COVINGTON & BURLING LLP

BEIJING BRUSSELS LONDON NEW YORK
SAN DIEGO SAN FRANCISCO SEOUL
SHANGHAI SILICON VALLEY WASHINGTON

1201 PENNSYLVANIA AVENUE, NW
WASHINGTON, DC 20004-2401
T 202.662.6000
WWW.COV.COM

January 10, 2014

BY ELECTRONIC DELIVERY

Mr. Donald S. Clark
Federal Trade Commission
Office of the Secretary
Room H-113 (Annex X)
600 Pennsylvania Avenue, NW
Washington, DC 20580

Re: Internet of Things, Project No. 135405

Dear Secretary Clark:

AAA appreciates the opportunity to comment on the issues raised at the Federal Trade Commission's recent workshop on the "Internet of Things." The workshop brought together stakeholders to begin the important work of highlighting the increasingly networked nature of our everyday life and developing consumer privacy and security safeguards that encourage consumers to use networked devices. AAA was pleased to be a part of the workshop's "Connected Cars" panel.

With more than 54 million members, AAA is a not-for-profit member services organization dedicated to improving the experiences of America's motorists. To that end, we have worked over many years with federal and state agencies to promote driver-friendly policies such as highway infrastructure investment, road safety, and fuel efficiency. We look forward to continuing our efforts on behalf of motorists by working with the FTC as it considers standards governing the privacy and security of connected vehicles and other networked "things."

AAA sees great potential for innovation and new benefits to drivers if a secure and competitive environment develops for connected-vehicle technologies. A recent survey of AAA members and non-members, discussed below, shows a high level of concern about car data and privacy. It is appropriate, therefore, to begin the work of addressing these concerns and setting out a framework that consumers can trust.

I. Introduction & Executive Summary

The number of Internet-enabled vehicles on the road is increasing at a staggering pace. By one estimate, that number will grow from less than one million in 2009 to more than 42 million in 2017.[1]

This rapid growth is no doubt due to the enhancements in convenience and safety that vehicle connectivity promises to provide to consumers. The potential safety benefits of connected-vehicle technologies are particularly promising. Vehicle-to-vehicle (or "V2V") and vehicle-to-infrastructure ("V2I") communications can warn drivers of potential collisions, dangerous road conditions and other impediments to safe travel. A range of crash prevention technologies integrated with communications systems—including intersection assistance, left-turn assistance, and "do-not-pass" warning systems—likely will reduce the number of crashes and increase safety in the coming years.

Connected-vehicle technologies will enable a car to transmit vital statistics on vehicle operation and health to ensure smooth operation and avoid repair surprises. And these technologies can also help drivers access an array of online services—from GPS navigation tools to Internet-connected concierge services—right from their dashboards. But safety must remain a top priority as these systems and features continue to develop. AAA advises against engaging in potentially distracting activities while driving and has called for limiting certain features' functionality to prevent mental distraction.

In short, the features and services that vehicle connectivity enables will radically transform the driving experience. However, because these features and services will depend in large part on the collection and use of data from and about consumers' vehicles, they must be designed and operated with privacy and security at the forefront so that consumers are in control. AAA believes that the core Fair Information Practice Principles that inform the FTC's 2012 privacy framework—namely, transparency, choice, and security—should guide the data practices of companies that make and operate Internet-enabled objects, including vehicles.

AAA recognizes the challenges of applying the FIPPs to many of the technologies that make up the Internet of Things because many networked "things" lack features (*e.g.*, user interfaces) that facilitate companies' communications with consumers about data practices and enable consumers to make choices in response to those communications. But, at least in the connected-vehicle context, we disagree with the conclusions of the Future of Privacy Forum white paper distributed at the workshop, which urged a "use-focused privacy paradigm" of the Internet of Things, rather than one based on FIPPs such as notice, choice, data minimization, use

---

[1] iSuppli Corp., *Internet: A New Driving Force for Auto Content* (2010).

limitation, and purpose specification.[2] AAA believes that it is both possible and appropriate for companies in the connected-vehicle space to adhere to these principles.

In what follows, we provide a brief overview of key car data practices and consumers' attitudes about vehicle connectivity. We then discuss how the FTC could approach the development of standards that would apply to the collection and use of car data.

