FTC Connected Cars Workshop: Privacy, Security Issues Related to Connected, Automated Vehicles
June 28, 2017
Segment 1
Transcript

KAREN JAGIELSKI: Good morning, everybody. I'm Karen Jagielski from the FTC, and it is my pleasure to welcome you to our Connected Car workshop that we're doing with our partners at NHTSA. And I'd like to say hello to the folks who are joining by live stream. And let's get started.

So I have to go through a few things in case disaster strikes, so please bear with me. So please silence any mobile phones and other electronic devices. If you must use them during the workshop, please be respectful of the speakers and your fellow audience members.

Please be aware that if you leave the Constitution Center building for any reason during the workshop, you'll have to go back through security screening again. Please bear this in mind and plan ahead, especially if you are participating at a panel so we can do our best to remain on schedule. Most of you received a lanyard with a plastic FTC Event Security badge. We use these for multiple events, so when you leave for the day, please return your badge to event staff.

If an emergency occurs that requires you to leave the conference center but remain in the building, follow the instructions provided over the building PA system. Please note where the emergency doors are, and remember that the closest one might be behind you.

If an emergency occurs that requires the evacuation of the building, an alarm will sound. Everyone should leave the building in an orderly manner through the main 7th Street exit. After leaving the building, turn left and proceed down 7th Street and across E Street to the FTC emergency assembly area. Remain in the assembly area until instructed to return to the building.

If you notice any suspicious activity, please alert building security. Please be advised that this event may be photographed, webcast, or recorded. By participating in this event, you are agreeing that your image and anything you say or submit may be posted indefinitely at ftc.gov or on one of the commission's publicly available social media sites.

Restrooms are located in the hallway just outside the conference rooms. The cafeterias are breakfast, 7:00 to 10:00, break 10:00 to 11:00. It's closed between 11:00 and 11:30. Lunch will be at 1:00, and there's limited meals available-- food available from 2:00 to 3:00. So that's it. Without further ado, it is my pleasure to introduce our Acting Chairman of the Federal Trade Commission, Maureen Ohlhausen.

[APPLAUSE]

MAUREEN OHLHAUSEN: Sorry. Well, good morning, everyone, and welcome to the joint FTC NHTSA a workshop on connected cars. I want to thank our colleagues at NHTSA for co-hosting this event, and their staff for all their hard work and putting it together. And in particular-

- and the FTC staff, as well. I'd like to thank Karen Jagielski, Peder Magee and Kate White from our Bureau of Consumer Protection, Mike LeGower from our Bureau of Economics, and Bill Adkinson from our Office of Policy Planning. I'd also like to thank all the workshop participants for taking the time from their very busy schedules to make this event a success.

Now it's no exaggeration to say that the automobile revolutionized the world. And it changed where we live and where we work and where we vacation. It shaped the urban and rural landscapes of our cities and our farms. It expanded the selection of what we can buy.

But it also destroyed many manufacturing jobs in the stable hand and buggy whip sector. But it created others, like auto mechanic and gas station proprietor. It sparked entirely new industries in gas and oil and steel and rubber, insurance and batteries.

And it affected the law of liability, introduced a major new cause of mortality, spurred innovation in medical trauma treatment, and drove the development of safety features. And it impacted our culture, becoming a literal vehicle for independence and self-expression. And these were radical changes, and nobody, not even in the industry, saw them coming.

Now, there is a story that in the early 1900s, researchers at a predecessor to the German car company Daimler-Benz, predicted that there would be a worldwide market for about 1 million automobiles. Yet in 2015, in the US alone, we had 263 million registered vehicles. Now, even stranger was Daimler's rationale for its prediction. It believed that there were no more than one million people available to be trained as chauffeurs.

So think of that. In 1900, the company didn't think people would drive their own cars. Now think of this. By 2015, 125 years later, they might be right.

So in January, earlier this year at the Consumer Electronics Show, I had my first chance to ride in a fully-automated vehicle. And this ride at the Consumer Electronics Show brought home to me the potential of the next step an automobile technology. So while the story about predicting the future cautions against specific predictions, I think I'm safe in making a more general prediction that connected car technology could revolutionize the world again.

So imagine the possibilities. The personal benefits are tantalizing. Finish last minute reports or projects on the way to a meeting. Squeeze in a nap during a commute. That would be one of my favorite things, because I have a long commute, or do more work, right? Or binge-watch your favorite TV shows together as a family during a trip.

Potential societal benefits are also significant, less traffic, less pollution, faster commuting, easier parking, and better transportation access for people who might have disabilities who can't, perhaps, drive regular cars right now. And I experienced that my own family, where my mother, all her life, has had a very serious vision problem and she's never been able to drive. And so to have the ability to have an autonomous vehicle in the future, that would give someone like her greater independence.

And I think we can expect urban development and population patterns to be greatly affected. And this technology of connected cars really has caught my imagination, and I expect many of you share my enthusiasm. Perhaps all of you, for coming to this event.

Now, of course, fully automated vehicles are only one type of connected car. Many cars today already have connected features, and today's workshop on privacy and data security is intended to cover the gamut of existing and future car technologies. These include cars on the road today with infotainment systems that drivers can sync with their phones, vehicles that can communicate with one another and with nearby traffic lights and traffic cameras to reduce accidents, and, of course, fully automated or driverless vehicles like the one I rode in, and those currently being tested across the country in cities like San Francisco and Austin and Pittsburgh.

Now, every speech and especially a speech about connected cars should have a road map, so here's mine. I'd like to discuss three topics. First, I'll talk about the FTC's history of considering privacy and data security in the connected car and related spaces. And second, I'll describe my hopes for what we'll accomplish today. And finally, I'll detail how this dialogue will develop after the workshop.

So first, how did we get here? The FTC began to look at connected cars when we put together our 2013 workshop on the internet of things. We specifically included a panel to examine the privacy and security implications of this expanding industry and in the four years since that workshop, the connected car space has grown exponentially.

