Comments from

THE FUTURE OF PRIVACY FORUM

to

U.S. DEPARTMENT OF TRANSPORTATION

National Highway Traffic Safety Administration
Washington, D.C.

Docket No. NHTSA-2016-0126

Request for Comment on "FMVSS No. 150, V2V Communications"

Lauren Smith, Policy Counsel

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

lsmith@fpf.org

www.fpf.org

April 12, 2017

Table of Contents

Introduction

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's (NHTSA) Request for Comment on FMVSS No. 150, V2V Communications, published in the Federal Register on January 12, 2017. Our comments focus on the privacy and security implications of the proposed rule.

The Future of Privacy Forum (FPF) 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. Our Connected Car Project focuses on advancing privacy practices and understanding as new in-car technologies come to market, and we serve as an active public voice about these developments, host stakeholder convenings on the topic, and work with automakers and technology companies to advance responsible data practices. 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 serves as an ongoing collaborative effort to pursue best practices for data in the automated vehicle ecosystem.[1]

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

Executive Summary

We commend NHTSA for its work to introduce a Vehicle to Vehicle (V2V) Communications system that takes privacy seriously in both the design and implementation of the system. We agree that great gains in road safety can result from broad-scale application of crash avoidance technologies like V2V. Overall, FPF supports NHTSA's approach to consumer privacy and the seriousness with which NHTSA has engaged this topic, working with partners to design a system that includes multiple technical, physical, and organizational controls to help limit potential privacy impacts on consumers. Below, FPF describes measures that could help clarify or bolster these privacy safeguards.

FPF is encouraged by NHTSA's "privacy by design" approach to building this system, which takes privacy into account throughout the entire engineering process from the earliest design stages to the operation of the system.[2] We also commend NHTSA for working with partners in order to implement layers of technical, policy and physical controls to mitigate potential privacy impacts of the V2V system. Further, we agree with NHTSA that the proposed ongoing privacy risk analysis is a crucial component of the V2V system.

FPF recommends that NHTSA:

1. improve the contemplated privacy notice in terms of content, usability, and delivery mechanisms, and undertake the proposed consumer education efforts;[3]
2. retain the proposed rule's approach to defining Personally Identifiable Information—an approach that is consistent with the Federal Trade Commission and other Federal entities' definitions;[4]
3. work with other regulators and partners to identify any protective technical or legal control that could limit third party collection, aggregation, or sale of V2V data, including considering encryption or higher Pseudonym Certificate rotation rates;[5]
4. consider what sorts of consumer privacy controls are appropriate (*e.g.* opt-out), when such choices are appropriate, and how such choices can be presented in the context of the operators' relationships with vehicles and service providers;[6]
5. ensure oversight and accountability mechanisms for the security entity that will run the proposed rule's credential management system;[7]
6. continue to study and mitigate the residual privacy risks created by the proposed rule.[8]

---

[2] Ann Cavoukian, Privacy by Design: The 7 Foundational Principles (Aug. 2009), https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf.
[3] *See* **Privacy Notice** below.
[4] *See* **PII and De-Identification Definitions** below.
[5] *See* **Third Party Access to BSMs** below.
[6] *See* **Consumer Privacy Controls** below.
[7] *See* **Security Entity for Credential Management System** below.
[8] *See* **Residual Privacy Risks** below.

Privacy Notice

We appreciate NHTSA's goal of providing notice to consumers by requiring the inclusion of a "V2V Privacy Statement" in vehicle owner's manuals and on manufacturer's websites, as well as by encouraging and advancing consumer education efforts. In this Section, we present potential improvements to the contemplated privacy notice content, usability, and delivery mechanisms.

The proposed V2V Privacy Statement[9] contains a great deal of detail that may be confusing to consumers. In addition to a longer notice in this style, we recommend that NHTSA permit and encourage the inclusion of a concise, easy-to-understand and meaningful disclosure in the form of layered notice as suggested in the *Privacy Issues for Consideration by USDOT Based on Review of Preliminary Technical Framework (Final – Rev A)* report (hereafter "MITRE 1"),[10] but we discourage NHTSA from solely relying on just-in-time notice, which can be distracting in some contexts.

