FTC Connected Cars Workshop: Privacy, Security Issues Related to Connected, Automated Vehicles
June 28, 2017
Segment 4
Transcript

[PANELISTS CHATTING]

HILARY CAIN: Yeah, I brought my own. BYOB.

PEDER MAGEE: Good afternoon. My name is Peder Magee from the Division of Privacy and Identity Protection. And with me is Maneesha Mithal, Associate Director of the Division and my boss.

This is the third and final panel of the day. And we'll try and touch on the few privacy issues that haven't already been discussed by the last panel.

[LAUGHTER]

I think this will be a very interesting discussion. And thank you all for sticking around throughout the day. Let me first introduce our fantastic group of panelists. And I'll ask you to take a look at the bio that we have for all their accomplishments. I'll introduce them quickly.

We've first got Hilary Cain from Toyota, Dr. Jason Carter from Oak Ridge National Laboratory, Charlie Haake from the Association of Global Automakers, Joe Jerome from the Center for Democracy & Technology, Andrew Koblenz from the National Automobile Dealers Association, the Honorable David Strickland from Venable law firm, and Adam Thierer from the Mercatus Center at George Mason University.

Maneesha and I are going to be guiding the discussion and directing questions a little bit. But I'm hoping that my panelists will jump in wherever they like. If you'd like to make a point or add to an answer or something, if you could just tip your name tag, we'll know to call on you. Or you can just start talking.

So we've heard about some of the amazing benefits that will be coming from connected cars--safety, increased mobility, environmental. We've also heard about some of the cybersecurity issues that these technologies present. And obviously, bad security in this space could be potentially devastating, a matter of life and death.

Perhaps less obvious are the implications for consumer privacy. So my first question was going to be, why is privacy important in this space? But I think I'll change it to, is privacy overrated in this space as cars become more connected and more automated? I'm going to ask Joe to get us started. And then please open it up to any of the other panelists who want to weigh in as well.

JOE JEROME: Well, so, first, thank you to the Federal Trade Commission for inviting me here to speak on behalf of the Center for Democracy & Technology. In some respects, I feel sort of

bad that you've put me in the position of being Mr. Doom and Gloom, since I think we all agree there are tremendous amounts of benefits that connected cars and autonomous technologies bring to both individuals and society at large.

That said, I do think privacy issues are incredibly important in the connected car. And as we add more and more sensors, as we add more and more cameras, and then as basically the ecosystem gets more and more complicated, it will lessen our privacy. 91% of US households own a car. For lack of a better expression, cars are for many Americans their second home. I don't think I'm exaggerating when I say that probably most of us have danced in our car, cried in our car, and we've yelled in the privacy of our car. And a lot of this technology sort of changes that dynamic. And it will cause consumers to have to develop new mental models that they probably do not have at the moment.

I think we also need to be straight up that how you drive reveals a lot about who you are. And I don't mean that just in the sense of geolocation-- knowing where you're from, where you work, where you pray. But all this technology is going to divulge a lot about when you drive, how you drive, what your interests are, what we perceive your interests to be. And it's pretty obvious that a lot of people are chomping at the bit for this information-- marketers, insurers, employers. So there's privacy issues.

And so, what are the big risks? So I guess I want to go back to the V2V rule-making, where NHTSA suggested that V2V and, I think, a lot of these technologies will result in a perceived privacy loss. As a privacy advocate, I don't think it's a perceived privacy loss. I think it's a real privacy loss. All this technology is going to make tracking and all sorts of inferences much easier to do.

And I think when you look at some of the stuff around automotive fingerprinting, there are some open questions as to how easy it is to actually de-identify this information. And there's also questions about how easy it might be to re-identify it. I think we really have to think about what sort of inferences can be resulting from this information. Are we going to be sharing this with health care providers? Are we going to be sharing this with insurers?

On the question of insurers, I think there are some really tough questions about how the Fair Credit Reporting Act applies to usage-based insurance. The FTC in its IoT and big data report discussed the issue with first-party data collection and the FCRA. So we sort of have to ask ourselves-- whether it's provisions that require the ability of consumers to access information and to correct errors, whether that's going to apply to usage-based insurance.

And frankly, I think we have huge, huge questions about how this information is going to be accessed. I think we have to recognize that this information is going to be used in, I think, PR disputes. It's going to be used in legal disputes, both civil and criminal. And this maybe isn't necessarily the forum for this, but we really have to figure out exactly how and what the bounds are on law enforcement access to this information.

I was happy to see my colleagues from the Electronic Frontier Foundation here earlier. I think we're going to move to a period in time where we're going to need to expect transparency reports

from auto companies. They did an edition of their Who's Got Your Back on the sharing economy last year. And I think we're moving toward a world where they should be doing an edition of Who's Got Your Back in the auto industry.

And then of course there's sharing unhinged. I would point everyone to efforts like Otonomo, which presents itself as a car data exchange platform. So, in other words, the data brokers have arrived for the connected car data. And it's been five years and we still haven't exactly figured out the transparency, access, and deletion issues around data brokers. And now they're going to have access to car information?

And then I think advertising presents issues, both the fact that we're going to have a lot of vectors for bad actors to be involved, and just basic terminology. There's one company out there that provides personalized advertising for ride-sharing and taxis. And its privacy policy says straight up, it doesn't collect personally identifiable information. It does, however, collect the beginning and an entire duration of a trip. That's the ballgame.

And then, I guess I would say, ultimately we have to have questions of who and when and how can you turn this off? There's been reporting out there already of people who have purchased a car and found their infotainment system online and up and running without the fact that they had really asked for it. And then they couldn't figure out how to turn it off. Their dealer couldn't say. When they tried to escalate that to the OEM, they couldn't exactly get a clear response from the OEM. So their response was to take self-help measures-- pull out the innards of their car, probably void their warranty, just because they didn't want an infotainment system. And that's sort of outlandish.

I think there's been a lot of great conversation here. And people are doing a lot of thinking. But as a consumer and a privacy advocate, I won't say-- it's certainly not the Wild West. But it's a complicated universe. And if I'm interested in these issues, I really have no idea who to turn to get the information I might want to know what's going on. And that's a problem.

PEDER MAGEE: Thank you. Andrew?

ANDREW KOBLENZ: Yeah. So I'm not necessarily a privacy advocate. But we are advocates for what makes our customers want to buy more cars, because we're in the business of selling cars. And we want them to buy cars from us.

And from that perspective, I can tell you that what we are hearing-- I heard on the earlier panels some comments that were not consistent with what we're hearing in the dealerships-- that customers are perfectly fine. They are not really caring that much about their privacy interests.

Quite to the contrary. What we're hearing is-- we're getting a lot of questions from consumers. They're asking the dealers; we're fielding the questions at NADA. What do I tell them when they ask me what's going on in my EDR, the black box in there? What's being collected? How do I sync my phones? How do I un-sync my phones?

In fact, there are some YouTube videos out there, if you go on. They're not professionally-made videos, but these are dealers who have gone out there and actually filmed videos about how to delete the communications information from your phone from your car. Why are they doing that? They're doing that because they're getting questions from consumers.

What the consumers are asking about is the information that they know that's out there. They know there's a black box because they've read about it. They know that their phone is synced because they see it syncing. So they are asking questions about the data in their car and how they can ensure that they're private.

In fact, we've gotten enough questions from consumers that, working with the Future of Privacy Forum, who pinch hit on the last panel, we've actually produced a brochure that the dealers are handing out in the dealerships about personal data in your car. Again, we'll get into some of the content of this. And I know there's going to be some more detailed questions. But the point I want to make here is, why did we produce this? We produced this because the questions were coming in.