In sum, AAA supports the FTC's development of appropriate standards for the privacy and security of car data because if the Internet of Things is going to deliver on its promise, then privacy, security and competitive concerns need to be addressed. A survey of AAA members and non-members in September 2013 found that a strong majority of respondents expressed a high level of concern about car data privacy.[3] The survey also showed that consumers overwhelmingly believe that vehicle owners should always be able to decide if data generated about their vehicle can be shared and with whom; they want control over the data. AAA hopes that the FTC's approach to connected-vehicle data will take into account motorists' views about the sensitivity of such data and the corresponding importance of allowing consumers to determine how this data is collected, used, and shared.

II. Background: Car Data Offers Benefits But Raises Consumers' Concern About Its Collection and Use

Connected-vehicle technology promises to make driving safer and more convenient in the years ahead. Wireless communications systems in vehicles increasingly will enable vehicles to communicate with each other, with highway infrastructure, and with automakers and third-party service providers.

As noted above, the potential safety benefits of connected-vehicle technologies are particularly exciting. Crash prevention technologies have the potential to reduce the number of automobile crashes in the coming years, and other technologies also will enable a vehicle to transmit wirelessly diagnostic information to service providers to facilitate vehicle maintenance and repair.

Through connected-vehicle technologies, consumers also increasingly will have access to an array of online services. These services, which range from GPS navigation tools to in-car concierge services, bring the conveniences of smartphones to consumers' dashboards. Some

---

[2] Christopher Wolf & Jules Polonetsky, *An Updated Privacy Paradigm for the "Internet of Things,"* Future of Privacy Forum (Nov. 19, 2013), http://www.futureofprivacy.org/wp-content/uploads/Wolf-and-Polonetsky-An-Updated-Privacy-Paradigm-for-the-"Internet-of-Things"-11-19-2013.pdf.

[3] AAA, *Car data Ownership Research* (Oct. 2013).

services, such as Ford's SYNC operating system, are designed to integrate smartphones into vehicle systems, while others, like GM's OnStar service, are standalone platforms through which various services can be provided.

These online services are, of course, made possible through the collection, use, and sharing of car data by automakers and service providers. Although consumers may have some awareness of the data exchange that comes with navigation and infotainment services that they directly interact with in the dashboard, they almost certainly are not aware of the full range of types and the amount of data that, thanks to connected-vehicle technology, can be collected about their vehicles from internal sensors and computers. The table below illustrates the stunning range of car data that automakers and others can collect remotely.

What Kinds of Car Data Can Be Collected Remotely?		
• Precise location	• Seatbelt status	• Driver attentiveness (by monitoring engagement of vehicle controls)
• Vehicle speed	• Tire pressure	
• Rate of acceleration	• Ambient temperature	• Cell phone use
• Cornering force	• Number of people in the vehicle	• Use of the radio, navigation system, and apps (on a smartphone or integrated platform)
• Headlight status	• Precipitation (via rain sensors in automatic windshield wipers)	
• Emission system warning indicators		

These and other types of car data can be used to provide an array of useful services to consumers. But the data also can be used to create rather detailed profiles of driver behavior. Consumers need to know what kind of information is being collected about their cars so that they can then make informed decisions as a result.

There are indications that automakers are seeking ways to increase the amount of data they collect and to monetize this valuable data.[4] To take just one example, in 2011 General

[4] *See, e.g., Telematics Update: Continental and Fiat to Reveal Their Thoughts on the Huge Revenue Potential of Big Data at Content and Apps for Automotive Europe 2014*, Telematics Update (Dec. 16, 2013), http://analysis.telematicsupdate.com/infotainment/telematics-update-continental-and-fiat-reveal-their-thoughts-huge-revenue-potential-big.

Motors' OnStar service announced a change to its privacy policy, which would have allowed the service to continue collecting car data—including location data—after consumers had cancelled the service.[5] The change also would have permitted OnStar to sell the data it collected to third parties.[6] Only after Senators Charles Schumer, Chris Coons, and Al Franken intervened did GM reverse course.[7]

GM's experience apparently has not deterred other automakers, some of whom are searching for ways to give advertisers opportunities to target drivers in desirable marketing segments.[8] Other players in the emerging car data "ecosystem," including operating system and application providers, have strong commercial incentives to seek ways to do the same.[9]

AAA does recognize that there may be some instances in which anonymous or de-identified data can be collected and leveraged by businesses and government for legitimate purposes, including but not limited to, addressing traffic safety risks, managing infrastructure and traffic, and improving the design of products and services. However, AAA believes that any of these practices should be carried out and disclosed within a framework designed to maximize consumer awareness, privacy, and control, as described herein.