Now, unlike four years ago, today, an overwhelming majority of new cars include connected features. Many also includes some variety of automated driving assistance, such as adaptive cruise control, blind spot sensing, or lane assist. And across the country and around the world, new partnerships between cities, AV manufacturers, and transportation companies have sprung up over the last four years, bringing autonomous vehicles to everyday consumers.

So in Pittsburgh, for example, Uber self-driving cars have been sharing the streets with their human-driven counterparts in September, and more recently, Waymo began offering free rides to the public in Phoenix, and announced that it had logged three million driverless rides, and partnered with Lyft to bring connected cars to the market. And this past April, the National League of Cities issued policy guidance for cities contemplating entering the autonomous car space.

Now, alongside the deployment of new features and innovation, industry has actively considered privacy and data security issues. And in 2014, we saw the Alliance of Automobile Manufacturers and the Association of Global Automakers issue their Consumer Privacy Protection Principles. In 2015, automakers form the Auto ISAC to share information about global cybersecurity risks, threats, and vulnerabilities.

So a lot has changed in just the last four years, which brings me to my next topic, what I hope to accomplish today. Today's workshop provides an opportunity for stakeholders to update us on these new technologies, issues, and methods for addressing those issues. And after I conclude, we'll kick off the discussion with a quick succession of expert presenters. NHTSA Acting

Executive Director, Terry T. Shelton, Jeff Massamilla, Chief Product Cybersecurity Officer at General Motors, and Vice Chair of the previously mentioned Auto ISAC, and Nat Beuse, NHTSA's Associate Administrator for Vehicle Safety Research.

And then, we'll hear from a series of panels. Now, the first panel will focus on connected car technologies. Now, connected vehicles will generate enormous amounts of data, and conservative estimates suggest by that by 2020, the average connected car will generate up to 30 terabytes of data daily. And now, some of this data will be highly personal and sensitive, like real-time geolocation information and biometric data, such as fingerprint or iris recognition to identify the car's user. And the panelists will talk about how cars collect or produce data, and current and future uses for that data.

And the second panel will at cybersecurity issues. Panelists will discuss potential risk to the security of the data collected by connected and autonomous vehicles. They will highlight industry efforts and discuss the role for self-regulation and government intervention, building on lessons from other industries like aviation.

The third and final panel will focus on connected car privacy issues. The panelists will explore how consumer notice and choice operates in the automobile context, and we'll discuss the role of federal agencies, including the FTC, in protecting consumer privacy and data security in connected cars.

Now on this last point, the role of the FTC, I have a few thoughts of my own. Our agency has long been at the forefront of protecting consumer privacy in the connected world, and will continue to do so in the transportation space. Our role is to protect consumers' personal and sensitive information and prevent unreasonable data security practices within a framework that allows continued innovation and growth. And our approach, I believe, is one of regulatory humility, remembering that predicting the future, including future benefits and harms, is very difficult.

Now, the FTC Act directs our focus to actual or likely consumer injuries, and it requires us to understand the likely benefits and risks of connected cars. And one key piece of context for that assessment is, according to the National Safety Council, in the US, approximately 40,000 people died in car accidents during 2016. Connected cars promise to significantly reduce such fatalities, and we regulators must keep that benefit in mind to ensure that our approaches to connected cars do not hinder such a positive outcome. And at the FTC, it means we must continue to work with our sister agencies, like NHTSA, to avoid unnecessary or duplicative regulation that could slow or stop innovation and ultimately leave American consumers worse off.

So finally, where do we go from here? I expected every stakeholder in today's discussion shares a common goal, to foster the development of connected cars while protecting the privacy of consumer data and encouraging strong security practices. And to achieve this goal, we need further work in three key areas.

First is consumer and business education. The FTC provides extensive business guidance and consumer education about privacy and data security. Car companies and other businesses can benefit from reviewing our materials on protecting personal information, our Start with Security campaign contains 10 key data security lessons, and our Careful Connection Guide, which specifically addresses connected devices. In addition to general materials on privacy and security, there may be additional, more specific opportunities for education.

So for example, last summer, the FTC issued guidance to companies and consumers on protecting consumer privacy in rental car transactions. And to rental car companies, we suggested that they establish policies and procedures to delete consumer data from infotainment systems when a rental car is returned. We also offered parallel advice for consumers, and I hope that today's discussion will generate ideas for additional consumer and business education.

Second, where necessary and appropriate, we will use our civil law enforcement authority under Section Five of the FTC Act to take action against manufacturers of connected devices, including connected cars, and potentially service providers. And in the past, we've brought cases involving connected routers, cameras, and TVs. But in the connected car space, we want to exercise our authority responsibly, while avoiding overlap conflict or duplication with NHTSA. And one way to do that is through regular coordination.

And I think we can draw lessons from our substantial experience with health privacy. And in that area, we coordinate frequently with the Department of Health and Human Services, and, for example, we often decline to pursue cases that HHS is itself pursuing. We also work together to provide guidance to the public regarding the agency's respective roles, and so last year, for example, we issued guidance about the laws each agency enforces related to health apps, and such coordinated guidance could be a fruitful area for future connected car work.

And then finally, I would encourage Congress to consider data security and data breach notification legislation to strengthen the commission's already existing data security enforcement tools, and to require companies to notify consumers when there is a security breach. Reasonable and appropriate security practices are critical to addressing the problem of data breaches and protecting consumers from identity theft and other harms. And notifying consumers of breaches after they occur helps consumers protect themselves from any harm that is likely to be caused by the misuse of their data. And these principles apply equally to connected cars.

So that's where we've been, and what I hope will accomplish today, and where we're going in the future. And today's workshop gives us the opportunity to further educate ourselves and the public about connected car technologies, and to continue an important conversation about how we can all work together to best ensure that the full benefits of this technology are realized. So thank you all for coming, and I look forward to today's conversation. Thank you.

[APPLAUSE]

KAREN JAGIELSKI: And now, it's my pleasure to introduce Terry Shelton from NHTSA. Terry is the Acting Executive Director for NHTSA's-- that's it. All right, yes. Sorry.

