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
Morning Session, November 10, 2016
Overall Guidance
Docket ID NHTSA-2016-0090-0001
Lauren Smith, Policy Counsel, lsmith@fpf.org

Thank you to Administrator Rosekind and the NHTSA team for the opportunity to submit preliminary comments here. My name is 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, and advances principled data practices in support of emerging technologies.

We commend the DOT and NHTSA for their forward-looking guidance and their acknowledgement that privacy will play a key role in promoting trust in connected vehicles. This guidance and the attention it pays to privacy is an important step in building that trust.

This morning I'd like to highlight the importance of privacy in this rapidly evolving ecosystem. I will focus on the value of smart regulation that stays relevant to and does not impede the technology; on DOT and FTC jurisdiction; on the value of self-regulatory approaches; and on the importance of consistency in state, local, and federal guidance.

As has been said, connected car and autonomous vehicle technologies have tremendous potential to transform the safety and convenience of the vehicles in which we ride. You have heard the statistics many times today so I will not repeat them. *[You will hear x]*

--

But it is important to keep in mind that many of the safety improvements promised by these technologies hinge on cars' ability to communicate with each other, and with infrastructure, to know what is ahead. Decisions that were previously manual or mechanized are now algorithmic, relying on data inputs collected from the many new kinds of sensors being built into cars. Our cars will become data-crunching devices that function more like computers and smartphones than the mechanical chassis to which we are accustomed.

As we welcome these new technologies it is critical that we build responsible data practices into them, just as we have with new and unfamiliar technologies that have disrupted other sectors.

--

Being optimistic about data does not mean we need to be naive about its risks. As autonomous 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 the privacy concerns that are developing.

It is nearly impossible today to anticipate the full range of privacy questions or concerns that will arise or even the full range of data that will be needed. 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.

In light of this new guidance, the management of data in the autonomous vehicle ecosystem should be guided by an understanding of the existing current mechanisms that protect automobile consumers and that help meet their expectations around data privacy and security for vehicles.

Corporate data practices are typically 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 practices.

While the guidance's focus on privacy is encouraging given the importance of the issue, DOT jurisdiction for privacy is largely limited to technologies that the agency has mandated or implemented, and may not extend to all aspects of consumer privacy in the vehicle. This makes it even 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 space to be proactive about privacy, and the guidance helps promote this approach by highlighting privacy best practices.

As the guidance mentions, the main automakers have committed to self-regulatory principles for data in connected cars. All companies who provide assurances to the public about their privacy practices are subject to FTC jurisdiction. Therefore, these

principles can be enforced by the FTC, and that incentives and regulatory oversight to deter unfair or deceptive business practices are already built in.

Model State Policy

It is incredibly important to promote standardization between federal, state, and self-regulatory regimes in this space because automotive companies design systems at a local, national, and global level. The Model State Policy is a helpful first step in this regard. Several states have begun drafting their own legislation; inconsistent rules would create barriers to operation of connected vehicles that are designed to cross state lines. Patchwork legislation could impede interoperability or render the cars incapable of driving across state lines. The DOT should encourage states to look to this guidance as a model for their own laws.

The DOT should also discourage states like California from adopting this guidance as law at this time; something it was not intended to be.

Conclusion

Thank you again for the opportunity to speak with you this morning. We welcome this guidance and appreciate the iterative process that you have put in place to incorporate stakeholder input and further data. I will offer more detailed comments on the privacy aspects of the guidance this afternoon.