Comments from

THE FUTURE OF PRIVACY FORUM

to

FEDERAL TRADE COMMISSION

and

U.S. DEPARTMENT OF TRANSPORTATION

National Highway Traffic Safety Administration

Request for Comments "Connected Cars - Workshop, Project No. P175403"

Lauren Smith, Policy Counsel

John Verdi, Vice President of Policy

THE FUTURE OF PRIVACY FORUM
1400 I St. NW Ste. 450
Washington, DC 20005

www.fpf.org

May 1, 2017

Table of Contents

On behalf of the Future of Privacy Forum, we are pleased to submit these comments regarding the Federal Trade Commission (FTC) and Department of Transportation and National Highway Traffic Safety Administration's (NHTSA) Request for Comment on "Connected Cars - Workshop, Project No. P175403." Our comments focus on the privacy implications of current and future connected motor vehicles.

The Future of Privacy Forum (FPF) is a D.C.-based non-profit organization that serves as a catalyst for privacy leadership and scholarship, and advances principled data practices in support of emerging technologies. Our Connected Car Project focuses on advancing privacy practices and understanding as new in-car technologies come to market, and we host stakeholder convenings on the topic, work with automakers and technology companies to advance responsible data practices, and serve as an active public voice about these issues. We also run a Connected Cars Working Group composed of over forty representatives from car manufacturers, technology suppliers, ridesharing companies, and connectivity providers. This group is an ongoing collaborative effort to pursue best practices for data in the connected vehicle ecosystem.[1]

FPF's extensive work in this area includes:

- Comments written in response to NHTSA's Request for Comment on Vehicle to Vehicle Rulemaking, "FMVSS No. 150, V2V Communications," available at https://fpf.org/2017/04/13/fpf-comments-nhtsas-v2v-rulemaking/
- Launch of a first-of-its kind consumer guide, Personal Data In Your Car, a first-of-its kind effort to inform consumer about the privacy impacts of automotive technologies, in partnership the National Automobile Dealers Association. The Guide is available at www.fpf.org/consumerguide
- Comments written in response to NHTSA's Request for Comment on the Federal Automated Vehicles Policy, available at: https://fpf.org/2016/11/22/fpf-submits-comments-on-nhtsas-federal-automated-vehicles-policy/
- An academic paper, *Shades of Gray: Seeing the Full Spectrum of Practical Data De-identification*, which suggests that rather than treat personal data as a black or white dichotomy, policymakers should view data in various shades of gray; and provides

[1] The views herein do not necessarily reflect those of our members or Advisory Board.

guidance on where to place important legal and technical boundaries between categories of identifiability, available at http://digitalcommons.law.scu.edu/lawreview/vol56/iss3/3.

- A white paper, *The Connected Car And Privacy, Navigating New Data Issues*, which surveys the collection of data inside the vehicle ecosystem and explores how connectivity and the connected car augment or change how that information is collected and eventually used, available at https://fpf.org/2014/11/13/new-fpf-paper-the-connected-car-and-privacy-navigating-new-data-issues/
- Launch of an interactive Smart Cities infographic, which maps the vast and growing network of connected technologies that power new and innovative services. The infographic includes a compilation of privacy best practices, highlights the role of smart transportation technologies in smart cities, and provides privacy-specific guidance for connected transportation systems, available at https://fpf.org/smart-city-privacy/

Our analyses are based on our own research, as well as interactions with members of industry, academics, advocates, and regulators.

Executive Summary

We commend the FTC and NHTSA for working together to host a public workshop focused on privacy and security issues related to connected vehicles. It is a valuable opportunity to expand the dialogue among regulators, industry, and advocates regarding expectations for consumer privacy in a rapidly evolving field.

As the automotive sector becomes more data-intensive, conversations of this kind are vital for fostering informed and constructive consumer protections. We look forward to participating in the workshop. Below, we highlight several items for consideration by the agencies and for the workshop.

