THE INTERNET OF CARS

JOINT HEARING

BEFORE THE

SUBCOMMITTEE ON
TRANSPORTATION AND PUBLIC ASSETS

AND THE

SUBCOMMITTEE ON INFORMATION TECHNOLOGY

OF THE

COMMITTEE ON OVERSIGHT
AND GOVERNMENT REFORM
HOUSE OF REPRESENTATIVES

ONE HUNDRED FOURTEENTH CONGRESS

FIRST SESSION

NOVEMBER 18, 2015

Serial No. 114–55

Printed for the use of the Committee on Oversight and Government Reform

Available via the World Wide Web: http://www.fdsys.gov
http://www.house.gov/reform

U.S. GOVERNMENT PUBLISHING OFFICE

97–974 PDF WASHINGTON : 2016

For sale by the Superintendent of Documents, U.S. Government Publishing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

JASON CHAFFETZ, Utah, *Chairman*

JOHN L. MICA, Florida
MICHAEL R. TURNER, Ohio
JOHN J. DUNCAN, JR., Tennessee
JIM JORDAN, Ohio
TIM WALBERG, Michigan
JUSTIN AMASH, Michigan
PAUL A. GOSAR, Arizona
SCOTT DESJARLAIS, Tennessee
TREY GOWDY, South Carolina
BLAKE FARENTHOLD, Texas
CYNTHIA M. LUMMIS, Wyoming
THOMAS MASSIE, Kentucky
MARK MEADOWS, North Carolina
RON DESANTIS, Florida
MICK, MULVANEY, South Carolina
KEN BUCK, Colorado
MARK WALKER, North Carolina
ROD BLUM, Massachusetts
JODY B. HICE, Georgia
STEVE RUSSELL, Oklahoma
EARL L. "BUDDY" CARTER, Georgia
GLENN GROTHMAN, Wisconsin
WILL HURD, Texas
GARY J. PALMER, Alabama

ELIJAH E. CUMMINGS, Maryland, *Ranking Minority Member*
CAROLYN B. MALONEY, New York
ELEANOR HOLMES NORTON, District of Columbia
WM. LACY CLAY, Missouri
STEPHEN F. LYNCH, Massachusetts
JIM COOPER, Tennessee
GERALD E. CONNOLLY, Virginia
MATT CARTWRIGHT, Pennsylvania
TAMMY DUCKWORTH, Illinois
ROBIN L. KELLY, Illinois
BRENDA L. LAWRENCE, Michigan
TED LIEU, California
BONNIE WATSON COLEMAN, New Jersey
STACEY E. PLASKETT, Virgin Islands
MARK DeSAULNIER, California
BRENDAN F. BOYLE, Pennsylvania
PETER WELCH, Vermont
MICHELLE LUJAN GRISHAM, New Mexico

SEAN MCLAUGHLIN, *Staff Director*
DAVID RAPALLO, *Minority Staff Director*
MICHAEL KIDO, *Staff Director, Subcommittee on Transportation and Public Assetts*
TROY STOCK, *Staff Director, Subcommittee on Information Technology*
SARAH VANCE, *Clerk*

SUBCOMMITTEE ON TRANSPORTATION & PUBLIC ASSETS

JOHN L. MICA Florida, *Chairman*

MICHAEL R. TURNER, Ohio
JOHN J. DUNCAN, JR. Tennessee
JUSTIN AMASH, Michigan
THOMAS MASSIE, Kentucky
GLENN GROTHMAN, Wisconsin, *Vice Chair*
TAMMY DUCKWORTH, Illinois, Ranking Member
BONNIE WATSON COLEMAN, New Jersey
MARK DESAULNIER, California
BRENDAN F. BOYLE, Pennsylvania

SUBCOMMITTEE ON INFORMATION TECHNOLOGY

WILL HURD, Texas, *Chairman*

BLAKE FARENTHOLD, Texas, *Vice Chair*
MARK WALKER, North Carolina
ROD BLUM, Iowa
PAUL A. GOSAR, Arizona
ROBIN L. KELLY, Illinois, *Ranking Member*
GERALD E. CONNOLLY, Virginia
TAMMY DUCKWORTH, Illinois
TED LIEU, California

CONTENTS

THE INTERNET OF CARS

Wednesday, November 18, 2015

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON TRANSPORTATION AND PUBLIC ASSETS, JOINT WITH THE SUBCOMMITTEE ON INFORMATION TECHNOLOGY,
COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM,
Washington, D.C.

The subcommittees met, pursuant to call, at 2:00 p.m., in Room 2154, Rayburn House Office Building, Hon. John L. Mica [chairman of the Subcommittee on Transportation and Public Assets] presiding.

Present from the Subcommittee on Transportation and Public Assets: Representatives Mica, Amash, Duckworth, DeSaulnier, and Boyle.

Present from the Subcommittee on Information Technology: Representatives Hurd, Farenthold, Walker, Blum, Kelly, Connolly, and Lieu.

Also Present: Representative Chaffetz.

Mr. MICA. Good afternoon. I'd like to welcome everyone to the Subcommittee on Transportation and Public Assets and also the Subcommittee on Information Technology hearing today. And this meeting will come to order. Without objection, the chair is authorized to declare at any time a recess.

The order of business will be as follows. Since we have a joint subcommittee hearing today, we'll have opening statements from myself, Mr. Hurd, Ms. Duckworth, Ms. Kelly. And after that we will hear from our witnesses. And then—well, after we have heard from all the witnesses we'll go into questions.

So with that, I'll give the first opening statement. And, again, welcome everyone.

It's interesting the age that we live in of new technology and communications. With all of the incredible technology that we see and take for granted every day, we're entering a new era in transportation technology. And there's some of the older panelists or members and audience will remember when you used to open the hood of a car and you could take out the various parts, identify everything. Now you need almost a Ph.D. degree to figure out what's in there, and its capabilities are just astounding. A lot of safety features in cars we didn't have before.

But we today are going to address the issues relating to, again, what we call the Internet of Cars and look at some of the implications of that technology. And I think some of this was highlighted just some time ago when, I guess it was a Jeep vehicle was hacked.

And fortunately it wasn't folks who chose to do harm, but it did demonstrate that vehicles with certain types of electronic capability can, in fact, be hacked, and it does pose some questions.

We've called together today leaders of industry and some others. We have NHTSA. But I particularly want to thank the private sector partners.

Several weeks ago we had a roundtable and an open and frank discussion of kind of where we are and where we're going and what the industry's doing to deal with some of these issues. And I think they've been most cooperative and I appreciate that. And we learned a lot from that particular informal meeting.

Today is a little bit more formal. We do have a lot that we can—a lot of benefits too. In 2010, there were 1.2 million deaths on the world's highways. The United States, some 10 years ago, we had 43,000 deaths. We have taken that down to 33,000. And there are a lot of positive things that have been done, again through safety, technology, warning systems, a whole host of electronic devices now in our vehicles that make us safer.

The positive economic benefit from connected vehicles is estimated to be $500 billion. And we want to ensure that the electronic systems we have in these vehicles can't be hacked, that, in fact, that we have safety provisions put in and protections for the consumer and for the public.

In 2012, when I helped author the MAP–21 bill, we directed the National Highway Traffic Safety Administration to complete a review and ultimately determine the needs for safety in vehicles and electronic systems. We'll hear from some folks today where they are in the requirement that we crafted and put in that bill. We're now a year and a half past the deadline we set in law.

Automakers have fortunately been setting their own cybersecurity standards, which is the good news. The bad news is that we have a lot of variety and people going in different directions. While the National Highway Traffic Safety Administration continues to move forward mandating dictated short-range communication devices in cars, we must make certain that this technology hasn't been surpassed by the next best thing that's coming up, and advances in technology are rapid.

We've spent over $500 million on testing just this technology that was discovered in 1999. And in 1999 the state of the art for some of our communications was the flip phones. And we've come a little bit further from that.

So while I fully support connected vehicle technology and help with its advancement, in the future we'll see vehicles that can talk to each other, we'll see safety provisions in vehicles that will make cars safer and more reliable and have a whole host of features that will benefit the consumer and the traveling public. But we must be able to allow a bridge to get to that environment as the new technologies come to light while remaining cognizant of the need for consumer privacy.

So this afternoon I look forward to hearing testimony from our potential witnesses. And I pledge to work collaboratively with everyone here on this side, both sides of the aisle, and with the industry. I think we're entering a new exciting era, but we want to be ready for it.

Let me now recognize Ms. Duckworth, the ranking member of the Subcommittee on Transportation and Public Assets, for her opening statement.

Ms. DUCKWORTH. Thank you, Chairman Mica. And welcome both to Chairman Hurd and Ranking Member Kelly. Welcome also to our witnesses.

Today there are an estimated 5 billion devices that make up the ecosystem that we call the Internet of Things. It's not just Fitbits, smartphones, and baby monitors that communicate over the Internet. Our motor vehicles are computers on wheels that rely on the same methods of communication. And as we've seen too many times, computers and computer networks are regularly the victims of hackers.

We've already mentioned the July instance this year when a vehicle was hacked. Less than a month later from that instance a researcher demonstrated how vulnerabilities in a different manufacturer's vehicle could also let hackers learn the owner's home address, steal credit card information, and much more.

So far there have been no known incidents of malicious attempts to hack vehicles. But I have to ask the witnesses here today, is that because the overall security of the vehicle computers is that good or have we simply been that lucky?

Congress gave the National Highway Transportation Safety Administration the responsibility to regulate cybersecurity in vehicles. But manufacturers and suppliers are in the best position to identify weaknesses in their own products. Ensuring the cyber safety of cars, vans, trucks, and motorcycles on the nearly 4 million miles of roads that crisscross the United States requires partnership of government, industry, and researchers. Each has an important role to play.

That's why I find it especially troubling that, according to Bloomberg, one of the automobile manufacturers involved in the July hack waited 18 months—18 months—to tell Federal safety regulators about the security flaw, while the other manufacturer reportedly knew about this vulnerability for 5 years.

Those failures by manufacturers to report cybersecurity vulnerabilities to the Federal Government undermine the partnership that is necessary to protect the public safety from cybersecurity threats. That is simply unacceptable.

As Transportation Secretary Foxx said in May, "Connected automated vehicles that can sense the environment around them and communicate with other vehicles have the potential to revolutionize road safety and save thousands of lives." I agree with him.

I look forward to examining these issues in more detail and thank the chairman for bringing this hearing. Thank you.

Mr. MICA. Thank you, Ms. Duckworth.

I'd now like to recognize Mr. Hurd, who chairs the Subcommittee on Information Technology, for his opening statement.

Mr. Hurd.

Mr. HURD. Thank you, Chairman Mica.

Today's hearing is one of a series of hearings the IT Subcommittee intends to hold on emerging technologies. And we are proud to join with you and the Transportation Subcommittee here today.

My first car was as a Toyota 4Runner, and I liked to call her Shirley Marie. I got her in the summer of 2000 and had the car up until the summer of 2013. We had a lot of adventures together, but one thing she couldn't do was connect to the Internet.

And flash forward to 2020. Gartner forecasts that about one in five vehicles on the road worldwide will have some form of wireless network connection by 2020, amounting to more than 250 million connected vehicles. A recent study by the McKinsey Global Institute predicts that the Internet of Things, which includes the Internet of Cars, could have a total potential economic impact of between $4 and $11 trillion by 2025. The report further states that the hype around the Internet of Things may actually understate the full potential.

I agree. The hype likely does understate the full potential, but only if policymakers, industry, consumers, privacy advocates, and other stakeholders understand where real value can be created and focus on supporting innovation and cybersecurity and privacy best practices. I worry that overeager regulators in Congress will overact to a stunt hack with restrictive regulations and heavy-handed legislation.

I look forward to hearing from our witnesses from the automotive industry today on what steps they are taking proactively to secure their connected vehicles and protect people's safety as well as their privacy.

I look forward to hearing from Mr. Garfield on what the many innovative companies he represents are doing to ensure the same, that people are safe, that their information is secure, so that they can be confident and embrace the benefits offered by connected vehicles.

And I look forward to hearing from Mr. Beuse on what NHTSA is doing to achieve the highest standards of excellence in motor vehicle and highway safety while staying strictly within their statutory authority and taking care not to hamper innovation.

I yield back.

Mr. MICA. Thank you, Mr. Hurd.

And I'm please now to recognize Ms. Kelly, who is the ranking member of the Subcommittee on Information Technology.

Welcome again, and you're recommended.

Ms. KELLY. I thank Chairman Hurd and Chairman Mica, as well as Ranking Member Duckworth and our witnesses for today's important conversation.

Today's cars have been dubbed computers on four wheels. They gather and store a vast array of personal information about their drivers, affording greater convenience and safety, but also greater erosion of privacy and security. Our automakers, as they long have, are inventing new technologies that have made the driver's experience more enjoyable and efficient. Over-the-air and vehicle-to-vehicle technologies, things that were once only science fiction, can save lives and help prevent accidents.

But with great innovation comes new questions over security challenges and how data is stored and used. As the number of Internet-connected cars grows, so too does the threat of vehicle hacking. If cars are going to store personal sensitive information about where the driver lives, the route the driver takes to get

there, and where the driver stops along the way, there should be assurances that the information is stored securely and protects the identify of the driver.

