditions, lane markings and obstacles, surrounding traffic, and more. Key technologies that rely on this external environmental information include blind spot detection, lane-departure warnings, assisted braking, and rear-parking detection.

- **In-Cabin Information** – Many of today's vehicles also contain sensors in the vehicle cabin. Microphones, cameras, and other devices may record information about vehicle occupants. These sensors may be required to communicate with emergency services or to utilize features such as hand-free telephone use.

- **User Recognition** – Some systems recognize users, by physical characteristics such as a fingerprint or face, and therefore may have physical, or biometric, information about users. Biometric information can also be used to determine who is behind the wheel and adjust systems accordingly. For example, rather than pressing a seat position button, the seat may adjust automatically after your face is recognized by a sensor located in the vehicle. These technologies can also detect a driver's attention and whether or not a driver is falling asleep behind the wheel.

- **Apps** – Your vehicle may include interfaces with third-party systems like Apple CarPlay, Android Auto, or other services. Your vehicle may also allow an interface between the applications on your phone and your vehicle. Be aware that if you enable apps provided through these interfaces or use apps on your phone that interact with your car you may be exposing data from your car to those third party app providers who have their own policies about what information they gather and what they do with that information. Consult their privacy policies for further information.

- **Other** – Vehicle manufacturers and their technology partners are constantly updating and improving your automobile. The sensors, features, and data gathered today are likely to be much different tomorrow. Make sure you work with your dealer to fully understand what your car can do for you, its features, and the data it gathers to provide you those features.



AUTOMOTIVE PRIVACY PRINCIPLES

Automakers are already responsible and trusted stewards of vehicle data. To further their commitment, many leading automakers have committed to ensuring that your information remains private and secure by developing the Automotive Privacy Principles, which will guide privacy practices in the automotive industry. These principles will go into effect beginning with model year 2017 vehicles and for subscription services beginning on January 2, 2016.

The Privacy Principles make three important commitments:

1. **Transparency** – manufacturers will provide you with clear and concise privacy policies.

2. **Affirmative Consent For Sensitive Data** – your consent is required before certain sensitive information is used for marketing or shared with unaffiliated third parties. This includes three types of data: (1) "geolocation" (where you are); (2) "biometric" (physical or health information about you or your passengers), and (3) driver behavior data.

3. **Limited sharing with government and law enforcement** – automakers will clearly state the limited circumstances where they may share your information with government authorities and law enforcement.

To learn more about the automobile privacy principles, go to: **AutomotivePrivacy.com**

Keep in mind that these commitments regarding data collection and use by automobile manufacturers may not extend to other third parties that may access data in your car (through your phone, an "app," "dongle," or other in-vehicle device).

PRIVACY CHECKLIST WHEN SELLING OR RENTING

Think of how you protect your privacy when using your smartphone or home computer. Similarly, you should also think of the sorts of information that may be stored by the services you enable in your vehicle, whether it is a car you have owned for years or a weekend rental.

What types of data would you want to remove before transferring the device to another person, and what subscription services would you want to cancel, such as mobile Wi-Fi hotspot or data services?

See below for general tips. Consult your owner's manual, and work with your dealer for details about resetting and removing your information from the system.

- ☐ **Phone Contact/Address Book** – remember that your personal contact information can be downloaded when you "sync" your phone with a vehicle. Remember to delete this information when selling car or returning a rental vehicle; also, be cautious when valeting or lending your car. Some vehicles are equipped with a valet function, which temporarily locks out access to this information, preventing unwanted intrusions.

- ☐ **Mobile Applications in the Car** – numerous personal mobile applications gather and store sensitive personal data, and when your phone is used with your vehicle, some or all of that data may be stored in the car as well. Reset/delete personal mobile applications that contain personal information; also, delete applications that you may have purchased and should not be accessed by others.

- ☐ **Vehicle Hard Drive Storage** – many of today's vehicles include built-in hard-drive storage (often for music or other "infotainment" features). Remember to delete the data on this hard drive when you selling or returning your vehicle.

