1400 eye street, nw | suite 450 | washington, dc 20005 · 202-768-8950 · fpf.org

Future of Privacy Forum Comments on the Federal Automated Vehicles Policy
Afternoon Session, November 10, 2016
Safety Assessment Letters
Docket ID NHTSA-2016-0090-0001
Lauren Smith, Policy Counsel, lsmith@fpf.org

Thank you Administrator Rosekind and the NHTSA team for the opportunity to submit additional comments. I am Lauren Smith, and I am Policy Counsel at the Future of Privacy Forum, a non-profit organization that serves as a catalyst for privacy leadership and scholarship, where we advance principled data practices in support of emerging technologies.

We commend the DOT and NHTSA for their forward-looking guidance and the acknowledgement that privacy will play a key role in promoting trust in connected vehicles. Including privacy among the cross-cutting areas of guidance in the safety assessment letters is an important step in building that trust.

I would like to highlight 3 key areas for this discussion: 1) the privacy section of the safety assessment letters with an emphasis on the Fair Information Practice Principles and de-identification; 2) the data recording and sharing section; and 3) ethical considerations.

I will begin by focusing on the privacy section of the Safety Assessment Letters.

We commend NHTSA for identifying self-regulatory efforts as the best approach to advance consumer privacy in connected vehicles.

Self-Regulation
In the absence of an omnibus U.S. privacy law, self-regulatory approaches have proven fruitful 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 guidelines can become enforceable commitments when companies publicly promise to abide by guidelines, as these efforts trigger the FTC's authority to ensure companies keep their promises.

Great strides have been made regarding privacy guidelines for automotive technology. The Auto Alliance and Global Automakers in 2014 released "Privacy Principles For Vehicle Technologies And Services," and 20 car manufacturers signed on to establish baseline principles for privacy that apply to connected vehicles. 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, such as geolocation, biometrics, and driver behavior information.

These Principles went into effect this year and represent a great first step toward addressing privacy risks raised by connected cars. Yet, as the Guidance recognizes, data-crunching 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.[1] Because of this, the DOT guidance 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" (p. 11). We agree with the DOT that consumer privacy protections should extend to these entities as well.

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 recognize the FTC authority to prohibit unfair or deceptive trade practices. But as the Guidance suggests, it could be helpful for stakeholders to articulate a framework on data use in the auto context. We support the idea of advancing self-regulatory efforts like those of the Auto Alliance/Global Privacy Principles for these parties in lieu of new laws given that self-regulatory efforts have the best chance to provide privacy guidance that can keep pace with this rapidly evolving technology. The Future of Privacy Forum would be happy to help convene such an effort.

FIPPS

The guidance wisely highlights several of the Fair Information Practice Principles for privacy that are particularly important in the context of connected vehicles. The principles of Transparency, Choice, Respect for Context, Data Security, and Accountability have steered privacy practices for decades, and can help ensure that entities in the connected car ecosystem will safeguard consumer privacy. We are

[1] Find FN

grateful that you included these principles and look forward to identifying a practical way to articulate and implement them.

Other FIPPs included here may be more challenging to apply in the context of the connected vehicle ecosystem. Principles like 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 this principle may risk limiting valuable research and the development of new services.

Additionally, providing data access and correction for consumers may involve different considerations based on whether a technology is safety-critical or not, and whether data is kept on the vehicle or shared through connectivity services. These are challenging considerations given the rapidly changing pace of these technologies, and definitional lines may prove difficult to draw at this time.

Next, I will focus on *De-Identification*
Proper de-identification of data will prove key for both the privacy section of the Safety Assessment Letter as well as the first section, Data Recording and Sharing section.

As autonomous technology advances, it may be important for entities to collect and share data about safety-related incidents. We support the guidance's suggestion that any data that is shared in this manner be de-identified and be shared in conformance with the manufacturer's consumer privacy and security agreements and notices. Proper de-identification is important for the increased data recording and sharing that NHTSA calls for, as well as for the data collected and managed by DOT and NHTSA. We plan to submit our guide to practical de-identification in our written comments.

We also support the definition of "personal information" used by the guidance, explained in Footnote 12 of the Data Recording and Sharing element of the Safety Assessment Letter. Defining "personal information" consistently with the FTC definition of data with reference to whether it is reasonably linkable to <a person?> is an important step in ensuring consistency across the automotive ecosystem.

DID NOT HAVE TIME: 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

Thank you again for the opportunity to speak here today. We look forward to submitting written comments with further detail.