Within the text of the proposed statement, we believe that the second and third paragraphs of section b) "Collection, Storage and Use of V2V Information" may confuse consumers. The high-level overview of these risks accompanied by NHTSA's disclaimer of responsibility for privacy risks that may arise from them could cause consumers concern, particularly in the absence of an opt-out or other consumer privacy controls.

We support NHTSA's intention to undertake a comprehensive public education strategy on the topic of privacy in the V2V system.[11] Given the rapidly changing landscape of data in the automotive sector, we believe that consumer education around the generation and use of this information, as well as on the existing privacy protections for automotive data will be crucial to adoption of new automotive technologies. We recommend that such education efforts extend to auto dealers and personnel as well, given that dealerships are the primary interface that consumers have with information about a new vehicle. It may be helpful to provide a version of the V2V Privacy Statement to consumers at dealerships in advance of or at time of purchase, at least until the educational efforts result in a more common understanding of the V2V system.

FPF has already taken steps to initiate such consumer education campaigns with our January 2017 launch of the Consumer Guide to Privacy in the Connected Car, which we developed in partnership with the National Automobile Dealer's Alliance.[12] The Guide, launched at the 2017 Washington Auto Show, was a first-of-its kind effort to build consumer understanding of the privacy impacts of automotive technologies. We hope to see a growth in similar consumer education efforts around data-intensive automotive technologies.

---

[9] DEP'T OF TRANSP., *Federal Motor Vehicle Safety Standards; V2V Commc'ns.*, Notice of Proposed Rulemaking, p.181 (Jan. 12, 2017), https://www.regulations.gov/document?D=NHTSA-2016-0126-0009 [hereafter NPRM].
[10] MITRE CORP., *Privacy Issues for Consideration by USDOT Based on Review of Preliminary Technical Framework (Final – Rev A)*, p.67 (Feb. 24, 2016), https://www.regulations.gov/document?D=NHTSA-2016-0126-0003 [hereafter MITRE 1].
[11] NPRM, p.183.
[12] THE FUTURE OF PRIVACY FORUM & NAT'L AUTOMOBILE DEALERS ASS'N, *Personal Data In Your Car* (Jan. 2017), http://fpf.org/consumerguide.

PII and De-Identification Definitions

The fact that V2V messages do not directly identify a person or their vehicle is critical to the privacy design of the system. In the pursuit of excluding such Personally Identifiable Information (PII) from the system, we commend NHTSA for using a definition of PII that is consistent with the FTC and other Federal actors' definitions. We believe that consistency of these definitions will facilitate both consumer and industry understanding and practice.

In the V2V Privacy Statement, NHTSA defines linkability in the statement, "V2V messages do not…contain data that is reasonably or, as a practical matter, linkable to you…V2V data is "reasonably" or "as a practical matter" linkable to you if it can be used to trace V2V 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."[13] This definition is consistent with that in the Federal Automated Vehicles Policy[14] and 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.

FPF supports this straightforward and consumer-friendly definition of linkability, but as stated in the following Section, we have concerns about whether the MITRE study, *Technical Memorandum: Modeling and Simulation of Areas of Potential V2V Privacy Risk*, (hereafter "MITRE 2")[15] reveals that the information produced by the V2V system could in fact be linked back to an individual "reasonably" or "as a practical matter," "without unreasonable expense or effort…after the fact, given available data sources." We recommend that NHTSA work with other regulators and partners to explicitly address this issue, and consider being explicit about these risks in consumer-facing information.