- ☐ **Home, Work, and Favorite Places on Navigation** – delete this information when selling car or returning a rental vehicle; also, be cautious when valeting or lending your car. Some vehicles are equipped with a valet function, which temporarily locks out access to this information, preventing unwanted intrusions.

- ☐ **Garage Door Programing** – reset all garage door programing when selling or returning a vehicle.

- ☐ **Optional Plug-ins** – remove any devices that you obtained for use in your vehicle, such as a dongle that may share car information with third parties. These devices are usually located under the steering wheel and are connected to a data port.

STAY UPDATED

As technologies develop, performance improvements, security improvements and other updates may be provided. Make sure your car stays up to date with any software updates for your vehicle. Contact your dealer for more information.

CONCLUSION

As vehicles become more connected, it will be important to keep up with new technologies and understand how your information is collected and shared.

For more information about the technology in your car, contact your local dealer and review your vehicle's owner's manual. For privacy information about new technologies of any sort, see **fpf.org.**

Imprint Area for Dealer/OEM logo.
(Gray Box Does not Print)

Personal Data In Your Car

National Automobile Dealers Association and the Future of Privacy Forum

NADA
8400 Westpark Drive
Tysons, VA 22102
nada.org

FUTURE OF PRIVACY FORUM
1400 Eye Street, NW, Suite 450
Washington, DC 20005
fpf.org

are intimately involved in the complicated and important privacy and security issues arising from the changes in connected and autonomous vehicles, which we believe represents a critical, but distinct component of any overall privacy regime.

NADA appreciates the effort undertaken by the NTIA with respect to these issues, and in particular, the humility, caution, and balance that is apparent in the Notice and in the NTIA's approach. We submit the following comments addressing a few specific issues from the Notice that we believe are critical as the Department and the Administration go forward.

1. Overall Privacy Concepts to Consider

First, we agree that the broad concepts as outlined in the Notice, in the FIPPs, and elsewhere are the best starting point to protect consumers. Consumers must understand what personal information they are sharing (or that it is being collected from them), who has access to that information, and how it is used. This transparency is and should be the backbone of any privacy regime. When consumers do not know what information is being collected, or how it is being used, it generates mistrust and heightens the potential for abuse, and that benefits neither business nor consumers. It is critical in our view that consumers have readily-available, standardized access to information about how their personal information is stored, by whom, and how it is used; a clear choice regarding its storage and use, and; a simple way to exercise that choice. In our view, consumers should be able to exercise that choice not only at the point and time of collection, but in an ongoing manner as well.

One additional issue that we believe will be critical but that is not specifically outlined in the Notice is that of consumer education. How will consumers be educated so that they understand the choices they have and the implications of those choices? We would urge the Department to consider this question, to work with interested industry participants and others, and to ensure that any overall privacy approach includes this important component.

We also agree that entities that collect and store personal information should also have duties, but they need clarity and consistency as well. They should take steps to ensure that the data they collect is accurate and secure. They should observe best practices in terms of limiting the data they collect, avoid maintaining data longer than needed, and they should limit access to personal information both within their organization and outside of the organization. They should

obtain consent where appropriate, but the issue of consent can be difficult issue in practice. That is because consumer consent is important, but only useful if consumers understand what they are agreeing to, and the implications of those choices. We also agree that entities should be accountable for their use of protected personal information but would urge caution with respect to the way this accountability is brought to bear, as discussed below.

2. **Beyond the Basic Principles**

In response to the questions in the Notice, NADA submits comments on the following issues related to the Notice and the issues the Department is considering:

(a) Critical terms and concepts that require definition, or further definition;

(b) Broadening the scope of entities responsible for protection of personal information;

(c) Providing tools to businesses seeking to protect consumer information;

(d) Enforcement considerations and an objective standard;

(e) A "safe harbor" approach to privacy, and;

(f) Automotive-specific privacy issues.

