Comments from

THE FUTURE OF PRIVACY FORUM

to

DEPARTMENT OF TRANSPORTATION

National Highway Traffic Safety Administration
Washington, D.C.

Docket No. NHTSA-2016-0090

Request for Comment on "Federal Automated Vehicles Policy"

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

November 22, 2016

Table of Contents

On behalf of the Future of Privacy Forum, we are pleased to submit these comments regarding the Department of Transportation and National Highway Traffic Safety Administration Request for Comment on the Federal Automated Vehicles Policy guidance, published in the Federal Register on September 23, 2016.

Introduction

We commend NHTSA for their forward-looking Federal Automated Vehicles Policy guidance (hereafter "Guidance") and the acknowledgement that privacy will play a key role in promoting trust in connected vehicles. This Guidance and its emphasis on privacy is an important first step in building that trust.

The Future of Privacy Forum is a DC-based non-profit organization that serves as a catalyst for privacy leadership and scholarship, and advances principled data practices in support of emerging technologies. We run a Connected Cars Working Group composed of over forty representatives from car manufacturers, technology suppliers, ridesharing companies, and connectivity providers. This group serves as an ongoing collaborative effort to pursue best practices for data in the automated vehicle ecosystem.[1] We offered oral comments at the November 10, 2016 public meeting, and thank you for the opportunity to delve into further detail with written comments.

Automated vehicle technologies hold tremendous potential to transform the safety and convenience of the vehicles in which we ride. 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.[2] NHTSA is right to recognize that evolving technologies can reduce the number of accidents on our roads, and also have the potential to increase mobility for the elderly and Americans with

[1] The views herein do not necessarily reflect those of our members or our Advisory Board.
[2] 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.

disabilities who may be constrained from driving altogether. We applaud NHTSA for releasing guidance that enables these technologies to enter the market, while retaining the flexibility necessary for the Guidance to evolve and improve along the way.

Some safety technologies under development may hinge on the ability of cars to detect and understand what is around them better than a human driver. In addition, decisions that were previously manual or mechanized may now be algorithmic, relying on data inputs collected from each of the many new kinds of sensors and computing being built into vehicles.

As we welcome these new technologies, it is critical that at the front-end of the connected car revolution, we build responsible data practices into connected cars—just as we have in other new and unfamiliar technologies that have disrupted other sectors. Being optimistic about the benefits of new data uses does not mean we need to be naive about the risks. As highly automated vehicles (hereafter, "HAVs") 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.

But it is nearly impossible today to anticipate today the full range of the privacy questions or concerns that will arise 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.

As these policies advance, it will be critical to ensure alignment between Federal, State, and self-regulatory guidance for the automated vehicle ecosystem. Consistency between federal, state, and self-regulatory regimes in this space are critical given that automotive companies design systems at a national and global level. Patchwork legislation could impede interoperability or render vehicles incapable of driving across state lines. Instead, NHTSA should encourage states to follow NHTSA's example in issuing guidance that can be easily updated in light of rapidly evolving technology, rather than adopting this guidance as law at this time.

In the following sections, we will detail our responses to the sections of the Guidance relevant to privacy.

Executive Summary

Our comments are based on a full review of the Guidance, with particular attention to the sections that focus on privacy. Overall, the Guidance articulates a workable model for the automated vehicle ecosystem that addresses important issues regarding the beneficial uses of data in the automated vehicle sector, the data privacy risks raised by automated vehicles, and the importance of establishing norms for responsible data practices in this emerging market.

We recommend that NHTSA:

1. be mindful of the existing mechanisms that protect automotive consumers and that help meet their expectations around data privacy and security for vehicles, while ensuring that the current NHTSA guidance, future versions of the guidance, and any future regulatory actions do not conflict with these existing protections;
2. maintain clarity regarding NHTSA's jurisdiction regarding privacy issues;
3. support existing self-regulatory efforts, including the Privacy Principles For Vehicle Technologies And Services published by the Alliance of Automobile Manufacturers and the Association of Global Automakers;
4. support any future complementary self-regulatory efforts by non-manufacturer entities to address privacy issues raised by automated vehicles;
5. continue to draw from the Fair Information Practices Principles for privacy in future revisions to the federal Guidance;
6. encourage both governmental and non-governmental entities to appropriately de-identify personal data related to vehicle operation in ways that support safety efforts while minimizing privacy risks; and
7. support self-regulatory efforts to better secure vehicles and vehicle data, such as the Auto ISAC.

