FTC Connected Cars Workshop: Privacy, Security Issues Related to Connected, Automated Vehicles
June 28, 2017
Segment 3
Transcript

SPEAKER 1: [INAUDIBLE] sorry.

KAREN JAGLELSKI: Here we go. [INAUDIBLE] no, it's not. It's panel two.

Sorry, it's been a long day. I do want to know off right off the bat that one of our panelists Joseph Saunders had a personal emergency and had to lead. Laurence Smith from the future of privacy agreed very kindly to step in her place.

SPEAKER 2: About 90 seconds ago.

KAREN JAGLELSKI: She said to me, when is this, and I said, now. And she very graciously took the bait. So I'd like to introduce our folks. So sitting with me is my colleague Alain Sheer.

He's also an attorney in the Division of Privacy and Identity Protection. Our distinguished panelists are Syed Hosain from Aeris Communications. And then next to him, we have Meg Novacek.

She's executive director of business development North America for Argus cybersecurity. And next to her is Dr. Miroslav Pejic an assistant professor in the Department of Electrical and Computer Engineering at Duke University Beside him is Marc Rotenberg, president of the Electronic Privacy Information Center. And--

DAVID SCHWEITERT: David.

KAREN JAGLELSKI: David-- we didn't get to meet earlier. And there's David Schweitert from-- he's the executive vice president of federal government relations and public policy at the Alliance of Automobile Manufacturers. Did I get that pronunciation right?

MARC ROTENBERG: It's perfect.

KAREN JAGLELSKI: Excellent. You were one of the ones who didn't reply to me, so I had to kind of wing it.

MARC ROTENBERG: Like to keep you on your toes.

KAREN JAGLELSKI: When you have the last name Jaglelski, you think about these things. And then next to her is the star of the hour, Lauren Smith from The Future of Privacy. Lauren is your-- what is your official title there?

LAUREN SMITH: I'm policy counsel, and I run our Connected Cars project.

KAREN JAGLELSKI: And she also is the author of this amazing infographics that was outside and apparently has gone-- I've been told has gone [INAUDIBLE]. So anyway-- so thank you so much and thank you all for joining us. And we're going to start questions with you, Dr. Pajic. So we heard Nat Beuse from NHTSA talk about the attack vectors present in modern day vehicles. But who are the attackers and who is it exactly that we're worried about?

MIROSLAV PAJIC: Well, first of all, thanks a lot for organizing this and I'm very happy to be here. So I would like to start with a [INAUDIBLE], but pretty much who isn't. From a few years ago when a group of grad students was able to hack into a car and show how if you get access to the OBD port, you can easily attack the vehicle.

Or if you mess up with the meta data on a CD drive, you can actually also take over the car completely. Then it was like, OK, if you just have physical access, you can access-- you can compromise the vehicle. Then it was easily shown how you can do that over the air.

So pretty much we do have from one side a standard threat of hobbyists who are doing that for whatever particular reasons. But we also have a way more serious situation where imagine if you find zero day exploit in most of the vehicles manufactured by one manufacturer or one of the OEMs. You would pretty much be able to launch a large scale attack and take over control over hundreds of thousands of vehicles at the same time.

So you do have this problem of security in vehicles also as a part of the national security efforts to address. And one thing that a lot of us don't want to directly admit when it's related to the security research, but we've seen in other domains people selling zero day exploits to other companies and people with financial interests that then would hedge their bets on the market against the security vulnerabilities there. So there is also that aspect of financial gain by either ruining a reputation or things along those lines from a certain common factors. And something along the lines of what was discussed this morning-- as the level of autonomy rises in these vehicles, we pretty much have to worry about the problem more and more and not only consider different attacks vectors but assume that the attacker would be there at some point and how can we design these systems to provide certain level of safety.

MEG NOVACEK: I'd like to add too. I think if we look at the evidence from other sectors, ransomware, it is very likely to be expected in automotive as well. I mean, just in the last month, two very large ransomware attacks-- so we need to be prepared for that.

KAREN JAGLELSKI: On automobiles?

MEG NOVACEK: Enterprise. I said other sectors.

KAREN JAGLELSKI: Oh, OK, yeah.

[INTERPOSING VOICES]

MEG NOVACEK: Right, yeah, if we look at what's happening in other connected systems, it's logical to expect that that would be happening-- or some people would try to do that in cars.

KAREN JAGLELSKI: So the range can be anywhere from nation state actors to everyday miscreants who want your data.

ALLAIN SHEER: You mentioned that people can sell exploits that they find. How well organized is the market for the sale of an exploit so that what you would have is kind of a super hacker who would figure out how to break into something, whatever it might be, and then package and exploit and be able to sell it to lesser skilled people? So how effective is that market? How big of a risk is there here?

MEG NOVACEK: In automotive, I still haven't heard about examples like that, but we've seen that in the domain of mobile computing. We have seen that in the domain of medical devices. So it's just a matter of time before we hear something like that in the automotive domain. Pretty much everything that has happened first in the cyber domain then moved a few years later in the embedded domain and now in the cyber physical systems domain. So my opinion, it's just a matter of time before we hear things of this sort.

KAREN JAGLELSKI: But what would the skill level-- so you hear these things, and I think we've all seen stories in the media about various hacks. How skilled does a potential hacker have to be?

I mean, does it need to be someone like you, people on this panel who have PhDs? Or can it be a dedicated hobbyist? I mean, what level of expertise do you need to do a successful hack?

MIROSLAV PAJIC: So first I would-- in federal building, I would like to say that I never was involved in such activities. And hopefully, that's on file. Second--

KAREN JAGLELSKI: It's been recorded.

MIROSLAV PAJIC: OK. That being said, it's getting easier because a lot of-- so 10 years ago, you would not-- it'll be very hard. You will have to go back-- if you wanted to access data from the OBD port, you will actually have to trace back the protocol and you will actually have to figure out what's going on.

Now you can buy these devices online. Now there is like shared libraries that you can easily use and easily get access to data in real time. So pretty much previously, you would have to understand for a specific vendor what kind of protocol is being used, what are certain bits meaning in these messages, how if you want to reprogram-- if you want to reprogram drivers on some particular device on the bus. What do need to do now?

That information is out there. So we cannot think and we cannot use the same approach as 10 years ago that the attackers are not aware of these things and that they don't have the knowledge and time and resources to do these kinds of things. Again, I wouldn't also like to be very-- start this on a very negative side, but we do see attacks in other sectors, in smart grids, in-- well, not so smart energy system in Ukraine.

But pretty much it is just a matter of time before large scale attacks occur. And the fact that these systems are open to the network and they use in most cases this kind of gateway base approach to security is allowing attacker, once it gets access to any of the devices inside the vehicle, to actually be able to wreak havoc. So at this point, I don't really expect it within the next six months or up to a couple of years we see a large scale attack on vehicles, let's say, in US. But it wouldn't be very surprising if a thing like that happens.

SYED HOSAIN: Let me add a couple of thoughts to that. One is that cars are becoming incredibly complex today, and the fact that there is communications pathways into the vehicle provides the opportunity. What may have been an OBD hack which still requires physical access to the vehicle is changing and evolving.

And it's now going to be access through the communications protocols, whether it's short range like the DSRC systems or long range like the cellular systems that are built into connected cars today. We have connected cars in a network that had been already running around for the past 10, 15 years-- 20 years in some cases. And in our network, we have companies have deployed connected cars doing exactly the kind of accesses that allow people to hack in.