TERRY SHELTON: Simple as that. So thank you very much, Acting Chairman Ohlhausen. It's a pleasure to be with everyone today. Safety is the number one mission of the Department of

Transportation and NHTSA. That means reducing fatalities, injuries, and the economic costs of motor vehicle traffic crashes. DOT and NHTSA are committed to fulfilling the potential of connected vehicles and other advanced vehicle safety systems to significantly reduce and even eliminate motor vehicle related deaths and injuries. To that end, we have worked hard to address issues of privacy and security.

NHTSA and the federal-- is a federal agency charged with keeping consumers safe from cybersecurity threats to motor vehicles. Privacy is also an important aspect of the public's acceptance of many advanced safety technologies, and for these technologies to improve safety, we need public acceptance. If you've been around as long as I have, you know that seat belts even were not accepted in the beginning. So when we go to something as serious as advanced safety systems, people really need to make sure they're comfortable with these. So privacy's-- it's a really interesting aspect.

Our work on vehicle technologies and now automated driving systems is part of a more than 50-year history of helping Americans drive, ride, and walk safely. In the '70s, '802, and '90s, the focus was largely on occupant protection. Safety belts, airbags, improved front and side impact crash performance, and widespread child safety seat use contributed to sustain reductions in traffic fatalities and injuries. In the late '90s, driver assistance technologies began to make their way into our cars and trucks, most notably, electronic stability control, which is now standard on all new vehicles.

Additional safety advances are now making their way into the fleet, including lane keeping support and automatic emergency braking. When you look at all of these vehicle technologies for the past 50 years, it has led to the lives-- 600,000 lives saved since the '60s. So 50 years-- more than 50 years, 600,000 lives savings from vehicle technologies, and there's so much more.

With automated driving systems, they represent nothing more than a revolution in automotive safety, and it could not come at a more important time. I'm sure you've seen the statistics after a steady decline of fatalities over the years, we saw an increase in 2015 of 7.2%. We now have 35,092 fatalities in 2015. It was the largest increase-- percentage increase in 50 years, so the numbers are going in the wrong direction. We need to do something different.

And what's disturbing is the causes of the fatalities are nothing new. Over 10,000 fatalities involve drinking and driving. 10,000 fatalities involve passenger vehicle drivers who did not buckle up. Another 2,000 were motorcyclists who did not wear their helmets. 3,000 crashes involved distracted drivers. Speeding was a key factor in 10,000 highway fatalities.

So what do all these factors have in common? It's the human. It's the driver. It's choices that someone is making, and in fact, we did a study a number of years ago this still holds true, that 94% of motor vehicle-- serious motor vehicle crashes are due to human error.

That's why automated driving systems are so potentially transformative. They could save tens of thousands of lives by addressing the human factors that cause crashes. NHTSA takes it's federal leadership role on automated driving systems very seriously. DOT and NHTSA are working to ensure the safe development, testing, and deployment of automated driving systems.

As many of you know, NHTSA issued a Federal Automated Vehicle Policy in September 2016, and as promised, the department is reviewing and updating this policy to take into account improvements and recommendations from numerous stakeholders. The new document will replace the previous guidance. It will provide a path forward for the safe deployment of automated driving systems by three things, supporting industry innovation, and encouraging open communication with the public and with stakeholders; by making department processes more nimble to help match the pace of the private sector innovation; and thirdly, to encourage new entrants in ideas that deliver safer vehicles.

Secretary Chao has asked NHTSA to accelerate the process of finalizing this voluntary framework. We're working very hard on that guidance, and I'm surprised they let Nat and Dee out of the building, because we're working on it right now. So when DOT was created 50 years ago, I guess, who would have thought that cyber security and privacy would be such a big part of traffic safety? But these issues have been, and continue to be, central to our work on automated driving systems, as well as other advanced vehicle safety systems.

To ensure a robust cybersecurity environment for these dynamic new technologies, NHTSA has adopted a layered research approach, modified its organizational structure, and is continually developing vital partnerships, encouraging members of the industry to take independent steps to help improve the cybersecurity posture of vehicles in the United States.

An example of this approach was NHTSA's support for the creation of the Automotive Information Sharing and Analysis Center. You all know that as the Auto ISAC. It's an industry-operated environment created to enhance cybersecurity awareness and collaboration across the global automotive industry, light and heavy duty vehicle OEM suppliers, and the commercial vehicle sector.

In 2016, NHTSA proposed guidance covering cyber security issues for all motor vehicles and applicable to all individuals and organizations manufacturing and designing vehicle safety systems and software. NHTSA also recognizes the importance and complexity of consumer privacy. We will continue to work closely with our colleagues at FTC to ensure that advanced safety systems do not place an unwarranted burden on consumer privacy.

I hope you enjoy today's workshop. I think there's some very, very interesting sessions ahead. And on behalf of NHTSA and DOT, thank you for attending and discussing these important topics. Thank you.

[APPLAUSE]

OK so I have the pleasure of introducing Jeff Massimilla. He was named the Chief Product Cybersecurity Officer for General Motors in 2014, and he serves as the Vice Chair of the Auto ISAC, so please welcome Jeff.

[APPLAUSE]

JEFF MASSIMILLA: Thank you, Terry. And good morning, everyone. And thank you to the FTC and to NHTSA for organizing and co-hosting this very important workshop. I'd also like to offer a special thank you to Maureen Ohlhausen, Acting Chairman of the FTC, and Terry Shelton, Acting Executive Director of NHTSA, for your agencies' ongoing leadership in the important areas of consumer privacy and product safety.

The FTC's passion for protecting consumer privacy and NHTSA's firm commitment to safety help guide our industry and truly protect us all. General Motors is honored to participate, and I'm thrilled to be here with you today. That's because this workshop recognizes how quickly the automotive industry as a whole is changing, and that we all have a role to play to make sure that drivers and passengers and everyone on the road remain safe and secure.