Please find our detailed recommendations in the following sections.

Jurisdiction

The management of data in the automated 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.

Corporate data practices are subject to the authority of the Federal Trade Commission under its broad Section 5 authority to bring civil enforcement actions against companies engaging in unfair or deceptive business practices.[3] Additionally, some data elements may be subject to additional existing state and federal laws relating to credit, insurance, employment, communications and children. But the widest range of data practices related to automated vehicles will be subject to the

[3] 15 U.S.C. § 45(a) ("FTC Act").

statutory authority of the FTC. The FTC has already demonstrated a willingness to bring enforcement actions based on such business practices in the context of the Internet Of Things.[4]

While the Guidance focus on privacy is encouraging given the importance of the issue, NHTSA 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. This makes it all the more important to ensure that any references to privacy are consistent with FTC standards.

It is nonetheless important for the Department to appreciate the effects that its proposed Guidance will have on the ecosystem. It is in the best interest of all actors in this sector to be proactive about privacy, and the Guidance helps promote this approach by highlighting privacy best practices.

Self-Regulation for Privacy

We commend NHTSA for identifying self-regulatory efforts as the best approach to advance consumer privacy in automated 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 efforts trigger the FTC's authority to ensure companies keep their public-facing commitments. The FTC has served as a backstop to provide oversight and enforcement for self-regulatory regimes.[5]

Great strides have been made regarding self-regulatory privacy guidelines for automotive technology. The Alliance of Automobile Manufacturers and the Association of Global Automakers in 2014 issued a set of "Privacy Principles For Vehicle Technologies And Services," (hereafter, "Principles,") establishing baseline Principles for customer privacy in vehicle technologies and services.[6] Twenty car manufacturers committed to adopt these Principles. The Principles are centered on the Fair Information Practice Principles of transparency, choice, respect for context,

[4] This 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 to notify consumers about software updates or other steps they can 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.

[5] *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.")

[6] *Privacy Principles for Vehicle Technologies and Services*, AUTO ALLIANCE, http://www.autoalliance.org/?objectid=865F3AC0-68FD-11E4-866D000C296BA163 (last visited Nov. 21, 2016).

data minimization, de-identification and retention, data security, integrity and access, and accountability—with a special focus on the most sensitive data collected, such as geolocation, biometrics, and driver behavior information.

The Principles became effective in 2016 and represent a great step toward addressing privacy risks raised by connected cars. Yet, as the Guidance recognizes, 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.[7] The NHTSA Guidance thus wisely applies beyond traditional vehicle manufacturers to include equipment designers and suppliers, entities that outfit vehicles with automation capabilities or HAV 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.

As NHTSA understands, it is important to be aware that many non-manufacturer entities in the automotive space already 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 engage in unfair or deceptive trade practices. But as the Guidance suggests, it could be helpful 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.

Privacy Section of the Safety Assessment Letter

Again, we commend NHTSA for recognizing the importance of privacy in enabling the automated vehicle ecosystem to advance while protecting consumer trust. Including privacy as a section in the Safety Assessment Letter certainly affirms the importance of building in privacy considerations to these technologies from the outset.

Applicability

To prevent duplication, we suggest that entities that are already signatories to the previously mentioned Alliance of Automobile Manufacturers and the Association of Global Automakers Privacy Principles should be able to satisfy this section of the letter by simply disclosing their status as signatory to those Principles. Adding an additional, distinct set of privacy principles and requirements onto entities that have already committed to a set of industry-negotiated privacy principles that NHTSA recognizes as beneficial would disrupt the purpose of those Principles and create an unnecessary logistical burden. The Principles are a dynamic document that should be updated to keep pace with evolving technologies.