So the question is, is it overblown? We think that these are legitimate questions about confidence in the car. And we need to be listening to what the consumers are saying.

And finally, there was some talk about some surveys that suggested it. I've seen a number of surveys that go the other way, that customers actually indicate that they're not ready to make some of those trade-offs. Whether or not survey data translates into actual market behavior is another question. In fact, we think that the consumers are concerned about this. And that's why this is a good conversation to have.

PEDER MAGEE: Thanks, Andrew. Jason?

JASON CARTER: Wow, there's a million thoughts going through my head right now. And I don't think I can talk that fast. But first, I'd like to thank the FTC for inviting me. I've thought about connected vehicles and, in particular, V2V communications for about four years. And maybe I'm on this panel because I've actually re-identified using de-identified data and understand what's involved with that.

So one of the comments that was made, I think, earlier and maybe just now was, some people may not be that concerned about privacy. And I think about that. And I think that we're moving into, like many have said, a new age where people don't know what the realm of the possibility is with this data. So it's not that they're not concerned. It's that they're not aware of what an adversary can do with the data.

And we talk about and use a lot of terms with this data, like it's anonymized, it's de-identified, it's sanitized. But we don't know exactly what that means. So I think we have to begin to be very clear. Not only what we're doing to protect people's privacy, but also inform them what the realm of the possibility is, and that we're protecting against that in terms of looking at it and informing people about the adversary and what their capabilities are.

So one thing that I wanted to make clear-- and there were some comments this morning. My expertise is in V2V. BSM, Basic Safety Messages that are in connected vehicle communications, they do not contain unique identifiers. They contain ephemeral identifiers. There are things in Basic Safety Messages that can be used-- so let me go back a second. So there's a difference between personal information-- and I would call BSM a personal information because it's a geolocation and a time. But it's not identifying information. I think we have to be clear about that.

And so, I guess my point that I wanted to lead off with is, this is such a complicated area, because I've looked at this data and I know how difficult it is to actually do some of the things that people think you can do. It's not trivial. There's not even a timestamp in the Basic Safety Message part one that you can work with. There's a rolling counter in that data. So if you just give people certain aspects of this data, it's very difficult to do some of these tasks. I'm not saying it's impossible, though.

PEDER MAGEE: Hilary?

HILARY CAIN: Yes, so your question was, why is privacy important? And I think as far as we're concerned, if we're going to expect that consumers will accept these new and emerging technologies, they're not going to do so if there is a lack of confidence and trust in the technology. And privacy is a key part of that.

You asked also, based on the last panel, whether privacy is overrated. And I think the resounding answer is no, which is why-- and this was alluded to in the last panel-- the auto industry came together a few years back and decided to put together what amounts to a self-regulatory code of conduct to govern the collection and use of vehicle data by automakers in the United States. Very much inspired by the FIPPs-- a lot of emphasis on transparency and openness and disclosure.

But also, to some of the issues that Joe raised, we went a step further and actually put some rather-- I would deem-- meaningful prohibitions and restrictions in the code of conduct. Things like, for example, we are prohibited from using sensitive vehicle data for marketing purposes in the absence of affirmative consent by the owner of the vehicle.

To the concern about data brokers, under the privacy code of conduct, we are prohibited from sharing sensitive vehicle data with unaffiliated third parties in the absence of affirmative consent. So we took some, I think, really robust and meaningful-- we're very, very proud of what we did in the privacy principles and they were to address a lot of these very concerns that we've been hearing about.

PEDER MAGEE: Great. So we heard the metaphor in the last panel, but it's repeated, that some people describe connected cars as these two-ton computers, or the rolling living room. Obviously there are differences, but with respect to privacy, is there anything particularly unique for connected cars? Or are the issues the same or similar to things we've already seen, like tracking of consumers' web browsing, or collecting information through the IoT-connected devices in the

home? And maybe I'll send this down a little bit to get everyone involved. David, if you'd like to take that one?

DAVID STRICKLAND: Certainly. And it's really nice to be here. Thank you for the invitation. It's nice to see the folks at the FTC I worked with for a long, long time over when I was at Senate Commerce, and my old former colleagues from NHTSA that are here. And I saw Dana Sayed over in the corner over there and a few others.

You know, the answer is-- I think the issue with the Internet of Things and privacy is, it needs to be a comprehensive approach. You can't delineate between because it's a vehicle that moves, versus a refrigerator that reads a barcode, versus a scale, versus a whatever it is. And we start writing different rules for all of these things. They're all collecting data. They're all leveraging data for particular uses.

And I think that, as Hilary said, everybody in the Internet of Things has to be cognizant of, no one is going to accept or use your product if people feel it is being leveraged in an inappropriate way. And I think that's just a general principle that I think we all need to be guided by, whether it's the auto privacy principles or other things.

So the answer is, do I think that automobiles are a unique case in terms of thinking about privacy of individuals and PI, things of that nature? No, I don't think it's unique. There are some unique situations when you interface that with the National Traffic and Safety Act to include defect authority issues and things of that nature, where information and vehicle diagnostics and the safety come into play. But I think once you divorce that specific engineering principle, in terms of how you sort of deal with-- does a vehicle work appropriately? Is there an unreasonable risk to safety? It becomes a part of the Internet of Things and I don't think you need to make that kind of distinction.

PEDER MAGEE: Jason?

JASON CARTER: Yes, so I come at this from a computer science perspective. And I just sort of look at the problem. It may be a little bit trickier-- or a little bit easier with connected vehicles, because they're constrained. There's a road infrastructure that they need to drive on. in terms of the V2V data, it's being broadcast at a very high rate. It's using very precise GPS. And so we need to think about it in terms of the context and the constraints around that data.

Now, in addition to that, if you look at cell phone data and the GPS that's pulled off that, of course people are unconstrained. So they can go places that are potentially more private than where you can go to in a vehicle. So that's in play as well.

PEDER MAGEE: Charlie?

CHARLIE HAAKE: Well, I think one thing I would add is that there may be some circumstances where you may strike a different balance between privacy and safety in the auto context than you would elsewhere. And that's because we all share the same roads. So there may be some circumstances where you might want to give a consumer in a non-auto context the

ability to opt out of having information gathered from them. But in the auto context you don't want to give them the opportunity to do so, because they're sharing the road with someone else. And they may have a circumstance where people need to know where they are or where they're going, so they're not hitting another car or causing some other sort of broader societal problem.

JOE JEROME: So I guess I would just jump in to say that I think one of the very big, big differences here-- and we have to keep this in mind-- is that cars are a significant investment for consumers. In the last panel we were discussing how in X amount of time most of these cars are going to be owned by someone else. But we're not there yet.

The vast majority of Americans still own their own car. And they spend a lot of money to do so. And I know that the Federal Trade Commission is spending a lot of time trying to figure out what exactly the value of privacy is. But there's plenty of studies that show that as consumers buy products, as they are paying for something-- regardless of whatever a company wants to promise them-- they are expecting more privacy. That just is a situation that exists.

And so as we are moving from this universe where I think a lot of-- at least my time in privacy has been focused on privacy issues where it's data in exchange for a free service. Well, we're not having that anymore. We're having A, significant upfront investment in a product, and then ongoing subscription services. And as a result, I think consumers have every right to expect more privacy. And I do give the industry credit and Hilary credit for being proactive. And consumers should be expecting that.