What has protected them so far is, A, a small community. It's not billions of computers around the world or however many there are. It's smaller groups, number one, of connected cars. But that's changing and evolving and it's only going to get worse when you have autonomous vehicles out there that have much more complex systems than that are there today. And the potential for creating large scale attacks just goes up.

And it's going to happen. There is no such thing as perfect security. It's going to get-- again, somebody mentioned it this morning and I think it was mentioned again. It's not if-- it's when. And the question is when.

There's an organization called FASTER which is the future of automotive technology security-- sorry, Future of Security Technology Research. We had a meeting in March earlier this year where I made a prediction which I thought was rash that there would be a ransomware attack on a car by the end of this year. So I think it might be sooner than was mentioned. Will that happen? I certainly hope not, but it certainly could based on the complexities of the cars that are out there today.

KAREN JAGLELSKI: Meg, I thought you had-- yeah.

MEG NOVACEK: Going back to the question of how difficult is it, it's really in phases. So the first attack of a certain style will take an expert. It'll take them many months of research and a whole team. And then as Miroslav said, once that information is public, it will become easier and easier as people create a how-to booklet. But that's why what Jeff and Nat said earlier today is really important.

It's important for the community to monitor what's going on so we can detect and then immunize the fleet. And so that is one of the things that-- I know Jeff mentioned that, the GM intrusion

detection and monitoring. Argus also offers such products and services. So you know, maybe there's the first attack.

If we take a center for Disease Control type of mentality, there's patient zero and maybe patient two or three. But then we detect that campaign and we can immunize. So even if there's a how to manual, we have a how to manual as well, and we say nope, no more. So it could become more easy, but it's also more easy for us to detect those patterns and stop them.

KAREN JAGLELSKI: Marc, did you have something?

MARC ROTENBERG: Sure. I first also wanted to thank the FTC and NHTSA for organizing the conference today. I think this is one of these issues that's creeping up on American consumers with enormous impact, and I don't think actually most people have a very good understanding of what the practical consequences will be of autonomous vehicles. When we first started looking at the collection of data in EDRs-- this was more than a dozen years ago-- we thought about it as a classic privacy issue.

And the question is, who will have access to the data? How will it be used? What are the protections?

Will the data be used in insurance determinations? Will it be used in criminal investigations? And you have many states of course jumping in and passing laws to protect the privacy of the information that was being gathered.

But of course this is all changing, and it's changing as cars move into the world of the internet of things, they become in effect the most complex, the most impactful devices on the network. And I think the public safety consequences are substantial. Now the conversation we've had up until now has largely assumed that somehow it's an anomaly that a car will be hacked or disabled. But in fact, last year after a bit of investigation, we determined that companies in the business of auto loans to low income people were building into vehicles starter interrupt devices so that they could remotely disable the vehicle if the payments were not made on time.

And I think if we begin to think about that category of engineering, we begin to see a wider range of attack space, of risk to users, than we might otherwise consider because you see, the remote deactivation as well as the remote activation of a vehicle may become a sensible model under some business approaches. Yet, as we've traditionally thought about cars, the idea that a company could take over control of the vehicle while you're driving it seems almost impossible to conceive.

So this is another dimension that I think we need to consider as we look at the cyber security risk. I will say also that I think on the personal data front, when it's combined with a cyber security risk you also have scenarios under which individual vehicles can be targeted precisely because there's a known operator or it's a known vehicle. And there may be scenarios from a law enforcement perspective where that becomes very attractive. If you have, for example, a person in a vehicle, you know there's an outstanding warrant, and you're trying to apprehend the vehicle,

the functionality to disable the vehicle, much like the company that's trying to recover payment, may be an attractive engineering option. But you can also see that being misused as well.

KAREN JAGLELSKI: Lauren, did you have something?

LAUREN SMITH: Yeah, I would add as we think about the different types of data that are generated within the car that we may when I think about different group of data differently. So operationally-- operational or safety critical data may wind up being needed to be treated differently from infotainment data, which is some of the more personal data. And that will come into play both in terms of security. We'll raise questions about partitioning and different approaches to sort of dividing what gaining access to those input points can get you in terms of impacting the operation of the vehicle and also, you know, even in terms of jurisdiction if you're talking about NHTSA and the FTC's different roles in this space. That's going to be part of the conversation going forward.

KAREN JAGLELSKI: Is it possible-- so is it possible from an engineering perspective-- and my brother's an engineer, so that kind of makes me an engineer too. Is there a way to engineer so you can segregate off safety critical functions from-- and I'll use this term probably-- like the telematics or, you know, things that will necessarily involve consumer data? Is that possible? Is it being done now.

MARC ROTENBERG: Well, that was one of the recommendations that was contained within the GAO report that came out last year, basically to separate entertainment functions and climate functions from navigational functions. But my understanding is that everything is moving toward the CAN bus, all functionality in the vehicle, so they can all be accessed. And much of that communication at work is not even encrypted.

So it seems to be that if you can approach it from any open port, you can get access to any of the functionality. Now, there are people more expert on the panel than me on that point, but perhaps you can tell us. Is that true today?

KAREN JAGLELSKI: Well, I think we're-- I'm sorry.

MARC ROTENBERG: Is that where we are?

KAREN JAGLELSKI: Oh [INAUDIBLE] see, I told them if they want to talk to turn their thing. And I thought he turned his thing.

MIROSLAV PAJIC: Well, the first set of attacks that were publicly reported in, I think, 2011, actually one of the things that they used was in most of the vehicles, you will have two types of networks that are used for to exchange data, and one was for safety critical functionalities like drive by [INAUDIBLE] and things like that. And the other would be related to the infotainment messages and things of that--

KAREN JAGLELSKI: I'm sorry, is this the Yoshi [INAUDIBLE] hack that you're talking about?

MIROSLAV PAJIC: I'm talking about 2010, results from UCSD group from [INAUDIBLE] yeah, that's the--

KAREN JAGLELSKI: Yep.

MIROSLAV PAJIC: So that's the reason why those attacks were very successful is that you do-- although initially for safety concerns in order to guarantee these kind of predictable and reliable communication, they split the communication busses for safety critical and other traffic. But you have components that are shared, meaning that they have access to both of those. If you are able to get access to some non-safety critical components like infotainment system or whatever it is and use that compromise device to program some-- reprogram some of the devices that also have access on the safety critical bus, then all of a sudden, you have a compromised device being able to send whatever kind of messages you send there.

KAREN JAGLELSKI: Meg? Oh, I'm sorry, I didn't--

MIROSLAV PAJIC: Just one thing that I would like-- we do talk about systems that-- you have to have compliance with all designs, and people didn't think about security until recently. And you put a lot of functionalities. You don't use standard security related mechanisms like encryption and authentication. And adding them now on the fly becomes very expensive. So you do need to sometimes redesign the systems with security in mind.

MEG NOVACEK: Yeah, I think there's a couple of different challenges. And I'll say that we can look at human behavior to tell us if isolation will make sense. So isolation as an engineer, we can do it.

We can do it all day long. Pretty easy to only connect the wires to safety critical and not to the infotainment. But the one of the highest demand features from customers is remote start and smartphone apps that allow you to unlock your doors. So customers are asking for the very thing that's going to connect the infotainment system to the safety critical system.

Because remote start connects them to the engine and the unlock connects them to the body controller. So keep that in mind. We can do-- as engineers, we can do anything.