FPF recommends that the FTC and NHTSA:

1. highlight the importance of transparency and communication around consumer data use, including through the provision of clear user interfaces and resources that are: 1) publicly available; 2) accessible before purchase; 3) reviewable throughout the life of a vehicle; as well as the incorporation of consumer privacy controls when appropriate
2. understand the importance of distinguishing between types of data in the vehicle context for any regulatory approaches to privacy (i.e. between data that is operationally critical or not, personally identifiable or not, sensitive or not), as well as the importance of accurately mapping data flows in a vehicle before apportioning responsibility between actors;
3. encourage alignment between federal and state regulatory guidance and encourage industry self-regulatory efforts;
4. consider the risks of connected vehicle data collection by state and local regulators, and propose guidance resources to support these regulators in data management best practices;
5. monitor new entrants to the market that may seek to monetize connected vehicle data without fully understanding existing consumer protections; and

6. recognize that this technological shift will have impacts beyond the automotive sector, particularly in the insurance and credit industries.

Introduction

While data collection in cars is not entirely new—computerized systems have been in vehicles since the 1960s—significant advancements are enabling a massive shift in the transportation sector. As vehicles incorporate sensors and data-heavy features with more computer chips and electronic components, they become more like computers than the mechanical chassis to which consumers are accustomed. The most significant changes that have taken place are the increase in volume, variety, and connectivity of data produced by vehicles. Some thinkers estimate that the average modern high-end car can contain 100 million lines of code[2] (more than a space shuttle), and that autonomous vehicles will generate 4,000 gigabytes of data per day.[3] The new types of data generated by modern vehicles include sensitive categories like location, biometric, and behavioral information—all of which can be considered sensitive information in certain contexts. And while acquisition of the previous types of data collected by cars would have required physical access to a vehicle—such as data from Event Data Recorders and On-Board Diagnostic systems—today's cars have built-in connectivity that can transmit information outside of the vehicle seamlessly.

Connected vehicle technologies hold tremendous potential to transform the safety and convenience of the vehicles in which we ride and drive. According to NHTSA's research, a full 94 percent of the 35,092 fatalities in U.S. motor vehicle accidents last year could be attributed to human error.[4] New technologies can reduce the number of accidents on our roads with features that mitigate human error. They also have the potential to increase mobility for the elderly and Americans with disabilities who may be constrained from driving altogether.

These safety improvements hinge on the ability of cars to communicate with each other, and to detect and understand the environment around them. Decisions that were previously manual or mechanized may now be automated, relying on data inputs collected from the many new kinds of sensors and computing devices being built into vehicles. This data enables features that enhance safety, convenience, and entertainment. While autonomous vehicles are most reliant on these features, most new vehicles today include some driving assistive features and connected infotainment services.

As we welcome the benefits of these new, it is critical that we build responsible data practices into connected cars—just as we have with new and unfamiliar technologies in other sectors. Being optimistic about the benefits of new data uses does not mean we need to be naive about the risks.

---

[2] *See, e.g.*, *Codebases: Millions of lines of code*, information is beautiful http://www.informationisbeautiful.net/visualizations/million-lines-of-code/

[3] *See, e.g.*, Damon Beres, *Autonomous cars will make your data plan look tiny*, Mashable (August 17, 2016), http://mashable.com/2016/08/17/intel-autonomous-car-data/ - yBAYycpLAqqI

[4] NATIONAL HIGHWAY TRAFFIC SAFETY ADMINISTRATION, *Critical Reasons for Crashes Investigated in the National Motor Vehicle Crash Causation Survey*, Traffic Safety Facts Crash Stats. Report No. DOT HS 812 115 (Feb. 2015), https://crashstats.nhtsa.dot.gov/Api/Public/ViewPublication/812115.

As connected vehicles develop and as we better understand the nature of the data and what is needed for these vehicles to operate, we also need to be sensitive to any privacy concerns that develop. We should ask tough questions around which parties have access to the data, who manages the consumer relationship, and which data is personal.