PEDER MAGEE: I think Andrew and then Hilary.

ANDREW KOBLENZ: Yeah, a couple of comments. One is, there are aspects of the vehicle that-- I agree with David that we need a comprehensive approach. But there are aspects of the vehicle that present some very specific types of activity that we need to address. The last panel actually flagged one of them. More than other IoT devices, cars are almost certain to have multiple owners. And there are transitional privacy issues when owner A is departing his ownership relationship and owner B is taking it over. And we can get in and talk about some ideas that we have to address that.

Secondly, vehicles have multiple users-- many users passengers in the car, not just the driver. So there are privacy concerns, depending on the nature of the data that's collected. Maybe some of the biometric or camera, physical data that's being collected, if we get to that, is a consideration that is not present with other things.

Third, and it was mentioned on the last panel, vehicles last for a long time. Actually, I don't think-- the useful life of a vehicle is 11 to 12 years. That's the average age of a vehicle in this country. The useful life is like double that.

SPEAKER 1: Yeah. Way more, about 20 years.

ANDREW KOBLENZ: So then we get into issues about keeping software up to date. And I want to tip my hat very strongly to the two manufacturer associations. They are really leaning forward

heavily-- unlike any other industry that I'm aware of-- in doing those principles. And they've made some commitments, fairly substantial commitments in there, which is great. The fact that these cars last for a long time means we have to look at those software updating issues to ensure that the privacy commitments that have been made are able to be maintained and kept.

I know the FTC had a case a while back with the Nest smart home hub, where the failure to support it-- actually it turned into a brick and the commitments that had been made weren't able to be honored. Well, we don't want to have that situation with the cars, because they last for a long time. So I think there are some very specific ways in which cars are different. They present new applications of privacy considerations that we have to focus on.

PEDER MAGEE: Hilary, do you want to--

HILARY CAIN: Yes. So I think earlier today someone made this distinction. I think it's a critical one. So I think there are parts of a connected car that are very similar to a web browser or another Internet of Things device. And I'm talking mainly about your telematics systems and that sort of thing. And then there is another part of the connected car that's, I think, very different than your connected refrigerator or your Nest thermostat or your web browser. And that's what we've been talking about in terms of automated driving and vehicle-to-vehicle communications.

And these are technologies that are intended to avoid crashes, right? And the reason I point out that there's two distinctions is because I think when we talk about privacy, there is sort of a the risk to privacy versus the benefits discussion that needs to happen. And I think that's a very different calculus when you're talking about telematics-- you know, accessing your OpenTable account from your vehicle-- versus an automated driving system that's intended to prevent people from dying in car crashes.

PEDER MAGEE: I think we'll get into that in a little bit. I just want to call on Adam. He hasn't gotten in yet.

ADAM THIERER: Thanks, Peter, and thanks for inviting me here again to another great workshop that the FTC is hosting. Because I was thinking, coming here today, how many of these I've been involved with. Feeling a bit of a Groundhog Day thing going on, where we're having the same discussion that I've heard and I've sat on panels on about online advertising, big data, IoT, wearable tech; about is privacy important and how best to protect it.

And I think we always basically come to the same general conclusion that, yes, absolutely, privacy is very important. It's one of many different values, of course, we have to take into consideration and weigh in the trade-offs associated with various technological products and services.

I think the thing that's different in this particular context is that you have these corresponding values of security and safety weighing heavily on everyone's minds, because we're talking about two tons of rolling code down the road, as opposed to just like a computer that might malfunction, or something like that. So those are clearly pressing values. But so, too, are cost and convenience factors.

My daughter right now is entering the phase where she wants her first car and she doesn't want dad's, mostly because she can't figure out how to connect Instagram or Snapchat on the dashboard, you know. Everybody does have different values. But she cares deeply about her privacy. And she would never-- she would totally reject the idea that this generation's somehow different in that regard. But she has many other values that she weighs in this calculus.

I think the other thing that's really different here is that it's clear to me the auto sector has really learned from these previous experiences and discussions that we've had about these other technologies. We've come out with a sort of standard set of best practices or codes of conduct in these other workshops that reflect an effort to instill the best of the FIPPs and other good best practices in terms of privacy and Security by Design into the product design and development process.

And it's very clear to me that the auto sector took that very seriously, and has embraced those principles preemptively, and put together, obviously, what I think is a best-in-class set of best practices, in terms of the consumer privacy protection principles. And I'm hard pressed to know how that could have been much better or what the higher bar would have really been in this regard, because I think it's better than probably any other sector of the modern technology economy in terms of what's been agreed to in terms of best practices.

PEDER MAGEE: We'll get into the principles a little bit. Maneesha's got some questions to start.

MANEESHA MITHAL: OK, so I want to move on to a new segment about-- I think one of the million dollar questions in privacy and, I think, the application of connected cars is really interesting. And that is, how do we apply the Fair Information Practice Principles? I feel like there's emerged Team Notice and Choice and Team Use Limitations. And I was going to ask for a show of hands as to who supports which. But I don't know that they're completely mutually exclusive. And there may be some overlap between those two categories.

So to kick off the discussion, I thought I'd start by asking the question of, in the connected car space are there unique challenges associated with providing notices and choice? One that I can think of off the bat is the multiplicity of actors involved in this space. You have the OEMs, the dealers, the rental car companies, the aftermarket products, the service providers, and suppliers. So what effect does that have on notice and choice?

And who wants to kick off the discussion? David, why don't you start?

DAVID STRICKLAND: I can give a little context in terms of where the responsibility lies on the safety side of things, which actually speaks to maybe-- flows down to maybe an imprint of maybe how the Commission could approach this. Ultimately the onus or responsibility for the vehicle falls upon the assembler, or the OEM, because you do have so many vectors into building a vehicle. You have the multiple tiers of suppliers and things of that nature. And ultimately, for the efficiency of trying to manage the safety universe, the responsibility is handed to the manufacturer. And then they distribute responsibility through contract to everybody else, in terms of if there was a defect problem.

If you think about it in the privacy context, I would say, Maneesha, that it really is contextual. There are some aspects of it in how you think about the FIPPs, as in my prior comment. It is an Internet of Things. And I think Hilary said it best. It's telematics, it's those things that are really more consumer facing where I think we have an expectation that it should not be, frankly, differentiated from, frankly, any other thing that has that sort of commercial facing.

But when you're talking about the way we evolve the vehicle fleet, and if you're talking the privacy practices or safety, you're going to have to collect a lot of data in terms of how you deal with defect investigations, how a manufacturer sort of deals with vehicle safety research on how they evolve their system. So there's going to be a lot of data generated by the vehicle that frankly the consumer has no understanding of-- or any utility value for. And it doesn't even speak to their particular PII or any impact upon them personally.

But it is the lifeblood of how the manufacturing community evolves and develops safety systems. I mean, we could talk about electronic stability control from 1990 all the way up through crash [INAUDIBLE] breaking up to recent times. So you have to think about the context of the information, of how it's being used and what it is for.

And I think that's part of the hard work of the privacy principles that the two associations have put forward. But then, how we can make sure that we don't starve research and development in making sure that we have safer cars in the future, or the development of automated vehicles.

MANEESHA MITHAL: OK. Jason?

JASON CARTER: There's a thought that always rolls around in my mind when I think about data. And I'll use this analogy. So I always think about seat belts; there's laws for seat belts. I put on my seat belt to protect myself. What we're talking about is--

SPEAKER 1: Thank you, doctor.