Our subcommittee's review of previous cyber attacks on government and corporate computer networks revealed that the same vulnerabilities show up time and time again. The interconnectivity of seemingly unrelated parts of the networks makes it substantially easier for a hacker to move through a network and locate sensitive personal information.

But it's not just computer systems that lack segmentation. Seemingly unrelated components of Internet-connected cars do as well. A modern car's brakes can talk to its radio. The radio can tell whether the doors are locked and the doors know whether the windshield wipers are on.

One of the key topics of today's hearing for me is whether the auto industry is designing cars with operating systems that securely store personal and technological innovation, I'll be focused on how automakers, Congress, and regulators can work together to secure our vehicles from malicious attacks and protect Americans and their data.

I thank our witnesses for their participation today and look forward to hearing your thoughts on how we can achieve this goal.

Chairman Hurd, Chairman Mica, I'd like to yield the remainder of my time to the gentleman from California, Representative Lieu.

Mr. LIEU. Thank you, Ranking Member Kelly, for yielding the time.

And thank you, Chairman Mica, Chairman Hurd, and Ranking Member Duckworth, for calling this important hearing.

The Internet of Things brings technology and connectivity into every corner of our lives, including our cars. With the pervasiveness of technology, cybersecurity standards and privacy protections become more important than ever. Unlike other sectors, security and privacy by design are not yet fully engrained in automotive manufacturing culture, as evidenced by the news regarding cars' cybersecurity issues with wireless entry keys and hacks of cars.

However, regulation can be slow, rigid, and discourage innovation if done wrong. Rushing to regulation is not, in my opinion, the answer, but neither is a lack of accountability or standards. The advances that the industry has made in the past year, such as setting up an Information Sharing and Analysis Center and a set of enforceable privacy principles, have been done in part because of public and government pressure.

The Security and Privacy in Your Car Study Act, also known as the SPY Car Study Act, a bipartisan bill cosponsored by Congressman Joe Wilson and myself, is a step in bringing industry advocates and government together to strike a balance between innovation and consumer protection.

I serve on Active Duty in the military. I'm still in the Reserves, and I'm trained to think about worst-case scenarios. So there are three overarching scenarios and questions I'd like to pose to the panel. Hopefully during the time today you might be able to answer it.

The first is, is it possible now or in the future for a hacker to remotely take control of a car and use it either as a weapon or cause an accident?

Second, is it possible now or in the future for a hacker to take control of a fleet of cars and use them as weapons or cause accidents?

And then, third, is it possible for a hacker now or in the future to take partial control over cars? So let's say you're going down a highway at 60 miles per hour and suddenly the brakes go on without your knowledge thereby causing an accident. And I'd be curious to know if, one, those are theoretical possibilities, and then, second, if so, what can be done to mitigate that aspect.

Americans have a right to drive cars that are safe and to keep their information about their daily lives private. I look forward to hearing the testimony from today's panel of witnesses and look forward to asking additional questions on this issue of public importance.

Thank you. And I yield back.

Mr. MICA. Thank the gentleman.

Since thereare no other statements, any other members have any quick statements?

Okay. Then the chair will hold the record open for 5 legislative days for any member who'd like to submit a written statement.

Mr. MICA. Let's turn now to recognizing our panel of witnesses. I'm pleased to welcome first Nat Beuse, who is the associate administrator, vehicle safety research, at the National Highway Traffic Safety Administration at the United States Department of Transportation. Mr. Harry Lightsey, who's the executive director of global connected consumer experience and global public policy at General Motors Company. Mr. Sandy Lobenstein, and he is the vice president of connected services and product planning at Toyota Motor North America. And Mr. Diarmuid O'Connell, and he is vice president of corporate and business development at Tesla Motors, Inc. Mr. Dean Garfield, he is the president and CEO of the Information Technology Industry Council. And finally, Ms. Khaliah Barnes, and she is the associate director and administrative law counsel at the Electronic Privacy Information Center.

So welcome all of our witnesses. I might tell you too in advance that I'll swear you in, in just a second. And we also try to get you to limit your statement, your verbal statement before the committee to 5 minutes. You can ask through the chair to have additional information or data put into the record.

So with that, we are an investigative and oversight committee and subcommittees of Congress. If you'd please stand and I'll swear you in. Raise your right hand.

Do you solemnly swear or affirm that the testimony you are about to give before this joint subcommittee meeting of Congress is the whole truth and nothing but the truth?

Let the record reflect that all the witnesses answered in the affirmative.

Thank you. Be seated.

Okay. We'll go right to our witnesses. And let me start first with Mr. Beuse. Welcome him again, and all of you, and thank you for your cooperation today. And he is the administrator of the vehicle

safety research at the National Highway Traffic Safety Administration.

Welcome, and you're recognized, sir.

And you all bring the mics up as close as you can so we can hear you.

WITNESS STATEMENTS

STATEMENT OF NAT BEUSE

Mr. BEUSE. Good afternoon, Chairmen Mica and Hurd, Ranking Members Duckworth and Kelly, and members of the subcommittees. I appreciate this opportunity to testify about how the National Highway Traffic Safety Administration, or NHTSA, is addressing emerging challenges associated with new connected vehicle technologies.

In 2013, there were over 5.7 million vehicle crashes in the United States that resulted in 32,719 deaths. The consequences of these crashes ranged from personal tragedies that will impact individual families forever to the billions in economic dollars that we can actually measure.

NHTSA's mission is to address these crashes and the increasing use of connected and automated vehicle technologies we believe can help us do that. When combined together, new technologies such as vehicle-to-vehicle communications, or V2V, and automated technologies have the potential to dramatically change the safety picture in the United States.

However, as the chairman pointed out, these new technologies also bring new and different challenges. For example, consumers hear a lot about cybersecurity as it is related to banks and personal information. Indeed, it often seems like every day or every other day there is a breach reported in the media. Now in the auto space cybersecurity is taking on new visibility, even showing up in TV shows as recently as this past weekend. NHTSA understands these dynamics but believes that the challenges associated with connected vehicles are addressable and they should not keep us from pursuing the innovations that can save lives.

Testing and analysis indicates that V2V can address up to approximately 80 percent of crashes involving two or more motor vehicles. This technology promises to be transformative and could even enable a new era of safety that not only saves lives, but brings other benefits as well.

When fully realized, this communication technology is extendable even beyond vehicles and the infrastructure. It can be deployed to other devices that would be carried by pedestrians and cyclists, thereby addressing those types of crashes as well. However, for V2V to be effective, it relies on a robust security system and for the vehicles themselves to be secure.

In exploring the potential of connected vehicles and other advanced technologies, NHTSA understood that cybersecurity would be essential to the public acceptance of new vehicle systems and to fulfill the safety promise they hold. To develop a robust cybersecurity environment, NHTSA modified its organizational structure, developed vital partnerships, adopted a layered approach, considered legislative actions, and encouraged members of the industry to take

independent steps to help improve the cybersecurity posture of vehicles. NHTSA's goal is to be ahead of potential vehicle cybersecurity challenges and seek ways to address them.

NHTSA consulted other government agencies, vehicle manufacturers, suppliers, and the public to develop its cyber program. The approach covers various safety-critical applications deployed on current vehicles, as well as those envisioned for future vehicles that may feature more advanced forms of communications and automation.

However, we also believe there are tremendous opportunities in this realm for proactive steps. In fact, such steps are essential. Regulation and enforcement alone will not be sufficient to address these risks. Cybersecurity threats simply move too fast and are too varied for regulations to be the only answer.

The auto industry can play an essential role by cooperatively establishing rigorous best practices that address the broad range of cyber threats, by reacting quickly and appropriately when such threats emerge, and by working closely with the government and independent security analysts to identify and defeat attacks.

NHTSA and DOT have also given special consideration to the security system that enables V2V technology. USDOT and many, many partners have spent some time developing the network and this trusted architecture that goes along with this system. While we have made significant progress, we believe that more testing is necessary and we plan to undertake that work.

The trust aspect of the system is based on PKI. Though extensively used today, NHTSA and its research partners actually tweak the design to balance security and privacy. We take consumers' privacy very seriously, and in the context of our notice of proposed rulemaking on vehicle-to-vehicle communications, we will address privacy as it relates to that system.

The effectiveness of V2V technology also relies on an allocated portion of spectrum. In light of growing demand for spectrum, spectrum sharing has been a topic of much discussion. DOT is not opposed to sharing the spectrum. Toward that end, DOT is working closely with FCC, NTIA, members of the industry, and other stakeholders on an expedited basis to test and evaluate potential sharing solutions for the 5.9 gigahertz spectrum. We are waiting for devices.

Under the leadership of Secretary Foxx, the Department has taken several steps to support the deployment of V2V and V2I technology. In August 2014, NHTSA issued an advanced notice of proposed of rulemaking. In 2016, we plan to follow that up with a proposal. And just recently the secretary announced some pilot programs, all aimed to further deploy this technology.

Connected and automated vehicles that can sense the environment around them and communicate with these other vehicles and with the infrastructure have the potential to revolutionize road safety and save thousands of lives. NHTSA is already laying the groundwork needed for the road ahead and looks forward to working with Congress, manufacturers, suppliers, others in the administration, and the American public in this exciting transportation future.

I look forward to addressing your questions.

[Prepared statement of Mr. Beuse follows:]

[Written statements can be found here: *https://oversight.house.gov/hearing/the-internet-of-cars/*]

Mr. MICA. Thank you. And we'll withhold questions until we've heard from everyone.

Let me introduce and welcome again Harry Lightsey, who is the executive director of global connected customer experience and global public policy a General Motors.

Welcome. You're recommended.

STATEMENT OF HARRY M. LIGHTSEY, III

Mr. LIGHTSEY. Thank you very much, Chairman Mica, Chairman Hurd, Ranking Member Duckworth, and Ranking Member Kelly. And thank you for the opportunity to testify before your subcommittees.

In the roughly 100 years of its existence, the automobile has impacted American life in ways unique to any other machine. It has impacted how we live and work, where we live and work, how our cities have grown, and how our country has grown.

Yet the machine itself remains basically what it was at the time of its inception: a gasoline combustion engine connected by a drive train to wheels on the road, driven by a human being. But we are now entering an era where all those basic tenets will change dramatically. Cars will more and more have different modes of mobility other than a gasoline engine. They will be connected to each other in ways that will make the driving experience safer and more enjoyable. And they will more and more relieve the human being of the driving task.

Because we know that humans are fallible and will have crashes in cars, the automobile industry and the National Highway Transportation Safety Administration, or NHTSA, have spent the last half century designing and building automobiles to be safer when they crash, with innovations like seat belts, air bags, and crumple zones. Today we are designing and building automobiles to avoid collisions entirely, with technologies like forward and rear collision warning, backup cameras, lane keeping, and blind spot warnings.

Increasingly, these technologies allow the machine to assist in the driving task itself when the human driver does not react appropriately or quickly enough to prevent a crash. Soon technologies like vehicle-to-vehicle communications will be deployed with the promise to impact over 80 percent of the crashes on today's roads. The savings in terms of lives saved, property damage prevented, medical costs, and congestion will be enormous.

At General Motors, we are moving quickly to take advantage of these innovations. We are the first automobile manufacturer to build connectivity into our vehicles. And GM OnStar has over 6 million customers in the United States and over 1 million customers connected on our 4G LTE broadband platform. We have deployed many advanced safety technologies into our vehicles, including announcing the deployment of vehicles with advanced review mirrors. And we are the only automaker that has announced the commitment to deploy vehicles with V2V technology with our Cadillac CTS model next year.

However, we must acknowledge that with change comes challenge. We must deploy these innovations in the safest manner possible. We must commit to our customers that we respect their privacy and will protect their information. Our automobiles contain software that may have vulnerabilities that bad actors could exploit to threaten our customers' safety and privacy, and we must do all we can to prevent automobile hacking.

We must realize that we are competing with other technologies for the use of scare resources like spectrum. We must be able to use these resources in an efficient manner so long as that use does not interfere with the safety-critical mission of our systems. If we have the freedom to innovate within these parameters, the promise of the future cannot be imagined today.

Thank you, and I look forward to your questions.

[Prepared statement of Mr. Lightsey follows:]

[Written statements can be found here: *https://oversight.house.gov/hearing/the-internet-of-cars/*]

Mr. MICA. Thank you.

And we'll now hear from Mr. Sandy Lobenstein, vice president of connected services and product planning at Toyota.

Welcome, and you're recognized.

STATEMENT OF SANDY LOBENSTEIN

Mr. LOBENSTEIN. Thank you. Good afternoon.

It's an exciting time for the auto industry. More vehicles are being connected and outfitted with advanced safety features and onboard connected safety services, as well as infotainment systems, and we have the ability to interact with these from a smartphone. The truth is, though, that we are only at the beginning of the beginning. The connected car of the future will far surpass the connected car of today with its features and capabilities.

To address questions about the use of vehicle data, the auto industry came together and developed privacy principles for vehicle technologies and services. These privacy principles include meaningful protections, including heightened protections on the use of certain vehicle data, like the vehicle's location or how someone drives.

For example, automakers agreed not to share data with third parties for their own use or to use this type of data for marketing purposes without the affirmative consent of the vehicle owner.

With 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 encouraged from the private sector and it should serve as a model for other Internet of Things sectors.

