TOYOTA

Statement of

Sandy Lobenstein

Vice President

Connected Services and Product Planning

Toyota Motor Sales, USA

on

"The Internet of Cars"

before the

U.S. House of Representatives

Committee on Oversight and Government Reform

Subcommittee on Transportation and Public Assets
Subcommittee on Information Technology

November 18, 2015

Chairman Mica, Chairman Hurd, Ranking Member Duckworth, Ranking Member Kelly, and members of the subcommittees, thank you for the opportunity to appear before you today to talk about the Internet of Cars.

This is an extraordinarily exciting time in the automobile industry. Over the last few years, major progress in advanced safety technology has contributed to significant reductions in traffic fatalities. Increasingly, cars are outfitted with cutting-edge technology that can sense an impending crash and take action to avoid a collision altogether. More and more vehicles are equipped with connected safety services, such as automatic collision notification and stolen vehicle locator, and with connected infotainment systems that are providing drivers and passengers with more real-time information on traffic and road conditions. And some vehicle owners are now able to interact with their vehicles from their smartphones to pre-heat their car on a cold day, check to see if they remembered to roll up a window or close the trunk, confirm that they have enough gas to get to work, or find out if their teenage son or daughter is driving safely.

But the truth is that we are only at the beginning of the beginning when it comes to the Internet of Cars. Just as modern smartphones compare to the mobile phone "bricks" of 30 years ago, the connected car of the future will bear little resemblance and far surpass the connected car of today with its features and capabilities. Vehicle-to-vehicle and vehicle-to-infrastructure communication, artificial intelligence, self-driving cars, augmented reality, new modes of urban transportation, and other technologies made possible and enabled through connectivity may get us closer to our goal of a society where cars don't crash, where there are zero traffic fatalities, and where almost every need of the driver or passengers is met.

Vehicle Data Privacy

Over the last few years, the auto industry found itself on the receiving end of growing questions about its use of vehicle data generated by vehicle services and technologies. The auto industry was confident that it was using vehicle data only in ways that were consistent with customers' expectations or the requirements of the services to which the customers had subscribed. However, since consumer trust is essential to the success of these technologies and services, the industry sought ways to proactively address these growing questions.

The auto industry came together and developed the *Privacy Principles for Vehicle Technologies and Services* ("Privacy Principles"). The *Privacy Principles*, which were unveiled last November and take effect in January of next year, include meaningful protections on the use of vehicle data and were inspired by the respected Fair Information Practice Principles. The *Privacy Principles* also include heightened protections on the use of certain vehicle data, including information about a vehicle's location and how someone drives a vehicle. For example, automakers agreed not to share this type of vehicle data with third parties for their own use or use this type of vehicle data for marketing purposes without the affirmative consent of the vehicle owner, or share location information with law enforcement in the absence of a warrant or court order. The industry chose to formally file the *Privacy Principles* with the Federal Trade Commission.

With the adoption and implementation of the *Privacy Principles*, the auto industry is at the forefront of protecting consumer data in the emerging Internet of Things. This code of conduct is precisely the type of effort that the government has been - and should be – encouraging from the private sector, and should serve as a model for other Internet of Things sectors. In addition, Toyota encourages other non-automotive companies and sectors that are independently accessing onboard vehicle data, such as insurance companies, to consider making similar commitments to those contained in the *Privacy Principles*. Consumers should be assured that their vehicle data is provided the same level of protection, regardless of who is accessing it.

Congress may have a role in encouraging other sectors to adopt similar consumer privacy commitments. For example, some have discussed the possibility of giving the Federal Trade Commission the authority to grant safe harbors to industries that adopt and comply with meaningful self-regulatory codes of conduct. Toyota supports this concept, and believes that the granted authority could be broad and apply to any meaningful self-regulatory code of conduct or could be targeted at specific sectors where Congress has a particular interest in promoting stronger consumer privacy protections.