[LAUGHTER]

JASON CARTER: It's the right forum.

[LAUGHTER]

So technology is fueled by data. And the tremendous improvement and promise of the safety impact of this, saving lives, is just amazing. But in order to do that, the data that we broadcast is about us. We're informing on ourselves and our driving habits in order to protect others. And that changes the equation. I always think about that when I think about notice and choice.

So I'll get into-- people have talked about data classifications. I think it's quite easy. There's safety-critical data and there's non-safety-critical data. When it comes to safety-critical data and safety-critical systems, notice and choice becomes a very difficult question, because we're thinking about mandating some of this technology in order to save lives. There is no notice and

choice if there's a law and we require certain devices broadcasting certain data out to individuals. So we need to do all that we can to protect personal privacy when we do that.

And then there's data that's non-safety-critical. When you get into a rental car and you sync your smartphone with your system so that you can do certain things and access your phone book, and you forget to erase that when you leave the car, I mean that's non-safety-critical data. That's a different model. So we have to think about that.

And notice and choice certainly becomes relevant there in a little bit different context. And I believe this data is mine when it comes to non-safety-critical data. And I need to be able to have a way of erasing it. And I need a way of knowing how it's being used and that it doesn't move between different parties that I'm completely unaware of how it's moving through when you read the privacy statements from various vendors, how that's working, so.

MANEESHA MITHAL: So I want to call on Joe. And Joe, feel free to make the point you were going to make. But I wanted to see if you could also respond to, I think, something I heard from Jason about this kind of distinction between safety and non-safety-critical functions.

So I think the argument sometimes goes that when you have a safety-critical function, if you allow people to opt out of basic safety messages or however it is, then you're going to create less safe conditions on the road. So how do you weigh-- as a privacy advocate-- that ability to have choice versus the safety features?

JOE JEROME: So, A, I'd say that's a tough question. Speaking on behalf of the privacy community, I think sometimes-- and this came up in discussion of security updates-- where we get concerned that somehow that this is a back door to doing commercial stuff otherwise. And this was a big concern that I think almost uniformly most of the privacy advocacy community is having around the rollout of DSRC, where NHTSA has been very clear that it's working on privacy and security for safety uses of DSRC.

But it has no authority to deal with anything outside of that realm. And it's, I guess I would say, many of our contention that when you're having these radios in the car, you're going to also be able to do all of the basic safety stuff. But then you're also going to be able to do commercial things and other things that are more questionable.

I guess my other response to that is-- well, so we've called for to have an opt out. And I completely understand that the system may not work if not everybody's on board. But I think we also-- and I applaud the FTC taking on a subject like connected cars, because I think in many respects we're talking about issues with many different time frames. Some of these are near term, medium term, long term. And it's all converging into one sector.

But frankly, when it comes to the deployment of V2V, you're going to have invisible cars for a very long time, until you basically mandate that every car on the road-- that's currently on the road has this technology. You're going to have invisible cars. You're going to have old cars. We're talking about the lifetime of cars.

My 1997 Subaru Impreza is still being driven around today. And it's probably going to be driven around for another 10 years. And so as a result, we're going to have, basically, opt-outs and people not on board the system by virtue of the fact that these cars are going to be around a long time. And it's going to be unclear exactly how you're going to force people into the system.

Now, what I was originally going to say about provisioning of notice, I guess we had hoped, seeing the privacy principles, that there would be a little bit more experimentation. What it boils down to is, I think what most of the automakers have done is they've provided notice in the same old format. It's available online, occasionally via PDF.

And it's a giant legal privacy policy. There's not a lot of other information about privacy that most of the OEMs make available. Now, there's obviously exceptions to that. But in general, it's the same old, same old. And that's sort of problematic, because the privacy principles are very much focused on notice. And if that notice just defaults to privacy policies, that's not really improving the situation.

Considering it's a small-enough universe of OEMs, one of our suggestions would be some sort of centralized portal that allows consumers to compare these different privacy policies. We've been sort of reviewing OEM privacy policies. And, you know, it's very hard to track what's going where.

When you start downloading their mobile apps, you get taken to literally PDF documents for European data-protection principles. You get privacy policies that haven't been updated since 2013, so pre-privacy principles. And we've got-- the Auto Alliance has automotiveprivacy.com. And I think there can be a lot more on that website than just a link to the existing principles.

MANEESHA MITHAL: So I'd love for Charlie to comment on the question of whether you agree that this is same old, same old. But let me just throw another question into the mix. So Hilary mentioned that the principles require affirmative expressed consent before collecting sensitive information.

HILARY CAIN: Using.

MANEESHA MITHAL: Using-- sorry, using.

HILARY CAIN: For certain purposes.

MANEESHA MITHAL: Using, collecting, OK. And so I guess my question is, would it suffice to have some sort of a ULA or owner's manual? And kind of by virtue of driving the car, that's the opt-in consent. I just wanted to get a better read on what we mean by affirmative expressed consent. And you can feel free to answer that question or another.

So questions in the mix are, what constitutes affirmative expressed consent, what do you think about Joe's contention or statement that this may be same old, same old, and anything else you might want respond to. Charles?

CHARLIE HAAKE: I'll go in reverse order. So the question of whether or not it's same old, same old, I don't think that's the case at all. I think it's an evolving circumstance, because as the cars are evolving and as manufacturers are now finding the way that best fits their business model and best fits their consumers on how to implement the privacy principles, you're seeing different ways of going about it.

So for example, some manufacturers will have a pop-up on their infotainment screen. Every time you turn the car on it gives the privacy policy, right? And then you can say, OK, I'm opting out of that. And I don't want to see that all the time. And then go and do it a different way. I think what happens is that automakers have to figure out, what is the best balance for their consumers, because I can see how some companies would think that that is going to be an annoyance to their consumers. I don't want to see the same old notice every time I turn my car on.

So is there another way of doing it? Some automakers will have a disclosure at the time of sale to their dealers, and then afterwards send an email to the owner, because you usually have to give an email address when you buy the new car. And say, OK, by the way, just in case you didn't see it before, here are our privacy policies.

Here's how we're going about it. Here's the things we're going to do with our data. Here's the ways you can opt in or opt out. So I think you're seeing multiple different models of how the companies are giving their consumers notice about how they handle privacy. I'm sorry, what was the other question?

MANEESHA MITHAL: It was about affirmative expressed consent. I think you answered it.

CHARLIE HAAKE: Yeah, and that's a different way of doing it, so-- yeah.

MANEESHA MITHAL: OK, so a lot of tents up. Let me just-- and I think we probably have to move on soon. But let me actually call on Andrew to get the dealer perspective here. So the principles apply to the OEMs. And you had mentioned earlier that the dealer is often the link to the customer.

ANDREW KOBLENZ: Sure.

MANEESHA MITHAL: And so you're getting the questions from the customers. So what do you think? What is the dealer's role in all this? And do you have a view of the principles?

ANDREW KOBLENZ: Yeah. So the answer is yes. First, I want to, however, offer my good friend Joe-- if you want a new Impreza with some great features--

[LAUGHTER]

HILARY CAIN: Nice.

JOE JEROME: We'll talk after.

[LAUGHTER]

ANDREW KOBLENZ: With respect to the principles, as I said earlier, I think the manufacturers were very forward-leaning. They did stuff that nobody else has done. I don't think it's business as usual. So I really give them a lot of credit. And I also think that they've stepped up-- part of the question was, we've got all these multiple people. Who should be-- how do we get through the delivery mechanisms?