But if customers are demanding services that are-- if they're demanding it, the car companies are going to provide it because that sells cars. So the challenge is how to do it securely. The other thing is a lot discussion throughout this workshop about the OBD dongle.

So again, the OBD port was put in for on board diagnostics. And it's the safety critical systems that will need to be diagnosed. They're the most complex things.

Those are the ones that the technician needs the data from in order to do their job. So the minute someone does an insurance dongle to that port, again, we can't isolate that as an industry when the demand is so high. So it's really a cultural problem.

SYED HOSAIN: I think one of the things we need to be careful of is to recognize that it is not the security aspect of the vehicle that we're talking about here. It is also the fact that it is the analysis of the consequence of a breach that matters, OK? So if you just knee jerk react and say everything needs to be infinitely secure, you're not solving the true problem because nothing's going to be perfectly secure.

We were in the middle of a release for a customer who was-- an OEM who was putting cars on our network, connected car network, more than 10 years ago. Very near to their product launch, there was a Rutgers University study about the tire pressure monitoring system that had been hacked. I don't know how many of y'all remember that.

But the consequence of that specific breach was an incorrect data reading on the panel. It wasn't going to affect the rest of the car because it was an unencrypted transmission from a sensor that didn't have any ability to impact anything else within the car. So we were able to get the car manufacturer comfortable that that was not something that couldn't be dealt with by simple encryption.

So you have to solve the problems by recognizing what's the consequence of the breach and then put in the necessary best practices at that time to be able to solve that problem and then be able to understand that if there is-- do the study. Security by design is incredibly important. Do a study to say, what if it is breached?

What can it impact? And therefore do the best practices at the time and then recognize that years later, you're going to come back and fix it. You're going to need to upgrade it. You're going to need to have some kind of over the air upgrade available to be able to fix the kinds of problems that could occur which you hadn't thought of at the time that the product was released.

ALLAIN SHEER: So what are companies doing to assess cybersecurity risks? And by that, I mean I'm asking about kind of the process that's used to determine to conduct a risk assessment, to mitigate the risks, to make sure that whatever safeguards are put in to address a particular risk actually works to address that risk. How is that being done?

SYED HOSAIN: Yeah, let me add one more comment to my previous one and I'll answer that in the same context, which is that we should recognize that the OEMs are not sitting still here. They recognize that this is a problem that they need to deal with before it becomes a legal or a liability issue. They are taking the necessary steps to hire the experts to retain the consultants to build in practices.

As you saw this morning with the presentation, from the gentleman from General Motors, people are worried about this and people are concerned about it. So what may have happened in the past with less connected cars is just something that they need to be aware of. So they're taking the best steps.

They're trying to find the people who have dealt with it in other domains-- the internet, the cyber-- the utility space, et cetera, that we have just seen an example where a security breach occurred and trying to apply those best practices to what is happening inside the car. The other

thing which is, I think, very important is to try and recognize that there are-- for large scale attacks, there's only a certain amount of points of contact, if you will, to the vehicle-- long range contact, either satellite or cellular. And therefore, if you can start building in all of the protection over there as much as possible and then reduce the likelihood of an attack getting through to the systems behind that point, you're going to do a better job.

And so they're recognizing that that's the point of-- where most effort is being placed today. On the other hand, individual changes to systems within the car for even a legitimate update of a functionality feature in the car needs to be thought through. There are complex systems that are growing up around this place.

DAVID SCHWEITERT: And Karen, I might add, I mean, obviously it's very dynamic as it relates to what we are facing in terms of cybersecurity. I mean, obviously, between threat vectors, I mean, the instances that the auto sector is facing aren't all that different from other industries. I mean, it's not so much that we have a particular threat vector against us. It's that, you know, manufacturers are increasingly using multiple layers, whether it's production, security by design, manufacturing updates, and then post-production fixes to try to address some of the things and the vulnerabilities. I think Syed and others referenced earlier that nobody's expecting or selling a vehicle believing that it's going be perfect forever.

But I think it really goes back to what Jeff [INAUDIBLE] earlier during his keynote as well as Nat from NHTSA were referencing is the whole generation of additional technologies that are being added to vehicles aren't being added arbitrarily. They're being added because they provide an overall benefit in some way, shape, or form.

So for consumers, that impacts people directly. It could be some of the conveniences that were referenced as it relates to remote start or remote lock, unlock, and that type of thing. But at the end of the day, it also goes back to vehicle functionality, which obviously then relates back to the benefit that the driver or the user experiences.

And it really gets back to some of the statistics that Nat and others were speaking to that in the past, in a traditional vehicle context, really weren't things that automakers, let alone regulators, could really wrap their arms around because they just weren't possible and, you know, the average age of a vehicle on the road is now about 11 and 1/2 years and the vehicles are getting more and more complex. But that's not necessarily a bad thing, and we're going to get into it as it relates to what that means for recalls and consumer impacts. Certainly there are cybersecurity challenges but it's a very dynamic process.

Obviously, there's been a lot that's been done by OEMs and suppliers in the larger ecosystem that will get us to the point where we're staying a step ahead. Does it mean it's perfect? No, but there's a lot of development that's ongoing, some of which I think is directly related to the fact that there hasn't been a commercial hack of a motor vehicle, partly due to some of the efforts that are being taken by the industry and our members.

Some of that relates to kind of the forward leaning aspects of the auto ISAC, which is obviously a component of the larger ecosystem. But you know, whether it's the security by design, some of

the standard setting bodies, whether it's SEE, ISO, some of these collaborative engagements that help to better share information, you know, it's that totality that really ultimately comes back. At the federal level here in the United States, we have a pretty strong regulator in terms of NHTSA when it comes to their very broad authorities.

Some may say that it's not as adaptable as they would hope or we need to legislate further, but if you look at the flexible manner in which the Safety Act applies, it's not just to traditional OEMs. It's also to software firms and parts suppliers and others. So we all have a vested interest in making sure that we get it right.

There are policies and protocols in place to make sure that it's iterative. So along the way if something is not working right, we have the ability to exercise from a federal standpoint recall defect authority to ensure that it's fixed. And some of those fixes will happen far faster in a manner in which the vehicles are connected versus a traditional vehicle will where you can't find who the owner of the driver is and you can't get an over the air update because the vehicle doesn't accept it.

So there's a lot of the technology that's being built into vehicles. Yes, it provides some potential vulnerabilities. But at the same time, the benefits we believe far outweigh the downside risks.

KAREN JAGLELSKI: Marc?

MARC ROTENBERG: Well, I think I have a bit of a role on this panel as the consumer. And I just want to--

KAREN JAGLELSKI: That's right.

MARC ROTENBERG: Thank you. But I want to push back a little bit and ask the question if we're giving full weight to the scope of the cybersecurity risk with connected vehicles. I mean, if we think about traditional failure modes for vehicles-- a collision, for example. It happens at a fixed place at a fixed moment in time.

It may be two vehicles colliding. It may be a vehicle hitting a fixed object or a person inside the vehicle hitting the car. We have a very good understanding of that problem, and over the years, we've developed lots and lots of safety procedures to make driving much safer than it once was. But everything about cybersecurity points to very different type of risk.

It's distributed. It's remote. It can be hostile.

It can happen at a future moment in time. In other words, people can deploy malware that doesn't go off now but goes off a year from now. And all of this suggests to me a degree of complexity combined with risk that, when there is failure, could be catastrophic. I was thinking the other day, for example, let's imagine a connected vehicle scenario on 495 where the network is disrupted.