However, it is nearly impossible to anticipate today the full range of the privacy questions or concerns that will arise in the connected car given the diversity of technologies, uses, and models being considered today, and those we cannot yet imagine. This is especially true as these new technologies begin to transform the relationship of consumers to vehicles altogether, such as through fleet-based and other models.

We applaud the FTC and NHTSA for highlighting the importance of consumer privacy protections in this area. We commend NHTSA for taking an approach through its Federal Automated Vehicles policy of issuing guidance that can be easily updated in light of rapidly evolving technology, rather than fixed legislation. We believe that such efforts can enable these technologies to enter the market today, while retaining the flexibility necessary for them to evolve and improve. We also believe that, as the leading consumer protection agency in the United States, the Federal Trade Commission is well positioned to be the lead agency when it comes to data privacy enforcement in this sector. As these technologies advance, it will also be critical to ensure alignment between federal, state, and self-regulatory guidance for the connected vehicle ecosystem. Patchwork regulation could impede interoperability and design for automotive companies that build systems for national and global distribution.

Transparency and Consumer Controls

As the automotive sector rapidly transforms into a data-heavy sector, consumers are just beginning to understand and adjust to this new reality. Privacy considerations around connected vehicles are top of mind for consumers. A 2013 Auto Alliance survey concluded that privacy in this space matters to consumers: 75% surveyed were concerned that self-driving car technology could be used to collect personal data, 70% surveyed worried that this data could be shared with government/law enforcement, and 81% surveyed were concerned about security and potential hacking of self-driving cars.[5]

We recommend that all stakeholders in this space find creative ways to communicate these developments to consumers, and that regulators incentivize such efforts. We recommend a focus on communication with consumers at key points of contact throughout the vehicle purchase, rental, and use cycle. This can include providing information through dealerships, government interfaces, commercial websites, or direct messaging to drivers.

User interface design can be crucial to ensuring that consumers understand the ecosystem around their vehicle data. Meaningful consent can be difficult for devices across the Internet of Things

[5] Auto Alliance, *Poll: Consumers Still Want To Be In The Driver's Seat, Self-Driving Cars Raise Concerns* (June 2013) https://autoalliance.org/INDEX.CFM?OBJECTID=156688B0-CD5D-11E2-8898000C296BA163

given limited screen space, and connected vehicles encounter similar constraints.[6] We recommend the use of a "privacy by design" approach to building connected vehicle systems, which incorporates privacy throughout the engineering process, from the earliest design stages to the operation of the system.[7]

Consumer communications should help consumers grasp the importance of thinking about today's vehicle like a computer or smartphone, and help them find privacy-related information and controls. Clear consumer communication could include privacy control screens, the use of icons to connote data collection or transmission, options to clear on-board data, and more. We recommend that privacy settings and options be communicated to consumers in advance of purchase, e.g. through manufacturer websites, as well as in the owner's manual, through in-car notifications, and in rental agreements. Pre-purchase can be particularly important in the vehicle context given that vehicle software choices are often constrained after the point of purchase, in a manner distinct from the online services to which users may be accustomed.

We also recommend the creation of consumer privacy controls where possible. It is important to consider that, in the vehicle context, privacy implications can extend beyond the vehicle owner and also affect an operator, a lessee/renter, or a passenger, who may not have had an opportunity to review an owner's manual or manufacturer website.

NHTSA's commitment in the Vehicle to Vehicle Rulemaking (hereafter "V2V NPRM") to a comprehensive public education strategy on the topic of privacy in the Vehicle to Vehicle system is a great example of planned consumer outreach in this space.[8] FPF has taken steps to initiate such consumer education campaigns with our *Consumer Guide to Privacy in the Connected Car*, which we developed in partnership with the National Automobile Dealers Alliance.[9] The Consumer Guide, launched at the 2017 Washington Auto Show, was a first-of-its kind effort to inform consumer about the privacy impacts of automotive technologies. We hope to see an expansion of consumer education efforts around data-intensive automotive technologies.