Cybersecurity is also a key focus, and although no criminal cyber attack on a vehicle has occurred, the auto industry is well aware that the cybersecurity risks that exist for other connected devices also exist for connected cars. We fully grasp the potential consequences of a successful real world attack.

In that light, the auto industry is forming an ISAC to exchange information about cybersecurity threats to vehicles. Toyota is pleased to be serving as the first Auto-ISAC board chair, and we're fully committed to the Auto-ISAC's success. We expect initial infor-

mation sharing from the Auto-ISAC beginning by the end of this year.

Some are making the case that automotive-specific cybersecurity best practices and standards are needed. The question is whether automotive best practices will look any different than existing best practices that guide cybersecurity in other contexts.

That being said, the auto industry recognizes that an effort to adapt existing best practices to the vehicle may be appropriate. That is why the industry has recently embarked on an effort to identify existing best practices that are being and can be applied to vehicles and to address any potential gaps.

For the very same reasons that the government has refrained from mandating cybersecurity standards in other sectors, there is a significant risk with the government mandating cybersecurity standards for vehicles. Industry can move quicker than government to update out-of-date practices or to adjust to new threats. In addition, setting specific government standards may encourage some companies to simply comply, not to do more to protect consumers.

Finally, a sector-specific approach will almost certainly have significant implications for the harmonious development of the Internet of Things at large.

As the Internet of Cars evolves, we are also on the cusp of a radical transformation in vehicle safety that will be made possible by vehicle-to-vehicle communications. Dedicated short-range communication, or DSRC, is a technology that will allow us to overcome the range, field-of-view, and line-of-sight challenges posed by sensor technology, enabling vehicles to identify collision threats at a greater distance or around a corner.

When the FCC allocated spectrum in the 5.9 gigahertz band for DSRC, it spurred an extensive collaboration between the USDOT and the automobile industry on DRC development. The FCC is also currently exploring opening up the band to unlicensed devices.

Due to the spectrum crunch, we support the prospect of sharing spectrum if it can be proven that no harmful interference will impair DSRC's safety-of-life mission. A promising proposal has been offered that has the potential to accomplish this goal. The proposal's developer and the auto industry have recently proceeded to validation testing, and we remain confident that it will be proven out as a workable spectrum-sharing solution.

In closing, I'd like to provide two final observations. 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 designed to directly communicate with vehicles. As the ecosystem continues to evolve, responsibility for protecting vehicles from potential cyber attacks and for preserving consumer privacy should also evolve to include all relevant players in this space.

Second, there's a number of Federal agencies that are seeking to oversee, regulate, or influence cybersecurity and privacy related to the Internet of Things either broadly or within narrow subsets. The resulting cacophony of working groups' efforts, initiatives, and proposals is exceedingly difficult to manage and prioritize. Without consolidation of these efforts, clarification of the roles of various

agencies and better coordination, the opportunity provided by the Internet of Things will almost certainly suffer.

Thank you for the opportunity to testify before you.

[Prepared statement of Mr. Lobenstein follows:]

[Written statements can be found here: *https://oversight.house.gov/hearing/the-internet-of-cars/*]

Mr. MICA. Well, thank you.

And we'll recognize Mr. Diarmuid O'Connell, and he's vice president of business development for Tesla.

Welcome, sir, and you're recognized.

STATEMENT OF DIARMUID O'CONNELL

Mr. O'CONNELL. Good afternoon. Thank you, Mr. Chairman, members of the committee. We appreciate the opportunity to come here today and for the opportunity to speak.

Tesla cars are known for being exceptionally safe. Independent testing by NHTSA has awarded Tesla Model S, our current offering, the highest possible safety rating, five stars, not just overall, but in every subcategory without exception. Approximately 1 percent of all cars tested by the Federal Government achieve five stars across the board. Safety is a watchword at Tesla.

Automotive injury and fatality rates have fallen significantly over the last several decades as a result of crash safety improvements such as air bags, energy-absorbing vehicle structures. And Tesla believes that in order to maintain the pace of reducing injuries and fatality rates, vehicles need to increasingly use computerized vehicle systems to avoid crashes with particular opportunity afforded in the fully connected vehicle space.

Two examples of Tesla's connected car functionality leading to significant safety benefits compared to nonconnected vehicles are the following. The first would be automatic emergency braking, a vehicle feature which attempts to avoid accidents by applying brakes when a collision is believed imminent. Tesla is one of 10 vehicle manufacturers whohave committed to making this a standard feature in all vehicles and Tesla has already delivered on this promise.

The same connected vehicle technology is applied to Tesla's autopilot functionality, where improvements are constant as vehicles effectively learn from varying road conditions and share those learnings with the entire fleet through connectivity.

Several studies demonstrate that uptake rates of recalls in general are about 70 percent. That is to say that for a given vehicle fault that warrants a recall, about 70 percent of the vehicles affected will get repaired. Put another way, 30 percent of vehicles will be left driving around in contravention of Federal safety standards or with a safety-related defect.

Connected vehicle technology offers a significant opportunity for us to do better. Modern vehicles are heavily software controlled and therefore software changes alone can often resolve a safety issue. In late 2013, Tesla became aware of a potential hazard believed to be related to incorrect third-party receptacle installation and wiring. After rapid investigation, a vehicle software change was identified. It was capable of detecting and solving the third-party fault. Because of Tesla's leading connected vehicle capabili-

ties, the software solution was automatically delivered to the entire fleet.

In contrast to the industry average, recall uptakes of 70 percent, Tesla's automatic software updates can achieve uptake rates of nearly 100 percent within a short amount of time, measured in days.

So precautions and concerns as we go forward. The first precaution is to ensure that any software updates to a vehicle are authorized by the manufacturer. This can be achieved by using industry standard cryptography, a technology referred to as signing.

The second precaution is to strongly isolate networks from the mechanical systems of the vehicle. If a processor on the vehicle has network connectivity, the processor should not also have direct connections to the vehicle's mechanical systems, i.e., steering, acceleration, brakes, and gear selection. We don't have gear selection, but that's a separate matter. Some manufacturers implement this isolation with technology referred to as a gateway.

The third precaution is to use industry standard encrypted communications protocols for connections to the vehicle. This ensures privacy and the integrity of data as it's transferred to and from the vehicle.

With respect to regulation. We're in a period of rapid innovation for automotive safety. Tesla vehicle safety already significantly benefits from investments in vehicle connectivity. We expect innovation and success in delivering enhanced safety to only continue as the full potential of connected vehicles is realized. Overzealous or more particularly premature regulation that does not allow for innovation or creative solutions can actually deter or block safety innovations, and as a result, any move in this direction must be considered carefully and only to the extent absolutely necessary, in our view.

Thank you again for the opportunity to provide this testimony, and we'll welcome any questions.

[Prepared statement of Mr. O'Connell follows:]

[Written statements can be found here: *https://oversight.house.gov/hearing/the-internet-of-cars/*]

Mr. MICA. I'd like to recognize Mr. Garfield. And he's with ITI. Welcome, and you're recognized.

STATEMENT OF DEAN C. GARFIELD

Mr. GARFIELD. Thank you, Chairman Mica, Chairman Hurd, Ranking Member Duckworth, Ranking Member Kelly, members of the committee. On behalf of 65 of the most dynamic and innovative companies in the world, we thank you for hosting this hearing. It is perfectly timed before 42 million Americans get on the road to engage in their Thanksgiving commute. And I would suspect that 5 to 10 years from now the cars in that commute will look quite different. And so I'll focus my testimony on that issue, which is the transformation that's occurring, the innovation that's taking place in that space, first. And then, second, what we're doing to ensure that we accelerate deployment, but in a secure and safe way.

It's often said that it's difficult to appreciate history when you're experiencing it and living in the middle of it. But from my conversation with our companies, we're living in an innovation renais-

sance. The convergence of almost ubiquitous broadband with exponential improvement in computational processing, as well as with low cost and almost unlimited storage, is transforming mobile computing. That includes the original mobile technology, which is the car.

We see that manifested today in advanced driver assistance systems, whether that is the adaptive cruise control or automatic braking, which I have in my car, which has prevented accidents on multiple occasions. We'll see that in the future in what the other panelists have mentioned, whether it's vehicle-to-vehicle or vehicle-to-infrastructure communication or in autonomous vehicles.

Our companies are working hard at deploying technologies to make those types of vehicles available sooner rather than later, whether that's dedicated short-range communications, advanced LTE, or 5G wireless. As a number of the panelists have noted, it is early days yet, and so it's impossible to tell which technology will work most effectively. What we do know is that there will be radical transformative improvement in safety, access, as well as how we view our cities.

The other panelists have spoken about some of the safety issues, so I won't repeat that. But think about all of people today who aren't able to drive because of a disability or because they're too old or because they're too young. Through connected vehicles or autonomous vehicles, those people will have access to transportation in a way that they don't today.

Similarly, when we don't have to think about cars being parked all the time, the way we think about our landscape on our cities will change dramatically. Our companies are investing billions of dollars to bring that to the market sooner rather than later and are partnering with many of the companies on this panel in order to make that possible, and as well working with the public sector to enable that.

A big part of our work is ensuring that consumers have confidence in the safety and security of those vehicles and security will become even more prominent in the future. For us, we have long experience working on security issues, particularly cybersecurity, whether it's protecting networks from the network edge to the cloud and everything in between.

And increasingly the norm is security by design, which is building in robustness, resiliency, and redundancy at the software and hardware level so it's not a latch-on later on. What that means is you can actually build into a chip set the encryption protocols to protect on unintended encroachment, as well as the ability to adapt if that encryption is circumvented.

We have found it quite productive to work with NIST in advancing that work. NIST has taken a collaborative approach in working with the public and private sector, working together in coming up with a framework of standards and best practices while allowing sufficient flexibility for innovation.

There is still work left to be done, and that speaks to the role that Congress can play. A number of the members of the panel have pointed to the number of efforts and initiatives that are being undertaken in this space. Congress can play an important role in bringing order to that cacophony, as Mr. Lobenstein identified.

Second, there is really a need, and Ranking Member Duckworth made this point, for a national Information of Things strategy. There is so much work taking place in this space, but not much of it is well coordinated into a national strategy that serves our economic, security, and safety interests.

Finally, once we look at what's being done and develop a strategy, there is an appropriate place for regulation to deal with market gaps, and we would advocate that the approach that's been taken by NIST in developing a regulatory framework that's based on best practices that also allows for flexibility is the appropriate approach.

Thank you.

[Prepared statement of Mr. Garfield follows:]

[Written statements can be found here: *https://oversight.house.gov/hearing/the-internet-of-cars/*]

Mr. MICA. Thank you.

And we'll recognize waiting patiently Khaliah Barnes, associate director and administrative law counsel at the Electronic Privacy Information Center.

Welcome, and you're recognized.

STATEMENT OF KHALIAH BARNES

Ms. BARNES. Thank you, Chairman Mica, Chairman Hurd, Ranking Member Kelly and Ranking Member Duckworth. I'm Khaliah Barnes, associate director and administrative law counsel for the Electronic Privacy Information Center.

EPIC is an independent nonprofit research organization focused on emerging privacy and related human rights issues. We thank you for holding the hearing today and for taking time to consider the important privacy implications of the Internet of Cars.

New vehicle technologies offer a variety of new services to American drivers and are quickly being implemented by car companies. But these new technologies, typically based on Internet connectivity, also raise substantial privacy and security concerns that Congress needs to address.

As cars become more technologically sophisticated, they collect a lot of personal data, including physical locations, destinations, text messages, and phone records. Most car companies and other companies, including Google, fail to inform consumers of their data-collection practices, and few give consumers true control over their data.

Auto companies also use personal driving information for various but vague purposes, which leaves consumers in the dark about who has access to their information and why. This information is often retained for years, if not indefinitely.

The very real possibility of remote car hacking poses substantial risk to driver safety and security. Connected cars can be remotely hacked and controlled from anywhere in the world via the Internet where hackers can take control of various features, including brakes, steering, and car locks. Wireless hacking can also provide access to the car's physical location using built-in GPS navigation systems, which can facilitate crimes such as stalking, harassment, and car theft.

Congress must enact meaningful safeguards to protect privacy and security in the Internet of Cars. Last year a group over 20 automakers, including General Motors and Toyota, signed a voluntary pledge for privacy and security. While the pledge is an important first step, it is no substitute for Federal baseline privacy and data security regulations. The pledge fails to provide essential privacy protections, lacks any meaningful enforcement, and supports the status quo of the wholesale collection of sensitive driver data.

To protect the privacy and security of American drivers, Congress will need to do more. First, Congress should act on pending legislation. The SPY Car Act of 2015 would establish Federal standards for connected cars. The act empowers NHTSA, in consultation with the FTC, to develop cybersecurity and privacy regulations for driver data. The SPY Car Act provides a good framework for meaningful safeguards.

There's also the House draft bill that would require car companies to develop modest privacy policies for the collection and use of driver information. The House draft falls short of providing robust privacy protections. The draft would not require manufacturers to actually develop or even implement privacy-protecting measures. Instead, the companies would only inform drivers about whether the company chooses to take various privacy-protecting measures. The draft also immunizes car companies from FTC scrutiny for simply developing a privacy policy. The draft would broadly criminalize vehicle hacking, including for research purposes.