Now if the network is disrupted for cell phones or for streaming videos, I mean, we may have to wait a while before Netflix or Hulu keeps loading the movie. If that happens with 10,000 vehicles on the beltway, it's going to be a whole other world. And what happens, by the way, when the network is restored? In other words, are all the vehicles at the same operational mode when network connectivity is recreated? So I would be very interested to hear the extent to which we've thought about some of those scenarios. As I said, it feels very unfamiliar in terms of traditional regulation and auto safety.

KAREN JAGLELSKI: Meg?

MEG NOVACEK: So my background is actually mostly in power train and control systems for the vehicle, and I migrated into software quality and then into cybersecurity. So the terms that we use in propulsion is the faulted reaction or the failsafe mechanism. So there was an earlier question about isolation and system isolation, but I would say especially when we have detection mechanisms on board, we can isolate the compromised functions.

So when you talk about loss of connectivity, I think earlier, one of the speakers said that the connectivity is really additional data. You know, no engineer ever turns down data. The car can still function without the connectivity. It just-- you might get stuck in a traffic jam.

You might be driving a little bit too slow for a slippery road. You might not have the weather conditions. So if we can detect that the connectivity is compromised, then it gets isolated and it gets blocked until there is proof that it can be trusted again. So I don't-- I'm personally-- my biggest concern is not some step change and, oh my god, we lost connectivity and all the cars start driving in circles. That's not-- the system is designed robust enough to not let that happen.

KAREN JAGLELSKI: Lauren, did you have something to add?

LAUREN SMITH: Yeah, I think it's important to keep in mind that for both security and privacy, the way in which this ecosystem is going to evolve going forward and that the future mobility won't require just cybersecurity on the part of the carmaker-- there's a growing number of entities involved in this space, some that have always been engaged in making parts of the cars such as suppliers that may be more likely to be privy to data now than they were before, from repair shops to aftermarket devices to telecom companies that now have increased interconnectivity with the car to other sorts of even phone mirroring devices and making sure that we're thinking about cybersecurity and data management within each of those as well as the car maker. I think that's going to be important to be able to assure consumers that we are taking care with and protecting their data. And then just a flag-- you know, one of the pieces that we tend to talk about in the privacy world is the fair information and practice principles, and there are a number of principles such as data minimization and purpose specification that in other sectors we use to ensure that we don't have too much data flowing around that we don't actually need.

That could cause problems. But one of the-- and then these were raised in the federal automated vehicles policy as well. But I think one of the challenges here is going to be that particularly with autonomous vehicles, having more data is often critical to enhancing safety, to ensuring that

machine learning can make these systems safer over the long run. And so how we approach some of these standard privacy principles may wind up needing to be a little bit different in the car space.

DAVID SCHWEITERT: I might just jump in. I know Meg really kind of hit it on the head as it relates to potential redundancies and failsafes that are built in. I think, you know, Marc's hypothetical is a fair one.

I think it needs to be taken into context. I know obviously if you reference 10,000 vehicles, that's probably two to three decades from now maybe in more of an AV context. But you know, at the end of the day, if there was to be some potential loss to the vehicle system, generally there's redundancies and failsafes that kick in.

I mean, obviously that is the backstop as it relates to what the OEMs are responsible, as it relates to NHTSA being the regulator on the safety side. And if something presents an unreasonable risk, it's going to be regulated subject to recall or defect authority, and it's going to have to be addressed. So at the end of the day, you know, a lot of these hypotheticals-- could they happen?

Potentially, but there's a lot of failsafes on the front end that ensure that if there was to be a loss of connectivity-- I mean, a lot of the manufacturers are approaching things in a different manner. So there isn't necessarily standardization as it relates to the technology that's being used in every application. You know, we can walk through the AV spectrum of 0 to 5 and, you know, any one manufacturer is most likely going to differ from their competitor based on what they may be doing in terms of AV level 2, 3, or 4 to the point where they've built in different systems to ensure that if there is a loss of connectivity, if it's necessary at all, that you might have lost some degree of functionality.

But at the end of the day, if it's a level two system, the driver is the fallback, or a level three system, the driver is the fallback. So I think the point Marc was making, fair hypothetical. But we're probably talking to three generations from now before there would be an incident of some type of lost connectivity that causes 10,000s of vehicles to be impacted simultaneously.

MARC ROTENBERG: If I can just ask, I mean, at level four or level five, there's really not a scenario where the driver is the fallback. I mean, you might have a vehicle without a steering wheel or an accelerator.

DAVID SCHWEITERT: No, that's fair, and I know Meg might want to jump in on this. I mean, at the level four or five level, you'd effectively operate in a safe driving mode or a fallback to the point where the vehicle would effectively take certain means to either pull off on the side of the road and not otherwise present a hazard to either the occupants or other motorists. So it just depends on the circumstances. But there is some differentiation between levels 1, 2, 3, 4, and 5 in that example that you were giving.

KAREN JAGLELSKI: Syed?

SYED HOSAIN: Yeah, just one observation I'd like to make which I'm hoping people will appreciate. Physics gets in your way. If you're assuming that autonomous vehicles will be run completely remotely, that's never going to happen, period.

You cannot get the data from any site, no matter complex it is, to the vehicle fast enough to take into account the things you need to do for the car to react real time to the events that are taking place around it, period. And therefore, the failsafe mechanisms that Meg mentioned and other people have mentioned have to take that into account. Most of the information that is going to be in an AV car of some sort, whether it's a fleet or even a consumer vehicle, is going to be local, is going to be information created from the sensor in real time, whether it's light or you name it, whatever the sensor is-- local.

You're not going to have the science fiction effect of remote controlling a car, period. You'd have to violate fundamental laws of physics to be able to do that. It's not going to happen.

So where a loss of connectivity could result in data not being sent or information not being received by the car, it's going to be non-mission critical stuff where the vehicle is not going to be, as Meg mentioned, running around in circles. It just isn't going to happen.

KAREN JAGLELSKI: Yes, Miroslav.

MIROSLAV PAJIC: So I would both agree and disagree and give a couple of examples. I completely agree that physics is something that is very important to take into account. And that's why most of the cars are designed the way that most of the pretty much every safety critical decision is done locally, and you just use extra information potentially for high level controllers like navigation and things of that sort.

So those are usually designed in this failsafe mode where if you lose connection to the outside world, you work OK. But that also brings us-- one concern is that I am worried about local attacks. I'm worried about malware being installed in components that are already on the bus that can start sending messages that will not trigger a false detectors.

So for example, in other domains, it was shown how it's super easy to take [INAUDIBLE] of course by slowly shifting GPS measurements. We did that for-- with the knowledge of the driver, with a car that we slowly start shifting away. And we also have for other automotive components a simulation and an experiment.

And it's shown how easy it is to not trigger false detectors and be able to insert these very subtle attacks that will at the end endanger the safety of the vehicle. We do propose some methods how to solve it, but that's on the other side. On the other hand, we do now-- maybe we don't rely on the outside information for local control.

But we are moving toward bringing these kind of mobile city challenges where we will not have intersection in the form where we have today, but we will actually have coordination between the vehicles so that we can increase the amount of vehicles passing through the intersection. So there I'm not again as worried as against denial of service attacks where you don't get to message

because, yes, it will create a bottleneck and no vehicles will pass there. But what if you are in certain nicely crafted messages?