Vehicle Cybersecurity

Connectivity in cars has also spawned cybersecurity concerns. The good news is that no criminal cyber-attack on a vehicle has occurred and any such attack would require a very high level of sophistication and resources. That being said, the auto industry is well-aware that the cybersecurity risks that exist for other connected devices also exist in the automotive context, and fully grasps the potential consequences of a successful, real-world cyber-attack on a vehicle. That is why auto companies like Toyota have already taken steps to apply and adapt recognized cybersecurity best practices and standards to vehicles and are committed to continuing their work to mitigate new, emerging, and evolving cybersecurity risks.

As you may be aware, in an effort to further strengthen automotive cybersecurity, the auto industry has announced the establishment of an Auto-ISAC. While we do not believe that the Auto-ISAC will be a panacea for the cybersecurity challenges facing the automotive industry, we believe that it is an important step for the industry to take to promote the exchange of information about cybersecurity threats to vehicles and their onboard networks and to facilitate the sharing of best practices for how to safeguard against and respond to such threats. Toyota is pleased to be serving as the first Auto-ISAC Board chair, and is fully committed to the Auto-ISAC's success. The Auto-ISAC has been incorporated, the Board of Directors has been constituted, membership agreements have been submitted, and a contract with a respected service provider was executed last week. We expect initial information sharing within the Auto-ISAC to begin by the end of the year, with more expansive information sharing capability coming online in January.

As a sector embarking on formal cyber threat information sharing for the first time, we strongly support government efforts to foster effective cyber threat information sharing, particularly among private sector companies, and to clarify the government's roles and responsibilities. To that end, Toyota supports cyber threat information sharing legislation pending in Congress and is hopeful that the House and Senate bills will soon be reconciled, passed, and enacted into law.

Some are making the case that automotive-specific cybersecurity best practices or standards are needed. A threshold question to such an effort should be whether automotive-specific cybersecurity best practices will look any different than existing best practices that guide cybersecurity in other contexts. The truth is that the ways to identify and assess potential vulnerabilities, prevent unauthorized access, and detect intrusions are consistent across systems and networks. General cybersecurity best practices already exist and they can be, and are being, applied to vehicles.

That being said, the auto industry recognizes that an effort to adapt these existing cybersecurity best practices to the vehicle ecosystem may be appropriate. That is why the industry has recently embarked on an effort to identify existing cybersecurity best practices that are being, and can be, applied in an automotive context, and pinpoint and address any potential gaps that may exist in those best practices.

However, for the very same reasons that the government has refrained from mandating cybersecurity standards in other sectors, there is a significant risk associated with the government mandating cybersecurity standards in the automotive space. The truth is that industry can move quicker than the government to update or modify out-of-date practices or adjust to new or emerging threats. In addition, setting specific government standards may encourage companies to do only what is required to meet the specified standards, and may discourage companies from exceeding them or innovating cybersecurity practices. Finally, a segmented and sector-specific approach to cybersecurity will almost certainly have significant implications for the harmonious development of the Internet of Things at large.

While the auto industry is taking steps to minimize cybersecurity risk, we encourage the government to review our existing laws to ensure that they adequately protect against malicious car hacking. While we believe that the *Computer Fraud and Abuse Act* covers car hacking, it might be useful for the government to confirm this belief or provide some clarity around this issue. In addition, while we appreciate the motivations of some advocating for civil penalties for car hacking, this approach could send an unfortunate message that car hacking is somehow less significant or less serious than other forms of hacking subject to criminal penalties under the *Computer Fraud and Abuse Act*.

Spectrum

We are on the cusp of a radical transformation in vehicle safety that will be made possible through vehicle-to-vehicle and vehicle-to-infrastructure communication. There have been remarkable advances in the crashworthiness of vehicles in recent years, resulting in an impressive reduction in traffic casualties and fatalities. Despite this, however, tens of thousands of people are still dying in traffic accidents each year in the United States. Toyota firmly believes that the next great opportunity to reduce injuries and fatalities from traffic accidents rests with the deployment of innovative new technologies that will prevent crashes in the first place.