I'm also excited for the opportunity to highlight to you that GM is prepared for this rapidly changing landscape of mobility as we know it. But before I go into that, I'd like to share a brief history lesson that is instructive to the challenges that we face today, a British history lesson, dating back, actually, to more than 150 years ago.

The Locomotive Acts, or, more commonly referred to as the Red Flag Acts, were acts-- a series of acts of Parliaments-- require-- of Parliament, regulating the use of mechanically-propelled vehicles on British roads. Responding to the growing use of engine-powered vehicles on ordinary roadways, Parliament wanted to protect everyone, drivers, passengers, pedestrians, even livestock, that might find their way into the path of these clattering, smoking, strange vehicles on the road.

To do so the law had a few main tenants. First, any car had to have three people to operate it, a driver, a mechanic, and a man with a red flag standing out in front of the vehicle to alert everyone that the vehicle was traveling behind him. Second, vehicles could only go four miles per hour in rural areas and 2 miles per hour in the city.

So while these were well-intended rules meant to guide the industry and protect everyone, they eventually proved to be too much. The emerging auto industry shifted from the UK, which had been an industrial powerhouse of the 19th century, to the US and to Germany. So that's not to say that anxieties about new technologies aren't appropriate or that norms and rules for these new technologies aren't necessary. But I think it is a gentle reminder that we need to embrace the future, taking the best from the past to enable the US's leadership in transportation innovation.

At General Motors, the safety and security and privacy of our customers are at the center of everything we do. This applies regardless of whether we are talking about crush zones and breaking distances, in-vehicle infotainment, or cybersecurity. The advent of electric propulsion, the growth of ride sharing, the developments in autonomous vehicles are all truly exciting. And they are major disruptors to our industry that we must prepare for and guide into development, keeping in mind our core principles.

GM has invested heavily in all these areas, even as we continue to develop world class cars, trucks, and crossovers, our core products, to set the stage for the future. As a result, we believe we are well-positioned to lead as we move into this new exciting era of transportation.

We've created an intersection between three very unique areas. First, ride sharing, with our Maven car sharing startup, and our partnership with Lyft. Second, our deep technical capability, which includes the purchase of Cruise Automation and the team developing autonomous technology, our leadership in connectivity in OnStar, and our ongoing investments in advanced vehicles, vehicle systems, artificial intelligence, and cyber security. And finally, our deep experience in designing, engineering, and manufacturing conventional and electric vehicles to the highest standards of quality and reliability.

The integration of these three areas of expertise gives GM a unique opportunity to define the future of transportation both in this country and around the world. And, as this audience well knows, it also puts GM at the forefront of making sure we continue to protect the safety, security, and privacy of our customers.

Back in January, we began a production of dedicated ground-up autonomous vehicles, based on our award winning Chevrolet Bolt EV, an affordable all-electric vehicle with 238 miles of range. So far, we are the only manufacturer to assemble self-driving vehicles in a mass production facility. To date, we have completed the production of 130 Chevrolet Bolt EVs equipped with our next generation of self-driving technology.

These vehicles will join more than 50 first generation self-driving Bolt EVs we already have deployed in test fleets in California, Arizona, and Michigan. We are putting the autonomous Bolt through a demanding testing program, which includes Cruise testing on city streets, and we're doing it with safety and security absolutely top-of-mind.

To help bring these challenges to life, I'd like to share a short time lapse video with you of an AV drive on the streets of San Francisco-- as many of us know, one of the most complex driving environments we face. This drive was done with zero driver takeovers, as you can see by looking in the lower left corner of the screen and watching the steering wheel. You'll see the Bolt AV navigating construction zones, pedestrians, bicycles, other vehicles, a double-parked truck, and even wildlife. Yes, wildlife in San Francisco.

But that's all in normal day on the streets of San Francisco, and I think it illustrates the reason we need to test large fleets of autonomous vehicles safely and securely in real-world conditions. We couldn't reach the same level of competency in such complex situations by testing in suburban environments or on our Proving Grounds. So let's check out the video.

[MUSIC PLAYING]

Now, that's pretty exciting. And actually, I'd say, the only thing I think that's more exciting than watching that video-- and I still get a thrill every time I watch that video-- is I had the opportunity to ride in one of these vehicles a few weeks ago in San Francisco, and that's a truly amazing experience. And I do have to point out, also, that my youngest daughter at home was a very, very happy that we saved the life of the raccoon in San Francisco.

So in addition to reducing deaths from crashes caused by driver errors, broad adoption of self-driving vehicles has the potential to reduce congestion, to supplement public transit systems, to provide connectivity between city and suburbs, and to facilitate, as was pointed out by Chairman Ohlhausen, a doorstep-to-doorstep mobility for elderly and disabled residents.

As I said, autonomous vehicles can provide many benefits to society in terms of convenience and quality of life. Most important, however, is, of course, safety. In 2015, traffic accidents costs more than 35,000 lives in the United States. That is the largest annual percentage increase in deaths per mile in a half century.

In addition to the great tragedy of lives lost, the total economic and societal loss from motor vehicle crashes is approximately $871 billion per year, according to NHTSA. That's an astounding figure, and it doesn't need to be that way. NHTSA has also estimated that 94% of fatal crashes involve driver behaviors or errors, errors that autonomous technology has the potential to reduce, or perhaps even eliminate.

We believe the social benefits and business opportunities of autonomous vehicles will be significant, and with the technical leadership of Cruise Automation, we intend that GM will be a leader in their development and deployment. But one thing we fully acknowledge is the rising concern regarding safety and privacy as our vehicles become even more connected.

In 2014, the participating members of the Alliance of Automobile Manufacturers and Association of Global Automakers collaborated on a set of seven proactive privacy principles that serve as the core privacy commitments for OEMs and suppliers developing in-vehicle technologies and services. GM is proud to have been a key architect in developing these commitments. And as the automotive industry continues to bring new and exciting technologies and services to our customers, we must continue to recognize our responsibility to act as thoughtful stewards of the information that can be created and collected from our vehicles and their connected systems.