Mapping Data Flows and Types

Any best practices or regulatory approaches to privacy in the connected vehicle would benefit from efforts to understand and map data flows and data types in the vehicle.

First, it is important to distinguish between "operational," or "safety-critical" data (used to enable vehicle decision-making) from other vehicle data (such as infotainment or convenience features). These distinctions may be complicated to draw, but will be useful when developing

---

[6] *See* Christopher Wolf & Jules Polonetsky, *An Updated Privacy Paradigm for the "Internet of Things,"* FUTURE OF PRIVACY FORUM (Nov. 19, 2013), https://fpf.org/wp-content/uploads/Wolf-and-Polonetsky-An-Updated-Privacy-Paradigm-for-the-%E2%80%9CInternet-of-Things%E2%80%9D-11-19-2013.pdf.

[7] Ann Cavoukian, Privacy by Design: The 7 Foundational Principles (Aug. 2009), https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf.

[8] Dep't of Transp., *Federal Motor Vehicle Safety Standards; V2V Commc'ns.*, Notice of Proposed Rulemaking, p.183 (Jan. 12, 2017), https://www.regulations.gov/document?D=NHTSA-2016-0126-0009 [hereafter V2V NPRM].

[9] THE FUTURE OF PRIVACY FORUM & NAT'L AUTOMOBILE DEALERS ASS'N, *Personal Data In Your Car* (Jan. 2017), http://fpf.org/consumerguide.

new privacy controls. For example, it is possible that more automated features, such as autonomous driving, will require sensitive data to function that we would otherwise recommend to be information subject to consumer control. Safety efforts such as Vehicle to Vehicle communication may similarly rely on the collection and transmission of such data from all new vehicles, without the option for consumer control or opt-out.

Second, it is important to distinguish between personally identifiable information ("PII") that is "reasonably linkable" to an individual and non-personal information. NHTSA and the FTC have established a definition of PII that is familiar to practitioners, consistent with established compliance regimes, and represents an important step in ensuring stability across business sectors and within the automotive ecosystem.

In the V2V Privacy Statement in the V2V NPRM, NHTSA defines PII as

> "Data that is reasonably or, as a practical matter, linkable to you… [D]ata is 'reasonably' or 'as a practical matter' linkable to you if it can be used to trace…messages back to you personally for more than a temporary period of time (in other words, on a persistent basis) without unreasonable expense or effort, in real time or after the fact, given available data sources."[10]

This definition is consistent with that in earlier NHTSA's Federal Automated Vehicles Policy[11] and long-standing FTC guidance.

While we are optimistic that both NHTSA and the FTC agree on a common definition of PII, we believe that this sector is nascent enough that no parties have defined which vehicle data meets the defined threshold of linkability. Any such definitions will be nuanced and dynamic, since data may move along the spectrum over time as new data sets or computing resources raise the risk of re-identification. Such an effort may require situating data points along a spectrum of identifiability, rather than a binary of "PII" or "not PII."[12] Moreover, a successful effort of this type would require first identifying and understanding each of the many types of data that flow through the connected vehicle ecosystem. We expect that the universe of this information will expand over time.

Among PII, certain data points should be considered more sensitive than others. Biometric, behavioral, and location information are particularly sensitive data. These types of data can reveal health information, location history, and precise. Industry privacy efforts have taken this consideration into account, including the *Privacy Principles For Vehicle Technologies And Services* advanced by the Alliance of Automobile Manufacturers and the Association of Global Automakers in 2014 ("Principles").[13] The Principles include a heightened notice standard for sensitive information and require affirmative consent before sharing these types of sensitive information for marketing or with unaffiliated third parties for their own use.