Each of these issues warrant a great deal of additional attention and consideration, and we would welcome the opportunity to comment further as appropriate as the Department continues its efforts, or to meet with the Department to discuss these or other issues in greater detail.

a. **Definitions**

Any privacy regime must have certain foundations – and defining the "personal information" that will be protected, or protectable is a critical first step. Currently, a broad consensus appears to have formed that, at a minimum, any personal information that could embarrass or financially harm a person should be protected in some way. Indeed, current U.S. privacy law is based in large part on these distinctions, with personal data about a consumer's health or finances, and personal information about children broadly protected under federal statutory regimes. However, there are also broad categories of information – where you go; who you associate with; political, sexual, or other preferences, for example – that also receive heightened protections as a matter of law or policy. In addition, there is a growing concern that the volume of disparate data available today *in and of itself* presents tremendous problems. Massive amounts if available data along with modern data analytics mean that otherwise benign

data, in combination, can reveal tremendously personal information about a person that should be protected.

The bottom line is that while there will be many definitional challenges, this definition is critical. We believe that the most logical outcome could include a tiered approach where certain information or combinations of data are always protected, while other information is deemed less sensitive and therefore provided lesser protections. This could mean that certain categories or types of data can never be shared, or requires certain consent or disclosure, while other data may never be gathered at all or must be deleted immediately.

The second definition that we would like to comment on is one that is not currently addressed – at least not adequately in our view. That is, a definition that distinguishes between the entities that obtain and store personal information based upon the context by which that information was obtained. We submit that data storage and use by some entities requires greater protections than others because they are more or less consistent with a reasonable consumer's expectations. This requires a clear and consistent definition.

For example, distinctions should be drawn between entities that require personal information to provide a service or for product functionality and those who require personal data only for a business model built on data obtained from third party sources. When an entity with whom the consumer has no business relationship obtains personal data about a consumer, we submit that use poses a far greater privacy risk to consumers than a similar use by an entity that has obtained personal information purposefully and knowingly provided by a consumer in connection with a purchase or business relationship because it is outside of the reasonable expectations of the consumer. A federal privacy regime should distinguish between entities with a direct business relationship and others. There are and have been similar distinctions under other federal laws that have proven effective.[1]

In addition, the nature and purpose of the use of the protected personal information may require different definitions as well. For example, use of otherwise protected personal

[1] For example, certain federal marketing regulations rules distinguish (or formerly distinguished) between a communication from an entity with whom a consumer did business and one with whom they had not engaged in any business transaction.

information to increase cybersecurity or safety of a consumer (for example, in the operation of a connected or autonomous vehicle) should be treated differently than a use without any such implications. It is of course important that any such definition must not artificially sacrifice privacy. Consumer privacy should not be a tradeoff with security or safety.

b. **Extend the scope of responsibility beyond the initial data gathering entity**

One of the key privacy principles is "accountability," and while we agree that entities that collect and use protected personal information must meet certain obligations and be accountable with respect to that data, we would urge the Department to think broadly about the nature and scope of that accountability. Indeed, we believe that one of the critical shortcomings of the current privacy regimes is the fact that the responsibility to meet those obligations often apply only to the entity that has initially obtained the data, and not to third parties who later obtain the data. For example, under the current regimes such as GLB and HIPAA, the regulatory compliance burden is placed largely, if not exclusively, on the entity that gathers and stores the protected data. The Notice itself states that "[*o]rganizations that control personal data should also take steps to ensure that their third-party vendors and service providers are accountable for their use, storage, processing, and sharing of that data*."[2]

We certainly understand the need to ensure that the entity that initially gathers and continues to store the data is responsible for that data, and takes steps to control vendors with whom they work. However, we believe that a *sole* focus on such entities is a mistake. The nature of personal information, particularly electronic information, means that it is simple to copy, highly "liquid," and in many cases, easily obtained by third parties – often without the knowledge of the entity from which it was obtained, and certainly not to the consumer. A privacy regime that focuses only on the entity that obtains the data ignores the overwhelming majority of entities with personal information, and in many ways encourages bad behavior with respect to the gathering and use of that information by these strangers to the initial consumer transaction.

[2] 83 Fed Reg 48602.