[7] *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.

Content

Consumer privacy is an important consideration for all entities in the automated vehicle ecosystem. Entities that facilitate a consumer relationship in the car and have not committed to the Principles or similar self-regulatory efforts may benefit from the framing in the Guidance description of the Privacy section of the Safety Assessment Letter.

The Guidance wisely highlights several of the Fair Information Practice Principles for privacy (hereafter FIPPs) that are particularly important for automated vehicle data that can be reasonably linked to an individual. The FIPPs have historically been a holistic set of principles that are flexible and interdependent. It will be important to apply the FIPPs in the vehicle ecosystem in a sophisticated and nuanced way that takes into account safety interests and other countervailing interests to privacy. Different FIPPs may be more or less relevant depending on the context of a business practice and the technology involved—leaning on some principles more than others is consistent with the FIPPs framework.

In the connected and automated vehicle context, data security, transparency, and de-identification will be key.

Data security is vital to ensuring trust and safety for all connected vehicle data. The industry should be proactive in pursuing data security practices. Ongoing processes in this space like the Automotive Information Sharing and Analysis Center and the NTIA multistakeholder process on Cybersecurity Vulnerabilities disclosure should be encouraged.

Transparency will be important to ensuring that consumers understand how entities in this space will collect, use and share their data. Clear, meaningful and conspicuous notices, typically a best practice for privacy, can be invaluable for building consumer trust, but may need to be administered differently in vehicle context than in other sectors. Best practices for mobile privacy notifications, such as just-in-time notices that appear on a phone's screen when opening an app, could be detrimental in the vehicle context where they could distract an active driver from the road.[8] Creative approaches to communicating company data practices should be encouraged, and should be flexible enough to account for the differences between consumers who purchase a vehicle versus those who participate in ridesharing or rental services, or passengers who ride along in another's vehicle. Affirmative education efforts may also play a useful role in communicating data practices and protections to consumers.

As discussed in the next section, data collection and sharing may prove particularly important to ensure the safety and advancement of automated technologies. Data minimization and retention limitations that are often central to protecting consumer privacy may therefore not be as relevant in this context, with proper de-identification playing a larger role in protecting such data. Data minimization can require organizations to specify all of the purposes for which they will use the data they collect, collect only that data needed to achieve those ends, and use the data only for specified purposes. Granular application of data minimization may risk limiting valuable research

[8] NHTSA's own work to reduce distracted driving reinforces the importance of minimizing pop-up notifications for drivers. *See* DISTRACTION, http://www.distraction.gov/

in the development of new services[9] and addressing safety. In the automated vehicle context, proper de-identification may accordingly become more important than minimization in protecting this data as it is analyzed and shared. Further detail on best practices in practical de-identification can be found in the next section of these comments.

Additionally, the treatment of personal data under each of the FIPPs may necessarily differ depending on whether that data is critical to the operation of the vehicle—particularly with regard to providing data access, correction, and choice for consumers. Fulfilling these FIPPs may involve different considerations based on whether collection of that data is crucial to vehicle operation and safety or not, and whether data is kept on the vehicle or shared through connectivity services. For example, it may be difficult to provide consumers with meaningful choice about whether location information is used in an HAV if the HAV software cannot function without such data. A policy that requires that a company provide a service even if the consumer opts out of those features could force companies to provide an impaired version of their service, or one that does not retain important safety data. It may be possible that a consumer in that instance could be offered choice about whether that data is shared outside of the vehicle or not, but not whether it can be collected in the first instance. These are challenging considerations given the rapidly changing pace of these technologies, and definitional lines may prove difficult to draw at this time.

It may also be important to consider who is best positioned to meaningfully implement a given principle. For example, connected car services can be provided by a number of entities, and the entity best able to provide transparency may not be the entity best positioned to secure the data—and neither of those entities may be best positioned to implement appropriate controls. In such circumstances it is important for entities to cooperate to ensure that appropriate consumer safeguards are in place.