I think the manufacturers have basically said they're willing and are the right people to be the stewards of this. They are not the only one there, but they are the dominant one there. They're building the cars. They know its capabilities. They know what it's collecting. They're often the users. They know how it's being used. They also know who else can get in, or at least how-- putting aside cybersecurity issues-- what it's been designed to allow in. So I think the OEMs are the important stewards. And we support that very much.

The dealers, as I said, have a very important educational role. For at least all-- 100% of the new cars and for a big percentage of the used cars, the initial acquisition of the car takes place at a dealership. And there's an opportunity there to do more than what we do in other contexts. Right now the American Law Institute is grappling over consumer contracts and click-through agreements, and the adequacy of those disclosures and whether actual assent is being manifested there.

Well, we have that challenge here. But we also have an opportunity to do better, at least often. We can't do it all the time, but at least often. Which is to look to the dealers to do the role that they do best, which is to help explain all the features on the car to the consumer. After negotiating the terms of the deal, there is an opportunity. The consumer is excited to get into it.

One of the high points of the transition-- there's data on this that shows it's when you sit down and go through all the whiz-bang technology that the OEMs have put on the cars. The consumers really enjoy that part-- for a short amount of time, before they get to drive it off the lot. And easily woven into there could be some information about the data and the protections that are being afforded, the notice that they're being given, and the choices, to the extent that they have them. So I think there is a role there.

One comment about the principles or about the adequacy or the comprehensiveness of notice-- there was a lot of talk about the OBD-II dingles-- excuse me, dongles.

[LAUGHTER]

SPEAKER 1: Dingle's a member. Dongle's a thing.

ANDREW KOBLENZ: Thinking about the congressional implications here. The OBD dongles. And that brings into play other people. And I think we do need to focus beyond the OEMs, because there are a lot of other people out there.

And one way to do that is to drive a little bit more information into the system. Right now, I don't think it's possible for an average consumer to find out what information is obtainable by someone putting a dongle into the OBM. So when they are approached by someone who's doing that and they say, well, I'm going to maybe give you a discount on your insurance, they don't know what else is being pulled and how that information is being used.

If that information was readily available then we could drive into the marketplace of ideas concerns. And there would be articles written about it and questions about it. And maybe we could encourage people-- those third parties that we're talking about-- to behave better. At lunch today I bought a product that said it was gluten-free. To my knowledge, there is no law in this country that says it's illegal to sell products that contain gluten.

But what has happened is information about the consequences, to some people, of gluten has been out there. And purveyors of those goods have said, I'm going to self-regulate myself and offer it, because that's what people want. And if we had more information in the marketplace, those kinds of good behavior could be driven.

MANEESHA MITHAL: OK. Let me tee up a last question, then I'll turn it over to Peder again. And so this kind of gets to the use limitation part of the discussion. And I wanted to draw Adam in here. So a lot of people often mention use limitations as an alternative to or supplement to notice and choice. And so you can imagine a world where you say, OK, you can collect all this data for safety and operational benefits. But you can't collect the data for certain other purposes.

So I wanted to ask, is that kind of a workable model? And beyond safety and operational purposes, where would marketing go? Where would insurance go, on that list of prohibited versus permitted uses, versus uses you can opt into? So, Adam, any responses?

ADAM THIERER: Yeah, and just briefly relating that back to the question about notice and choice, it's important when we have a discussion about these things or these principles that we identify whether we're talking about notice and choice infusing a set of best practices or codes of conduct in a more voluntaristic way versus being applied more rigidly in a top-down fashion by law.

Because how these things are implemented and how they play out in practice are going to very much depend upon whether or not this is done through a multi-stakeholder best practice approach, which is exactly what's happened here and where notice and choice can play an effective role in infusing the process of how these best practices play out. Versus in a more legalistic or regulatory fashion, where it might become more of a rigid straight jacket and not allow more development of dynamic systems or policies.

As far as use restrictions go, there's a lot of discussion in the academic literature about privacy policy these days on all fronts, about whether or not we should move away more generally from the more rigid conception of FIPP and notice and choice and into a world of use restrictions or limitations on potentially very sensitive particular types of activities or behaviors that we might not want any data collected about.

You can always imagine sort of Chicken Little scenarios about like, oh my gosh, will they have things recording me in the cabin of my vehicle having this sensitive conversation, or smoking some weed or something? And will they report that back to somebody? These are not real-world scenarios for me. I'm just saying these are hypotheticals. But you can imagine, yes, there is a hypothetical there. And there have been instances of this becoming a problem in other contexts.

But the reality is, that hasn't seemed to manifest itself today. These are sort of truly hypothetical worst-case scenarios. And they shouldn't drive policy. But if we want to draw a narrow class of uses or behaviors or things like this where we might want to identify and say, this is what's off the table. That's certainly preferable to a world where everything's off the table and you've got to get permission to have any sort of innovation or experimentation with data up front.

Because if you spend-- this is what I focus a lot of my work on, is if you spend all your time obsessing about hypothetical worst-case scenarios and then base public policy upon hypothetical worst-case scenarios, then best-case scenarios will never come about.

MANEESHA MITHAL: OK. Does anybody want to respond to Adam? Charlie and then David, quickly. And then we can turn it over the next topic.

CHARLIE HAAKE: Yeah, I just wanted to echo what he just said. I think it's exactly right. I think the problem with use restrictions is if they're taken too far, then they can stifle innovation, right? So imagine a circumstance where, let's say, 10 years ago there was a use restriction that says that, thou shalt not take geolocation information and beam it off the vehicle to a third party.

Well, then that might have impeded a development of a system that'll allow you to let first responders know that your car got in an accident and let them come to the accident. So I think it's important that you not let, as they were saying, these potential worst-case scenarios to impede the type of innovation that we may not have thought about today, but may make our cars safer and more consumer-friendly tomorrow.

MANEESHA MITHAL: OK, David?

DAVID STRICKLAND: Very quickly, I just wanted to touch back on what Joe mentioned about V2V very quickly, and then I'll go to use restriction. At the end of the day, when you're talking about a safety system that's going to, frankly, require the broadest deployment to have the societal good, there's going to have to be some very difficult choices. And I appreciate that. And opting out of the system actually impedes the effectiveness of the system.

And ultimately when you're talking about-- not only are you trying to mandate it in every new vehicle, but you actually probably have add-on units so people can have benefits such as-- is it a '97 Impreza that you own? If you have a '97 Impreza and you want some congestion benefits, such as a "here I am" beacon that can actually change a light from red to green where there's no oncoming traffic, there's actually going to be a way to actually pull other people in, into the legacy market as well, which will actually help build that data.

So we have to be very careful about how you're going to cut this either way. Because ultimately, if V2V is done correctly and fully deployed, it addresses up to 80% of crash scenarios in unimpaired drivers, which is huge.

On the use restriction issue, I just want to put in mind, in terms of talking about level four or level five self-driving vehicles, which is a little more far-flung than a connected car concept. But when you're thinking about passengers that are no longer going to be drivers anymore, thinking about how like, you no longer have driver's licenses. How are you going to be able to convey certain information-- folks that are disabled, and how they're going to be able to use transportation networks.

So thinking about use restrictions in sort of a universe of today, versus how transportation networks and how level four, level five vehicles are going to come into the market, you're going to have to have some flexibility as to how data is conveyed and used before just simply setting forth a framework of thou shalt not. Because you will actually limit and stifle innovation, and frankly may cut off communities from individual mobility with that concept.

MANEESHA MITHAL: OK. I'm going to turn it over to Peder.