The Senate bill comes much closer to safeguarding the interests of American drivers than does the House draft. In fact, we would oppose enactment of the House draft, which would be a step backwards for Americans who are concerned about privacy and security.

Second, Congress should establish fines for hacking connected cars, but only where there's malicious intent. This will permit research to uncover security vulnerabilities, many of which we've discussed today, while punishing hacking that is intended to cause harm.

Third, Congress should grant NHTSA authority to issue privacy rules. The SPY Car Act of 2015, with its emphasis on enforceable NHTSA rules and civil fines for offenders, provides the type of privacy and security safeguards drivers need. As Congress moves forward, it is critical that NHTSA has rulemaking authority over the emerging industry. NHTSA's rules should incorporate practices detailed in the Consumer Privacy Bill of Rights, which is a sensible comprehensive framework for privacy protections that provide substantive privacy protections and would help establish fairness and accountability for the collection and use of driver information.

Every day without car privacy and safety protections places countless drivers at risk of having their personal information, or worse their physical safety, compromised. It's time to put consumers back in the driver's seat when it comes to privacy. Congress must act swiftly to combat the current and future privacy threats posed by the Internet of Cars.

Thank you for the opportunity to testify this afternoon, and I would be pleased to answer your questions.

[Prepared statement of Ms. Barnes follows:]

[Written statements can be found here: *https://oversight.house.gov/hearing/the-internet-of-cars/*]

Mr. MICA. Well, thank you. And I'll thank all of our witnesses. And we'll go right into questions.

First, let me get to Mr. Beuse with the National Highway Traffic Safety Administration. In 2012, when I helped craft the MAP–21 legislation, I put a section 31402, Electronic Systems Performance, and it said specifically, "Not later than 2 years after the date of enactment"—that was July, I'd give you August of 2012—that "the Secretary shall complete an examination of the need for safety standards with regard to electronic systems in passenger motor vehicles." Then it has a couple of criteria.

It says, "Upon completion of the examination...the Secretary shall submit a report to committees." And I see I screwed up. I should have put the Department of Transportation in here too, because they don't have one, but we have Commerce, Science, and Transportation of the Senate, and Energy and Commerce in the House.

Have you completed that report?

Mr. BEUSE. No, Mr. Chairman, that report is still under review. What we have done, which is unprecedented, which was we put the entire research program that we developed in consultation with other government agencies, the private industry, et cetera, out for public comment.

Mr. MICA. So it's not—I mean, I guess I just put these things in law and then we just forget them. But it should have been July, we'll give you August, of 2014.

Ms. Duckworth, isn't this 2015 and November? Okay. So we're a little bit behind.

Mr. BEUSE. Agree, it's taken way too long.

Mr. MICA. And is there a draft?

Mr. BEUSE. There is a draft that's entering——

Mr. MICA. Because I tried to get a draft from the committee, and they said they did not have one. This is from the—either of the committees. Can you submit to the joint subcommittees here a draft?

Mr. BEUSE. I'm not sure if I can, but we will take that back.

Mr. MICA. You're not sure if you can?

Mr. BEUSE. The work that has been done that my office is responsible for——

Mr. MICA. Yeah, well, we want to see it. You can, and you will, and we'll have it here within 10 days, okay?

Mr. BEUSE. Okay.

Mr. MICA. All right. That's the way we operate here. So you didn't comply.

We don't have any penalties now, do we, if someone hacks a vehicle? Ms. Barnes?

Ms. BARNES. That is correct.

Mr. MICA. Yeah, so the law is still pending. You favor the Senate's side as far as privacy in your testimony. But we have seen that they can be hacked. That's also correct.

Ms. BARNES. That's also correct.

Mr. MICA. Yeah. And so far no one with malintent has hacked, but you could probably stop an engine, you could disable brakes or

steering, because all of those have electronic components. Would that be a good assumption? I'm not technologically competent, but——

Ms. BARNES. That is correct, Chairman.

Mr. MICA. Okay.

Ms. BARNES. You would be able to disable those features.

Mr. MICA. So they haven't acted and Congress hasn't acted. I have to put blame also on us.

Then we gave a lot of money, maybe——

Mr. GARFIELD. If I may.

Mr. MICA. Yes, go right ahead, Mr. Garfield.

Mr. GARFIELD. To suggest the implication of that colloquy suggests nothing is being done, when, in fact, much is being done.

Mr. MICA. Well, it's not that nothing is being done.

Mr. GARFIELD. Particularly on cybersecurity.

Mr. MICA. We give certain directives. I was going to get to the question of them working with you all, both, and you did talk to NIST——

Mr. GARFIELD. Correct.

Mr. MICA. —which sets standards, and had pretty good report back, and NHTSA, both—everybody has participated?

Have you participated, Mr. Lightsey, with them?

Mr. LIGHTSEY. Yes, Mr. Chairman, we embrace the NIST framework. We have adopted that into our——

Mr. MICA. With both of those Federal agencies or with a private sector group?

Mr. LIGHTSEY. We have had discussions with NIST and with NHTSA.

Mr. MICA. Okay.

And you, Mr. Lobenstein? Yes?

Mr. LOBENSTEIN. Yes. We have also had discussions.

Mr. MICA. Mr. O'Connell?

Mr. O'CONNELL. To be factually perfectly accurate, I'm certain we are absolutely involved with NHTSA on an ongoing basis. I can't testify to the involvement with NIST.

Mr. MICA. Okay. I just want to find out. And again, I commend you for coming together as an industry and working, and I don't want to imply that nothing has been done. But my job is to give certain directives to agencies, and then see if—I'm not here just, you know, to look good. I know I do. But——

Mr. GARFIELD. Yes, you do, Mr. Chairman.

Mr. MICA. But my job is to hold their feet to the fire, and when you put something in law, some of the newer members will find around here, you can put it in law, I put things in law three, four times, and they still don't comply. But we won't go there today.

Again, we gave you a lot of money. We spent about $500 million in taxpayer funds testing the dedicated short-range radio communications devices. What's NHTSA currently doing to address the potential issues with security credential management system? Where are we on that?

Mr. BEUSE. Those funds are not NHTSA funds. Those are the JPO funds, Joint Program Office funds.

Mr. MICA. Is that under you or——

Mr. BEUSE. That is not under me, sir.

Mr. MICA. Who is it under?

Mr. BEUSE. It's under the Joint Program Office, which is now part of the Office of the Secretary. I can't tell you——

Mr. MICA. It's under DOT.

Mr. BEUSE. It is under DOT, sir.

Mr. MICA. Yeah, okay. So I can say under you, okay, under DOT. But they have had half a million. What's the result there?

Mr. BEUSE. Sure. So what we're doing, what the Department is doing——

Mr. MICA. Half a billion.

Mr. BEUSE. —is putting sort of hardware behind that system. I alluded to it in my testimony. What's been done to date has been a lot of hard work with a lot of smart people coming up with the design, but now we feel we need to actually build this and operate it to see what are the vulnerabilities and do some large-scale testing.

Mr. MICA. Do you have any idea exactly where? I'm told that some of what you have done were really actually slid behind sort of the advances in technology. And how much more money, how much more time will it take? Do you know?

Mr. BEUSE. I think that's exactly why the Secretary of Transportation has committed to putting this technology out for public comment as part of a NHTSA proposal in 2016.

Mr. MICA. So that's not till next year?

Mr. BEUSE. I guess in 2 months or so we'll start 2016, but that is the goal. He asked us to accelerate that rulemaking, which we have.

Mr. MICA. Well, we have spent a lot of money and we don't see a lot of progress. And when would you have your final report, the report that I requested here? It's in draft. You're going to give us the draft. When will you have that finalized?

Mr. BEUSE. I can get back to you on the record on that, sir.

Mr. MICA. Within the next 10 days.

Mr. BEUSE. Absolutely.

Mr. MICA. I want a date, a firm date.

Mr. BEUSE. Absolutely.

Mr. MICA. And then I want it made part of the record, okay.

Mr. BEUSE. Absolutely.

Mr. MICA. I'm sorry. Don't mean to be, you know, demanding, but——

Mr. BEUSE. Sir, I understand your frustration.

Mr. MICA. Okay. Again, we try to act responsibly and we expect the agencies to do the same thing.

So right now, just my final question, cars can be hacked with electronic systems. We don't have in place either a standard or ability to stop that. I guess that's a simple way to put it. Is that correct, Mr. Lightsey?

Mr. LIGHTSEY. Mr. Chairman, thank you. GM has invested a lot of time and effort into making it as difficult as possible to hack into cars. As I indicated, we have embraced the NIST framework.

Mr. MICA. No, that's an individual effort. We applaud you for that. But my question is, we really don't have a standard, we don't have the ability to prevent that developed, do we?

Mr. LIGHTSEY. We have the ability to implement things as a business, which is what we are doing.

Mr. MICA. So your cars can't—General Motors' cars can't be hacked?

Mr. LIGHTSEY. I can't say whether they can be hacked or not. I can say that we are making them as difficult as we possibly can.

Mr. MICA. Okay, but that's your individual, and I'm asking about do we have a standard. We don't that I know.

Mr. Lobenstein.

Mr. LOBENSTEIN. Yes, Mr. Chairman. I think we are trying to be proactive. We——

Mr. MICA. But again, the question—and I applaud each of you, and Telsa—Tesla—that's wrong—but Tesla will tell us they are five star and all of that. But my question was, is there a standard developed and is there a protection in place? The answer is for you.

Mr. LOBENSTEIN. We have actually begun working as an industry——

Mr. MICA. Okay.

Mr. LOBENSTEIN. —to establish cybersecurity.

Mr. MICA. But we don't have that in place.

Mr. O'Connell.

Mr. O'CONNELL. I'm not aware of an industry standard. The one thing I would add, sir, is that there is a difference between sort of hard access hacking and wireless hacking, and that's something—we've seen the former, which is people with access to a vehicle then being able to modify certain access.

Mr. MICA. So hard access can——

Mr. O'CONNELL. Hard access hacking has happened on isolated cases. I am personally unaware of any wireless hacking that has gone——

Mr. MICA. But there are no protections or standards.

Mr. LOBENSTEIN. As I said, no standards that I'm aware of.

Mr. MICA. Or if it can be done.

And then, again, part of the responsibility is Congress has set no penalties. We haven't held the agency's feet to the fire.

I will give you the last word, Ms. Barnes. Anything you want to comment?

Ms. BARNES. Sure. I will just point out, and it is in our written testimony, key examples of computer scientists and other researchers finding ways to wirelessly hack into vehicles.

Mr. MICA. Okay.

Mr. Garfield.

Mr. GARFIELD. There is a difference between there being standards and there being laws. There are certainly standards being developed around cybersecurity, and there are certainly laws in place that would punish someone, whether it's the Computer Fraud and Abuse Act or the Digital Millennium Computer Act, from folks hacking into cars or anything else. The question is, are there laws mandating particular standards, and I would argue that mandating a particular standard would be the absolute wrong approach.

Mr. MICA. Well, we don't have that, but we still don't have industry-wide standards or protections on hacking, on privacy, a whole host of things we have heard today.

Let me, I have taken more than my time.

Mr. BEUSE. Mr. Chairman, just on that last question. The industry group, the SAE International, just recently, like within the last week, has developed a set of voluntary industry best practices. We just got it, so we are just looking at it, but I just wanted to make sure you knew that that was out there.

Mr. MICA. Usually things happen just before the hearing.

Let's go to Ms. Duckworth.

Ms. DUCKWORTH. Thank you, Mr. Chairman.

So I want to speak, gentlemen and Ms. Barnes, to ISACs, the sector-specific Information Sharing Analysis Centers, which are nonprofit, member-driven organizations formed by critical infrastructure owners and operators who share information between government and industry about cyber threats and lessons learned; not necessarily in the automobile industry, but in other areas.

Mr. Beuse, can you talk about what sort of mechanisms or organizations have been instituted by NHTSA, and also by the industry, to work towards secure Internet-connected vehicles?

Mr. BEUSE. Sure. There has actually been quite a bit of work done. NHTSA was really at the forefront in trying to encourage the development of the ISAC, and we are very pleased that it is actually up and running now. There are some additional steps that we think probably are necessary. One is clarifying what the role that it will have in its interactions with the agency, and also how that group will be expanded to other sectors, including suppliers.

Ms. DUCKWORTH. I would like to speak to the suppliers portion of it. This is something that has come up in my work on the Armed Services Committee on military equipment. Cybersecurity is certainly something of great, great potential harm to our military. And one of the things that I found out, that for a military weapons platform, something as critical as the new F–35 fighter jet, there is not complete security of the supplier network.

Could any of the three gentlemen from the three automobile manufacturers here talk a little bit about what you have done to secure or safeguard or ensure that your supplier network is one that you can trust? I have in my congressional district Huawei, which is a chip manufacturer, which has been identified by the U.S. Government and different folks as a problematic company that actually engages significantly in espionage, both in corporate espionage as well as in governmental intelligent espionage as well.

What are you doing to make sure that the chips that you are—I'm assuming you don't make your own chips. But what are you doing to make sure that your supply network is also secure?

Mr. LIGHTSEY. Thank you, Ranking Member.