To that end, GM's Privacy Program implements privacy by design principles to reflect these commitments and responsibilities. And while the type of information generated by a vehicle can vary by make, model, model year, or even an individual's usage of that vehicle, the vast majority of the data is neither transmitted outside the vehicle nor retained permanently in the vehicle systems. In other words, it's used for decision-making on the vehicle.

GM continually seeks to improve the channels in which we communicate our data practices to consumers, an edict firmly rooted in the privacy principle of transparency that is so critical in establishing consumer trust with evolving technologies. Going one step further, at GM, we believe that safety, security, and privacy of our customers is further enabled by a robust cyber-- product cybersecurity strategy. So in order to better prepare for these new reality of the connected services and technologies, we have developed and implemented such a strategy.

GM was the first major automaker to create an integrated and dedicated Global Product Cybersecurity Organization, now nearly three years ago. I lead that product cybersecurity team, which is well-funded, well-resourced, and deeply integrated into GM's product development process, and extends to the testing and development of Cruise on autonomous vehicles.

Our cybersecurity organization is global in reach and comprehensive in scope. We look at threats from end to end, from the back office to all aspects of the physical vehicle itself. Further, we have re-engineered our vehicle development process to include cybersecurity considerations from the earliest stages of vehicle design. In other words, we're designing cybersecurity into our vehicles from the start, rather than building-- working solutions into our cars and trucks that we've already built.

The vehicle attack surface is large and complex. A breach of any unprotected system would likely have undesirable consequences. Therefore, we employ a defense in depth approach, putting multiple layers of protection in place to defend the vehicle and its systems. We've developed threat monitoring, detection, and response capabilities, and we have a robust incident response plan, which we continue to vet, test, , and rework through several tabletop exercises and real-world incident responses each year.

We scan and test systems throughout the development process and after the vehicle launches to manage vulnerabilities. We have our own internal red team, which conducts regular penetration testing of all of our vehicle programs. We also rely on third party expertise and even the research community through our Coordinated Disclosure Program. Because it's not a question of if our industry will ever see a serious cyber incident, but when. And when that breach occurs, a successful response will depend on how prepared we are to deal with it.

This highlights the importance and value of solid working relationships with and regular interactions with agencies like the FTC and NHTSA. Our open lines of communication and collaboration come in many forms, communicating directly with the agencies, participation in the Auto ISAC, and GM Security Vulnerability Disclosure Program. With this program, researchers now have an easy-to-use, clearly-defined process to find vulnerabilities in our systems and vehicles and to alert us when they do. And it's amazing how good they are at it. We've had many actionable submissions thus far, and it's gone a long way toward helping us maintain our cybersecurity leadership in the industry.

Defending against cyber attacks requires collaboration like this among all stakeholders. There are very real benefits to building partnerships across the automotive ecosystem, and with the industries outside of ours. There are great opportunities to learn from aerospace, defense, the consumer electronic industries, and in turn, share our learnings with them.

I think it's also important to recognize the great work being done by organizations such as NIST, SAE, and ISO, just to name a few-- which I know a few are on the webcast here today-- which are setting standards and guidelines to help shape our collective efforts in vehicle cybersecurity. We also recognize the importance of cybersecurity not just as a company but as an industry. A cybersecurity issue for one of us affects all of us. That is why we support and are fully committed to implementing the NHTSA Best Practices for Cybersecurity, published last year.

Also GM, helped form the Automotive ISAC in 2015, and today, member companies account for 99% of the vehicles on US roads. It includes OEMs and partners, and we've recently added members of the heavy trucking industry and the commercial sector. Members of the Auto ISAC share cyber threat intelligence and known threats, practice incident response activities, and are working together to develop a comprehensive set of cybersecurity best practices for the automotive ecosystem. Members interact with their peers, key stakeholders in the government, and others in the community, inside and outside the automotive industry. A very important point to stress is that the auto industry has taken steps to address cyber concerns before our customers experience a serious cyber incident.

The global auto industry today is changing faster today than it has in 100 years. Many facets of the traditional industry are being disrupted, and this creates exciting new opportunities to rewrite the rules of vehicle use and ownership to benefit our customers. It is essential that leaders from a wide cross-section of industries, from automotive to defense to aerospace, work together with government, law enforcement, academia, research, and the cybersecurity community to develop proactive solutions to the cybersecurity challenges we all face.

I hope that the US government and the rest of our colleagues in the auto industry will continue to leverage our collective strengths and institutional knowledge to protect our customers and their privacy each and every time they get into their vehicle. Let's move this industry forward together into a new age. Thank you.

[APPLAUSE]

TERRY SHELTON: So I have the pleasure of introducing Nat Beuse to the stage. He's the Associate Administrator for Vehicle Safety Research, which means he's in charge of vehicle safety research at NHTSA, including the Vehicle Research Test Center out in Ohio.

NAT BEUSE: Good morning. Thank you, Terry. See if we can get slides going before 11:00 AM. So normally not my style, but we'll see what we can do to liven things up.

So I think one thing that can't be understated is, why in the world are we focused on this in the first place? I mean, you guys have heard all morning about the numbers. You heard about them going up. Those are all good reasons, but take a look at, also, what's been happening for the past, let's say, eight years or so. We've kind of plateaued.

While we made great progress and we've implemented a lot of safety technologies, you've heard some of the numbers that spoke to that, but we actually plateaued, and that's one of the reasons that we're so focused on some of these new technologies. And so what I hope to do through my talk is actually just explain what the heck all this stuff is, because already this morning, I've heard about, I don't know, nine or 10 different terms for what is generally called the suite of these technologies.

I think the other thing to point out is this curve is not static, meaning that there are huge predictions about how many elderly folks are going to continue to drive, because vehicles maybe become that much easier to use, et cetera. So I think this is kind of a wake up call for all of us that we're already facing what many people describe as a crisis, really, as an epidemic, and we're going to add more to this with more drivers continuing to drive later in their years, and so this is really something that we need to focus on. And while technologies all have challenges, we cannot forget this picture.