Consumers are increasingly attuned to the importance of the privacy and security of their vehicles' data. In September 2013, AAA surveyed 350 AAA members and 650 non-members about their views on the privacy and security issues relating to car data.[10] When respondents were informed about the kinds of data that vehicle-connectivity technologies can generate, they expressed deep concern about their privacy and security: *68 percent of those surveyed indicated*

---

[5] John R. Quain, *Changes to OnStar's Privacy Terms Rile Some Users*, N.Y. Times (Sept. 22, 2011), http://wheels.blogs.nytimes.com/2011/09/22/changes-to-onstars-privacy-terms-rile-some-users/?_r=0.

[6] *Id.*

[7] *See* Jonathan Schultz, *Senators Criticize OnStar for Proposed Changes to Privacy Terms*, N.Y. Times (Sept. 27, 2011), http://wheels.blogs.nytimes.com/2011/09/27/senators-criticize-onstar-for-proposed-changes-to-privacy-terms/; Eric Engleman, *GM's OnStar Reverses Privacy Shift That Drew Senators' Wrath*, Bloomberg BusinessWeek (Sept. 27, 2011), http://www.businessweek.com/news/2011-09-27/gm-s-onstar-reverses-privacy-shift-that-drew-senators-wrath.html.

[8] *See, e.g.*, *Telematics Update, supra* note 4.

[9] *See, e.g.*, Lucas Mearian, *By 2018, Cars Will Be Self-Aware*, ComputerWorld (Jan. 6, 2014), http://www.computerworld.com/s/article/9245206/By_2018_cars_will_be_self_aware.

[10] *See* AAA, *supra* note 3. An additional seven people were also surveyed, but they did not know whether they were AAA members.

they were concerned, and this figure increased significantly when respondents were told that automakers and others could get access to this information.

Consistent with these feelings of concern, *79 percent of survey respondents agreed with the proposition that consumers should always be able to decide if information generated about their vehicle can be shared and with whom.* Remarkably, respondents' concern about vehicle privacy and security was greater than their concern about other leading data protection issues, including privacy and security issues surrounding the use of mobile devices, shopping online, email, and search engines.

III. Ensuring the Privacy and Security of Car Data

At AAA, we believe that the promises of connected-vehicle technologies can be realized without sacrificing the privacy or the security of car data.

The following recommendations are consistent with the core FIPPs, which AAA believes should continue to inform the FTC's approach to privacy and security as the agency develops best practices for the Internet of Things. As noted above, a Future of Privacy Forum ("FPF") white paper distributed at the workshop urged a "use-focused privacy paradigm," and indicated that the traditional FIPPs, such as notice, choice, data minimization, use limitation and purpose specification, may not be appropriate standards for the Internet of Things.[11] FPF also noted that many connected devices will not have user interfaces, and thus will not be able to provide choice and transparency directly to the consumer from whom the device collects data.

Although AAA recognizes the challenges of applying the FIPPs to many of the technologies that make up the Internet of Things, we believe that in the connected-vehicle context, the FIPPs can and should be applied similarly to how they have been applied in the context of PCs and mobile devices. AAA believes that the means exist to provide consumers clear notice about the data companies collect and meaningful opportunities to control the use and sharing of their vehicles' data.

A. Transparency

Consumers have a right to know what kinds of data are being collected about their vehicles and by whom.[12] And as the FTC has explained, consumers should be given this

---

[11] Wolf & Polonetsky, *supra* note 2, at 5.

[12] A Government Accountability Office ("GAO") report issued this week underscores the need to improve transparency in the connected-vehicle space. The report, which addresses privacy issues arising from in-car location-based services, notes that most companies that provide these services do not clearly disclose how they use location data. As the GAO noted, these disclosures (continued...)

information in a clear, short, and standardized form.[13] AAA recognizes that providing consumers notice about car data practices poses unique challenges. But we disagree with those who believe that the importance of providing notice in the connected-vehicle context is diminished because of those challenges. As explained in more detail below, AAA believes the means exist for collectors of car data to communicate with consumers. Making these communications effective, however, will require innovative thinking about how and where to present them.