And those are kind of things-- those are the networking attacks that are now used. With connected cars, the next step is coordination between them. And once you start messing up with the information on which you base the coordination between vehicles, you actually have a lot of calls.

MARC ROTENBERG: I just wanted--

KAREN JAGLELSKI: [INAUDIBLE] oh, OK. You've got enough questions. OK, Marc.

MARC ROTENBERG: Well, I just wanted to respond to Syed. I'm not quite as sure as he is that there isn't a scenario for remotely operated vehicles. We've done a lot of work over the last few years concerning drones, which are remotely operated, unmanned vehicles.

And the intent, of course, is to deploy drones in the national airspace. And there are lots of scenarios under which drones collide, drones crash, drones fall to the ground. And even to pick up on Meg's phrase, the failsafe scenario for a drone, which is to return to waypoint doesn't work if the drone's battery has been diminished and it doesn't have the energy to return to the waypoint.

So I think there is at least some value in trying to look at some similar regulatory challenges anticipating what some of the risks might be. Miroslav mentioned GPS, for example. The GPS signal is not encrypted, so of course, spoofing a GPS signal is not a difficult thing to do. And there are some security measures that are taken, but there are also a lot of attack scenarios that are based on sending a vehicle or a drone to a different location.

KAREN JAGLELSKI: Syed?

SYED HOSAIN: Yeah, I don't disagree with the comments that have been made by Miroslav and Marc. The point I'm making over here is that there will be some functions which are augmented by communications. But ultimately, the information that a vehicle needs to have-- because it's constrained mode of operation.

Its mode of operation is far more of a problem than a drone is today, even today. And most people who are operating drones are either relatively short range or, if you look at some of the military applications, they're worried about the latency and long range control of what can happen. But there are things you simply have to react to in near real time in a car, on a street, with the people and raccoons and whatever else is out there that you have to take local action, which is way more rapid than any remote control could be done.

KAREN JAGLELSKI: I think that's-- what I hear all you saying, I think-- and one of the questions we wanted to ask was what is unique about cybersecurity issues in this space versus-- besides the fact there's a two ton vehicle that can cause great damage. I mean, is there something unique about the cybersecurity issues in a car versus, say, my laptop? Meg.

MEG NOVACEK: First thing is there's 50 to 100 computers in a car. So that's number one. The complexity is just so much higher than IoT. Two is the lifespan. The 11 and 1/2 year life that people expect is another huge challenge. So having a system that can be updated, whether it's technology updates or security updates, is going to be a huge-- is a huge challenge for the community.

KAREN JAGLELSKI: And part of it is historically, consumers don't bring in their cars for recalls. A friend of mine has three open recalls that she really needs to get fixed. So how realistic are over the air updates at some point?

How can we address that issue of-- I forget the percentage. My friends at NHTSA know better than I do. But it's-- Dave, you know.

DAVID SCHWEITERT: Yeah, I mean, I don't want to jump in if anybody else wants to answer. I mean, if you look at recalls generally, so holistically, recall participation rates vary. The longer a recall on a vehicle is open, the longer it takes to remedy.

NHTSA, I believe, the statistics are at around maybe 72% on average as far as recall participation, and recalls run the gamut. It can be everything from a decal that needs to be updated to something like an airbag, which some of us have experienced firsthand. And that gets back to what I was alluding to earlier as it relates to increased technology. We believe from a manufacturing standpoint that technology being added to a vehicle not only helps as far as the vehicle performance, but it also helps the manufacturer as far as lessons learned, things that can be repaired ahead of time.

But then on the repair side, it also provides another touch point by which the OEM and/or the dealer and whoever is taking care of the repair actually knows how many of said vehicles are in a particular region as far as what is necessary, if it requires some type of replacement part. If it doesn't, the recall update, if it was to be an update, over the air or otherwise, can remedy something that in the past could have otherwise been fixed. So we believe that on the recall side, technology actually facilitates greater recall participation and remedy versus traditional recall.

KAREN JAGLELSKI: Meg?

MEG NOVACEK: To add to what Dave said, the over the air allows a higher penetration of the recall. And for those cars that aren't connected-- they're in Montana. They're on vacation.

They're part at the airport for a couple of months, whatever. The manufacturer knows or the over the air service provider knows that they have not been updated. So the least you have the data.

KAREN JAGLELSKI: Is it realistic-- I mean, is that a realistic thing? I know some cars are already doing over the air updates, but is that as common as, say, you know, either having to go to the dealer--

MEG NOVACEK: There's several companies doing it today, and there's a lot of development for the rest of the companies to go that direction. So I can't state what percentage and when we'd all be there, but--

SYED HOSAIN: It's definitely something that is going to happen. One of the things we have to be careful about is right now, the rules for recall are essentially voluntary. If the owner of the car chooses not to do something, as in your friend's case, it doesn't get done.

So there is a question here in my mind. Should an over the air update be forced on a car owner? It's their car. It's their systems.

It's their multiple computers inside their car. If one can provably say this is a safety issue that relates not to their vehicle and their car, but their public presence on the roads, then maybe one could argue that is possible. But I don't think that those rules exist.

I think that's maybe where some of the legislation perhaps needs to be-- that in certain safety related issues beyond the individual owner of the car, there may be a need to be able to do this. But is OTA happening?

We're certainly getting ready for it. There's no doubt about that. And some car manufacturers are doing it already today and others are-- I mean, our systems are designed to allow the car manufacturer to do it. But we have to think through when and how and where and who's giving them the permission to do it, et cetera.

KAREN JAGLELSKI: Meg.

MEG NOVACEK: A couple of things there-- I'm not sure if you'd call in a research group or what, but it's a couple-- you know, at least University of Michigan and New York University are sponsoring a group called Uptane, which is focused on secure over the air updates, and several companies in various roles within the automotive ecosystem are participating in that to make sure that it's a robust approach so that we as a industry can do secure OTA. The other challenge, I think-- I get the idea of a safety or security recall may preempt the driver buy-in or the owner buy-in. The challenge with that is that many of them are layered.

So let's say one update was for functionality. So version 1.1 was functionality. Version 2.0 is for security, but 2.0 can't go in until 1.1 has happened. So I see us as a community, we need to find a way to, I'll say, enforce those updates so that the customer is not 10 layers behind and it's not updateable because they're not going to want to go to the dealership at that point.

KAREN JAGLELSKI: Marc?

MARC ROTENBERG: Well, that's actually an important point. It's a subtle issue in consumer protection but one I know that the FTC has had to consider. Companies oftentimes use updates to change terms and conditions to the advantage of the company and diminishing the privacy of the consumer.

And given the choice, you might say, well, I really don't want that update because I want the controls I had in the last version. But of course if the update is related to security and safety, then you should be taking the update. So I think the FTC may have a role in this space trying to ensure that the security updates which the consumer should be taking don't come at a cost to the consumer that would lead the consumer to, you know, second guess the decision.

KAREN JAGLELSKI: David?

DAVID SCHWEITERT: On recall side? One of the interesting things-- I know we have former NHTSA administrator David Strickland here, so he might want to weigh in on this at the next panel. But if you look at things from a functional standpoint, you know, auto manufacturers, for those that aren't aware of how recall process notification works-- so in the instances, you, a manufacturer, NHTSA, compelling a recall, you then have to provide notification.

You have to provide notification via US Mail to the requisite owner and if you have that material. If you don't, you need to track it down. Sometimes as the vehicle changes hands two if not three times, it gets harder and harder to find where that consumer is.