---

[10] V2V NPRM, p.181.
[11] DEP'T OF TRANSP., *Federal Automated Vehicles Policy*, p.104, (Sept. 2016), https://www.transportation.gov/sites/dot.gov/files/docs/AV%20policy%20guidance%20PDF.pdf.
[12] Jules Polonetsky, Omer Tene & Kelsey Finch, *Shades of Gray: Seeing the Full Spectrum of Practical Data De-identification*, 56 SANTA CLARA L. REV. 593 (2016). http://digitalcommons.law.scu.edu/lawreview/vol56/iss3/3.
[13] *Privacy Principles for Vehicle Technologies and Services*, AUTO ALLIANCE, http://www.autoalliance.org/?objectid=865F3AC0-68FD-11E4-866D000C296BA163 (last visited Nov. 21, 2016).

Lastly, we believe that advocates, regulators, and consumers could benefit from a clearer understanding of data flows in and through the vehicle. Data flowing through any given vehicle could be managed and processed by an OEM, a supplier, a connectivity provider, an app interface, an OBD-II plugin, or numerous other entities. We believe that proper mapping of data flows will be critical to ensure that consumers understand which entities manage the consumer relationship, and so that both the industry and regulators understand how to accurately attribute responsibility for the management and transfer of this information. It will also be important to consider how other actors in the ecosystem, such as dealers, car rental agencies, or repair shops interact with, generate, and manage consumer data.

This last consideration is particularly relevant with regard to in-vehicle infotainment applications. The main three connectivity models for in-vehicle applications are: 1) Original Equipment Manufacturer (OEM) provided apps, 2) third party apps on OEM platforms, and 3) mirroring of mobile devices (e.g., Apple CarPlay or Android Auto). We believe that it will be important to look to other sectors for examples of how data management responsibilities are apportioned between hardware, application platforms, and software. The OEM should not be considered responsible for every piece of data that flows through its display in the same manner that smartphone and TV manufacturers or app platform operators are not always responsible in other contexts. While the automotive sector includes complex contractual relationships between OEM, supplier, and technology companies that can add complexity, OEMs should be treated consistently with other hardware manufacturers and software platforms.

Regulatory Landscape

The management of data in the connected vehicle ecosystem should be guided by an understanding of the existing federal mechanisms that protect automobile consumers and that help meet their expectations around data privacy and security for vehicles.

As discussed, many of the considerations and questions raised in this space are not unique to connected vehicles. The Federal Trade Commission is well-positioned to be the lead agency for data privacy enforcement for connected vehicles, as the lead consumer protection agency in the United States. A wide range of data practices related to connected vehicles will be subject to the statutory authority of the FTC.[14] The FTC has already demonstrated a willingness to bring enforcement actions based on unfair or deceptive business practices in the context of the Internet of Things.[15] While FTC authority over vehicle-related data is therefore not a new development, the growing use of data in transportation will likely lead to increased FTC engagement with the transportation sector.

---

[14] 15 U.S.C. § 45(a) ("FTC Act").

[15] Last year, the Commission settled allegations against a device manufacturer, alleging that critical security flaws in its routers placed the home networks of hundreds of thousands of consumers at risk, and that the routers' insecure cloud services led to the compromise of thousands of consumers' connected storage devices, exposing their sensitive personal information on the internet. The consent agreement included a requirement that the company establish a comprehensive security program and notify consumers about software updates or other steps they could take to protect themselves from security flaws. *See* FEDERAL TRADE COMMISSION, *ASUS Settles FTC Charges That Insecure Home Routers and "Cloud" Services Put Consumers' Privacy at Risk* (Feb. 23, 2016), https://www.ftc.gov/news-events/press-releases/2016/02/asus-settlesftc-charges-insecure-home-routers-cloud-services-put.

While NHTSA's highlighting of privacy considerations in the Federal Automated Vehicles Policy and the V2V NPRM is encouraging given the importance of the issue, NHTSA's jurisdiction for privacy is limited to carrying out safety programs and overseeing technologies that the agency has mandated or implemented as part of these safety programs; NHTSA does not have comprehensive jurisdiction over consumer privacy issues related to vehicles.