This creates a problem for businesses of all types and sizes because consumers are increasingly demanding instant electronic interface with these businesses, and those businesses in turn are generally more reliant than ever on professional IT service providers in every aspect of their business: to store, process, securely transmit, and utilize customer information. These service providers will often then subcontract many of these duties - data storage, for example – to subcontractors[3] who then have access to customer information. The volume of data and the complexity of these networks have grown exponentially in recent years. In addition, the nature of data itself leads to an asymmetry of information between the initial entity and the third party with respect to the protected personal information, so that it is ultimately only the third party who knows with certainty what they are or are not doing with respect to that data.

All these changes have been profound and have unfortunately been accompanied by an increase in the number and scope of efforts by bad actors to impermissibly obtain this information. Recent history has demonstrated that in many cases, the real risk to the privacy and security of personal information lies with third parties who are strangers to the initial data gathering. We have seen an increasing number of high-profile data breaches and security incidents at institutions of all kinds where service providers are the attack vector through which a security incident takes place. The irony of all this is that for many businesses (often small businesses) who are not in the business of "leveraging data," who are doing their best to control and protect that data, but who may be themselves the victim of a third party's actions are also held responsible for the bad acts of that third party. This is not fair to those businesses trying to do their best, nor does it do enough to protect consumer privacy rights.

Privacy obligations must attach to the personal information itself – no matter who has that data. In particular, they should apply to third parties who may or may not have legitimately accessed that information, but who obtain and use it nevertheless.

c. Provide additional tools to businesses to protect consumer data

[3] Who then in some cases subcontract to sub-subcontractors.

Because of this reality, business that obtain and store consumer information need improved tools to protect that data vis a vis third parties. We would urge the Department to consider how to provide to businesses that are storing and seeking to better protect the consumer personal information they have, the tools they need to protect against third parties and bad actors.

We are concerned with the sentiment expressed in the Notice that "*there should be a distinction between organizations that control personal data and third-party vendors that merely process that personal data on behalf of other organizations*."[4] While we agree that in certain contexts it would be reasonable to place a greater burden on the "controlling" entity, we fear this may be missing the true market reality for many businesses.

In short, the activity that any privacy regime should seek to address is activity inconsistent with the wishes and expectations of consumers, and that goal is not furthered by a built-in presumption that the "controlling" entity is more likely entity to engage in such activity. Indeed, it is often true that the opposite is the case, and these "controlling" business need an enforcement mechanism to allow them to hold third parties and others accountable for improperly accessing, using or sharing personal data. Those tools simply do not exist today. It is not enough to give these tools to consumers or regulators, businesses who care about privacy and want to protect consumer data must have the ability to hold third parties accountable as well.

d. Regulatory enforcement should be based on objective standards

Another important component of "accountability" is regulatory enforcement against entities that refuse to meet, avoid, ignore, or in bad faith fail to meet privacy requirements. The FTC has become the de facto privacy regulator in the United States. The Notice submits that "*the FTC is the appropriate federal agency to enforce consumer privacy laws*."[5] However, privacy enforcement must be based on a clear set of well-defined and reasonable rules, and we are concerned that the current standards under Section 5 of the FTC act are likely too broad and ill-defined for this type of enforcement activity. Simply put, privacy enforcement cannot be based on whether an activity or disclosure is "unfair" or "deceptive." While these terms are

[4] 83 Fed Reg 48603.
[5] *Id*. at 48602.

broadly defined and there is a growing "common law" of FTC enforcement activity that provides some broad guidance, that standard still fails to provide the legal clarity that businesses and consumers need. Privacy enforcement should be based on instances of clear and impermissible failure to meet an objective privacy requirement or criteria. Enforcement under this current standard often leads to "after-the-fact" enforcement – that is, enforcement against activity that viewed in hindsight is "unfair" to consumers.

