FTC Connected Cars Workshop: Privacy, Security Issues Related to Connected, Automated Vehicles
June 28, 2017
Segment 2
Transcript

MIKE LEGOWER: Take your seats, please. I'd like to welcome everyone back from our break to our first panel for the day, where we're going to be discussing the data collected and generated by the technologies that we talked about at length this morning. I'm Mike LeGower I'm from the Bureau of Economics at the FTC and joining me is my co-moderator's going to be Kate White from the Bureau of Consumer Protections division of Privacy and Identity Protection.

I'm going to briefly introduce our panelists and then we're just going to get started, get right into our questions for the panelists. We're going to open up a section at the end of our panel today for questions from the audience. There are comment cards out on the table in the entryway, so please feel free to pick up a comment card and fill it out, and then when we open it up for questions from the audience, you can just raise your comment card and somebody will come around and collect it to answer your question. Or to pose your question to the panel.

So joining us today are Steven H. Bayless, who is the Vice President for Public Policy and Regulatory Affairs at the Intelligent Transportation Society of America, or ITS America. He is responsible for providing guidance to ITS America's Board of Directors and senior staff on matters involving new technologies, including evolving automotive platforms and intelligent transportation infrastructure.

Steven previously served as a Presidential Management Fellow in the US Secretary of Transportation's Policy Office and the White House Office of Science and Technology Policy, and had cabinet-level lead in policy related to traffic safety research, research and development, space and aviation policy, and spectrum management and telecommunications.

Next is Jeremy Gillula, who's a Senior Staff Technologist at the Electronic Frontier Foundation, or EFF, a nonprofit organization defending civil liberties in the digital world Dr. Gillula advises EFF lawyers and activists on a wide range of technical and policy issues, including big data, drones, mobile and online privacy, net neutrality, and autonomous and connected vehicles. During his academic career, Dr. Gillula's research focused on robotics and machine learning, including sensor fusion systems for autonomous vehicles, machine learning systems for drones, and the design of guaranteed safe machine learning algorithms.

Next is Dr. Christopher Hill, Principal at Booz Allen, where, he leads the firm's transportation business. This includes Booz Allen's work for the FAA the surface modes at US Department of Transportation, Amtrak, and the US Postal Service. Chris has more than 30 years of professional experience focused on intelligent transportation systems and connected vehicles.

Next, we have Brian Markwalter, a Senior Vice President of Research and Standards for the Consumer Technology Association, or CTA, a trade association promoting growth in the 285 billion dollar United States consumer electronics industry, and owner of the International

Consumer Electronics Show. Mr. Markwalter is responsible for CTA's extensive consumer research, market data, and forecasting capability, in addition to CTA's accredited standards development program used by industry in millions of products every year.

Next, we have Carrie Morton, who oversees day-to-day operations of Mcity, the University of Michigan's public private partnership, devoted to advancing the development of connected and automated vehicles. She joined the university in 2011 after more than a decade in the automotive industry, primarily with the Robert Bosch Corporation. In her last role at Bosch, she was Manager at Government Projects and responsible for leading all publicly funded research projects, with a focus on engine combustion.

Next, we have Stephen Pattison, who is the Vice President for Public Affairs at ARM, which designs microprocessors used in many products, including over 90% of cell phones. In addition to oversight of ARMS Corporate Responsibility Program, Stephen is responsible for ARMS contribution to public policy thinking across the world on key issues, including Internet of Things, smart cities, data protection, energy efficiency, and security.

And finally, we have James C. Wilson, who is the head of US Government Relations and Senior Legal Counsel at BlackBerry. He's responsible for a number of legal and business issues, including matters pertaining to BlackBerry QNX, a leader an autonomous vehicle operating systems, with software in more than 60 million cars. I'd like to welcome all of our panelists for joining us, and thank all of them for joining us today.

So to start off, I'm going to direct this question to Carrie Morton. We've heard a lot today about safety and vehicle operation, but to sit-- sorry. We've heard-- as we've heard this morning, in order to provide all the potential safety and efficiency and convenience benefits, connected cars are going to need to collect a tremendous amount of data. What types of data will be collected for advanced safety systems, vehicle-to-vehicle communications, and automated vehicles?

CARRIE MORTON: Well, thank you. That's a great question, and I think Nat did a great job of sort of laying out the overall picture of that. But I think we see the future as electrified, connected, automated, and eventually shared. And so in order to do that, we have to envision the vehicle becoming truly part of the Internet of Things.

Consumers are going to be a lot less tied to the individual vehicle that they're in, and in addition to the safety aspects that those vehicles will be acquiring and sharing data for, they're also going to be a tremendous amount of consumer experience inside the vehicle, which I'm sure Brian can talk about. Imagine the trillions of dollars worth of our time we spend in vehicles and how we bring content to the drivers is going to be an important part of that. But I'll focus a little bit on the safety and automation aspects.

So first of all, having access to the OBD port, as Nat mentioned. So what is on that port and why is that important? So a lot of vehicle communications about the subsystems in the vehicle that sort of-- let's think of it as the muscles, the brain connecting to the muscles. It's part of the central nervous system of the vehicle, exchanging lots of detailed data about the operation of those subsystems.