So technology can help. One of the things that we've been doing at the agency is trying to get early indications on what are the technologies that are actually working, and trying different ways to get those technologies deployed. I have listed a few here. That first category at the top is what you would call moreso warning systems, right? The driver gets some information and they're expected to act.

We're kind of reaching the stage, though, where those are becoming more mature, and we're actually leading to a stage where some of these technologies will actually start to perform some sort of automated function. So for our part, what we've been doing is trying to highlight for consumers when we have information that show they're beneficial that they actually look for these technologies in their vehicles. But one of the challenges that we've faced is that, for a long, time people understood kind of crash protection, right? It used to be a joke about people going to dealerships and saying, I just want to know how many airbags this thing has, and if that was some measure of safety.

So consumers understand that sort of self-protection. They really don't understand that they need help driving, right? Everybody in this room, I'm sure, is a perfect driver. It's everybody else. And that is part of the challenge, is getting consumers to understand that it's OK to get help from some of these assistive type technologies.

But we're not alone in that. I'd have to say, there's been a kind of a coalition of the willing between government and industry working together to really push on these technologies. We had this very historic announcement with the auto industry and with the insurance industry, really highlighting that when we find stuff that works, how do we get it into the fleet faster?

And one of the things that the auto industry agreed to was actually outfit the majority of the vehicles for sale in the United States with something called Automatic Braking Technology by 2021, which was well in advance of anything that we could probably do as a regulatory approach. And likewise, probably much more advanced than what we could have done through some sort of ratings programs. And it is to say that the industry is behind all of this and behind supporting the deployment of these technologies when they work.

The other thing that we've been doing is focused on this sort of self-driving or highly automated vehicles. And one way that we've done that is with the Federal Automated Vehicle Policy, which was our attempt at trying to help guide the industry for looking at ways to make safety part of the vernacular, not just running around talking about how many miles they drove, as if that was a good measure, but really concrete measures of safety. Why I bring it up here, because one of the elements that we asked folks to think about was privacy.

Another one was cybersecurity. Those two pieces, no matter who you talked to in the automated vehicle space or self-driving space, those two things always come up, right? Everyone's always talking about, oh, you know, the car that's going to get thrown into the Jersey wall because some 16-year-old kids somewhere else hacked his vehicle and did some bad things.

I think that for our part, what we want to see happen is industry continuing to push on the levers that they're already pushing on. You've already heard about the ISAC. You've heard about best practices. Those are all good things, and they need to mature and they need to continue to evolve, and the ecosystem has to grow. But these are all ways in which sort of industry and government are really working together to really work on these problems.

So terminology is important. It's kind of funny because one of the small things we did, we thought, in the policy, was adopt the SAE definitions for automated driving systems. And it sort of seemed like a no-brainer to us, but there was so much discussion before that about competing definitions and no one understands the levels, and what the heck does all this stuff mean, so I'm going to attempt to explain this in very simple fashion.

In these lower levels, we'll call them zero, one, and two, there is no self-driving. The driver is supposed to be on the driving task, paying attention to the roadway, not texting and driving, et cetera. Those are technologies that are on the road today. You can go to a dealership. You can get those technologies today.

And in the lower levels, we would say most of that stuff happens in the background, meaning that there is a difference between a safety system like automatic emergency braking and something that's more like adaptive cruise control. For the public's mind set, they don't understand that distinction. In our minds, as a safety agency, there is a big distinction between, let's say, those two technologies.

One only activates if you're in an event, no matter how you get there, whether you're distracted, it doesn't matter. The technology is agnostic. That's why it's so promising, is because it activates no matter what. The other one is more like a convenience feature. You have to push a button and the vehicle takes over some part of the driving task. But those lower levels sometimes get confused with, quote unquote, "self-driving." So I'm here to tell you that's not true.

When you to make the leap into-- and it is a leap-- from level two into level three, in a level three vehicle, this is where the system is sent telling you the driver, OK, driver, you can tune out for some period of time. Read a book. Do whatever. The vehicle will handle the scenarios that it's supposed to be designed for.

Meaning that it's not ubiquitous, everywhere, it doesn't mean that the system can operate at night time. Doesn't mean it can operate in the daytime. It doesn't mean any of that. And it's all vehicle-specific or system-specific, so you can have a system at a level three that only operates on Monday, Wednesdays, and Fridays on a five-block radius, and everybody should be OK with that. That's OK. It's when it goes outside of that, that's when we have to worry.

When you go up to level four and level five, this is where you have more sustained, and there is no fallback to the driver. Let me say that again. In level three, if the system encounters a situation what we call the fallback condition, or a safe state is it could be given back to the driver. So the driver still has to be paying attention. IN four and five, that's not the case. And that's why you see, in level four, here, we've kind of shaded out the steering wheel to show that you kind of don't need it, in some cases, or you may need it in some cases, depending, again, on the design domain of that vehicle.

And then with level 5, it's sort of what everybody thinks about self-driving, that's the, I'm getting in the back seat of my car. That's, I'm binge watching Breaking Bad. It's whatever you're doing, but that's what the public imagines when we talk about this stuff. And I think that's why we have to be very careful about making sure, whether we're talking about cybersecurity or whether we're talking about data, that we're also being very clear about what level of technology we're talking about. Because they are very distinct and they're very different.

So a little bit about what's going on out there, because all of these technologies are being talked about all the time. For the most part, I would say a lot of focus is being placed on what I would call on-board technologies. This is sensors like cameras, sensors like radar, sensors like ultrasonics. That suite of sensor technology is what's driving for collision warning, automatic emergency braking, those lower-level systems. We had this other thing called V2V, which is really what I would broaden out to be just communications technology in general. And I'll talk a little bit about that later.