PEDER MAGEE: Thanks. So I wanted to ask a few followup questions about the auto's privacy principles. The notice and choice principles are directed to vehicle owners or a registered user. And my question is, what sort of protections are afforded to passengers or non-owner operators? And anyone can answer that.

CHARLIE HAAKE: Well, I think generally, it depends on the context. So, for example, if you are a passenger of a ride-sharing service then the question becomes, whose responsibility it is to let that passenger know, or the user of the service, what information's being collected. I think our position would be that it should be the service provider. So it should be the Ubers of the world saying, OK, if you've got our app and using our service, then we're the ones who need to tell you what may be collected about you as you're riding in our vehicles. So I think that's what we look at from that perspective.

JOE JEROME: So I just want to say that one of the things that I've found to be incredibly interesting about the way I think the OEMs have tried to deploy these privacy principles is-- GM, for example, if you look at their OnStar privacy policy, they have a section on drivers' obligations that state that drivers should be obliged to tell their passengers and secondary owners about the technology in the car, which I guess I give them credit for trying to address that in a privacy policy. I'm not sure that's the best place where they should have gone about doing that. But I think that that's really creative.

I think one of the things that I guess I would like to push back on about the privacy principles, and I've noticed Adam-- perhaps it was a Freudian slip, but he was talking to them as best practices. I still think there are some serious issues about what these principles oblige automakers to do, and what as a result they would oblige other people in the automotive ecosystem to actually do. Certainly they are grounded in the Fair Information Practice Principles,

but they by no means actually detail exactly what-- how they're operationalizing each of those things.

I will concede that car companies are giving users more information about their cars. But there's nothing really firm in the privacy principles about access or deletion rights. Again, data minimisation, de-identification, and data retention are three really interesting issues here. And they get one sentence in the privacy principles. And then I see sentences in here, that reasonable and responsible practices may vary over time as business practices and consumer expectations evolve. That's a relatively innocuous sentence. But looking at it from the view of a privacy advocate, it looks like a one-way ratchet against privacy.

PEDER MAGEE: Hilary-- and feel free to respond to what's been said or go back to the idea of what sort of protections are afforded to the passenger or--

HILARY CAIN: Yeah.

PEDER MAGEE: --non-registered owner.

HILARY CAIN: Yeah, so the development of the privacy principles was a long and, at times, arduous process. I mean, we struggled over a lot of the very same issues that are being raised today. And in some cases we were able to reach a consensus position and put that down and document it in the principles. And in other places we weren't.

And one of the areas that we did struggle with was, and ultimately came down on-- and I'm not saying it's the exact right place to be, but it's where we were able to achieve industry consensus, was on the principles covering owners and lessees-- if it's a leased vehicle-- and then registered users. So if you were to sign up for a subscription service through the OEM, that you would be afforded the protections that were in the principles.

So there are areas like passengers in vehicles that aren't addressed in the principles. There are areas like second owners. That was one that we struggled with for a very long time and didn't-- just like we don't have the answer today on this panel or in this room, we didn't have the answer in 2014 when we developed the principles.

But I think what you did see through that dialogue and that discussion, and I think what you are seeing in individual automakers now, is a desire to still-- this wasn't the end. I don't think anyone viewed the development of the privacy principles as the stopping point. It was the beginning point.

And I think you're seeing auto companies starting to think really creatively about what to do about some of these unaddressed questions. And maybe we'll come back at some point and codify some of them in the four corners of the document. But I don't think-- just because they're not in the privacy principles, that it doesn't mean that there aren't issues that the auto industry and the auto companies are still grappling with and trying to find resolution on.

PEDER MAGEE: That's a great point. And one of the reasons about asking the question, as to passengers, is it was an interesting concept that came out from the last panel. Which is, at some point people think that this autonomous vehicle technology may change the ownership model so that it's a mobility service. In which case, I don't own the car but I still need to get around. And if I don't have any privacy rights as a passenger, what are my options? Charlie?

CHARLIE HAAKE: On that-- I hate to use a legal term-- I think it's a question of privity, right? So if you are someone who signs up to use a ride-share service you have privity with the company that gives you that service. And it's that relationship. that would dictate who is responsible for what from a private standpoint. And so I think you're right. You need to be thinking about things from a different model, but then you have a different privity relationship between the consumer and the one either providing the good or the service.

PEDER MAGEE: Jason, I think you wanted to weigh in.

JASON CARTER: Yeah, a couple of comments. Just from some of my research about passengers, this may or may not-- I think it pertains a little bit. When you've got a vehicle and it's driving and you've got passengers in it and you're trying to use the data that comes off the car, the geolocations, when you have passengers it makes it much harder to re-identify people. And that's because the vehicle makes stops in very unusual places that you wouldn't necessarily expect. So in one sense, adding passengers to the equation makes things a little bit harder.

I'd like to follow that up with saying, this idea of opt-in, opt-out, and V2V-- I think privacy is improved if there's more people in the system. And that's because you see more data. It's harder to untangle the data, because all these identifiers are changing quite frequently. And so as your penetration rate of the technology gradually grows, I think things get better and better.

And another interesting thought that I had in all these discussions has to do with ride-shares and fully-autonomous vehicles and changing the ownership model. And that is, part of what I've investigated is how to fingerprint how people drive. And as you move towards a fully automated model in a vehicle, that automation removes that ability to fingerprint.

So fully-automated vehicles may make things more private, because all vehicles are consistently traveling in the same way. And this technology, part of what it facilitates is being able to have smoother traffic flows and less recognizable characteristics and features when you talk about drivers. So I think it's an interesting dynamic in how some of this technology affects privacy.

PEDER MAGEE: That is interesting. And it goes-- or I think it touches upon this concept of anonymization. And I know that the auto principles have a carve-out if you've de-identified or anonymized data. That can be a difficult standard. It's open-ended. Technology changes quickly.

We've seen cases where supposedly anonymized data, if you get enough of it together and you find some other touch point, you're able to re-identify it. Is there any standard out there right now on what's anonymized data, or what steps you need to take to anonymize it? And that's open to anyone.

JASON CARTER: I'll take it, because it's my research. That's my research area.

[LAUGHTER]

Yeah, this is a great question, standards. So with geolocation data, there are no real standard ways to do de-identification when you're talking about trajectory data, which is just time-sequenced geolocations. Lots of people are looking into it. It's a very complex problem. As the resolution or time granularity of the data becomes smaller and smaller-- for V2V it's a tenth of a second-- it becomes even more challenging.

There are a lot of techniques that have been applied from the medical community, like a researcher famously developed this method called k-anonymity and used it on medical data. It doesn't translate so well to the data that's coming off vehicles because of the dimensionality of the data. Medical databases may have 10, 12, 20 fields, whereas a trajectory on a vehicle that lasts 30 minutes may have hundreds of thousands of points. And you can treat each one of those as a dimension.

So there are a lot of strategies that people are using-- suppressing some of the data, generalizing the data, which means making it less granular. That has problems and impacts for safety-related research. If you take out precision of the geolocation, how is that going to affect how you analyze an intersection when your vehicle is 50 meters away from where it actually was. If you change the speed profile on vehicles, how does that change how you can do some of the dynamics? So this is a very active area of research. I think it's fascinating.

The one thing that I would say is, anonymization is the act of really confusing and being able to make indistinguishable different peoples within what we call an anonymity set. And when you have this high dimensional data that's coming off of vehicle trajectories you just cannot do that, because it would destroy all the value of the data.