So you've got participation rates on newer vehicles up around 100%, and then it really drops off after that, particularly as the vehicle changes hands over time just because the touch point with the dealer who effectively provides the repair at no cost to the consumer has no way to compel the change. But at the same time, the manufacturer is being urged or instructed to follow through on the remedy, but it's contingent upon a person following through for something at no cost for them to get repaired. So not to say in all instances potential over the air updates or software updates for that matter fix everything, but it does have the potential to rapidly increase what otherwise can be a very cumbersome process regardless of the age of the vehicle.

KAREN JAGLELSKI: Lauren.

LAUREN SMITH: And I would add, I think it's worth at least theorizing that when you have level four or five vehicles, if they need to be brought into the shop, the dynamics will change when you're done with the car for the day. The car says, you know, I'm going to take myself into the shop. It's hard to predict exactly how that will, you know, change rates of adhering the recalls. But that's certainly a future that will probably come at some point. And it's also worth thinking about, you know, if a lot of cars are managed by fleet managers, the incentives might be different for them to be able to bring a batch of cars in for a repair than they are if each individual needs to bring one in.

DAVID SCHWEITERT: Or the fact that as a consumer, you know, during the off peak hours, you know, your vehicle can go to the requisite dealer and be repaired during off hours.

KAREN JAGLELSKI: And that would be awesome.

DAVID SCHWEITERT: I think the public would see significant buying in those instances.

KAREN JAGLELSKI: Right here.

SYED HOSAIN: Let me add one more point to that, which is that I think there's going to be a slightly different change in the AV market that we are not anticipating as easily today, which is I don't think those AVs will be owned by us the consumers in the majority of cases. It will be transportation or mobility as a service. Therefore, the owner is fuzzy.

It's not the person who has the car sitting in their garage because they want to use it the next morning or which drives up because they now need to go to work. It will be somebody else. And then the question comes up-- who's giving permission to have what done to the car based on whether it's a safety recall or whether it's a feature update? And you need to think through all of those things down the road because it's going to happen. AV cars will mostly be owned by corporations, not by people.

KAREN JAGLELSKI: David, I want to just get back to you quickly. So how are car manufacturers and OEMs communicating to consumers their cybersecurity practices?

DAVID SCHWEITERT: Some of that really differs by OEM. I mean, obviously some of it's being done either through notifications, part of the owner's manual, or via website, that type of thing. It's going to differ manufacturer by manufacturer. Some of it's more explicit than others, but it's not linear.

ALLAIN SHEER: OK, so now you've got some cyber security risks that have been identified. How do you go about remediating, deciding which ones are going to be remediated first? What are the factors that should be taken into account to decide that vulnerability A-- say, vulnerability A should come before vulnerability B?

DAVID SCHWEITERT: Yeah, some of it depends. I know others will probably want to jump in on this. I mean, is it a safety critical system? Is it something having to do with other functionality in the vehicle?

I think some of that has to be weighed by the manufacturer in terms of their overall scope, and it's going to differ. But at the end of the day, I think depending on the connectivity of the vehicle, I think that they have probably an easier means of notifying the consumer, whether it's explicit through other means or through some type of notification through the vehicle that something is in need of an upgrade or a repair. Is that the aspect of what you're--

ALLAIN SHEER: No, I'm actually asking something different. I'm really asking what factors are taken into account deciding which vulnerability is going to be addressed first. So it's things--

LAUREN SMITH: By the OEM itself.

ALLAIN SHEER: Are you concerned? Is a factor the probability that it will be exploited, the amount of harm that might result if it were exploited, how much it would cost to fix it, or something else?

DAVID SCHWEITERT: Yeah, I think to claim that somehow a cost benefit is going to be the overriding factor is certainly not the case. I think ultimately, it comes back to the manufacturer,

the brand reputation, and then the system and the potential exploit. So some of that is happening in real time today as it relates to the auto ISAC, which our association and others have stood up, which includes not only manufacturers but tier one, tier two suppliers.

And one of the mechanisms there is to ensure that information is shared across the platform to ensure that others can learn from what may be playing out in real time. So you know, it's going to differ. I think, you know, would some say, well, one manufacturer is going to make a decision differently than another? Absolutely. It depends on what their overall design decisions are and how they factored it in.

ALLAIN SHEER: Does it make a difference, though, if the information-- what's at risk is safety as opposed to what's at risk is consumer information that might be stored on the system?

DAVID SCHWEITERT: Oh, absolutely. I'd say that there would-- in that case, I think this is maybe what you're looking for, that there certainly would be a tiered approach in terms of how an OEM would face that type of cyber vulnerability based on their responsibilities with--

ALLAIN SHEER: But what goes into the tier? That's what we're trying--

DAVID SCHWEITERT: And I-- you know, representing an association, I can't give you a definitive as it relates to what one OEM would or wouldn't do, nor would, I think, you'd want that shared in this context.

KAREN JAGLELSKI: Meg-- but I think Meg wants to share that with us.

MEG NOVACEK: And it's not OEM specific. It's really a-- I think most of you will be able to relate to it. It's obviously-- well, to me. I'll just say my opinion.

So safety is first. You know, I think if someone is driving-- I'll say if I'm driving in a car and my safety is at risk or my privacy and I want some to decide which they're going to handle first, I'm going to vote for my safety every day. That's just my personal preference.

The range of the hack, if it can only be done 10 feet away or it can be done many miles away from another state, that's going to be a higher priority in general. The ease of developing a remediation, either a solution to block the vulnerability or to prevent the effect of it-- so understanding how it happened and how to protect against it will help you move faster. You can just imagine for your own personal planning and anything you do. If you feel like, oh yeah, all I have to do is this and I'm good to go, those are going to get in faster than the ones where you have to sit there and bang your head and go, well, that may be, but this one.

So there's multiple teams working on the items that were found in vulnerability assessments. So I think the scenario that was brought up is really, there's not a hack in the wild. You did some research.

You hired a consultant to come look at your system, and they came up with a list of things that you need to improve. How do you prioritize which ones you're working on? And the answer is,

you know, companies have more than one person working on it, and there's a lot of activity in parallel.

And that's how they're going to prioritize it. The other is what-- so once the experts figure out how to address it, whether it's blocking the vulnerability or remediating the impact, whether or not that solution can be applied to the car as is is another factor. Do they have to change hardware in order to change the software?

Is it a software only? Can be done over the air or does it have to be brought in? All of these things come into account.

And then if the car has to be brought in, again, I'll say it. Myself as a customer? I don't want to have to go in every other day.

So I'm going to want them to bundle the work only if I have to go in. So all of these things are taken into account when companies are figuring out how. Marc?

MARC ROTENBERG: I don't really disagree with Meg about prioritizing safety over privacy. But I do want to point to a very interesting privacy risk that I wish the manufacturers would prioritize, and it has to do with a Bluetooth pairing of cell phones and rental cars. It's almost everybody's experience nowadays that when you rent a car with Bluetooth connectivity and it asks you if you want to enable your cell phone-- which is a safety feature, by the way, because it enables hands free driving, which we should encourage-- it captures your entire contact list and all the rich data associated with that and stores it on the vehicle. Now it would seem to me to be a priority to ensure that after the rental period was over, that data was routinely deleted because the risk of identity theft and financial fraud and a zillion other things seems quite obvious. And my question is, is some progress being made on that particular cyber vulnerability?