We acknowledge that the FTC is operating under the statutory authority it has been given and that an objective privacy standard will likely require legislative enactment. However, until such specific statutory authority is enacted, the potential application of a broader standard that was never specifically intended to apply to privacy enforcement would not provide the clarity that businesses and consumers need.

e. Consider a "Safe Harbor" approach

One thing that is clear is that perfection cannot be achieved, and perfect conformity with privacy principles should be the goal, but not the legal standard or even the expectation. One reasonable way for the Department to provide consumer privacy protection while also providing the needed legal clarity for businesses with respect to consumer data privacy is to promote adoption of a "safe harbor" approach. In other words, to seek implementation of a privacy a regime whereby a business who meets, or in good faith seeks to meet, objective privacy requirements will have "safe harbor" protection, even if an event occurs that results in a failure of the privacy ideal. There are many analogs for such safe harbors under federal law, and this is another context in which this approach is the best balance between privacy ideals and reasonable best efforts in the real world.

f. Automotive Specific Issues

We would also like to comment briefly on privacy concerns in the automotive context. We believe that such concerns are particularly acute and are becoming more so every day. We understand that these issues are not squarely before the Department in this Notice, and that a number of industries face their own privacy challenges. However, we also believe that it is

important that policy-makers understand and address automobile privacy issues specifically because we believe that unique challenges are presented given the cybersecurity and safety implications that privacy considerations may have in the automotive context. Exhibit A contains a link to the NADA comments submitted to the FTC in connection with the FTC connected car workshop in 2017. It provides some additional detail on some of the privacy and cybersecurity issues with the modern automobile and highlights the applicability of some of the concepts outlined herein to the automotive and dealership context. We would urge the Department and other policymakers to look at automotive issues closely and thoroughly as you move forward because addressing the unique privacy issues in the car is critical to consumer privacy protection and adoption of these exciting new technologies, and they may require specific consideration outside of, or in addition to any overall privacy regime.

Conclusion

We applaud the Department and the Administration for their balanced approach to this important topic, and in particular for the focus on harmonizing the regulatory landscape. NADA believes that this is a critically important issue for consumers, businesses, and for ensuring the continued competitive posture of the United States. We appreciate the opportunity to comment on this matter and believe that this Notice should be one of a continuing series of steps to develop the best approach to this complicated issue. Please feel free to contact us if we can provide further information that would be useful to the Department in their efforts going forward.

Sincerely,

/s/

Bradley Miller
Director, Regulatory Affairs
National Automobile Dealers Association

EXHIBIT A

May 1, 2017

Filed Electronically at https://ftcpublic.commentworks.com/ftc/connectedcarsworkshop

Office of the Secretary
Federal Trade Commission
Suite CC-5610 (Annex A)
600 Pennsylvania Avenue, NW
Washington, DC 20580

Re: Connected Cars Workshop P175403

Dear Secretary:

The National Automobile Dealers Association ("NADA") [1] submits the following comments in response to the Notice seeking comments on the FTC/NHTSA Connected Cars Workshop ("Workshop") that the Federal Trade Commission ("FTC" or "Commission") published in connection with the above captioned matter.[2]

In a modern car, there is no key, you press a button and you watch an operating system load, and you watch it connect to your devices and the internet. Today's vehicles are not simply a connected computer, but a connected network.[3] Computers control your steering, brakes, and other systems. Indeed, virtually every aspect of your car has some sort of software exposure. These software systems gather, create, store, and transmit data about the vehicle, the driver, its occupants, and its surroundings in ways that consumers generally do not yet understand, and in many ways they do not expect. Currently (or soon to be) available sensors gather data about the

[1] NADA represents over 16,000 franchised dealers in all 50 states who (i) sell new and used cars and trucks; (ii) extend vehicle financing and leases to consumers that routinely are assigned to third-party finance sources; and (iii) engage in service, repair, and parts sales. Our members collectively employ over 1 million people nationwide. Most of our members are small businesses as defined by the Small Business Administration.

[2] Available at https://www.ftc.gov/system/files/attachments/press-releases/ftc-nhtsa-conduct-workshop-june-28-privacy-security-issues-related-connected-automated-vehicles/notice_connected_cars_workshop_with_nhtsa_1.pdf

[3] The average modern vehicle contains dozens of individual computers.

FTC Connected Car Workshop_5_1_17.p