And so one additional area that's very important in this space-- and people have hinted at it all over the place today-- is, what are we using this data for? So when you anonymize data, what does it do to your ability to analyze it and produce meaningful results on the back end? That's a very important question and another one that we're looking at. Anyways, that's--

PEDER MAGEE: Andrew, did you want to weigh in on it?

ANDREW KOBLENZ: I just wanted to make one comment about something else that was said. I would caution against us making too many policy decisions based upon the inevitability of the ownership model shifting. I know there was a speaker on each of the prior two panels that said it with kind of definitiveness, that the ownership model is going to change. Acting Chairwoman Ohlhausen cautioned us against making too many categorical predictions about the future.

There is one person who is the most important person in the auto industry. It's not Mary Barra at GM. It's not Secretary Chao. It's not David Strickland. It's not me. It's the consumer. The consumer is going to tell us what that model is going to look like. And I think there's an awful lot of indications currently from what the consumers are doing, saying, and wanting that shows us

that personal ownership of the vehicles-- even with all the advanced technologies-- is still very much in the future. So I'd just urge us to not assume the inevitability of that shift.

PEDER MAGEE: David Strickland is the second most important.

DAVID STRICKLAND: Hardly. Well, my one sidebar to Mr. Koblenz's comment is, you have a rancher in Cheyenne, Montana, with a Ford F-250, I'm not quite sure he's going to be all into the shared-fleet model of utilization. Just saying.

PEDER MAGEE: That's a great point. With that, we're going to pivot a little bit. Maneesha's got a few questions.

MANEESHA MITHAL: OK. So we're getting some great questions from the audience. So let me just kind of ask the final question that I had planned, which was, we're here at a workshop sponsored by the FTC and NHTSA. We are government agencies. What do you all think is the appropriate role for government in this space? And maybe I could start with the end of the table, with Adam. And we can move on down the line with anybody who has a comment on that.

ADAM THIERER: Sure. Well, we've already heard a lot of the answers provided today, starting with the basic authority of NHTSA and FTC to enforce its broad-based authority to go after unfair and deceptive practices in the FTC context. And NHTSA has other powers to recall and other federal safety standards. So there's already a lot of law on the books. And the question is really how it plays out or how it's enforced for new technologies.

I'll let others comment more specifically about that because I want to focus on something that's often forgotten, which is that when we talk about regulation we sometimes think too narrowly about sort of preemptive administrative mandates. Whereas regulation can mean a lot of different things, both legally and sort of culturally.

But let's just stick with legally-- and let's not forget that the automotive sector, for better or for worse, is one of the most heavily-litigated-against sectors in the US economy. And we have torts, and we have product liability, and we have common law more generally, to address cases and controversies that develop that we cannot foresee with great ability.

And this is exactly what Chairman Ohlhausen was talking about this morning, and having some humility about the future and our inability to have a crystal ball to be sort of a technological Nostradamus and perfectly predict exactly what the threat scenarios will look like, whether they be for safety, security, or even privacy. And we do have privacy torts that can address some of these things. And maybe after we've exhausted those sorts of approaches, then we go back and fill gaps as is necessary.

We have done this for many other technologies prior to this. And I think this is going to be the model that will probably play out in this context as well, buttressed with the sort of multi-stakeholder best practices approaches that we're seeing play out on this front that mimic what we're seeing across the entire landscape of emerging technologies, which is really sort of a new

model of soft law governance for technology, as opposed to more of a traditional rigid hard law approach.

And then just one final point. One thing that I think both agencies do quite well today, and I think we need more of, is more of a consumer education focus. A big part of what a lot of these agencies are doing in a soft law context is revisiting how best to do risk education. And it's a complicated thing. I think the FTC does a really nice job with a lot of what it does with things like OnGuard Online and Stop.Think.Connect and the YouTube videos that are up there, and all the promotional materials that go out.

And really it's a question of how to get those messages across to the consumer in the best, most usable way-- fashion. I know that's complicated. But I can find many great examples of where we've done this quite effectively. I talk about them in my writing quite a bit. And I think seat belts probably may be one of the best examples. It did have some law.

But think about how we changed cultural attitudes through education to the point where if I get in a car today and I don't have my belt buckled within five milliseconds, my kids are screaming at me, right? It's a totally different world than the one I grew up in 40 years ago, when I was bouncing around in the back of my mom's Gremlin without a belt on in a big glass death bubble, right? The world changes.

MANEESHA MITHAL: So I want to call on David. And I think Adam raised a great point about tort law. I think we're not operating in a vacuum here. We also have state laws that apply to these issues. So David, commenting on the role of government, keeping in mind we are not operating in a vacuum and there's state laws and tort law and others.

DAVID STRICKLAND: Absolutely. I'm actually going to use more of-- actually a true case study between the authorities of NHTSA and the authorities of the FTC, and how the two agencies work very well together and with particular jurisdictional spaces.

The new car assessment program that is run by NHTSA, the five-star safety rating program-- you know, more stars, safer cars-- has existed for over 30 years. And every manufacturer has adhered to the principles of, you can't do anything other than advertise a direct rating that you have been given by the agency. Well, for the first time, when I was administrator, we actually had a manufacturer violate that-- first time ever.

And also what we realized as an agency is that we have no enforcement authority on the NCAP program. We can't punish a manufacturer that has said, we have 5.9 stars. So what did I have to do? I had to go over and see Chairwoman Ramirez at that time, and have a conversation on how our two agencies can work together, clearly with the authority of the FTC, to help enforce the integrity of the five-star safety rating program.

Which once again goes to show, you don't necessarily need to go through and create a structure or fill direct bubbles for what you might think might be-- looks like a gap to me in 2017. The agencies appreciate and understand where their authorities are. And I think they work very well together in recognizing those. And I think that we had to be very circumspect.

I think Adam did a great rundown of why we have to be very careful about how we try to fill in bubbles that we may foresee versus actually having the agencies work through these issues thoughtfully. And if we do get to a point which is, frankly, not solvable through all the other jurisdictional authorities that deal with those things, then we may have to go for further law.

But I think the system works well. It worked well when I was there, and I'm not the world's best administrator. So the fact that it worked well speaks testaments to how great these two agencies are, so.

MANEESHA MITHAL: OK. Quickly, Andrew, Joseph, then Charlie. And then I'd like to move on to audience questions.

ANDREW KOBLENZ: I have two quick points. One is, the two agencies can cooperate. One thing they should cooperate on is trying to bring the rest of the world, the rest of the people in the ecosystem within-- to where the OEMs are with respect to their privacy principles. That's one.

And the other, I just want to underscore the importance of consumer education. We have partnered with both NHTSA and the FTC. With the FTC we have a actual brochure, comparable to this one, on vehicle financing that we have co-branded with them. And we would welcome the opportunity to work with both agencies to help get the word out. We are the place where the consumers are first touching this stuff.

MANEESHA MITHAL: Joe?

JOE JEROME: I guess I just wanted to quickly say, I think this workshop is a great, great start. I think many of us were advocating for something like this for a long time. And so it's great to see co-hosted workshops.

To the extent of what I think the Federal Trade Commission can do, I think you have incredible latitude to do more-- further investigations, both informally and formally. And then, it's always good to see the commissioners-- and hopefully new commissioners-- out and about speaking about these issues and sort of hammering the message home when they're at various auto trade-- basically, auto events and conventions. And there you have a lot of leverage, I think, to sort of push other people to get involved in the ecosystem. And join the OEMs in doing some proactive things.