In addition to existing U.S. privacy statutes, self-regulatory approaches have been productive in advancing responsible data practices for rapidly emerging industry sectors and technologies. Self-regulatory approaches are often industry motivated and led, creating opportunities to establish norms for quickly shifting technologies where law and regulation may not be able to keep pace. Self-regulatory frameworks can become enforceable commitments when companies publicly promise to abide by these frameworks, as these commitments trigger the FTC's authority to ensure companies keep their promises. These are particularly helpful for rapidly evolving technologies, such as connected cars. The FTC provides oversight and enforcement for self-regulatory regimes.[16]

Car manufacturers have established self-regulatory privacy guidelines for automotive technology, notably the aforementioned *Privacy Principles For Vehicle Technologies And Services*. Nearly all car manufacturers committed to adopt these Principles, which established baseline practices for customer privacy in vehicle technologies and services. The Principles are centered on the Fair Information Practice Principles of transparency, choice, respect for context, data minimization, de-identification and retention, data security, integrity and access, and accountability—with a special focus on the most sensitive data collected by connected vehicles, such as geolocation, biometrics, and driver behavior information.

The Principles became effective in 2016 and represent a positive step toward addressing the privacy risks raised by connected cars. Yet, data intensive automotive technology is no longer limited to traditional vehicle manufacturers. As many have observed, the transportation sector will change more in the next five years than it did in the last fifty.[17] The NHTSA Federal Automated Vehicles Policy thus wisely applies beyond traditional vehicle manufacturers to include equipment designers and suppliers, entities that outfit vehicles with automation capabilities or highly automated vehicle equipment, transit companies, automated fleet operators, "driverless" taxi companies, and other entities that offer services utilizing highly automated vehicles. We agree with NHTSA that consumer privacy protections should extend to these entities as well.

Many non-manufacturer entities in the automotive space have digitally and data-focused business models and are thus already conscious of consumer privacy safeguards and well aware of the FTC authority to bring enforcement actions against companies engaging in unfair or deceptive trade practices. But as NHTSA suggested in the Federal Automated Vehicles Policy, it could be helpful

[16] *See* Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUMBIA L. REV.583, 598 (2014) ("The FTC thus would serve as the backstop to the self-regulatory regime, providing it with oversight and enforcement.").

[17] *See, e.g.*, Kathleen Burke, *The Auto Industry Will Change More in Next Five Years than Prior 50, Says GM's President*, MarketWatch (June 12, 2016), http://www.marketwatch.com/story/why-gms-president-says-you-wont-be-driving-its-cars-2016-06-01.

for these entities to articulate a framework on data use in the auto context, and FPF looks forward to participating in further discussions about such efforts.

Data Requests by Regulators

As cars and cities become smarter and more connected and sensitive consumer data is collected by more sensors and technologies, industry actors will not be the only entities generating, collecting, and analyzing data. State and municipal governments may request or require transportation data from the private sector for the purpose of improving city services, or understanding local industry efforts. It will be incumbent on all parties to ensure that regulators are able to collect the data they need to support their citizens, but also to take into account rapidly-changing privacy risks. The ability to respond and adapt to such risks requires a technical capacity that many local regulators may not currently have or desire.

Recent efforts to hire Chief Information and Chief Technology Officers in cities across the country are a promising step. But as datasets grow, there will be challenges that regulators are not ready to handle, or will not expect. When state and local agencies request large sets of data but fail to follow privacy best practices, citizens' privacy winds up at risk.

One example took place earlier this year, when the New York Taxi and Limousine Commission began collecting ridesharing data that included time, date, and precise geolocation of pickup and drop-off locations for all for-hire vehicles in New York City. The rule was adopted despite concerns voiced by privacy advocates and riders who urged the city to revise the proposal to protect citizens' privacy. In response to the initial proposed rule, leading privacy and technology advocacy groups called for the TLC to 1) tailor the data collection more narrowly to the stated purpose by focusing on trip duration rather than the location of passengers' trips, 2) collect less precise, neighborhood-level geographic information, and 3) enact policies and procedures that detail the privacy and security protections for such sensitive data. The TLC did not adopt these recommendations in the final rule.