AAA submits that the FTC should urge stakeholders to work together to develop short privacy notices for the connected-vehicle context. The development process could be modeled on self-regulatory efforts that have produced codes of conduct for other privacy-sensitive activities, such as online behavioral advertising. The National Telecommunications and Information Association's multistakeholder meetings to develop short privacy notices for mobile apps also could provide a model for such a process.

B. Choice

Consumers should be provided with meaningful choices about the collection, use, and disclosure of car data. The FTC has explained that consumers generally should be given the ability to exercise choice regarding practices that are inconsistent with the context of a particular transaction or a business's relationship with a consumer.[14] But there are also situations in which choice must be provided regardless of context, such as where a company collects sensitive data.[15]

Where choice is required, the FTC has noted that it should be provided "at a time and in a context in which the consumer is making a decision about his or her data."[16] "In most cases," the

---

typically are "broadly worded and potentially allow for unlimited data collection and use." Gov't Accountability Office, *In-Car Location Based Services* 13 (Dec. 2013). AAA agrees with the GAO's statement that "[w]ithout clear disclosures about the purposes [for which data is collected], consumers may not be able to effectively judge whether the uses of their location data might violate their privacy." *Id.*

[13] Fed. Trade Comm'n, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers* (Mar. 2012) [hereinafter "FTC Privacy Report"].

[14] *Id.* at 48-50.

[15] *Id.* at 58-60.

[16] *Id.* at 58.

FTC has explained, "providing choice before or at the time of collection will be necessary to gain consumers' attention and ensure that the choice presented is meaningful and relevant."[17]

AAA believes that applying these principles to the connected-vehicle context yields three conclusions:

- First, companies should be required to secure consumers' ***affirmative express consent*** before collecting car data.
- Second, to the extent possible and safe, choice should be provided through vehicle communications systems.
- Third, consumers should have the ability to choose not only whether and how data will be collected and used, but also with whom it will be shared.

We discuss each of these, in turn.

1. Companies should be required to secure consumers' affirmative express consent before collecting car data.

The collection of "sensitive information" requires choice regardless of the context in which the information is collected.[18] The FTC has made clear that collecting this information requires that the company secure the "affirmative express consent" of the consumer ***before*** collection takes place.[19] Car data is sensitive data: in addition to location information, which the FTC has expressly identified as "sensitive,"[20] the types of data that automakers and others can collect are nearly all sensitive in that their misuse can cause substantial economic or physical injury to consumers. In light of this, AAA believes that companies should be required to secure the affirmative express consent of consumers before collecting *any* information generated about their vehicles that can be personally identifiable with a driver, vehicle owner, or vehicle.

Importantly, providing this consent should not be a condition of purchasing a vehicle or of using vehicle services that do not require the transmission of car data. We note the FTC's guidance on so-called "take-it-or-leave-it choice," the practice whereby a company conditions a consumer's ability to use a product or service on the consumer's agreement to allow the

---

[17] *Id.* at 50.

[18] *See id.* 57.

[19] *Id.* at 59.

[20] *Id.*

company to collect data about the consumer.[21] The FTC explained that take-it-or-leave-it choice is particularly inappropriate for certain markets, such as the market for broadband access, where consumers have few choices. Although the auto market is not such a market, AAA submits that take-it-or-leave-it choice is nonetheless inappropriate because of the significance the purchase of a vehicle has for most consumers.[22] Faced with one of the largest investments they will ever make, consumers should not be forced to agree to reduced privacy protections as a condition of purchasing the vehicle that is right for them.