Moreover, it is worth considering that the FTC's current de-identification standard hinges on whether there is "a reasonable level of justified confidence that the data cannot reasonably be used to infer information about, or otherwise be linked to, a particular consumer, computer, or other device."[16] To determine when data are not "reasonably linkable," the FTC has established a three-part test. The test determines that 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").[17]

---

[13] NPRM, p.181.
[14] 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.
[15] MITRE CORP., *Technical Memorandum: Modeling and Simulation of Areas of Potential V2V Privacy Risk*, (March 8, 2016), https://www.regulations.gov/document?D=NHTSA-2016-0126-0002 [hereafter MITRE 2].
[16] FEDERAL TRADE COMM'N, *Protecting Consumer Privacy in an Era of Rapid Change* 21 (2012), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.
[17] FEDERAL TRADE COMM'N, *Protecting Consumer Privacy in an Era of Rapid Change* 21 (2012), https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

The third pillar of this test plays an important role in protecting consumers, and we encourage NHTSA to work with other regulators and policymakers to propose protections that would be analogous to what would be expected of a private company for the V2V system.

Manufacturer Responsibility Under the Principles

The NPRM mentions an intent to collaborate with motor vehicle manufacturers to build on the principles advanced by the Alliance of Automobile Manufacturers and the Association of Global Automakers in 2014 "Privacy Principles For Vehicle Technologies And Services," ("Principles") that established baseline principles for customer privacy in vehicle technologies and services.[18] Nearly all automakers committed to these Principles.

The V2V system has been designed to prevent communication of PII, therefore, our understanding is that the privacy protections afforded by the Principles are not relevant in this context. The definition of "covered data" under the Principles includes: "1) Identifiable Information that vehicles collect, generate, record, or store in an electronic form that is retrieved from the vehicles…or 2) Personal Subscription Information provided by individuals subscribing or registering for Vehicle Technologies and Services." Given NHTSA's own characterization that the BSM information is not linkable PII, data from the BSM is thus not "identifiable information."

We believe the industry could benefit from an explicit statement from NHTSA clarifying the extent of the rule's application to carmakers and applications, as well as the interaction between V2V data and the Principles (including with regards to applications that rely on this data.)

Third Party Access to BSMs

Our greatest privacy concern relates to third party access to BSMs outside of the V2V system. While the privacy-centric design of the V2V system goes to great lengths to protect privacy and avoid creating PII within the system, the messages are freely distributed within physical range on DSRC, and the MITRE 2 study reveals that significant privacy risks can arise from third party collection of these messages.[19] While NHTSA correctly acknowledges their limited jurisdiction regarding third party collection or use of this information, it is important that NHTSA work with other regulatory agencies to consider and study the potential privacy ramifications of enabling third parties to access this data. Regardless of jurisdictional issues, through this rule, NHTSA creates a system that generates significant quantities of data that is communicated, unencrypted, into the outside world where any party with a reasonably accessible device could collect it. We recommend that the final rule consider legal or technical controls that would prevent third parties from aggregating, analyzing, and potentially re-identifying this information.

We are concerned about this possibility even though BSMs within the system are not readily linkable to an individual, given that the MITRE 2 study concluded that for third parties aggregating such data outside of the system, "trip origin, destination, and route could be used in conjunction

[18] AUTO ALLIANCE, *Privacy Principles for Vehicle Technologies and Services*, https://autoalliance.org/connected-cars/automotive-privacy-2/principles/ (last visited April 12, 2017).
[19] MITRE 2.

with data sources outside of the V2V system to develop a profile of the individual who owns or operates the V2V device/vehicle broadcasting BSMs."[20] This "outside information" could include readily available public information, such as the ability to impose a given device's coordinates onto a map that could enable it to be linked to physical addresses, such as home or work locations of an individual. Our concerns are heightened given that the MITRE report demonstrates that the path of a V2V device can be tracked with 100% certainty when 100% of all BSMs transmitted during a trip are collected and available for analysis.[21]

Our understanding is that while all DSRC roadside units (RSUs) that are part of the V2V system as well as any third party "transceivers" which send signals over DSRC require authorization and are subject to regulation by the Federal Communications Commission, devices that are designed to only *receive* BSM messages may not require authorization or be subject to any regulatory oversight.[22] If this is indeed the case, they could therefore be deployed at-will by third parties limited only by their interest and resources, who could aggregate, re-identify, and potentially sell content of the messages.