We recommend that federal regulators consider both the benefits and risks of such data collection, and propose guidance or best practices to state and local regulators.

Privacy Challenges Raised by Emerging Business Models

It will benefit regulators to understand and track the potential for monetization of vehicle data. Some analysts have predicted that the monetization of car data could become an up to $750 billion industry by 2030.[18] This monetization could occur through direct sale of services, tailored advertising, sale of data in bulk, and other approaches.

Startups and new automotive sector entrants seeking to monetize car data may be uncertain about existing consumer privacy protections, including by being less familiar with the enforcement capacity and criteria of the FTC than more established technology companies. These

[18] MCKINSEY & CO., *Monetizing Car Data* (Sept. 2016).

developments provide a market opportunity for companies who take a responsible approach, but pose genuine challenges in terms of ensuring consumer protections are maintained.

Impacting the Insurance and Credit Industries

The automotive industry will not be the only sector affected by this shift to connected vehicles. The growth of data in the auto sector has the potential to transform the insurance sector as well. Today, car insurance companies use proxies to estimate risk. Current proxies (age, gender, traffic tickets, etc.) are imperfect. There is potential for data from connected vehicles to drive more accurate estimations of risk.

Insurance companies are already embracing the growth in vehicle-generated data by developing usage based insurance applications built to harness the data available from on board diagnostic systems. These applications provide insurers with information on how a vehicle is driven in order to enable safe driver programs and personalized insurance rates. A user who wishes to enable these features must either order a separate telematics device that plugs into their car's OBD-II port, or install an app on their smartphone. These devices can transmit real-time behavioral driving data to the company in exchange for insurance plan benefits.[19] These programs can enable precise customization of plans—one Ohio insurance company is offering discounted rates to Tesla drivers whose regular driving routes include significant time on roads where Tesla's autonomous driving features can be used.[20]

The use of data to drive insurance decisions is typically subject to the Fair Credit Reporting Act. Insurance entities will need to consider how to ensure access, accuracy and correction of such data as required by FCRA.

Auto lending could be impacted as well, as highlighted in news stories documenting that auto lenders have begun attaching GPS trackers and starter interruption devices to the vehicles of subprime borrowers. A New York Times investigation revealed that some lenders used these features to remotely disable cars and track consumer movements even when borrowers were current on their payments.[21]

We recommend that the FTC and NHTSA monitor downstream effects and evolving features enabled by vehicle-generated data, even outside the automotive technology sector.

---

[19] *See, e.g.*, Nationwide's "SmartRide" https://www.nationwide.com/smartride.jsp; Progressive's "Snapshot" https://www.progressive.com/auto/snapshot/. Other companies enable smartphone apps to serve the same purpose, *e.g.*, AllState Drivewise https://www.allstate.com/drive-wise.aspx and State Farm "Drive Safe & Save" https://www.statefarm.com/insurance/auto/discounts/drive-safe-save/mobile-app.

[20] ROOT Insurance, *ANNOUNCEMENT: New Discount for Tesla® Drivers*!, March 9, 2017 Https://blog.joinroot.com/tesladiscount/

[21] *See, e.g.*, Michael Corkery and Jessica Silver-Greenberg, *Miss a Payment? Good Luck Moving That Car*, The New York Times (September 24, 2014), https://dealbook.nytimes.com/2014/09/24/miss-a-payment-good-luck-moving-that-car/?_r=0.

Conclusion

A cohosted workshop by NHTSA and the FTC is an important step in enabling advocates, industry, and consumers to build an understanding of the regulatory landscape of this rapidly evolving sector. We commend the agencies for working together, and we look forward to participating in the beginning of this dialogue around an emerging field.

Please contact FPF Policy Counsel Lauren Smith, lsmith@fpf.org with any follow-up or questions.

Respectfully submitted,

Lauren Smith
lsmith@fpf.org
Policy Counsel

John Verdi
jverdi@fpf.org
Vice President of Policy