2. To the extent possible and safe, choice should be provided through vehicle communications systems.

As the FTC has explained, where choice is required to be provided, it should be provided "at a time and in a context in which the consumer is making a decision about his or her data."[23] Although the Internet of Things comprises many technologies that may not be able to offer consumers such contextual choice, AAA believes that connected vehicles can and should do so. As more and more vehicles include user interfaces in the dashboard, such choices could be offered there. The importance of obtaining consent to collect car data does not, of course, trump the importance of vehicle safety, but AAA believes that automakers and others can design systems that do not distract drivers while still providing consumers meaningful options about the collection of their data.[24]

Even if using a dashboard user interface to secure consent is not feasible, automakers and service providers still should find ways to obtain the informed consent of consumers before collecting car data. Automakers and service providers could develop websites or other online services that explain car data practices, educate consumers and, in turn, allow them to make choices about those practices. These companies also could communicate with consumers via email, phone, or text message (provided the user agrees to such communications). In short, there is a range of ways in which companies that collect car data can communicate their practices to consumers and obtain informed consent to those practices.

---

[21] *Id.* 51-52.

[22] The terms "purchase" and "owner" in the context of these comments are intended to also include "lease" and "lessee," respectively, since the privacy issues and related concerns are identical regardless of whether a person is purchasing a vehicle or entering into a long-term lease.

[23] Privacy Report at 58.

[24] Some automakers have already done this for embedded navigation systems, which prevent consumers from entering certain information while the vehicle is moving.

3. Consumers should have the ability to determine with whom car data will be shared.

In the connected-vehicle context, a consumer's choice about whom he or she shares car data is nearly as important as the decision to permit collection of the data in the first instance. This is because protecting a consumer's right to make choices about car data serves to promote both privacy and competition. These twin objectives are particularly urgent in the connected-vehicle context. Because the ability to access car data is now necessary to perform many kinds of vehicle maintenance, consumers' ability to choose who receives their vehicle's data can mean the difference between perhaps paying more for vehicle repairs at a dealer or paying a lower price or getting more convenient service at a local repair shop.[25]

In addition, the market for connected-vehicle services is still developing, and the possibilities for services that make vehicles safer and more convenient are tremendous. But the potential of this market for data-driven services will not be realized if automakers and their affiliates prevent consumers from sharing a broader range of car data with the service providers of their choice. AAA is concerned that some companies may attempt to corner the market for car data by setting such limitations, which will harm consumers by depriving them of competition for innovative services, The FTC should be wary of a model that "locks in" consumers to services provided by one entity, such as the manufacturer.

---

[25] A range of studies show that charges for auto repair can vary but independent shops consistently come out on top with the best value. For non-warranty maintenance work during the first three years of new-vehicle ownership, excluding complimentary service, consumers spend considerably less out-of-pocket, on average, at independent repair shops ($44) than at auto dealerships ($118). *See* J.D. Power & Associates, 2013 U.S. Customer Serv. Index (March 13, 2013), http://autos.jdpower.com/content/press-release/gMEbEQI/2013-u-s-customer-service-index-csi-study.htm.

Other studies have shown that, on average, vehicle repairs cost 34 percent more at new car dealerships than at independent repair shops. *See* Automotive Aftermarket Ass'n, *Motor Vehicle Owners' Right to Repair Act: Legislation Aimed at Preserving Competition for Consumers in the Vehicle Repair Market* 1 (Mar. 2009), www.righttorepair.org/downloads/docs/whitepaper_righttorepair.pdf.; *see also* Jerry Edgerton, *Auto Repair: Save $300 by Avoiding Dealers*, CBSNews.com (May 25, 2010), http://www.cbsnews.com/news/auto-repair-save-300-by-avoiding-dealers/ (noting a study that found "avoiding dealerships in favor of independents when you have work not covered by the warranty, [consumers] can save an average of $300 a year).

C. Security

The FTC has long stressed the importance of providing security for consumer data, and has taken action against dozens of companies that have failed to do so. AAA submits that the FTC should pay particularly close attention to the security practices of companies that collect car data, as well as to the companies that design wireless data systems for vehicles. As Chairwoman Ramirez and others noted at the workshop, the security of vehicle computing systems is particularly crucial given the serious consequences of failing to provide strong security. A security failure that resulted in a malicious actor gaining access to the vehicle's computers could lead to theft, harassment, mischief, or the serious injury or even the death of a motorist and other road users. Given these stakes, strong security for connected-vehicle technology is vital.

* * *

Again, AAA appreciates the opportunity to work with the FTC as it develops consumer privacy and security protections for the Internet of Things. We hope these comments are helpful, and we would welcome the opportunity to discuss them with the staff.

Respectfully submitted,

Gerard J. Waldron
Stephen P. Satterfield
Counsel for AAA