GM, as I was indicating to the chairman, we have invested a substantial amount of resources and time into the whole cybersecurity issue. In fact, we created a global organization whose sole mission is end-to-end cybersecurity of our products and services. And that organization is headed by our chief product cybersecurity officer who reports to the senior management of the company, including the CEO, and to the board at regular intervals about the cybersecurity status of our products and services.

That includes our supply chain, and we have requirements that our suppliers must meet. We audit them on those requirements, and we test their products, and we have those products as part of—

we certainly embrace security by design. So from the very beginning of the design of those products, all the way through to production, those products are tested by both internal and external experts.

Ms. DUCKWORTH. For cyber vulnerabilities are you talking about——

Mr. LIGHTSEY. Yes, for cyber vulnerabilities, penetration testing, other techniques that are common and standard.

Ms. DUCKWORTH. Okay. Mr. Lobenstein, and then Mr. O'Connell.

Mr. LOBENSTEIN. Yes, for Toyota, cybersecurity and safety is of paramount interest to us, and we also use industry standard best security practices, including security by design, risk assessments, multilayer defense. Even in our telematics group we have our cybersecurity team embedded in our activities from the day that we put pen to paper on a strategy, 4 years before a product is launched, through development, through engineering, and even through the operations.

One thing I also wanted to mention is that in the Auto-ISAC we have also invited our automotive suppliers to participate in that. So we are bringing them in that ISAC so we can share information with them as well.

Ms. DUCKWORTH. Mr. O'Connell.

Mr. O'CONNELL. Yeah, a couple of thoughts. Many of the things we do are consistent with what my colleagues have just mentioned with respect to looking at cybersecurity and general robustness of the system. A couple of things that differentiate Tesla, one is our concern, based on being an industry leader in the electric vehicle space, we have a unique concern about the integrity of our operations, because as a new industry entrant we are uniquely subject to these risks.

That said, we take a systems-level approach especially in our software development, but also on our vehicle side. So we have a much higher degree of vertical integration. Many of our software systems are designed from the ground up as a whole system rather than relying on outside providers of software.

With respect to our chip technologies, we are largely, to my knowledge, sourcing from domestic sources. But we are wholly, you know, focused on the vulnerabilities as any Silicon Valley company would be.

Ms. DUCKWORTH. I'm out of time, Mr. Chairman.

Mr. HURD. [Presiding.] Thank you, Ms. Duckworth, and I always appreciate your insightfulness in your questioning.

I now recognize my colleague from the great State of Texas, Mr. Farenthold, for 5 minutes.

Mr. FARENTHOLD. Thank you very much, Mr. Chairman, and I appreciate the opportunity to be here.

Are you pronouncing your name Mr. Beuse? Is that correct?

Mr. BEUSE. Beuse, yes.

Mr. FARENTHOLD. Okay, Mr. Beuse.

There is a huge amount of investment that automakers and U.S. tech companies like Google, Uber, Intel are making in autonomous vehicles overall and autonomous vehicle crash prevention technologies that don't rely on DSRC at all. What if any steps is NHTSA taking to support this type of innovation which is one of

the reasons the U.S. leads globally in intelligent transportation systems?

Mr. BEUSE. So with respect to the automated vehicle technologies we couldn't agree more. We think that there is a future for both connected and automated. So we are pushing hard on both. If you see recent examples by the Secretary on automatic emergency braking, for example, we just included that technology into our new car assessment program, which is one of the most visible programs at the Department in terms of consumer information.

The other thing we have done is we have encouraged industry to slowly make that technology standard, slowly by meaning trying to get to a place where they can offer that as a standard feature on all vehicle models without a regulation. And that was the September announcement that just happened. And so you can see we are pushing on those automated technologies. Likewise, on connected vehicle technology, we believe that it's a mandate that's necessary to get that market to go.

Mr. FARENTHOLD. So how are we going to tie this in with the proposal to mandate DSRC in all light vehicles? Are you going to require these companies to put DSRC on top of their own technologies and are we forcing a standard on folks that we may not be ready for?

Mr. BEUSE. I think that's exactly what the proposal is meant to find out, sir. I think if you look at the approach of the Department, it is to try to get this technology out of the research phase and ready to deploy and ask some of these very difficult questions of the technology about if it's ready to deploy. We certainly believe it's ready to deploy. We believe the two technologies are complementary, they are not in competition with each other, and there is a role for both.

Mr. FARENTHOLD. All right. Well, thank you very much.

And, Mr. O'Connell, I want to visit a little bit about what you guys are doing at Tesla. You all take a different approach to determining security issues and other concerns where you basically have a bug bounty on there and employ white hat hackers. Can you talk a little bit about what you do and why that's a good thing and how it's working?

Mr. O'CONNELL. Sure. Our approach is really consistent with the sort of software development, if you will, Silicon Valley approach to hardening software over the course of time, and it relies on a system of incentives whereby we encourage folks to test our system, both in professional and informal environments, and we reward them when they identify vulnerabilities.

This is consistent with the sort of incentives and disincentive systems that I think generally works in the human environment. But we find it works. It's worked very well in most software environments, and it's working very well for us as well. And it allows us to rapidly identify problems and rectify them and then through connectivity, as I mentioned before, implement the solutions.

Mr. FARENTHOLD. All right.

And, Mr. Beuse, recently the U.S. on an international basis supported a global standard for DSRC in the W band at 77 gigahertz, while we are looking locally at a whole different frequency range, around 50 gigahertz. Is this an example of one hand not talking to

the other? Wouldn't we be better off with one international global standard?

Mr. BEUSE. I'm not exactly familiar with that particular issue. I do know that on the technology radio side of things we have worked very hard to make sure that we have same standards on both sides of the Atlantic, so to speak, so that we can have one common set of hardware.

Mr. FARENTHOLD. Mr. Lobenstein, would you like to address that?

Mr. LOBENSTEIN. So we fully support the idea of spectrum sharing. There has been some deployment actually in the Japanese market near the 5.8 gigahertz band. We also think it's important to protect this bandwidth within the United States because DSRC provides lifesaving services, and we need to make sure that that——

Mr. FARENTHOLD. Is there a technical reason it is not going to work at 77 gigahertz like the rest of the world is talking about?

Mr. LOBENSTEIN. I'm sorry, Mr. Farenthold, but I'm not a technologist, so I'll have to pass on that.

Mr. GARFIELD. Well, actually, if I might?

Mr. FARENTHOLD. Sure.

Mr. GARFIELD. It speaks to the point we were making earlier about all of the different—the disparate efforts in this area and why an agency that is focused on standards and standards development globally like NIST has to be a part of this conversation.

Mr. FARENTHOLD. Okay. I see I'm out of time. I look forward to a second round of questions.

Mr. HURD. Thank you, Congressman Farenthold.

Now I'd like to recognize the ranking member of the IT Subcommittee, and my friend, from the great State of Illinois, Robin Kelly, for 5 minutes.

Ms. KELLY. Thank you, Mr. Chair.

The promise of Internet-connected vehicles is that they bring greater levels of comfort, convenience, and safety, but that same Internet connectivity means that these computers on wheels face the same cyber threats and vulnerabilities as other computers.

Mr. Garfield, given the volume of successful compromises of corporate and government networks, in your estimation, how likely is it that we will see hackers instead of just researchers succeed in hacking connected cars and especially in light of Ms. Barnes' testimony?

Mr. GARFIELD. It's hard to predict the future, but I think the likelihood is real and that it is likely. I think the information that Mr. O'Connell shared about the approach in the software industry on taking an agile approach where we adjust continually, we are testing continually, and integrating security and privacy by design with redundancy, resiliency, and robustness, so we are not compromised completely, is the proper approach.

Ms. KELLY. Is there anything that keeps you up at night, any scenario that concerns you the most?

Mr. GARFIELD. Generally, I sleep quite well. But actually, I think part of my worry is that all of the great things we have been talking about will be a dream deferred because our policy apparatus won't be as agile as our software development to keep up with

these shifts. And so I get the instinct to act, and we should act. What we are suggesting is that we act in a strategic coordinated fashion that ensures our shared interests are achieved.

Ms. KELLY. Thank you.

And Mr. O'Connell, Mr. Lobenstein, and Mr. Lightsey, when you think of new features that you are adding to your cars, is there anything, not that you would do it on purpose, but that you're adding that you think could be negatively compromised as you're getting more connected, I guess?

Mr. LIGHTSEY. Yes. So as we have said, we certainly embrace all the tenets that Mr. Garfield has spoken about, and we incorporate security by design, defense in-depth strategies throughout our review. And so from the very beginning that any service or hardware begins to go through the design cycle for our automobiles, that cybersecurity posture of that particular element is being evaluated, the risk is being assessed, and appropriate measures are being taken to mitigate that risk. And that goes all the way through production and into the lifecycle of the vehicle itself.

Ms. KELLY. Thank you.

Mr. LOBENSTEIN. For Toyota the safety and trust of our customers is paramount. And as I mentioned before, on the telematic side we employ the same cybersecurity best practices that have been mentioned here today. We include our cybersecurity experts from the very beginning and they provide feedback to us that we implement, and I think as we go forward we will continue to expand on that. And we also look forward to working as an industry to develop cybersecurity best practices that we can all employ.

Mr. O'CONNELL. You didn't ask me, but I sleep well at night too, and for two reasons. One, I know that we are employing within Tesla some of the industry's best, as far as developing new applications and considering issues, important issues such as privacy and cybersecurity.

The other piece that gives me peace at night is that we are working within a context, as Representative Farenthold referred to, of open innovation whereby it's not wholly—the integrity of our systems is not wholly reliant on the capabilities of Tesla, but rather looks to resources outside of Tesla to improve the systems that we are developing and to rapidly implement those systems.

Ms. KELLY. Thank you.

Lastly, at the beginning of your testimony, Mr. Beuse, you talked about some of the statistics of people dying on the highway.

Mr. Garfield, your testimony references the tremendous economic and societal benefits that can be derived from autonomous and connected vehicles. In your opinion, what should Congress be doing and the Federal Government more broadly to ensure the potential of this technology is realized? What more can we do?

Mr. GARFIELD. Yeah, thanks for asking. There is certainly important work for Congress. There are so many different agencies that are working on the Internet of Things, and connected cars are a part of that. Congress can play a great role in bringing clarity on a path forward in filling gaps where they exist. So, for example, Representative Lieu spoke about the SPY Act that's going through the House and trying to bring order to all of the work that's going on. We think that would be quite valuable.

Ms. KELLY. Okay, thank you. And I yield back.

Mr. HURD. Now, I'd like to recognize the gentleman from North Carolina, Mr. Walker, for 5 minutes.

Mr. WALKER. Thank you, Mr. Chairman.

About 5 or 6 years in the early 1990s I worked in the automobile industry on the retail side, and I can look back on those 20 years and see how much paperwork on the dealer side was required then to how much is required now. So the last thing that we want is more Federal regulations on these men and women who are working hard to provide jobs out in the industry.

So I do have a couple of questions, though, to make sure that we are headed in the right direction for Mr. Beuse. What role, if any, in the Internet of Cars can only be filled by the Federal Government? I'd like to hear your thoughts on that.

Mr. BEUSE. So one of the things we're doing is really trying to ensure kind of proactive steps from the get-go. It's been mentioned a couple times about security by design. We think that's absolutely paramount. And one of the things we have been doing all along is we saw this coming from very far away, that in order to see the vision of the future with automated and connected vehicles we really had to start focusing on that. And so we have been pushing and prodding as best we can to get that happening.

Mr. WALKER. Sure. In your opinion, do we really need an auto industry-specific regulator and auto industry-specific best practices an standards here, or is the National Institute of Standards and Technology voluntarily cybersecurity framework sufficient enough or the right approach? Can you address that?

Mr. BEUSE. Sure. It might be all of that, sir. It really might be all of that. Right now what we have concentrated on is a kind of a two-prong approach with that. First is actually working directly with NIST to work with the auto industry on a set of best practices. But as a regulatory agency, we have to keep in mind that that is our job, and if there's a need to set a floor, we will do so.

Mr. WALKER. Fair enough. Let me switch gears here but stay with you, Mr. Beuse, for just another minute or 2.

Does the Federal Trade Commission currently have jurisdiction under Section 5 to police the privacy policies of automakers to the extent they collect customer personal information from these connected car devices?

Mr. BEUSE. So that's probably a question more directly directed at the FTC, but what I can tell you is that we have been working very closely with the FTC on privacy issues.

Mr. WALKER. Okay. Does the Department of Transportation, or the NHTSA, have particular expertise that would warrant having them, rather than the FTC, to answer your response, oversee the privacy policies related to the connected car devices?

Mr. BEUSE. So we have do have privacy experts. That is one of the things we will be addressing in our V2V rulemaking. And so we have expertise at the agency, in our Department.

Mr. WALKER. Is there a certain timeframe that you're—is this a date or conference or meeting that you will be addressing this? Is there a specific meeting for that?

Mr. BEUSE. Sure. Sure. What we will be doing is in the context of our notice of proposed rulemaking on V2V communications we will have much discussion on the privacy aspects of V2V.

Mr. WALKER. Last question for you. And I've got—hopefully have time for one more for someone else on the panel.

Most of the technologies that are in development are independent of the DSRC and do not rely on the DSRC. What is the NHTSA doing to enable further technology adoption and take care not to hamper the innovation that we're seeing?