We recognize that NHTSA's Privacy Impact Assessment, when evaluating the privacy impacts of the rule, relied in part on the fact that easier, less expensive methods of vehicle tracking exist.[23] However, our understanding is that the relatively low cost and size of RSU receivers and the large potential commercial opportunity posed by collection and sale of this data could mean that collection and analysis of BSM data by commercial or other parties is within the realm of possibility given the MITRE study findings. We do not believe that the expense or difficulty of installing such a network—especially in an urban area and when the technology could fit in a space as small as a smart lightbulb—would prevent such an effort if an actor saw a sufficient market opportunity.

When considering this concern, it is important to consider that the devices necessary to collect this information are accessibly priced today,[24] and are likely to become more affordable over time. It is important to keep in mind the rise within the last two decades of the multi-billion-dollar consumer data industry. Some analysts have predicted that the monetization of car data could be an up to $750 billion industry by 2030,[25] and we anticipate that as the automotive and consumer data industries develop, entities could determine that the significant resources expenditures to create a widespread system of this sort could be worthwhile investment. It is within the realm of possibility that such entities might build the 100% coverage network for certain areas and invest resources into the data transmission, analysis and storage that MITRE found could transform de-

[20] MITRE 2, p.15.
[21] MITRE 2, p.31.
[22] MITRE 1, p.2; FCC Safety and Special Radio Services, 47 C.F.R. §§ 90.7, .371,.373, .375 (defining roadside unit as a "transceiver that is mounted along a road or pedestrian passageway…[that] broadcasts data to on-board units or exchanges data with on-board units in its communications zone."; stating the basic operating and licensing rules for DSRC RSUs and referencing the ASTM-DSRC standard.).
[23] Dep't of Transp., *Privacy Impact Assessment*, p.11 (Dec. 29, 2016), https://cms.dot.gov/sites/dot.gov/files/docs/Privacy%20-%20NHTSA%20-%20V2V%20NPRM%20-%20PIA%20-%20Approved%20-%20122016.pdf [hereafter PIA].
[24] The NPRM estimates the total direct component costs to OEMs were estimated to be $162.77 for one DSRC radio. NPRM, p.278.
[25] MCKINSEY & CO., *Monetizing Car Data* (Sept. 2016).

identified BSM data into linkable PII. We believe that it is possible that this data, if it is as linkable as posited by the MITRE study, could lead to a data brokerage industry based on collecting, analyzing, and selling this information.

Moreover, extensive collection and analysis of this data by municipalities and law enforcement agencies could lead to unique, heightened Fourth Amendment concerns. In the concurrence in *U.S. v. Jones*, a majority of Supreme Court justices posited that long-term, comprehensive electronic vehicle tracking could trigger Fourth Amendment protections by violating a person's reasonable expectations of privacy, even if alternative, less comprehensive methods existed to gain the same information.[26] Five Justices in the concurrence supported the idea that future electronic modes of vehicle surveillance that do not require physical invasion of property could lead to circumstances in which "relatively short-term monitoring of a person's movements on public streets accords with expectations of privacy that our society has recognized as reasonable,…[b]ut the use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy."[27] If municipalities and law enforcement gain access to and rely on V2V information to prosecute crimes, Fourth Amendment concerns could arise. This concern is particularly relevant if V2V is a system that requires no trespass but offers users no opt-out choice or other consumer privacy controls.

Given the demonstrated privacy risks highlighted in the MITRE 2 study, we recommend that NHTSA work with other regulators and partners to:

1. Undertake further study to identify any protective technical or legal control that could limit third party collection, aggregation, or sale of BSMs and BSM data, including by entities operating receive-only DSRC devices. For example, encryption is an oft-used control to enhance privacy, and we would welcome a study of whether latency issues would prevent using encryption to protect BSMs. Are other technical controls possible?
2. Consider increasing the Pseudonym Certificate rotation rates given the MITRE 2 study findings that linkability is reduced when they rotate more frequently.