Additionally, it is important to consider whose privacy specifically is being considered, given that an automated vehicle may collect information about an owner, an operator, a lessee/renter, a passenger, and bystanders.

Data Recording and Sharing

Effective data recording is a key aspect of safe testing of HAVs and one of the primary means through which companies are improving their technology. However, the recording capabilities are specific to each company's proprietary systems. As HAV technology advances, it may be important for entities to collect and share data about safety-related incidents. No mechanism exists today to share the type of data specified in the "Data Recording and Sharing" section of the Guidance, and advancement of any such program should be an opportunity for industry to take a leadership role.

We suggest that NHTSA coordinate such an effort with industry, with a focus on establishing proper processes to determine what data would be shared and for what purposes, the appropriate

[9] *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.

sharing mechanism, which entities manage and retain the shared data, proper security practices, and which entities would have access to the database.

At a minimum, any such data should be limited such that it does not require sharing data at a proprietary or functional level. Consumer use data from ridesharing or other platforms should also not be included, as this data is particularly sensitive for consumers and should not be necessary for safety analysis. Proper de-identification is important for any increased data sharing that NHTSA calls for, including the data collected and managed by NHTSA itself. These considerations should also apply to any enhanced government data collection tools or additional government data collection considered in the Guidance.

"Personal Data" and De-Identification

Lastly, we support the Guidance's definition of "personal data." In Footnote 12 of the Data Recording and Sharing section of the Safety Assessment Letter, NHTSA defines "personal data" consistently with the FTC's definition of "personally identifiable information;" both definitions are consistent with longstanding definitions established in FIPPS-based frameworks, including the Administration's Consumer Privacy Bill of Rights. The definition used in the Guidance focuses on whether information is "reasonably linkable" to an individual. This definition is familiar to practitioners, consistent with established compliance regimes, and represents an important step in ensuring consistency across business sectors and within the automotive ecosystem.

Proper de-identification of shared data will be crucial for entities when addressing sections of both the "Data Recording and Sharing" and the "Privacy" sections of the Safety Assessment Letter. We agree that it is important to de-identify sensitive data, including biometric, behavioral, and geolocation data, where practicable.

According to the FTC, data are not "reasonably linkable" to individual identity to the extent that a company: (1) takes reasonable measures to ensure that the data are de-identified; (2) publicly commits not to try to re-identify the data; and (3) contractually prohibits downstream recipients from trying to re-identify the data (the "Three-Part Test").[10]

We urge NHTSA to recognize that "reasonable measures" as set out by the FTC may include administrative, contractual, and technical measures, and may differ based on the level of identifiability of the data. This consideration should be understood to take into account factors such as the utility of the data, whether the data is intended to be kept confidential or made public, the sensitivity of the data, as well as legal, technical and administrative measures, in order to determine the risk of re-identification for particular datasets. A further reason to link this assessment to "reasonable measures" is that it allows the standard to be adapted over time as different de-identification concerns are identified and different technical and industry protections are developed.

[10] FEDERAL TRADE COMMISSION, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE (2012), at 21, https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

For a detailed review of issues around de-identification as well as a practical roadmap, please see our recent academic paper *Shades of Gray: Seeing the Full Spectrum of Practical Data De-identification*, in which Jules Polonetsky and Omer Tene describe data on a spectrum of identifiability, from explicitly personal data, to pseudonymous data, de-identified data, and finally, to fully anonymous and aggregated data such as high-level statistical data.[11]

Ethical Considerations

Lastly, we thank NHTSA for recognizing the important and challenging issues regarding ethical considerations for HAVs. This is an important and challenging topic. We look forward to working with all stakeholders to advance this important discussion

Conclusion

This Guidance is a productive first step in establishing a consistent path forward for HAVs. We thank NHTSA for recognizing the importance of privacy and look forward to remaining engaged as the guidance evolves. Please contact FPF Policy Counsel Lauren Smith, lsmith@fpf.org with any follow-up or questions.

Sincerely,

Lauren Smith
Policy Counsel

John Verdi
Vice President of Policy

[11] 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.