United States Senate
WASHINGTON, DC 20510

August 4, 2016

The Honorable Tom Wheeler
Chairman
Federal Communications Commission
445 12th St. SW
Washington, DC 20554

Dear Chairman Wheeler,

We write to convey our concerns about consumers' safety and privacy as car manufacturers deploy vehicle-2-vehicle and vehicle-2-infrastructure communication technologies in their automobiles. We have entered the Internet of Things (IoT) era, where our cars, transportation infrastructure, and devices can all be interconnected. Today, new cars are really just computers on wheels. These promising new technologies could improve automobile safety, reduce congestion, and cut carbon emissions. But make no mistake, IoT can also be considered the Internet of Threats if appropriate safety, cybersecurity, and privacy safeguards are not put in place.

Last year, we sent inquiries to over a dozen automakers asking for information on each company's protections against the threat of cyberattacks or unwarranted invasions of privacy related to the integration of electronic systems into and within automobiles. This followed a report Senator Markey released detailing major gaps in how auto companies are securing connected features in cars against hackers. This report found customers are often not made aware of data collection and, when they are, often cannot opt-out without disabling important features, such as navigation. Further, nearly all vehicles on the market include wireless technologies that could pose vulnerabilities to hacking or privacy intrusions. Despite this threat, security measures to prevent remote access to vehicle electronics are inconsistent and haphazard across the market.

Last year, our concerns became a reality when researchers wirelessly hacked a Jeep Cherokee from miles away, showing how hackers could remotely control a vehicle's transmission, brakes, and steering. As a result, Fiat Chrysler recalled 1.4 million vehicles to fix this vulnerability. Further, J.D. Power found that technology-related issues, including Bluetooth connectivity and built-in voice recognition systems, are now the most problematic area on most vehicles.[1] And just this year, a man operating a Tesla with the autopilot engaged was killed when the car failed to detect a white 18-wheel tractor trailer crossing the highway.

Vehicle safety, cybersecurity, and privacy threats could grow over time as more and more vehicles become interconnected. Soon, automakers will debut vehicles equipped with vehicle-2-vehicle and vehicle-2-infrastructure communication technologies. These technologies use Dedicated Short Range Communications (DSRC) to share speed, direction data, and other transportation information to prevent accidents and reduce congestion. However, the DSRC

[1] J.D. Power. *Technology Woes Continue to Drive Up Problems: J.D. Power Vehicle Dependability Study*. N.p., 24 Feb. 2016. Web. 21 July 2016. <http://www.jdpower.com/press-releases/2016-us-vehicle-dependability-study-vds>.

band may also be used for non-public safety commercial purposes, such as allowing drivers of connected vehicles to pay for tolls, parking, drive-through restaurant meals, or gasoline without taking out their wallet.

While these technologies are promising, we are concerned that DSRC systems could increase vehicles' vulnerability to safety, cyber, and privacy threats. For example, hackers could remotely access one vehicle or one commercial application and then use its DSRC system to spread malware to other vehicles and systems. That could allow hackers to commandeer vehicles and intentionally cause crashes. Further, businesses could collect and analyze sensitive driving information, such as where the vehicle travels and how long it stays there, without the knowledge or consent of the consumer and then send targeted advertisements via dashboard consoles, in-car entertainment systems, or digital billboards.

In this new IoT era, safety, cybersecurity, and privacy cannot be an afterthought. We must ensure that these vehicles have robust safety, cybersecurity, and privacy protections in place before automakers deploy vehicle-2-vehicle and vehicle-2-infrastructure communication technologies. With the National Highway Traffic Safety Administration (NHTSA) now considering mandating that all new cars have DSRC systems, we must act without delay. There should be mandatory rules in place for vehicles. That's why we introduced the Security and Privacy in Your Car (SPY Car) Act, which directs NHTSA and the Federal Trade Commission (FTC) to establish federal standards to secure our cars and protect drivers' privacy.

Fortunately, as the agency in control of the nation's wireless services, the Federal Communication Commission (FCC) could help ensure that automakers and other commercial entities using DSRC spectrum have robust cybersecurity and privacy protections in place. We are pleased that the FCC issued a public notice on July 25th seeking comment on this matter. Accordingly, we encourage the Commission to consider the following:

1. Ensure that DSRC spectrum is only used for vehicle safety and not commercial applications that may make vehicles more vulnerable to safety, cyber, and privacy threats.

2. Mandate that automakers, commercial entities, and anyone else licensed to use DSRC spectrum submit privacy and cybersecurity plans to the FCC.

3. Require entities using DSRC spectrum to periodically update their privacy and cybersecurity plans.

4. Require DSRC spectrum users to notify appropriate law enforcement, government agencies, and consumers if a serious breach occurs and take appropriate steps to mitigate the harms of such a breach.

We encourage you to collaborate with NHTSA and the FTC on this matter and take steps to help protect the millions of Americans who travel on our roads every day.

Thank you for your attention to this important matter. We respectfully request that you reply by August 25. If you have any questions regarding our request, please contact Daniel Greene (Daniel_Greene@markey.senate.gov) in Senator Markey's office or Anna Yu (Anna_Yu@blumenthal.senate.gov) in Senator Blumenthal's office.

Sincerely,

Edward J. Markey
United States Senator

Richard Blumenthal
United States Senator

cc: The Honorable Anthony Foxx, Secretary, Department of Transportation
The Honorable Edith Ramirez, Chairwoman, Federal Trade Commission
The Honorable Mark R. Rosekind, Administrator, National Highway Traffic Safety Administration

National Security Archive,

Suite 701, Gelman Library, The George Washington University,

2130 H Street, NW, Washington, D.C., 20037,

Phone: 202/994-7000, Fax: 202/994-7005, nsarchiv@gwu.edu