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

- 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.

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 cruis

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 єrashltsocnd '95(p)-3. wmnd s and(a)4(nve)4(n wa)4(dva4(c) a)4(e)-6(y)20(d0(w)2(a)4(l)-2(k s)-1(a)4(f)3(e)412

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.

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

es3 0 Td5.66-1(,)-1hnde0 Tw 9.01s2.27-1(,)-1d

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.

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.

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

practices. Those are all good things, and they need to mature and they need to continue to evolve,

And then with level 5, it's sort of what everybody thinks about self-driving, that's the, I'm getting

But when we were talking about the future and we're trying to explain this to consumers, if we start by--

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

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.