November 21, 2016

U.S. Department of Transportation
1200 New Jersey Avenue, SE
Docket Management Facility, Room W12-140
Washington, DC 20590

Federal Register Number: 2016-22993

On behalf of the Center for Data Innovation (datainnovation.org), we are pleased to submit these comments in response to the National Highway Traffic Safety Administration's (NHTSA) request for comments on its Federal Automated Vehicles Policy.[1]

The Center for Data Innovation is the leading think tank studying the intersection of data, technology, and public policy. With staff in Washington, DC and Brussels, the Center formulates and promotes pragmatic public policies designed to maximize the benefits of data-driven innovation in the public and private sectors. It educates policymakers and the public about the opportunities and challenges associated with data, as well as technology trends such as predictive analytics, open data, cloud computing, and the Internet of Things. The Center is a non-profit, non-partisan research institute affiliated with the Information Technology and Innovation Foundation.

Automated vehicles can improve public safety, increase transportation efficiency, increase autonomy for people with disabilities, and offer many other social and economic benefits, so it is encouraging to see NHTSA proactively develop a policy framework that supports the development and adoption of the technology. Importantly, NHTSA should encourage data collection and sharing among vehicle manufacturers, transportation safety regulators, and other stakeholders. The goal should be to create a rapid-learning transportation network that is capable of harnessing massive amounts of data to quickly generate new knowledge and enable stakeholders to make informed decisions about public safety. However, the Federal Automated Vehicles Policy should not include rules on consumer privacy as part of its safety policy. Though privacy will of course be a consideration for data collection in automated vehicles, it is not directly part of safety. As a

[1] U.S. National Highway Traffic Safety Administration, "Agency Information Collection Activities; Proposals, Submissions, and Approvals: Federal Automated Vehicles Policy," September 23, 2016, https://www.regulations.gov/document?D=NHTSA-2016-0090-0001.

transportation safety regulator, NHTSA should keep its focus explicitly on safety issues and allow consumer privacy regulators, such as the Federal Trade Commission, continue to lead in this area. By avoiding creating duplicative and possibly contradictory rules, NHTSA can create a more innovation-friendly regulatory environment for automated vehicles and avoid creating unnecessary regulatory barriers for the development of the industry.

Please find our responses to the relevant questions in the attached document.

Sincerely,

Daniel Castro
Director
Center for Data Innovation
dcastro@datainnovation.org

Joshua New
Policy Analyst
Center for Data Innovation
jnew@datainnovation.org

1. DATA RECORDING AND SHARING

Better information can help regulators, vehicle manufacturers, and others make better decisions about vehicle safety. In particular, better data can help determine the cause of accidents, identify safety problems in existing vehicles, and determine whether software updates to automated vehicles have the desired effect. As part of the Federal Automated Vehicles Policy, NHTSA correctly recommends that vehicle manufacturers and other stakeholders developing highly automated vehicles (HAV) establish a clear process for collecting a broad range of data about automated vehicle performance, such as incident reports, malfunctions, and crashes. The policy would establish a minimum threshold for data collection, consisting of all data related to a particular event, ranging from the HAV's performance leading up to the event to whether or not a human driver was controlling the vehicle. With widespread collection of this data for all HAV operations, manufacturers, transportation safety regulators, and other stakeholders can establish modern, HAV-specific safety metrics to compare the performance of different HAVs, and, most importantly, promote data sharing among HAV stakeholders to accelerate the development of the technology. The goal of these efforts should be to create the data infrastructure necessary to establish a rapid-learning transportation network that can leverage large amounts of data to quickly discover new insights and allow stakeholders to make informed decisions about public safety.[2]

NHTSA recognizes that data standards, for the purposes of data sharing, are still emerging and correctly concludes that regulators should not mandate the use of any particular standard. NHTSA instead encourages industry cooperation with standards bodies to develop common, industry-wide standards for HAV data collection and sharing. To accelerate this process, NHTSA should consider its capacity to play a convening role in the HAV sector and facilitate interactions between manufactures, standards bodies, and other stakeholders, both nationally and internationally. NHTSA should also use its convening authority to encourage the private sector to develop industry standards for testing and validating data quality.

[2] The goal of establishing "rapid learning networks" to create evidenced-based interventions is well-established in other emerging data-intensive industries, such as health care and education. See, for example, Lynn M. Etheredge, "Rapid Learning: A Breakthrough Agenda," *Health Affairs* 33, no. 7 (July 2014) http://content.healthaffairs.org/content/33/7/1155.abstract.

2. PRIVACY

NHTSA proposes that all HAV manufacturers voluntarily submit a safety assessment for each HAV system. As part of this safety assessment, NHTSA proposes a set of recommended practices regarding consumer privacy. The merits and flaws of these recommendations are irrelevant because NHTSA, and the Department of Transportation as a whole, should not expand its authority to become a consumer privacy regulator. The data use practices of HAV manufacturers can and should be subject to the same kind of regulatory oversight as other technologies, but this oversight should come from existing regulators, such as the Federal Trade Commission, which has purview over these issues already. While NHTSA's intent is likely to demonstrate that it is aware that consumer data is a necessary ingredient in the development, testing, and improvement of HAVs, developing its own recommendations for data privacy creates redundant and potentially conflicting regulatory barriers for HAV developers and does little to protect consumers. Moreover, it could lead to consumer and business confusion. Would consumer data transmitted through a connected car application have different levels of privacy protection than if the same information was being transmitted through a smart phone at home? If so, how would consumers and app developers and other businesses make sense of these differences? In short, privacy rules should not be tied to the type of technology, such as a connected car, a smart device in the home, or a mobile phone at work. Moreover, the vast majority of the data collected and shared for safety purposes will not contain personally identifiable information. While there may be some exceptions. NHTSA should focus its efforts on how data collection and sharing can make HAV's safer and not on consumer privacy.

CONCLUSION

NHTSA should be commended for creating a policy framework intended to advance the development of HAV's. However, NHTSA should revise the Federal Automated Vehicles Policy to strike the counterproductive and unnecessary recommendations related to consumer privacy which are not relevant to vehicle safety, have the potential to create duplicative or conflicting rules, and which are outside the immediate expertise of the agency.