Consumer Privacy Controls

The fundamental privacy building blocks of notice and choice are core to the Fair Information Practice Principles, existing privacy principles in the automotive space, and DOT's commitments under its own PIA template. The DOT PIA template includes a section on "Individual Participation and Redress," which states that "DOT should provide a reasonable opportunity and capability for individuals to make informed decisions about the collection, use, and disclosure of their PII. As required by the Privacy Act, individuals should be active participants in the decision making process regarding the collection and use of their PII..."[28]

[26] The Supreme Court decision in *United States. v. Jones* noted that "[i]t may be that [tracking GPS location of a vehicle for four weeks] through electronic means, without an accompanying trespass, is an unconstitutional invasion of privacy." *United States v. Jones*, 565 U.S. 400, 412 (2012).
[27] *United States v. Jones*, 565 U.S. 400, 415 (2012)
[28] MITRE 1, p.14.

Given these frameworks, we believe that the availability of an opt-out or other consumer privacy controls within the V2V system deserves further study. We recognize that the success of an interdependent network like V2V relies on widespread use of the system, and that this is a fundamental motivating principle behind the V2V mandate overall. We also recognize that NHTSA has gone to great lengths to ensure that the system does not exchange PII, mitigating many of the concerns that the FIPPs were designed to address. However, given the residual privacy risks and the concerns addressed in the Third Party section of these comments regarding the possibility of extensive third party aggregation and re-identification of BSMs, we recommend further study into what sorts of legal safeguards, technical measures, or consumer privacy controls, such as opt-out, might mitigate these risks.

The automotive sector is rapidly transforming into a consumer data-heavy sector, and consumers are just beginning to understand and adjust to this new reality. We recommend that NHTSA create consumer privacy controls where possible to ensure that consumers remain open-minded to the safety-enhancing features that these technologies enable, by allowing them to maintain control over their information wherever possible. Moreover, as always in the vehicle context, the impacted parties can extend beyond the vehicle owner, who may have had an opportunity to review an owner's manual or manufacturer website, to also affect the privacy of an operator, a lessee/renter, and a passenger.

Security Entity for Credential Management System

In the section of the Privacy Impact Assessment focused on Accountability and Auditing, NHTSA acknowledges that DOT expects to play a central role in developing the policies and procedures that will govern the National SCMS, including those relating to accountability and auditing. It notes that "[a]dditionally, DOT expects to enter into agreements with a private entity to manage and coordinate SCMS functions that will include minimum policy and procedure requirements designed to ensure continuity of function, cybersecurity and appropriate privacy-risk controls."[29]

It will be important to establish evaluation mechanisms or requirements for security and privacy practices of the SCMS operator. It could be helpful for NHTSA to articulate in greater detail the structure of the Government role in oversight and accountability mechanisms for the SCMS operator.[30]

Residual Privacy Risks

NHTSA acknowledges that despite its best efforts, this Rule creates new privacy risks. We appreciate NHTSA's commitment to mitigating such risks as an ongoing process, as well as NHTSA's commitment to undertake ongoing privacy research. We would suggest that a final rule contain a concrete set of commitments for timeframes at which the Privacy Impact Assessment would be reassessed, and/or other privacy evaluations would be required to take place.

[29] PIA, p.16.
[30] NPRM, p.209.

Conclusion

This NPRM is an important step toward safer roads, and we blieve that the proposed Rule includes thoughtful, careful privacy protections in a complex system. We urge the Administration to consider our recommendations and outstanding questions to improve the final regulation. We thank NHTSA for recognizing the importance of privacy in the context of V2V technologies, and look forward to remaining engaged as the rulemaking advances. 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