The bar represents not some sort of absolute number, but sort of what's really happening out there. So we have a lot of systems that are on the kind of on-board side, maybe a few systems that are on the true connected vehicle side, that are dealing with safety, not telematics, safety. And then this idea of self-driving, which is a different set of sensors, let's say. Might involve map data. Might involve something that's not invented yet.

And we're at this many on the road right now, right? There's a lot of testing going on, but you can't go to a dealership and buy one. I think the other thing that's unique about this is the possibility of how these technologies will be deployed, right? The first two are very much, you go to a dealer you say, I want this car with these technologies.

What we're starting to see, and Jeff talked about this a little bit, is sort of this kind of regional deployment phenomenon going on, where maybe these types of vehicles only show up in certain cities, maybe in certain states, depending on, again, the operational conditions that the vehicle is designed to. But again, as policymakers, we have to keep a watchful eye on this, because we're not in the business of picking technology winners and losers, but we want to make sure that all of these technologies get out there if they're going to save some lives.

So I don't expect you to read all the words on this slide, but this is really just a sample of if you were to go to a dealership today and say, I would like some safety features dealing with crash avoidance, what you might find. And so and this covers the gamut, right? There is everything from warning systems, which have been on the market for about eight to 10 years, I would say, give or take, to what's coming on now within the past six years, really, a kind of a full pace is the braking stuff.

Those systems, yes, while they are incorporating data from their environment, they're-- they all have cameras, right? Some use cameras and radar, some only use one or the other. Some use ultrasonics. All that data, yes, is on the vehicle. Sometimes the systems are integrated with each other, sometimes they're not.

One thing to keep in mind, though, is it's not to say that all this data is actually being actively stored on the vehicle. It's one of the things that we continually have to educate folks on is that just because a vehicle has a camera that's looking at the Ford roadway, it doesn't mean, automatically, that that vehicle is recording every license plate and taking that data back to some back-haul and doing something with it. As the Chairman mentioned, there's all sorts of estimates out there about how many trillions and billions of terabytes of data are going to be out there.

But it's important to note, again, why is this happening, right? If a vehicle is going to take a breaking maneuver, it needs to know what's in front of it, right? So it needs to have that camera. And if a vehicle is going to be smarter about that, meaning needs to avoid a scenario where it's not a Coke can in the middle of the road, then it might need some additional data, and it might need to classify that data.

And it might need to do some algorithms to figure out, OK, I think I've seen this can before. It's really a can and not a kid in the roadway. And so when you manufacture and are integrating these technologies, there is a lot of discussion about data. But it's not to say, again, that all this data is being recorded and shipped off.

Now, you will open up the paper and you will read, just like, I think two weeks ago, a certain manufacturer said, indeed, that's what they're doing. But that is very unique, and that is a very specific case with a very specific platform. If you think about 17 million new vehicles a year. If every vehicle had that capability, could you imagine the amount of data that would have to be taken somewhere and the amount of infrastructure necessary to do that? I think we need to keep all that in mind as we're talking today about really drawing these distinctions between what one manufacturer may be doing and not implying that it's kind of the whole universe is doing that.

The other thing to point out about this slide is these same technologies are also becoming quickly available on commercial vehicles. So at NHTSA, we're not just focused on light passenger vehicles. There is a lot of benefit to be had on the commercial side with respect to these technologies, and that's really important, because there, the operating environment is completely different. In that environment, most of those fleets already have some sort of safety management process, they have lots of data that's being taking off vehicles from all sorts of sensors, not necessarily the safety ones, to manage the driver and to manage the safe operation of that vehicle.

So again, I think when we talk about these technologies and data that's on vehicles, it only helps that we clarify what we're talking about, whether it's light vehicles, commercial vehicles, because consumers are understanding what we're saying, and if we're not careful, we're going to confuse them. And we lose all the benefits that we're trying to get.

So a little bit about communications technology. So I've kind of broadened this out to be more than just what people generally think about when NHTSA talks about communications technology, because generally, we're talking about vehicle to vehicle, vehicle to infrastructure, which is a very specific technology known as DSRC. But for the purposes of this meeting, I thought it would talk about the two flavors that are going on, really.

So one flavor of communications technology is truly, we'll call it, hard core safety. Now, some are saying you can do that through DSRC. Some are saying you can do it with cellular technology. I'm not here to debate the two merits of those, but what I'm here to say is there is a place for those technologies in the safety realm. The risk will be different, of course. The data will be different, of course.

But when you look at a picture like this, if you're not an aficionado, one might say, oh, my gosh, these vehicles are shipping off data every three nanoseconds, and it's my whole life history being shared with another vehicle. Again, some of that is a bit of a myth because it doesn't actually operate that way. I think the other thing to point out is that when you look at the cellular side of what we call communications technology, some of these are opted-in services, meaning that if you want to sign up for a concierge service where you can buy movie tickets or whatever, the amount of information that is in that transaction is different than what would be in a safety transaction.

And so, since I'm the safety guy, I focus mostly on the safety side of this and really looking at what is the data that you would need in order to even make a system work correctly, right? How do you make two vehicles talk to each other or talk to the infrastructure such that they're exchanging the necessary amount of information, not too much, but the necessary amount of information in order to make a decision. Do I warn this driver or not?

The other thing to point out is this technology is not really the same as pairing it with the on-board stuff. That's an important distinction, because the term connected has kind of grown in meaning over the last couple of years. That's not to say that they're in competition, but it's to say you can have either or, in most cases, you probably want both. I've never met an engineer that says they want less redundancy. And so, I think it's important to note that the way that this data would be treated, and the way that the manufacturers are using this data is going to be different than how they're going to use data from their own sensors.

And then last but not least is this sort of category of automated driving systems. And I threw this slide together to really point out a couple of things. None of these are production vehicles, even though some of them try to look that way. It's to point out that nobody knows, yet, what the sensor suite is going to be needed for in these vehicles. So there's a lot of experimentation going on.

Most of these vehicles are all focused on the higher levels, three, four, and five. But even in that scenario, it's still really unclear exactly, are you going to have map data or not? Are you going to have this Kentucky Fried Chicken bucket on top of the vehicle or not? Are you going to have some super sleuth technology that's not even built yet or not?