Mr. BEUSE. We're using all the tools at our disposal, including consumer information, regulations where appropriate. It really is an era that we can—when we see lifesaving technology, we really want to push to get it deployed as soon as possible.

Mr. WALKER. All right. Let me slide over to Ms. Barnes for just a minute if I could please.

In your testimony you noted the sensitivity of consumer information collected by the connected vehicles. You did a great job sharing that. But just to review, can you describe what types of personal identification information might be collected and what entities would be collecting it other than the vehicle manufacturers?

Ms. BARNES. Thank you for your question. Some examples of personally identifiable information that can be collected is location information, which can reveal an individual's pattern, her habits. There's also the collection of biometric information, also the collection of credit card information with certain telematics placed inside of the car. Individuals can within their car speak into their system for a text message, so that's audio and that's also text messages.

And looking at the privacy policies of certain auto manufacturers, it's almost an endless amount of outside entities. Oftentimes car manufacturers do not specify the various third-party entities to which they give information to. We know in certain contexts it's marketers. We know that there is an increased market for insurance companies to gain additional access. And without sufficient legal requirements, law enforcement could also gain access to this sensitive information.

Mr. WALKER. All right, thank you. That was very well articulated.

I have got a few seconds left, but just maybe get a quick answer from our manufacture guys. Regarding connected vehicles, in what countries are we seeing the most innovation on this right now? Are you able to address that and just maybe just go down the line in 8, 9 seconds? And with that, I'll yield back then.

Mr. LIGHTSEY. I think this is certainly a very globally competitive part of our industry. I think right now the United States, it leads in terms of deployment of advanced technologies. But I think this is rapidly changing, and I think the proper policies need to be in place to assure that this innovation continues in the United States.

Mr. LOBENSTEIN. Thank you.

I agree. I think we are moving very quickly in the United States to adopt these types of technologies, although in countries like Japan technologies, for instance DSRC, V2V, and V2I, have already been put in place.

Mr. O'CONNELL. I won't refer to our unique regional hubris, but I think that the most advanced efforts are taking place in the U.S. right now and I would like to see us continue to be on the leading edge of this.

Mr. WALKER. Thank you. I yield back.

Mr. HURD. Mr. DeSaulnier, you are recognized for 5 minutes.

Mr. DESAULNIER. Thank you, Mr. Chairman. I want to thank the chairmen and the ranking members for this hearing.

Mr. O'Connell, you can go on and talk about the hubris of the Bay Area as long as you want to. I'm representing that area of the country.

First of all, Mr. Chairman, I request that a statement from the Center of Democracy and Technology be entered into the record.

Mr. HURD. Without objection.

Mr. DESAULNIER. And then maybe to Toyota and General Motors. The whole issue of independent researchers, Mr. O'Connell has talked to Tesla's advocacy for such comments, a colleague talked about other technology companies doing that. Could you tell me if Toyota and General Motors has the same feeling that they will allow for independent researchers to help them to make sure that their software is working properly? And I say this somewhat in the context of what's happened in the industry vis—vis Volkswagen. So maybe you could respond to whether you agree with Mr. O'Connell and Tesla's approach or whether you have a different one.

Mr. LIGHTSEY. Yes. So we generally agree with this approach. We have specific relationships with certain groups of security researchers and academics. As I said, they perform valuable services for us in terms of testing the vehicle software and the systems on the vehicle to help us design, make them better in design, so that hacking them is more difficult.

We also publicly disclose that we're looking very hard at a security vulnerability program. Whether or not it's exactly like the one that Tesla described will be determined. But we should be rolling that out very quickly. And we want to know, if our software has vulnerabilities, we want to know that both from folks within the company and outside the company.

Mr. DESAULNIER. Mr. Lobenstein.

Mr. LOBENSTEIN. We at Toyota also welcome information from so-called white hat hackers. We have regular communications with them. We have relationships with them. We also attend some of the same conferences that they do. And we also do employ third-party cybersecurity testing on some of our systems to ensure that we have got all the most up-to-date information and we are patching any vulnerabilities that we might find.

Mr. DESAULNIER. Okay. Switching subjects to privacy. So the privacy principles are exciting to look at. But given Ms. Barnes' concerns, and I will say my concerns, in the California legislature we had very spirited debates about providing for an opt-out for any third-party data, and the industry lobbied heavily against it. It didn't get out of its first Policy Committee.

So in that context, I think with the language that you have in the privacy agreements that you have come up with and the value you place on consumer confidence and what you are using and the

concerns that have been expressed here today as well, can you provide a comprehensive list of all the data currently tracked and stored in your vehicles, Mr. Lightsey? Can you provide that information and can you provide it to the committee, borrowing on the chairman's earlier comments of within a couple weeks?

Mr. LIGHTSEY. Sure. Definitely.

Mr. LIGHTSEY. Our customer relationship is certainly the most valuable thing that we have in our company, and we respect the privacy of our customers, and we want to protect their information. I will say that before we disclose any information to any third party we get a specific affirmative consent from our customer to do so.

Mr. DESAULNIER. Mr. Lobenstein.

Mr. LOBENSTEIN. We also follow a similar process. We want to be very transparent with our consumers on the data that we're collecting and how we are using it. In four instances where location-based services are used, we ask for the affirmative consent of our consumers because those services sometimes provide lifesaving services like crash notification.

Mr. DESAULNIER. I appreciate that.

Mr. O'Connell.

Mr. O'CONNELL. Yeah. So several levels of protection involved at Tesla. First of all is the opt out. I mean, people have the option to not share any of their data with us. When we do share, when there is bidirectional flow of data, we anonymize that data and we aggregate it such that not only can you not identify the user, but you can't even identify the vehicle. So that's our philosophy.

But the intent of, as I'll remind, the intent of all of this is to increase principally the safety of our vehicles, and then secondarily, but of great concern, the utility of our vehicle to our customers and drivers.

Mr. DESAULNIER. I appreciate that. And hopefully we will hit all of them.

Mr. Garfield, maybe you could just comment on the industry's privacy standards in your view that related to other tech privacy protections.

Mr. GARFIELD. In general, the privacy norms in the United States and actually globally are driven by the FIPS standards, which also is at the heart of the FTC regulation in this area, which over time has become more expansive, not just to deal with expectations that are explicitly articulated but those that are normative.

Mr. DESAULNIER. Thank you, Mr. Garfield.

Mr. Chairman, I yield back.

Mr. HURD. Thank you, sir.

And I'd like to recognize myself for 5 minutes.

Mr. Beuse, can you take 30 seconds and tell me, just to make sure I'm clear, what DSRC is?

Mr. BEUSE. Dedicated short-range radio communications.

Mr. HURD. And how is it going to be used?

Mr. BEUSE. To send basic safety messages between devices.

Mr. HURD. And this is being developed by the Department of Transportation?

Mr. BEUSE. In conjunction with a whole host of alphabet soup.

Mr. HURD. Agencies, Federal agencies.

Mr. BEUSE. Federal agencies, suppliers, manufacturers, companies.

Mr. HURD. So here is my concern about that. DOD and VA spent over half a billion dollars trying to get two electronic health records to work together. And after 4 years, they said: Uh, this is really hard, we are going to have to go separate areas.

And now we are talking about being in an industry where you have so much private sector investment that are figuring this out, why are we even thinking about the Federal Government getting involved in doing this when that standard hasn't developed out of the private sector? The private sector is going to be a little bit better equipped to develop this type of technology and the thing is probably going to work a little bit better.

I don't know. Mr. Garfield, do you have some opinions on this?

Mr. GARFIELD. We do.

Mr. HURD. I'd like to hear them.

Mr. GARFIELD. Our view is, and I shared it implicitly in my testimony, is that there are complementary technologies that are being developed, including advanced LTE and 5G, that we can't tell which is going to prove most effective. And so we think having the ability for all of those, including DSRC to advance, but without a thumb on the scale, including the thumb on the scale of the Department of Transportation.

Mr. HURD. Yeah. And, Mr. Beuse, why do we think that the Department of Transportation should be doing this and why this is going to be helpful in the concept of interconnected cars? And I also appreciate you talking about the safety concerns related with interconnected cars.

Mr. BEUSE. So maybe just to clarify, I think there's a misconception about what we are doing at the proposal level, right? So we are writing a proposal to ensure interoperability, security, and everything else that is needed to support communications between vehicles. If at some point in the future or even in response to the proposal data comes in that shows there is an alternative technology that can meet the safety potential, then——

Mr. HURD. Do we not think that that's already there? I think Toyota is doing it. I think Tesla is doing it. I think GM has even tinkered with this. I think it's—the cat's out of the bag.

Mr. BEUSE. In response to the ANPRM, none of those comments came in. There was not one person that responded back saying that this technology shouldn't be mandated, it's not the right technology.

But again, I think we are writing that rulemaking with an open mind, and it's just a proposal, and so the idea is we'll get comments and we'll evaluate where we are. I think the whole notion of going this step is really to take it out of the research where it's been for so long and really shine a light on it so we can——

Mr. HURD. Absolutely, because I had dear friends in a recent car accident and there was a fatality, and the car that came and hit them, first eyewitnesses said that the car never—there was no braking involved. And the technology, advanced emergency braking, that Tesla is developing—I think other manufacturers are—I want to see this as quickly as possible.

And, Mr. O'Connell, my question to you is, you know, is there any barriers that are preventing you all from moving even faster on deploying this technology?

Mr. O'CONNELL. No. I think it's human will and open communications both, you know, between the parties here at the table and with government bodies, so that, you know, confidence is obtained all around. Use the convening power of our separate agencies and share information. That's what's going to solve this problem.

Mr. HURD. Yeah, because if we can protect more citizens from crashes, you know, this is going to be a great thing for all of us.

Mr. Lobenstein, my question to you, and this is from you having your hat as the new chair of the Auto-ISAC, have you been given any information, any intelligence, been briefed on anything of known attackers targeting specifically vehicles, types of vehicles? Is Russian organized crime creating, you know, focused on getting access into vehicles? Have you seen that kind of information?

Mr. LOBENSTEIN. I apologize, Mr. Chairman. I'm not actively involved in the Auto-ISAC myself, so I don't have that information. I can get that for you.

Mr. HURD. Ms. Barnes, are you familiar of anything like that where there is briefing on known attackers, Russian organized crime, Chinese state sponsors, that are looking at getting access to vehicle information?

Ms. BARNES. At this moment, no. I'm sorry. I'm not aware.

Mr. HURD. Because again, one of my concerns is that, you know, I did this for a living. We did this on trains. We did this on subways, and, you know, looking at how can you take advantage of it. We've got to know what the threat is, and this is why I think this creation of the Auto-ISAC is important.

And if you're not getting the kind of information sharing—because the Federal Government should be sharing as much information as it possibly can with the private sector, for the private sector to protect themselves, and to protect consumers—and if you're not getting that, let me know.

And my last point is, the Office of Personnel Management had difficulty protecting the records of 23 million people. And they had the audacity to not even say "my bad" when they sent out the letters to the people that did receive the letter that they were compromised. By the way, I was one of them. And at least when some of these issues have been—arise within the auto industry, that I got a letter pretty quickly talking about how you fix it, how you do it. And there was a responsiveness that I wish the Federal Government had.

And so I think it's—I'm always concerned when we put too much faith in Federal agencies to protect our information. And it's cooperation. It seems like it is, Mr. Beuse. I appreciate that. But this is where we need to work together and we need to make sure that innovation and entrepreneurship is allowed to grow.

With that, I'd like to——

Mr. GARFIELD. Actually, if I can make a quick plug for data breach——

Mr. HURD. You got a couple seconds.

Mr. GARFIELD. —data breach legislation, which has been pending for quite some time, almost a decade, is long overdue, and could be helpful here as well.

Mr. HURD. I would like to recognize my colleague from Virginia, Mr. Connolly, for 5 minutes.

Mr. CONNOLLY. Thank you, Mr. Chairman, and welcome to the panel.

Maybe, Mr. Garfield, I'll start with you. Can you tell us the difference between autonomous and assisted vehicles?

Mr. GARFIELD. In common nomenclature the idea is that an autonomous vehicle doesn't necessarily rely on vehicle-to-vehicle or vehicle-to-infrastructure communication, so it is truly not connected to another car or to communication from infrastructure.

Mr. CONNOLLY. Or to a driver?

Mr. GARFIELD. Or to a driver, correct.

Mr. CONNOLLY. And assisted would be?

Mr. GARFIELD. It's assisted by some network communication, either with the infrastructure or with another——

Mr. CONNOLLY. But also might be driverless in that sense?

Mr. GARFIELD. Correct.

Mr. CONNOLLY. Okay.

Maybe we can start with you, Mr. Lightsey. You know, I represent northern Virginia here in the Nation's Capital. The national capital region as measured by A&M's Urban Mobility Scorecard now has the Nation's worst congestion as measured by these metrics: 82 hours stuck in traffic every year on average; 35 gallons of gas wasted idling every year; and at least $1,800 in lost time every year.

How could these technologies assist a region like this with arguably the worst congestion as measured by those metrics?

Mr. LIGHTSEY. Yes, thank you.