MEG NOVACEK: So if I can just butt in here because I don't want to tread on panel three's toes too much because he'll be mad at me. And I would say that the FTC did-- we did issue a consumer and business education piece in this area. I think that's right. For example, my husband bought a used car, and on the car was the previous owner's data. So--

MARC ROTENBERG: But is it the driver's-- see, this is where we get into very interesting, you know, liability allocation issues. Is it the responsibility of the driver to figure out how that data has been downloaded and to subsequently try to delete it, which is not an easy thing to do? Or should it be on the manufacturer, service provider, which it could be a routine procedure to ensure the data is deleted? And I think there are lots of issues that look like this particular one. And it would not be fair to put the responsibility on the driver where the service provider could manage the problem more efficiently.

MEG NOVACEK: I think Peter will be sure to address that issue in panel three. Right, Peter?

DAVID SCHWEITERT: OK.

SPEAKER 2: Me too.

SYED HOSAIN: So two questions that you raised, one of which I think has to do with the fact that how does the OEM know the car got sold. So I don't think you can put the onus on people who actually have no possible way of recognizing when something needs to be done. And you've got to be careful about that.

So where does that answer to that question lie? Maybe all they have to do is make it easier than it is today and let the onus lie on the driver who either purchases or sells-- excuse me, the person who sells the car and says, I'm going to get rid of all my personal data, and go from there. With regards to download of priorities and updates and how often and when you do it, it's a matter of not just doing an update willy-nilly.

I love to draw analogies and I don't know how many people in this room ran Windows 7 systems at their home and woke up one morning and, lo and behold, they were running Windows 10 and it was done without their permission or knowledge. That is the kind of thing that corporations need to avoid. We need to be careful to make it a choice, an informed choice, as best as we can-- and cars are darn complex systems-- as best as we can to make that happen.

So prioritizing the kind of updates that you need to do a car has to be done with a, what's the consequence? You do not want to break a car. PC is easy.

You do not want to break a car. And you've got to be careful that what you're doing hasn't caused some other system, if it is a security or safety system in particular, to have lost its functionality completely. That would be a dangerous thing.

KAREN JAGLELSKI: Miroslav, and then we're going to go to questions from the audience.

MIROSLAV PAJIC: But does the-- going back to your comment, it also goes to this kind of interesting perspective that if you decide not to update your car and your vehicle gets compromised and you endanger someone else as a part of the traffic. So we fully-- I mean, we have insurance industry where we are trying to spread that risk. Should be fully put that into the consumer's angle?

SYED HOSAIN: Well, let me ask you a dumb question. If you have an airbag that is subject to a recall and you have chosen not to do it through laziness or just didn't get it done and you loan your car out to somebody drives it and they get into an accident, who's at fault?

MIROSLAV PAJIC: But again, I--

SYED HOSAIN: It's a tricky question, right?

MIROSLAV PAJIC: Yeah I completely agree with it. But the question here is-- one thing is you making your own responsible decisions that affect only you and you making decisions that affect everyone else. And moving toward increased autonomy, more connections, coordination between vehicles, the decisions that you make affect everyone else around you.

SYED HOSAIN: I goes back to the point I made, which is that I think AV vehicles will not be owned by the people who use them. It will be owned by somebody else, and we've got to figure out how to deal with those liability issues and ownership issues and how and when to update issues quickly.

KAREN JAGLELSKI: OK, so we have 13 minutes and 48 seconds left. So we have a number of questions from the audience. So I'm going to start with the first one. How do you foresee potential legislation possibly mandating the certification of cybersecurity solutions for vehicles? Anybody?

SYED HOSAIN: I'll just-- OK, I'm a science fiction buff, so I'm going to talk about something that maybe people will-- it may be extreme. Larry Niven wrote a story years ago. Person on trial-- the conviction would have resulted in that individual being given the death penalty.

The clincher of the story was he was arrested for speeding. So we need to make sure we understand exactly what penalties we think we're going to apply and who is going to get that problem dealt with. And where do we draw the boundary of legislation? Where do we decide that some things have to be done, some things are necessary?

That's a fuzzy question in my mind. I'm not a lawyer and I have no clue where that answer is going to lie. But I think that we need to take those steps to understand liability very quickly.

KAREN JAGLELSKI: David?

DAVID SCHWEITERT: I think this is obviously a live ballgame. I mean, we're witnessing a lot legislatively before the US Congress both in the House of Representatives and the US Senate in terms of autonomous vehicle legislation where the topic of cybersecurity is currently ongoing. So as people talk about what the rules of the road are from a federal perspective, trying to encourage the adoption of increased technology to assist, whether it's for mobility purpose or safety or otherwise, cybersecurity is not something that people are ignoring. The ultimate question is at what point-- or what capabilities does the federal government have to dictate some type of a cyber standard?

And up to this point, I think the realization is is that Congress cannot, in its infinite wisdom, pick something that is static today that's going to meet the needs of tomorrow. So at the end of the day, there's the backstop. The backstop is that it's an ongoing iterative process.

NHTSA has very broad authority both in terms of its defect recall and investigations to ensure that if there is unreasonable risk, whether it's cyber or mechanical systems, that it has to be dealt with. And actually, NHTSA the last year exercised some of that defect recall already on the cyber front. And if I remember correctly, the remedy that was provided resulted in 100% participation.

KAREN JAGLELSKI: And I think when we're talking safety risks, that's true. But what about security risks to consumer data? Is there any need for any kind of federal legislation?

MARC ROTENBERG: Yes. I mean, I've been at this for a long time, and I think the United States does need a comprehensive approach to data protection that would most certainly include vehicles. I don't think the notice and choice approach which people talk about works at all for privacy protection. I mean, if we're speaking frankly, notice and choice operates really as a disclaimer or a waiver.

It's a company saying, this is what we're going to do with your data if you purchase our vehicle and do business with us. And if you don't like it, don't purchase our vehicle. But you see, that's not privacy protection.

So the way we solve privacy protection is by saying to a company if you choose to collect the data, which is the choice the company makes-- it's not a choice that the individual makes-- you bear the responsibility for the consequences if the data is misused. And I think that is almost always the right approach to privacy protection. It can be technologically neutral. It can be service neutral, and it has also the benefit of encouraging companies to think carefully about whether they really do want to store, for example, unencrypted credit card information. Many companies were doing that until they faced liability and they realized it was not such a good idea and they stopped storing it.

KAREN JAGLELSKI: Lauren?

LAUREN SMITH: Sorry [INAUDIBLE]

SYED HOSAIN: Just a quick--

KAREN JAGLELSKI: [INAUDIBLE]

SYED HOSAIN: Oh, Lauren first?

KAREN JAGLELSKI: Lauren-- Lauren.

LAUREN SMITH: So you know, I think it's important to drive home the point that it's not a wild west when it comes to protection of consumer data. I mean, we have the Federal Trade Commission that has been active in consumer protection around data privacy within the internet of things for years. Cars are not that unique in this particular area, and it sounds like, you know, obviously there's increased interest at the FTC in this growing quantity of data in cars. There's also, you know, self-regulatory principles that the FTC can hold entities to.

So in 2014, you had the Alliance and Global-led automotive privacy principles that nearly every car maker has agreed to. And you know, that type of effort is something that is self-regulatory but has enforcement mechanisms through the FTC. And you know, we should I think communicate to consumers that there are entities that can enforce against unfair, deceptive trade practices, that this isn't a wild west.