MANEESHA MITHAL: OK. Last word on this, Charlie?

CHARLIE HAAKE: I just wanted to comment on the use of tort and product reliability law. And while I agree it's an important tool to make sure that bad actors are required to compensate victims of their bad actions, I think if you rely on it too much you lack-- well, there's two problems.

One is, you may have a lack of consistency because what a judge or jury in San Francisco might think is reasonable maybe conflict with what a judge and jury in Montgomery, Alabama, thinks

is reasonable. And it deprives manufacturers or defendants of notice of what may or may not be considered bad conduct. So I think it's important that that reliance-- it does have its limitations.

MANEESHA MITHAL: Great. OK, so we have an interesting question from the audience. So I think many people are familiar with the kind of browser-based tools for deleting cookies. And you can reset your "at" identifier in your mobile device. And so this question comes from the audience, if there is any thought being given to a uniform method for a simple factory reset for PII for non-safety issues?

HILARY CAIN: On board the vehicle-- or I guess we don't know.

MANEESHA MITHAL: It can be anything.

HILARY CAIN: Yeah, I mean one-- we were talking about this, I think it was in the last panel. And I'll just jump in here. We were talking in the last panel about like the rental car situation, or the second owner situation. And, my goodness, I guess we have to do more education in that space, because it's actually-- at least on Toyota vehicles, I can't say-- quite easy to find the button.

Because I just turned in a car a couple months ago and wanted to see how easy it was to find it. I didn't have to open the owner's manual or anything. I just clicked through a couple screens and there it was-- delete my data. And I-- are you sure you want to delete your data? Yes. And it was done. So maybe we do need to do a better job of educating consumers that that option is there and that it's quite easy, just a couple clicks and you're done. But it is there, at least on our vehicles.

ANDREW KOBLENZ: Yeah. We're not technicians. I can't tell you how to design it. But, boy, that would be a very big consumer satisfier. The way you can confidently either return the leased vehicle, trade it in, we have a checklist in here of all the things that you should go do-- your garage door opener, your home identifier on that. And we would love to see that big reset button, so it just puts it back to factory specs when you're changing ownership. That would be a great development.

MANEESHA MITHAL: OK. Peder?

PEDER MAGEE: Sure, I'll take a look at-- here's an interesting--

ADAM THIERER: Can I just say, while you're finding the next question, just one word of caution about these. When I hear sort of technocratic, silver bullet-type solutions to privacy and security, I always get a little wary. I think it sounds great that we would have like a little big button a big button on our dash that we click and it says, all data is data is deleted.

It seems to me like that's probably a bit simplistic, and probably entails some unintended consequences, not all of which I can imagine today, but I can see that that becomes a problem in the future. So I'd be worried about that, if mandated.

PEDER MAGEE: OK. An audience question-- can we have a car Alexa? Alexa would tell us about latest privacy policies. We would ask her to clarify. We would tell Alexa what date to remove, et cetera.

JOE JEROME: I think that is a phenomenal idea. No, I--

SPEAKER 1: Invent it and market it.

HILARY CAIN: That's what I was going to say.

JOE JEROME: I think what we really have to think about is-- and I don't want to point fingers at anyone, but automakers and the car industry spends a tremendous amount of resources designing these incredibly attractive and design-friendly machines. But then they're not really at the same level of making the software as intuitive as some of the software companies. And as we move into the IoT and you're having manufacturers involved in software, I think it raises a whole host of new design questions.

And we always look at things like the personal assistants-- so like Alexa, and like Home, which are an audio interface. And initially these products didn't actually let you ask questions about privacy. And now, increasingly, they do. That seems like a great idea. And it seems like something that-- the next generation of cars is to have more and more of these features, it should be pretty easy to just ask those sorts of questions.

ADAM THIERER: I would just say it sounds great in theory until the reality hits, when you say, Alexa delete all my locational data. And you say, well that's fine and done. And then the next day you go in your car and you're like, well, Alexa find me this thing that I went to last week, or three months ago. Right? And it's gone.

JASON CARTER: Or when that Alexa opens up another threat vector for cybersecurity.

HILARY CAIN: I was going to say, I don't know that there's a lot of privacy confidence in Alexa.

SPEAKER 1: Yeah, exactly.

[LAUGHTER]

HILARY CAIN: I don't hear that.

CHARLIE HAAKE: The problem is, the more you offer consumers by way of safety and convenience, the more you have to balance risks like cybersecurity and privacy.

JASON CARTER: I think, quickly, the intent of the question was, are there better ways to inform the users.

HILARY CAIN: You re-ask the question.

JASON CARTER: Yeah. And I think the idea is great. But yes, it is another attack vector, and somebody's going to take that out.

PEDER MAGEE: You've got to be creative, but you got to balance.

JASON CARTER: Yeah, but I think there are-- I mean if you think about your iPhone or your smartphone of choice, I mean the user interface-- there's a lot of research that went into that. And there should be the same research that goes into, how do you inform people about their choices in terms of privacy?

JOE JEROME: Better articulated than what I said.

MANEESHA MITHAL: OK. So here's another interesting one. So is location data on its own sensitive information? What about when it's coupled to information linking it to a specific vehicle? And what about when it's coupled to information linking it to a specific individual? OK. So we'll go Hilary and then Jason.

HILARY CAIN: Well I-- because this is an issue that we addressed in the privacy principles. So the privacy principles call out three types of data-- buckets of data-- as being sensitive. The first one is location information. The second one is driver behavior information, so how you drive your vehicle. And then the third one is biometric data. And to take it a step further, so it's not geolocation in and of itself. It's geolocation under the privacy principles that is linked to a particular vehicle or registered user, or reasonably linkable.

And I also will note that we took things a step further. We didn't just say linked. We said, or reasonably linkable. So if you couple, under the principles, location with linked or reasonably linkable, it is afforded a much higher level of protection.

MANEESHA MITHAL: Jason?

JASON CARTER: My perspective is, there is no-- two people can't occupy the exact same space at the same time. Therefore it's sensitive information. Because we can start to use that. And they're geotagging everything. So if you have that location and time-- and time is important-- then you can start building a case, and evidence, and start to do things that you really would never have dreamed you could do. Can you always do it? No. But it does start to open you up. So definitely it is sensitive information. And we need to be careful in how we handle it.

PEDER MAGEE: Well, there's just one last question I'll ask from the audience, because I think it'll be very quick. The question is, are the auto manufacturer privacy code principles voluntary? I believe they are.

HILARY CAIN: Well, they're voluntary, except for there's a list of companies that we signed our name that we committed to them. So once we did that and then filed them with the former chairwoman of the great commission here, I think we're-- they're not voluntary for those who signed on.

PEDER MAGEE: That's correct. The FTC has Section 5 authority.

HILARY CAIN: We knew that full well when we handed them over to you.

PEDER MAGEE: And the second part of that is, where could a consumer find out which companies have signed on?

CHARLIE HAAKE: You can go to-- I know the Alliance has a portal on their website. Global Automakers has a portal on their website. Some automakers actually have the document itself linked their privacy principles. So I think if you type in, automobile privacy principles FTC, you'll pull up the document and see, I think, all of the major OEMs, representing about 99% of the market, have signed up to them, so.

PEDER MAGEE: Thank you. And thanks to the panel. This was a great session, probably the best one of the day.

[LAUGHTER]

[APPLAUSE]

PEDER MAGEE: Great perspective.

HILARY CAIN: Thanks, guys.

PEDER MAGEE: Yeah, no.