Future of Privacy Forum Oral Remarks on Guidelines for the Safe Deployment and Operation of Automated Vehicle Safety Technologies
Public Meeting at Stanford University
April 27, 2016
Lauren Smith, Policy Counsel

New vehicle safety technologies are rapidly transforming the safety and convenience of the vehicles we drive - ranging from automated lane-keeping to voice-powered messaging and navigation. Future improvements will take advantage of the ability of cars to communicate with each other and with infrastructure, to know what is ahead, around, and behind.

But the full safety benefits associated with a vehicle reducing and removing human error altogether from driving will come with the advent of autonomous vehicles - early examples of which are being tested on U.S. roads by manufacturers and researchers today. Earlier this year, twenty automobile manufacturers—representing more than 99 percent of the United States automotive industry—recently agreed to have automatic emergency braking a standard feature on virtually all new cars no later than 2023. This semi-autonomous feature relies on on-vehicle sensors such as radar, cameras or lasers to detect an imminent crash, warn the driver and apply the brakes if the driver does not take sufficient action quickly enough. To enable this type of automation, data is essential to powering the technology and the decisionmaking of the vehicle.

Cars have long collected data to power Event Data Recorders for safety investigations and On Board Diagnostics, but over time our cars will rely on more sensors to collect and process greater types and quantities of data. Data describing a vehicle's environment will be crucial for a vehicle to safely handle the real-time driving task, and power other new in-vehicle features.

Autonomous and semi-autonomous technologies can do more than transform automotive safety and convenience for preexisting American drivers; they can increase mobility for the elderly and Americans with disabilities who may be constrained from driving altogether. Yet the debate over the management of data and technology in society has become a charged one. Some industry observers believe that no data protections are necessary to protect the general public as automotive technologies advance and that there is no potential for serious harm. At the same time, other advocates and civil rights experts worry about data and technology vulnerabilities and risks, as well as government surveillance.

Being optimistic about data does not mean we need to be naive about its risks. As autonomous vehicles develop and as we understand the nature of the data and what is needed for these vehicles to operate, we need to be sensitive to the privacy concerns that develop. But it is nearly impossible today to anticipate today the full range of the privacy questions that will arise or the data that will be needed, especially as we support the potential of these new technologies to transform the relationship of consumers to vehicles altogether through fleet-based and other models.

The management of data in the autonomous vehicle ecosystem should be approached, as with other new technologies, with an understanding of the current federal enforcement mechanisms that protect auto consumers and protect their expectations around data

privacy and security for vehicles - in light of the operational guidance that NHTSA is currently developing. First, NHTSA's notice of comments around its enforcement authority for emerging technologies indicates that "when vulnerabilities of such technology or equipment pose an unreasonable risk to safety, those vulnerabilities constitute a safety-related defect" the agency will be able to take direct action - whether that applies to vehicles today or the autonomous vehicles of the future. In addition, NHTSA's authority to issue operational guidelines would permit it to take further enforcement actions against companies who hold themselves to comply with the guidelines but are in violation of both the guidelines and specific motor vehicle safety provisions in statute.

Outside of NHTSA's authority and the process at the heart of today's public meeting, the agency charged with protecting consumers, including purchasers of vehicles or even users of ridesharing services, is the Federal Trade Commission. The FTC has reiterated consistently its authority covers the privacy and security of new technologies under Section 5 of the FTC Act, which empowers the Commission to take action against deceptive or unfair commercial practices. To date, the FTC has brought more than fifty cases against businesses that allegedly failed to maintain reasonable security" and has initiated work streams, workshops, and reports to cover privacy around the Internet of Things - which have included emerging vehicles.

Self-regulatory efforts around data management in emerging technologies properly focus on the Fair Information Privacy Principles centered on transparency, purpose specification, and data minimization. Efforts tied to voluntary self-regulation on privacy using the FIPPS as guidelines have recently emerged in both government processes - like the NTIA's multistakeholder process on UAV privacy - and industry processes - like the Auto Alliance and Global Automakers' Auto Privacy Principles. Companies who make statements to the public about their practices will be subject to FTC jurisdiction, with built-in incentives and regulatory oversight to deter unfair or deceptive business practices.

One of the biggest risks to privacy stemming from autonomous cars may be from the actions of law enforcement and regulators. Uber's recently released transparency report revealed in the last five months of 2015, regulatory agencies requested data affecting 11.6 million Uber riders and 583,000 drivers. State regulators may lack the data handling expertise that technology companies have to protect user information that they make public, and there is a risk that information like pickup and dropoff locations may allow government agencies—or anyone else who obtains this information through FOIA and other mechanisms—to identify individual riders by associating it with publicly available records.

These challenges may become more central with the data that will be produced through the Vehicle to Vehicle and Vehicle to Infrastructure technologies being shepherded by NHTSA. Obviously, NHTSA, the NTSB, and local law enforcement investigators will have safety needs for data, but they will need to be balanced with privacy protections for users and riders.

However, if safety-enhancing technologies are stalled by inflexible policies, we will forego the promise of connected vehicles to reduce the 90% of the 35,000 annual motor vehicle deaths that are caused by human error. We will continue to have accidents caused by

human distraction, and Americans with disabilities will continue to see their mobility unnecessarily constrained.

The benefits for facilitating the deployment of autonomous vehicles are so compelling and policymakers should be doing all they can to smooth and speed the way for these technologies to improve as quickly as possible. Applying current best practices around data privacy, paired with existing federal enforcement mechanisms, should facilitate, not stall, this opportunity.