So first of all, let me backtrack a little bit to Chairman Hurd's questions about DSRC and just let me say on behalf of the industry and on behalf of GM, private industry has also invested a substantial amount of money, equal to or greater than the amount of money that the government has invested in this technology. And we very much view this as complementary to the onboard sensor technologies that are also being used with many of these safety systems.

So DSRC has the advantages, as Mr. Beuse referenced in his introduction, it has the advantage today of being the only technology we know of that meets all of the latency requirements to actually be able to have these vehicles talk to each other in time to prevent a collision or crash from happening, and works in bad weather with obstructed vision, without obstructed vision, and those are the advantages that we see to DSRC.

But I think if you take together all of these collisions, all of these technologies, you know, any time that we can prevent a crash from happening, we get the attendant benefits of all of the congestion that happens when you have a crash.

Mr. CONNOLLY. I concede that, but that's really not my question. I think we have covered safety and I completely concede that. And for some people their intuitive reaction when you talk about driverless cars, I'm going to put it that way, is well, I'm not in control,

what if something happens, what if it goes awry? And I think, well, 94 percent of current fatalities are due to human error. Surely we can do better than that and we can reduce, I think, significantly.

Mr. GARFIELD. And you are seeing better already with advanced driver-assisted systems.

Mr. CONNOLLY. Yes.

Mr. GARFIELD. So it will only get better and better.

Mr. CONNOLLY. But how can it work in helping to alleviate and better manage congestion in areas like ours? I guess that was kind of what I was getting at.

Mr. LIGHTSEY. Right. So if you take the whole system, certainly as we bring the infrastructure into play and traffic signals become more aware of what cars are flowing in what direction, they can time themselves to optimize the traffic flow. Autonomous vehicles, as being better controlled than by a human operator, will be able to follow each other a little bit more closely in a safe manner and, therefore, make more efficient use of the roadways that we already have instead of us having to continually add new lanes to our highway system. Those are the kinds of things that we are talking about.

Mr. CONNOLLY. Well, I want to give Mr. Lobenstein and Mr. O'Connell from the manufacturing point of view an opportunity to comment as well. But I have got to observe, and this is the Nation's Capital, we are not that good at deploying technology currently. I mean, in terms of traffic management, not much. And I have been involved in local government for a long time. We tried to get it, you know, deployed. I think, Mr. Lobenstein, you mentioned Japan. Japan is light years ahead of us in the deployment of technology for managing traffic control. But why don't you two comment.

Mr. LOBENSTEIN. They do have V2V and V2I technology deployed already for improving traffic flow. And I think if we look at the technology, traffic information was provided one way to vehicles years ago, and now the vehicles understand and can communicate back their flow and we know real-time when there is traffic and where there is traffic. And I think expanding the communication, whether it is V2V or V2I, allows us to then improve routing, which improves safety, it has improvements in productivity for individuals as well as business, when you think about delivering goods and services, and it has the capability to improve emissions as well.

Mr. CONNOLLY. Mr. O'Connell.

Mr. O'CONNELL. On topic but slightly tangentially, there is a great YouTube video that shows 20 cars put on a racetrack with individual drivers all given a green light to start moving at a certain time at a certain speed, and something within like two or three laps they are all congested. So human systems are not great, as you note.

Infrastructure is also hard. My comments are most salient within the context of Tesla. We are already fielding driver assistance technology, what we refer to as autopilot, which relieves the driver of certain control responsibilities at certain times and within responsible contexts. So presumes that the driver is there, presumes that their hands are on the wheel, but in certain speed environments,

low-speed environments, such as congestion, a vehicle can modulate its own position within traffic and keep traffic flowing.

I mean, it's tempting to think that this sort of technology could be implemented rapidly across a fleet. It's too bad the connectivity doesn't exist across the fleet so that we can't rapidly uptake systems. But I think you are going to see it implemented more and more quickly over time.

Mr. CONNOLLY. And if I could just observe at the end here, Mr. Chairman, I think what's hopeful is how rapidly we already are adjusting to technologies that assist us in this effort. So, you know, on our own, we are getting on this and finding out what's a better route because of congestion. I can even look at reports coming in for what's causing the congestion and then I can make a judgment as to whether I want to go or not. GPS has revolutionized. I have to explain to my young staff what a map was. We've become hooked on this already, and it is an efficiency. So I'm confident that actually as we really advance technology, I think we are going to adjust.

Thank you so much for being here.

And thank you Mr. Chairman.

Mr. MICA. [Presiding.] Thank you, Mr. Connolly.

I recognize the chairman of the full committee, the gentleman from Utah, Mr. Chaffetz.

Mr. CHAFFETZ. Thank you.

And thank you all for being here.

This is one of the most exciting parts of our economy. This is somewhere we can lead the world. It's something that's going to create real jobs and have a real impact, I think, on people's lives as long as the Federal Government doesn't come in and screw it up—which we have prone to do in the Federal Government.

One of the raging discussions and topics that we are going to have in this Nation, particularly in light of the horrific terrorist acts in Europe and what we have experienced here in our own homeland, is a further discussion about encryption. Because I think one of the big questions before our Nation is how much privacy, how much security are we going to give—how much privacy are we going to give up in the name of security?

And it's a difficult question when you see friends and loved ones and people on television being killed. It's a very difficult thing. But on the other hand, I also want my wife, my kids, myself, my friends, my neighbors to be as safe and protected from would-be people who want to cause them harm and tap into information.

So maybe if I could start with Mr. Garfield here. If you could address the whole encryption issue, how does it really work? Because you really can't create a key just for the good guys, just for law enforcement, right? It's either encrypted and secure or it's not. Give me your perspective on that, particularly in light of what this country is dealing with right now.

Mr. GARFIELD. Thanks for the question, Mr. Chairman. I would start by saying that the people that I work with are patriots and so are as sickened by what they saw in Paris as everyone else in this room.

The context in which we are having this conversation actually speaks to the issue, because when we're talking about security and

safety encryption is an important tool for enabling that. And so the conversation is not either-or, it's how do we advance security with encryption as a tool, while also making sure that national security is protected?

And I think there are ways to do that. I think a folly is to think that creating backdoors or making keys available to just some people is that solution, because ultimately, if you create vulnerabilities, they'll be widely exploited.

Mr. CHAFFETZ. Yeah, but can't you just give it to the guy at the genius bar and your wife and just call it a day? Explain to the person who is not as familiar with this how this works or doesn't work.

Mr. GARFIELD. Well, the challenge with just giving it to the person at the genius bar is the same challenge that we're talking about with 90 percent of traffic accidents are caused by human error. And so you're entrusting one person who may be vulnerable to being compromised with the security for everyone. And so that is the problem with empowering the guy or the gal at the genius bar, is you're creating a vulnerability that could then be widely exploited.

Mr. CHAFFETZ. Anybody else want to address this? Anyone else on the panel here?

Mr. O'CONNELL. Probably not.

Mr. CHAFFETZ. Do you want to have it be encrypted?

Mr. O'CONNELL. I'll, at some risk to myself, maybe I'll do that. You know, I think it's an issue of philosophy, right? I mean, as Mr. Garfield said, none of us—implied—none of us has a unique repository of knowledge or capability.

I think open systems are ultimately the best systems to innovate and to protect. It's a dynamic process. But it's one where, I guess, you vest hope either in the inherent goodness of man or the inherent badness of man, and I prefer to vote for the former. I think that it's the minority that are malignant, and that in a truly open system, where innovation is encouraged and rewarded, where there's sufficient penalties for malignant behavior, you're going to see a net positive benefit over the course of time.

Mr. CHAFFETZ. Well, thank you.

And I think as members on this panel and in the Nation grapple with this, I think that the 99 percent of our population that does deal with things in a safe and secure way, they are good, honest, decent people. I think the bigger obligation is to protect them as best we can. And certainly there can be carveouts for law enforcement needs. If you have a probable cause, articulable suspicion, you have a terrorist type of activity going on, of course there are things, whether it be geolocation or other types of things, that they should be able to tap into.

But if you're a suspicionless American, if you're somebody who is leading a good, decent, honest life, I think you have an expectation of privacy in this Nation. And that will certainly come into play not only with cars, but the Internet of Things. And everything that's going to be connected, I think this is going to be one of our big questions we're all going to have to grapple with.

Mr. GARFIELD. If I can add one more thing.

Mr. CHAFFETZ. Sure.

Mr. GARFIELD. I think how we approach these issues have to be grounded in something, and I think what they need to be grounded in is our values. And part of our values here in the United States is that we act consistent with laws, right? There are certainly legal frameworks for gaining access to that information, and we will work with law enforcement to ensure that our national security is protected while at the same time there's a fundamental belief that people's rights will be protected as well. And we figured out how to strike that balance and we'll continue to do so, and that's partly why we're viewed in the way that we are around the world.

Ms. BARNES. And if I may just briefly add onto that if I could have a moment. Another way in which to ensure both the privacy and security is we're hearing a lot about privacy in design, which is building privacy into the cars. But more privacy protective would actually be privacy-enhancing techniques which would minimize or eliminate the need to collect personally identifiable information, so that when there is a report of a malicious hack, those who need information regarding the hacker only getting the absolute necessary information about the hack, removing the personally identifiable information. It's not important where the driver was going or what she was speaking out inside of the car, but instead that a system has been compromised.

Mr. CHAFFETZ. Well, thank you.

And as I yield back, I do hope members are able to look at the geolocation legislation, the GPS Act that we have here, that you would need a warrant, or articulable suspicion certainly, but a warrant to actually track somebody's geolocation, because I do think that is the content of their life.

So I appreciate the time. I yield back.

Mr. MICA. Thank you, Mr. Chairman.

Other members have questions?

Mr. Farenthold.

Mr. FARENTHOLD. Thank you very much.

I'd like to take up a little bit on where Chairman Chaffetz left off.

Ms. Barnes, earlier the automakers testified that they are very careful with the information they collect and they don't share it. Reading your written testimony, I'm not sure that you would agree with that.

And, you know, there's a lot of information that's tracked. I haven't turned off geolocation on my phone. So this is my Veterans Day map. On a map it shows everywhere I was. I can slide over. It tells me I got into the Houston airport and were there for 32 minutes at 4 in the morning. I had breakfast in Refugio. I went home and took a shower. I went to Robstown, Texas. I went to the USS Lexington. I went to Brewster Street to welcome some bicycle riders. I then went to Applebee's to greet some veterans. I went to the Veterans High School.

It knows everywhere I was, how long I was down there, and has deduced where I live and where I work without me having told it a thing. This is turned on by default in almost every person's phone. I would imagine that cars collect the same information. And unless I'm aggressive about turning it off or telling them I don't want it shared with marketing partners, I'm going to have some-

thing pop up, say, "You're near a Whataburger. Why don't you stop for a burger and fries?"

So, I mean, there's a lot of information that's out there. Do you want to comment on that and maybe we need a better opt out on this?

Ms. BARNES. So I always advocate for stopping at Whataburger.

But opt out routinely fails consumers. This idea that there's such an information asymmetry that the auto manufacturers, as well as their third-party services who are contracting with them, can gobble up all of the information and the consumer is simply unaware.

And when we are looking at the privacy pledge, it also—the consumer doesn't have any type of choice. But choice is simply not enough for the consumer. That's why we need some type of standard where a consumer will have guaranteed privacy protections.

The onus should not be on the consumer to turn off her location information at every single subset. And when you look in the Car SPY Act, there's a provision that would allow an individual to turn off data collection should she choose, but still retain the functionality.

Mr. FARENTHOLD. So how easy is it? Okay, we can talk about hackers, but let's talk about the government. How easy, right now under current law, is it for the government to contact Google or contact Tesla, Toyota, GM, and say, "I want the information for XYZ person?" And do they need a warrant, or is it just, I mean, is it a letter? What do they need?

Ms. BARNES. So in certain contexts it would depend exactly about what type of personal data it is. Some of the information may be protected under ECPA and other statutory provisions. But in the absence of full-on protection for all of the types of information that is collected, not only by auto manufacturers, but as well as their third-party services, that's why there needs to be——

Mr. FARENTHOLD. They could potentially be subpoenaed by private parties as well.

Ms. BARNES. Easily, yes, sir. Insurance companies, marketers, those are some of the provisions to prevent marketers to get it as well.

Mr. FARENTHOLD. So do any of the auto manufacturers have an idea how many of these they get a year, requests for information from the government, be it a subpoena or a Federal agency?

Mr. Lobenstein, you look like you have an answer.

Mr. LOBENSTEIN. So I'm not aware of the number of requests we get, but we have had a longstanding policy that any time we do get requests for that type of information we require either a court order or a warrant before that information's released.

Mr. FARENTHOLD. Mr. Lightsey?

Mr. LIGHTSEY. We have that same policy. We will not give away any of our customers' private information unless there's a due process of law.

Mr. FARENTHOLD. All right. Thank you very much.

And let me ask, I've got another minute or so here, we talk about encryption and all the technology that's in the cars, in the computers, but we look at—we also have created a system where we're now making it difficult for us to repair our own cars, to modify our own cars. We've basically killed the industry of being able to go out

and buy another radio for our car because it's all integrated in the GPS system and the auto control systems.

There was recently a case with a John Deere tractor where they wouldn't let him fix it, saying the copyright on the security and the anticircumvision provisions of the Digital Millennium Copyright Act made it illegal for them to fix it without going to a John Deere dealer.