So I think in order to have a reasonable conversation about these vehicles, whatever data they might have, and whatever security risk they might have, we have to keep in mind that they're not here yet. There's a lot of testing and development going on, which needs to happen. Jeff mentioned that it needs to happen on public roadways. Completely agree. The department is fully behind that. That's one of the reasons why we put out the policy.

But when we were talking about the future and we're trying to explain this to consumers, if we start by-- the conversation by saying, this vehicle knows every map location you've ever been at, and oh, by the way, knows where your kids go to soccer practice, et cetera. We don't know that, yet.

There's just right now, as in any testing scenario, there is a lot of sensors, more so than one would probably normally have in a production vehicle, to drive the software development, to drive the validation, all those things that need to happen. And I think what's been interesting for me to watch is over the past, let's say, five years or so, or eight years, a lot of the testing that's been going on, if you look at previous technologies, would have been out of the public eye.

And so that's what's happened is you would see-- I'd go to Michigan all the time. You'd see lots of test vehicles running around with all sorts of things on them. No one's talking about that because no one was talking about self-driving automated driving systems. But now, the public is fully engaged in this conversation, and they understand that these test vehicles are running around. And I think there's a lot of jump to conclusions being made about well it's going to be that vehicle and it's actually going to look like that.

I wish I had a time lapse photo to show kind of how some of these vehicles have morphed from what you would see that bottom left there, which is really interesting looking vehicle, all the way up into what Ford just showcased last year. So I think we need to keep that in mind, and I'm sure the panelists will talk about that when they get talking.

So the last thing I'm going to end on is cybersecurity. So cybersecurity is something that is constantly moving. You're never done with it. I've had a lot of conversations with the auto industry about how are we going to address cybersecurity. And again, I'm going to focus on cybersecurity dealing with safety. So you already heard all the things going on with the ISAC and the best practices and all that good stuff. What I'm going to talk about is something a little bit different.

What I'm going to talk about is the approaches to dealing with cybersecurity and why it's relevant, regardless of whether we're talking about current technology on the road today, communications technology, or ultimately self-driving. It would be really hard-- I would say, impossible-- if the entire industry and the government went around and tried to tackle every entry point into a vehicle. This is not even everything that's there, right?

There's aftermarket stuff that consumers can buy, there's these insurance dongles that if you put them on your car, you might get a lower rate. Those are all things that the customer controls, right? The customer is the one that can go get or choose that and put that on their vehicle. You can go to the App Store and buy some app that connects to the OBD port and talks to your phone and also gives some information or might transmit your data somewhere else.

But for us, what we've focused on is rather than trying to police innovation is really kind of go back down to basic principles. It's the vehicle's responsibility, at some point, to deal with all these entry points, and Jeff talked about that a little bit in his talk, but I'm going to expand on it. You could put up here cameras. You could put up here infotainment systems. You could even put up here how someone could jury rig GPS and make the cars think it somewhere else. All true, right? If you read the literature all that stuff is probably possible.

But how the vehicle responds to that is what really matters, right? It the vehicle understands that it's doing checks within itself to know like, hey, my camera is seeing this, but the GPS is telling me I'm going somewhere else, then I probably should ignore one of those signals. And the manufacturers are generally looking at those integration techniques right now to sort of figure that out.

I would say that one of the things that we're focused on is how to detect whether you've been intruded or not. That seems to be something that's very promising. So how do you know someone broke in your house, right? You go in and probably door's busted open or the window's broken or whatever. It's really hard on a car to know when your car's been broken into. For a long time, they've not been designed with sort of that frame of reference.

And so what we've done in collaboration with the auto industry has really come up with this sort of in-depth-- cybersecurity in-depth approach where you have multiple layers of defense, and you really focus on guarding against all those different layers, versus running around trying to figure out, how am I going to safeguard TPMS? What am I going to do about the OBD port, that everybody is concerned, about we're concerned about? If you focus just on that, you're going to miss a whole bunch of stuff.

So I think the other thing we'll have to figure out is how to educate consumers. I think there's a misnomer with the public that the OBD port was designed for what it's being used for. That port was initially designed, and it's still designed, really, as what it says, a diagnostic port. You're supposed to be a technician, or if you're a hobby shopper and you've inputted some chip in your vehicle to get extra performance on the racetrack, whatever you did, that port is designed for that, and it's really an emissions port, on top of that.

Over the years, it's grown to provide more information. And because of that it's actually unleashed another set of innovations where people have figured out like, hey, if I can collect this data, I might be able to write an algorithm to do some cool stuff with it. That's perfectly fine, but what we need to figure out is how do we safeguard that port, now?

And it's good that we've been talking about this, because the auto industry is already proactively looking at, how did they do that? Right? How do we make sure the right people are accessing and making changes that they're supposed to? How do we make sure that the port maybe rejects certain things? Those are all conversations that are actively going on right now.

So while in the public's frame of reference it seems like, oh, my gosh, nothing's happening. I can tell you behind the scenes, there is a lot of work going on. We're trying to figure out how to guard just that port, and in general, on cybersecurity across the board. Because this is not something that we can fall asleep on, because if we do, the benefits from these technologies, we won't see.

And so I know there's a whole plan on cybersecurity. And I know people are going to talk about different issues. But again, it's important to note, safety versus something that might be more privacy-related, because that's an important distinction when we talk about to the public, which is who we want to adopt these technologies, that yes, there are concerns across the board, and there is work going on both fronts, but we need to make sure we're clear about safety versus privacy.

So with that, I'll stop and wish everybody a good conference.

[APPLAUSE]

KAREN JAGIELSKI: OK, folks we're way ahead of schedule, so why don't we just all take-- we can take a break now, until 11:45. We'll get back on schedule. The cafeteria, which is down the hall, closes at 11:30-- from 11:30 to 12:00, so if you want coffee or something from there, you should go right there. So see you back here at 11:45.