And you know, as Nat even mentioned earlier, you know, we're not sure what sensors these cars are actually going to wind up needing. I think we're not sure how we're going to wind up

defining safety data in the long run, especially as we have more autonomous cars. So I think, you know, coming out with legislation today on this specific issue would be really challenging.

I think we need to have these conversations and figure out how we can improve notice and choice, you know, particularly with something as easy as your phone syncing your contacts through Bluetooth. It seems like there is room for improvement there. There's room for giving consumers more choice within the interface and their cars, a little more notice, and figuring out how do we answer the question of who owns what data in practice. And I think these conversations are happening at events like this and we need to have them sort of more rigorously going forward before we come up with a sort of prescriptive fix right now.

KAREN JAGLELSKI: Syed?

SYED HOSAIN: One of the concerns that I have is that we do have to be careful not to knee-jerk overreact to scenarios. While I totally agree that we need to find that right balance between privacy and protection of information, et cetera, but we have to be careful. We're a global company.

We offer our services not only here, but in Europe. And I can tell you a lot of our customers are incredibly chilled by the provisions for penalties in the GDPR. If you're not familiar with that, this General Data Protection Requirement that the EU has put out has to be in place by May of 2018. It's not that far away.

And it has an incredibly chilling effect on innovation and what can be done because most companies, almost all companies, aren't out there with malicious intent. They're out to do something fundamentally good with the data they collect and with what they're trying to achieve. And if they can make the appropriate-- anonymize data if necessary if that's what's needed-- available for purposes that do general good, why not? And if there is a consequence of a breach causing a severe penalty, then that has some issues that you need to deal with.

The second part of it, I'm going to be a little bit contrarian here. So please bear with me. Hopefully, it'll get people angry at me. I don't know, maybe.

We should ask ourselves one very important question. Is privacy overrated? Let me explain what I mean by that.

We have reached the point where the next generation, some of whom are in the room today, think that they can willfully and willingly and openly put all their personal information on the internet and nothing will ever happen. OK, so there's people are helping protect them behind the scenes. But that trend is going to continue, period.

And we need to think through what we protect, what we don't protect, and maybe understand that some information, particularly if people are participating in the potential for that data monetization, then it'll be OK. I have a lot of personal private information. Hey, if you pay me for it, I'll give it to you because I know the consequences of a breach don't matter as much.

DAVID SCHWEITERT: Karen, I know you've got another panel that's really going to focus on this, so I'll just maybe conclude with this point. And you know, if you look at what's happening with the privacy principles, I'd be shocked if there was another industry that has been as forward leaning as the auto sector, both in terms of the privacy principles that Auto Alliance and Global Automakers have charted. I mean, this is something that was effectively hammered out, that it's dynamic. It's not static.

And it is FTC enforceable. So as it relates to something that needs to happen legislatively, I would say it's always important to reiterate to the public that what they may witness either on their internet at home or their personal device is far different than what otherwise is executing in the vehicle. And data-- all data is not created equal.

There's a lot of steps being taken by manufacturers. It's going to vary as far as how they roll it out. But in terms of anonymizing, minimizing, and those type of things, Marc did raise some fair points. But I'd be hard pressed to think of another industry that's been as forward leaning as the autos in terms of how they manage data.

MARC ROTENBERG: Could I make just one point on privacy and innovation?

KAREN JAGLELSKI: No. Hey, I'm telling you. Pater is going to leap across the table and grab you by the neck, but go ahead.

MARC ROTENBERG: This is a good conversation to have, and I know it's a conversation that's taking place across the industry, and we do appreciate it. But in fairness, you know there is a view which says an innovative product is one that maximizes the technology in the public benefit and minimizes the risk to privacy and personal data. And what the GDPR is attempting to do is to reduce the risk of the misuse of personal data.

You can collect endless amounts of emission information, safety information, breaking information, acceleration information. Go for it, right? It's not the case that privacy rules try to restrict data analysis analytics.

It's simply the recognition that there's a certain category of data that really does adversely impact people. It affects their insurance rates, their health payments, their employment opportunities. And if you're gathering that data, then I think there's some responsibility.

ALLAIN SHEER: [INAUDIBLE]

KAREN JAGLELSKI: Sure.

SYED HOSAIN: Very quick. I don't disagree. That's not the point I was trying to make, I guess.

I think the real fundamental flaw that I have of having looked to the basics within the GDPR is the fact that it is being administered by people who don't necessarily understand the intent of what is going to be done, number one. Number two, it's the penalty phase where if you look at

what is required, the companies that matter, the larger corporations to whom it could be a serious issue, are going to think twice, and it's going to slow them down. Is that a good thing?

It could be. I mean, they may think through some of the privacy issues that they should have thought through better. Otherwise, it could be an issue.

ALLAIN SHEER: All right, this is the second question from the audience, and it assumes that there's some kind of certification as to cybersecurity practices. And the question is, wouldn't the automakers simply falsify their cybersecurity data?

KAREN JAGLELSKI: It's from the audience.

MARC ROTENBERG: Is that a real question?

ALLAIN SHEER: It's from the audience.

MARC ROTENBERG: No. I know we-- no.

MEG NOVACEK: Yeah. The answer is-- the answer no, right?

KAREN JAGLELSKI: And I just-- because Alan left out part of the question, and part of it has to do with admissions falsifications.

MEG NOVACEK: Yeah, that was read between the lines.

KAREN JAGLELSKI: OK.

MEG NOVACEK: I would say that I'm going to refer to-- and I'm just going to appeal to some of the geeks in the audience because I think there are a few. ISO26262, which is a functional safety ISO standard, really pressures, challenges the industry to abide by functional safety best practices, and that as long as you're following the best practices, that you're not punished as much as if you weren't following them. Though I think we should as an industry consider emulating that approach to security and let there be-- because it's been mentioned many times there are industry groups. I mean, the experts in this industry want to do a good job, want to keep customers safe, and want to give them an enjoyable experience.

And so between AUTO ISAC and Uptane and Faster and, you know, there's all these different-- the joint SAE ISO committee on cybersecurity product development practices or whatever they're called. There's a lot of people trying to find the right way for the industry to do work. So as long as there's safety in numbers, that might work from a peer pressure and I'll say legal enforcement perspective as opposed to certifications and regulations.

SYED HOSAIN: I would only add that I think OEMs by this time, if they haven't learned their lesson, they deserve to get nailed the next time they do something like that. Not going to happen.

MIROSLAV PAJIC: But I would say so in the example today I guess everybody is suddenly referring to, the falsification of evidence was done to pass the test. But then the car would improve the overall experience of the user. Falsifying security related data would not, at the end result, if there is a vulnerability there, improve safety of-- improve the overall experience of the driver.

So from that perspective, I don't think that there is the same motivation between those things. I think if more goes according to the Meg's comment, it goes to the user standard practices, something that you have in FDA in certification of medical devices or in avionics. So there is a way how you can reason about safety of these very complex systems. I mean, cars are complex, but they're not as complex as Airbuses or Boeings of the world. So we can reason about a security in a similar manner. And there is a push both from academia and industry to build these kind of assurance cases that can be presented to the government and certification authorities to say, yes, we did follow some practices, and we provide some guarantees that security concerns have been addressed.

KAREN JAGLELSKI: All right, well, we're out of time. So I'd like to thank all the panelists and in particular Lauren, who stepped up to the plate. But thank you. All I think it's been very interesting, and we appreciate you being here.

MIROSLAV PAJIC: Thank you very much.

[INAUDIBLE]