I'm afraid we're going to see this in the car and we see the death of the corner garage or we see the death of your ability to do any sort of modifications to your car, you know, whether it's with bigger tires to jack up your pickup truck or do things to enhance performance.

Mr. GARFIELD. Actually, the example you gave is a great example of regulatory processes working. And so every 3 years the copyright office has to evaluate the DMCA to ensure that good faith research is able to be advanced. And recently the copyright office said that as a part of doing good faith research you can do so on a car, right, and get beyond the encryption systems. And so it's a great example of an agile system working effectively.

Mr. FARENTHOLD. My concern, of course, is you never really own your vehicle because there's so much software involved you actually may just be licensing the software to, you know, operate something that would become a brick if you tried to modify it or transfer it or do something else. But that's something——

Mr. GARFIELD. Not to be overly contentious, but we can't have it all ways, right? So we can't say we want connected cars moving down the highway and be secure and safe while at the same time saying we want everyone to be able to get into that and be able to stop it while it's moving.

Mr. FARENTHOLD. I think Mr. O'Connell is saying we want open source software where we can actually see what's being in and have control over your own vehicle. I mean, where's the line there?

Mr. O'CONNELL. To be clear, I didn't necessarily advocate for open source software, but I do advocate for an open system of improving software. So that's an important differentiator.

And I would add, though, that, to the point of your last comment, there are models out there which posit that people don't even want to own their car anymore. So this may be—the specific problem you reference may no longer be a problem, which opens up the possibility that there are others, but you for reference.

Mr. FARENTHOLD. All right. Well, I appreciate you all's comment on that, and yield back.

Mr. MICA. Well, thank you.

Any other questions at this time?

Just I guess in closing, well, I'm sitting here thinking my wife is a pretty smart lady, and she does all of the computer work at the house and paying bills and everything. And on a Sunday afternoon she's on the computer and she gets a call from Microsoft service center, and they ask for some information and she reluctantly kind of gave it to them. The next thing I know is her computer is locked, and it's an extortion attempt.

And I got on the phone. I found out they were Pakistanis. I'm a Member of Congress, so I contacted—we have a whole communications network. We have the Capitol Police. We have access to

the FBI and folks you don't even want to know. And they basically told me: You're screwed. And it was extortion. I mean, I could see extortion to can't start your car, someone has hacked it. So, I mean, this just happened with our little home computer.

It was interesting, though, we bought some new software and it was at a location not our principal residence, so we didn't have a lot on there. But after we bought that, then she found out from the software company that they keep another lock behind—protection behind that and can—and actually can release the system. But they get you to think we have incredible capability.

I was in a General Motors car. I love the—you had it displayed here—the teenager device. I just told the Gonzaga High School, I spoke there just—I think it was yesterday. I told all those teenagers what's coming. And they were aghast, you know.

But the things you can do are unbelievable. And I told the class, too, I said: Your biggest—you know, whoever was paying attention to Paris and the terrorist threat—but those kids get in a car and that is the biggest cause of death for our teenagers. We've gotten deaths down from 43,000 to 33,000. But a huge percentage of those are kids. And the device I saw in the General Motors car was pretty astounding, how you can control that.

But, again, I guess a question more than the comment is, the private sector's come up with some incredible innovations. You're setting standards and trying to protect the owner and the consumer. You've got a good association coming together trying to bring folks together. I'm anxious to see your report, I guess you cited, Mr. Garfield, that was just turned over. The role and scope of government in all this, like the chairman said, we usually overlegislate and then the government usually overregulates. So trying to get it right, you want to also protect rights, which Ms. Barnes has said.

And I hammered on DOT because it's now 3 years ago I said let's see where we're going with this and tried to set a schedule, which hasn't been adhered to. So a bit of frustration in that. It is complicated. They need to work with you. It sounds like for the most part they are. We don't want them to come out with standards or requirements or technology mandates that are obsolete or by the time we enact them sometimes they've an overreach. So that's a challenge we face.

Maybe in closing any quick guidance on how to proceed? Mr. Lightsey, I want to hear from the private sector. I know we're going down a certain path, but what do you think, again, the proper role of government?

The standards, I've worked with NHTSA. And I just told Ms. Duckworth I tried to get a biometric standard after 9/11. That was three times I put in law a biometric standard for iris. And I think we may be there, it's 12 years later. Hauled them in, tried to get them, they're very difficult to nail down. And with changing technology, you've got sort of it's like trying to change the wheels on a vehicle that's moving down the highway at 75 miles an hour.

But tell me how you would like to see this unfold, Mr. Lightsey, Mr. Lobenstein, and Mr. O'Connell, the three guys who are representing the companies that actually produce vehicles. Go ahead.

Mr. LIGHTSEY. Yes. So thank you, Mr. Chairman. And with all due respect, our industry can't afford to wait for government and

we're not doing that. We're investing a substantial amount of resources and energy into innovating with our products and services to make our products safer and to make them more enjoyable by our customers who are——

Mr. MICA. Now, once again I have to nail you down. What's the proper role of government regulation, law? Where do we go?

Mr. LIGHTSEY. Well, as I was saying, Mr. Chairman, I think our industry has shown time and again that we can and do work well together for our customers. And I think that the industry needs the freedom to innovate and to do that work.

Mr. MICA. And who in government would you put? Should we leave it with NHTSA or DOT or where? How should it be structured, responsibility from the Federal level?

Mr. LIGHTSEY. From the Federal level, we work well with NHTSA, we have a good relationship with them, and we've proven that we can do that. I think that in this space obviously the Federal Trade Commission is active in this space, and we've begun to work with them as well, and we will work with whatever agencies that Congress in its wisdom decides are the ones that need to be involved in this.

Mr. GARFIELD. If I could interject——

Mr. MICA. Well, after I hear from Lobenstein and O'Connell. I didn't really get a real handle on—we haven't even talked the FTC. God, no.

Let me hear your take, Mr. Lobenstein.

Mr. LOBENSTEIN. Thank you, Mr. Chairman. I think, first of all, we appreciate the work that has taken place between the auto industry and NHTSA so far on DSRC. That's been a 15-year-long road to get to where we are today, and we think we have a good technology that's ready to go. And once we get this spectrum issue closed, I think we can move forward with that safety-of-life mission that DSRC promises us.

In terms of cybersecurity, you know, we've looked at the NIST framework, and we think that NIST is a good agency for us to partner with and as an industry to create the same types of best practices and self-guiding principles that we've already done in terms of privacy and security.

Mr. MICA. NHTSA at one level, NIST at another level?

Mr. LOBENSTEIN. Yes, sir.

Mr. MICA. Okay. Mr. O'Connell.

Mr. O'CONNELL. Mr. Chairman, a couple issues of principle and then a direct answer to your question.

You know, it's all about incentives. At Tesla no one could be more interested in our own survival, especially as a small young company, than we are. So putting the right incentives in place is key.

I think that whatever we do and whatever agency it resides in, we need to foster innovation, number one, and then sharing. So putting the proper incentives in place to innovate and to share.

I think an instructive case of how this proceeded was advanced emergency braking, where rather than resisting an impulse to regulate, NHTSA and other agencies fostered the sort of development of the technology and then encouraged the deployment of that tech-

nology and did so, as far as I know, without the benefit of any sort of regulatory norms.

The hazard with standards is that of course in a long process you move toward lowest-common-denominator behavior, and so that's to be encouraged in some cases, but not—I mean, the standard-setting process—but not wholly appropriate in innovative arenas like this.

As to the agencies, I don't have any particular point of view, I'm afraid to say.

Mr. MICA. Okay.

Mr. Garfield.

Mr. GARFIELD. The only thing I would add is that one of the real challenges here is that these are cross-cutting issues that impact and implicate multiple agencies. And one way that Congress could certainly help is bringing order to that by making sure that there is greater coordination among all the agencies.

So it's not to suggest NHTSA be cut out and the Department of Commerce be brought in. It's really Congress can play a critical role in making sure the FTC, the FCC, NHTSA, and NIST at the Department of Commerce are actually coordinating and working with each other to achieve the things that we all have in mind.

Mr. MICA. Well, again—you did a very good job, Ms. Barnes, giving us your agenda recommendations. Thank you— on the privacy side—but thank you for participating.

I look forward hearing back, seeing some of your plans, sir.

What I'd like to do is we'll leave the record open, without objection, for 10 days. We may have additional questions, there are quite a few here that we didn't even get to, to submit to the witnesses. They'll be made part of the record.

So without objection, that's so ordered.

Mr. MICA. And, again, I'm looking forward to having a report and the other items we requested today from NHTSA made part of the record.

And, again, thank you, each of you. Very interesting. Probably they'll look back in 10 years and we'll have made such incredible progress. But we want to do the right thing at this important juncture, and that's bringing out these issues, and your progress and where we need to go is important.

So there being no further business before the subcommittee, the dual subcommittees here, we will adjourn this hearing. Thank you.

[Whereupon, at 4:12 p.m., the subcommittees were adjourned.]

APPENDIX

MATERIAL SUBMITTED FOR THE HEARING RECORD

Consumer
Technology
Association

1919 S. Eads St.
Arlington, VA 22202
703-907-7600
CTA.tech

November 24, 2015

Chairman John Mica
Subcommittee on Transportation and Public Assets
Committee on Oversight and Government Reform
2157 Rayburn House Office Building
Washington, D.C. 20515

Ranking Member Tammy Duckworth
Subcommittee on Transportation and Public Assets
Committee on Oversight and Government Reform
2471 Rayburn House Office Building
Washington, D.C. 20515

Chairman Will Hurd
Subcommittee on Information Technology
Committee on Oversight and Government Reform
2157 Rayburn House Office Building
Washington, D.C. 20515

Ranking Member Robin Kelly
Subcommittee on Information Technology
Committee on Oversight and Government Reform
2471 Rayburn House Office Building
Washington, D.C. 20515

Dear Chairman Mica, Chairman Hurd, Ranking Member Duckworth, and Ranking Member Kelly:

On behalf of the Consumer Technology Association (CTA)™, please accept our comments for the record for the Oversight and Government Reform Internet Technology Subcommittee and Transportation and Public Assets Subcommittee joint hearing on the Internet of Cars on November 18, 2015.

The Consumer Technology Association (CTA)™, formerly the Consumer Electronics Association (CEA)®, is the trade association representing the $285 billion U.S. consumer technology industry. Every day, our more than 2,000 member companies are busy innovating; introducing extraordinary products and services and creating American jobs. CTA believes that innovation holds the key to safety for all drivers and is proud that our industry is constantly developing new technology to help make the driving experience even safer.

We appreciate the committees' attention to the growing benefits connected cars will bring consumers. Vehicle technology gets smarter and more connected every day, providing drivers and passengers with a better, safer experience in the car. Soon our cars will be able to provide and share real-time data – like windshield-wiper activity, drive times and outside temperatures – that can keep us safer on the road. The benefits of car data collection and consumption are about to be realized in life-changing ways.

As the technology in our cars advances, we have to consider and balance real privacy and surveillance concerns with the benefits consumers will receive from the analysis of non-confidential or anonymized data. While guarding consumer privacy interests is important, we must not undercut the benefits that data can provide to convenience, consumer safety and the environment.

Producer of
CES

Consider real-time data on traffic bottlenecks or icy road conditions. Other following drivers, public safety and transportation officials would benefit from having this data immediately, so they can act quickly and prevent accidents. Drivers are generating reams of useful information as they traverse our roadways. And car companies should not be handcuffed by outdated government-mandates to limit the sharing of this data.

Potholes – a year-in, year-out problem in colder climates – could be solved more quickly by data sharing. If trailing drivers and city officials had instant access to pothole data, the cars that follow could slow down and avoid car damage and city officials could deploy road service crews faster and more efficiently.

Some data collected by our cars is so valuable to the public good, and so inconsequential personally, that car companies should be encouraged to share it. In theory, cars equipped with onboard navigation systems can identify where collisions can occur and air bags deploy. Maps can and should be provided to local officials showing frequent-accident locations. Unfortunately, most of this data is collecting cobwebs because of ambiguous laws or privacy concerns.

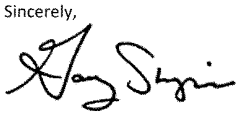
Cars are rapidly changing – in many ways they are indeed our largest mobile connected device. What makes the data gathered by our cars truly valuable is that it aggregates thousands of data points, and aggregated data by its very nature protects privacy.

As our vehicles become more connected and intelligent, manufacturers and service providers will continue to focus on making good decisions about the privacy and security of the information they collect and share. Consumers will benefit most from the advancements that can be achieved through data. CTA and our members are continually exploring these issues and how best to ensure consumer privacy and security, while enabling new technologies to develop and flourish. We believe that industry-driven solutions are the best way to promote innovation while protecting consumers.

In this dynamic and rapidly changing environment, governments should exercise regulatory restraint. Overly prescriptive mandates or technologically biased regulations will stymie growth and become outdated. Government should not attempt to regulate based on hypothetical concerns, but should proceed slowly with targeted solutions to actual problems.

Thank you for holding this important hearing and for accepting the Consumer Technology Association's comments on connected cars and driver privacy. We look forward to working with the committees in the future in this exciting and innovative space.

Sincerely,



Gary Shapiro
President and CEO

○