Companies like Toyota are leading the way by outfitting vehicles with top-of-the-line sensors, radars, and cameras that can anticipate potential collisions. However, these existing technologies have important limitations with respect to range, field-of-view, and line-of-sight.

Vehicle-to-vehicle and vehicle-to-infrastructure communication using Dedicated Short Range Communication (DSRC) is the technology that will allow us to overcome these challenges by enabling vehicles to identify collision threats at a greater distance or with a vehicle that is around a corner or behind a truck.

DSRC is a two-way, short- to medium-range wireless communication protocol that allows vehicles to communicate with each other to detect and avoid hazards. DSRC-equipped vehicles broadcast precise information - such as their location, speed, and acceleration - several times per second over a range of a few hundred meters. Other vehicles outfitted with DSRC technology receive these "messages" and use them to compute the trajectory of each neighboring vehicle, compare these with their own predicted path, and determine if any of the neighboring vehicles pose a collision threat. If a DSRC-enabled vehicle determines that a potential collision or other hazard exists, the on-board system can warn the driver or take action to avoid the accident.

As you may be aware, in 1999, the Federal Communications Commission (FCC) allocated 75 MHz of spectrum in the 5.9 GHz band to be used specifically for DSRC and, in 2003, the FCC adopted the licensing and service rules for DSRC systems operating in the band. This kicked off an extensive collaboration between the U.S. Department of Transportation and the automobile industry focused on the development and field testing of DSRC to demonstrate its feasibility for crash avoidance systems. In addition, detailed technical work within reputable standards development organizations took place to develop the common technical standards for 5.9 GHz DSRC technology. In 2013, a model deployment in Michigan, involving nearly 3000 vehicles from different manufacturers, verified the maturity and stability of the technology and the standards, and opened the door to widespread deployment of DSRC technology in the United States.

The FCC issued a Notice of Proposed Rulemaking in 2013 that solicited comments on opening up the 5.9 GHz band to use by unlicensed devices. Toyota recognizes and fully appreciates that there is a spectrum crunch and that we must find new and innovative ways to maximize the effective use of the limited spectrum that is available. We have been – and continue to be – generally supportive of efforts to open up more spectrum for unlicensed uses, and we support the prospect of sharing spectrum with unlicensed devices in the 5.9 GHz band if it can be proven that no harmful interference will impair the safety-of-life mission for which that spectrum is allocated. The good news is that a promising sharing proposal has been offered that Toyota believes has potential to accomplish this goal. The auto industry and the proposal's developer have recently proceeded to validation testing of the solution. At this point in time, we remain confident that it will be proven out as a workable spectrum sharing solution that will open up 75 MHz of spectrum for unlicensed uses without upending or unnecessarily disrupting this transformational auto safety technology at its advanced stage of development.

Additional Considerations

Before closing, I would like to provide a couple of general observations that may prove useful to the Committee on these issues going forward.

First, the Internet of Cars ecosystem is evolving. Technology companies, telecommunications providers, insurance companies, and others have introduced – and will

continue to introduce – products and technologies that are designed to interact directly with vehicles. As the ecosystem continues to evolve beyond the automotive companies, responsibility and accountability for protecting vehicles from potential cyber-attacks and for preserving consumer privacy should also evolve to include all of the relevant players.

Second, there are a number of Federal agencies that are seeking to oversee, regulate, or influence cybersecurity and privacy practices relating to the Internet of Things broadly or to different subsets of the Internet of Things. The resulting cacophony of working groups, efforts, initiatives, and proposals is exceedingly difficult to manage and prioritize. Without consolidation of these efforts, clarification around the appropriate roles of the various agencies, and better coordination among agencies, the potential and opportunity presented by the Internet of Cars will almost certainly suffer.

Thank you for the opportunity to testify before you today. I look forward to your questions.