So why would one want to access that information? So you can think about things like your throttle position, your speed, how you're applying the brakes to the vehicle. A driver's applying the brakes-- all of that information can be pulled off of the CAN bus through the OBD port.

That's interesting for a number of reasons. If we envision a future where connected and automated vehicles are more efficient, having access to the operation of those vehicles is really important, and understanding, for example how can we inform the driver of even a partially-automated vehicle to operate that vehicle in a more efficient way? We need all of that detailed information. And that would have to be shared at least on board with the vehicle, or on board with the driver of that vehicle.

We see, as Nat mentioned, dongles also taking advantage of that information. If I am an insurer, I can tell a lot about how you drive based on the relative throttle position when you're driving the vehicle, as well as your braking habits. How many times do you, for example, apply the brakes in a panic braking situation? Which might lead you to make some assumptions about how often you might have a rear end-- be involved in a rear end collision, for example.

But some of that information can also indicate the state of the health of the vehicle. Vehicle manufacturers may be able to glean from that information when certain subsystems are not behaving properly, whether it be safety-related, related to, for example, the engine operation. And by providing that data back to the vehicle manufacturer or dealership network, you can bring those issues to the consumer so the vehicle can be looked after.

This is going to be even more important when we think about automated vehicles being deployed out on their own to be able to communicate the state of health of the vehicle, including the state of the health of the safety subsystems that are critical for operation. That's going to be really important.

And then finally, thinking about a vehicle-to-vehicle information. They're specifically related to DSRC, or Dedicated Short Range Communication. These vehicles, through years of standards work are now in interoperably sharing their precise GPS location, their vehicle speed, their predicted path, and whether or not they're in an emergency braking scenario. And they're doing that 10 times a second, and that allows the vehicles to warn the driver of an impending crash scenario. But it's important to note that that data is in a broadcast format. It's not being stored onboard the vehicle. It's just there to inform the other vehicles in the surrounding area.

And, as Nat also mentioned, when we think about AVs as the next step and the sensors there, you can think about all of the sensor or perception technologies sort of like our five senses, and each one of them has vulnerabilities, and being able to understand those vulnerabilities-- when does lidar have challenges in performance or perception, versus cameras, radar, lidar?

Adding conductivity is like adding another sense where we can see beyond line of sight, and the cameras, lidar, radar, all the OEMs are collecting data now, but it's not clear that that will be-- to train models, machine learning algorithms, for example, to train these models. But it's not clear that that data, in any way, is going to need to be recorded or transmitted in a future state in a production state. So, I think that's-- Yeah.

KATE WHITE: No, what about today-- maybe this question is best for you, Brian. Today, when people are getting into their cars and they're sort of putting aftermarket products into cars, what sorts of information is being collected then?

BRIAN MARKWALTER: Sure, so there is a huge range, and I appreciate the care that was taken by some of the speakers today. Well, first of all, let me thank you for inviting us here and for the shout out for CES and Acting Chairman's trip in an autonomous vehicle. But I do appreciate the care that has been taken in trying to distinguish where we are in the road map of things, and that we are not really at automated vehicles, at least from a consumer perspective, today.

There are a huge range of aftermarket products available. Carrie just mentioned some, so there are insurance dongles that are provided, and there have been ODB to port diagnostics available for a long time, plus things you carry into your car. So I think most of those are done, I'd argue, all that are driven by consumers, and it's a consumer choice.

So it's a pretty well-understood-- there, I would expect no, if they're putting a device into their car, their insurance company says, we're going to monitor your driving and give you better rates, which is pretty much the pitch that's made. And that's well-understood. And so there obviously has to be some driving-related data to it.

And then there are aftermarket backup cameras. Almost everything you see that's being developed, sometimes ahead of the OEM market and sometimes after, there are aftermarket analogies to that. So I think our belief is that these are helpful, particularly to the extent they increase safety or provide some convenience. I think most consumers are willing to make some trade off of, I'll provide some information in order to get a better service.

That's, in some ways, the basic proposition of a navigation app like Waze is you're clearly sharing information. Sometimes you're literally telling it information. You're also serving as a form of a pilot vehicle, which companies have tried to do for a long time. And there's a huge benefit to everybody involved, I'd argue, even a societal benefit, based on knowing what's ahead in the road and improving your transit times. So anyway, we'll, I'm sure we'll get into more of this as we go along.

KATE WHITE: And going forward as we start to-- I know we can perfectly see the future, but as we start to get towards more automation, do we think that there'll be a lot of driver behavioral or even biometric data that might be collected?

BRIAN MARKWALTER: So I can tell you-- we see a lot at CES, our show. So there are systems in cars today, I believe, Audi, Mercedes, and maybe one other. So there are systems that are, for example, let's just look at distract-- or, drowsy driver systems, that pay attention and try to get some warning about alertness of the driver. That's available today, as an OEM product. Those systems look at, as far as I know, they are looking at vehicle behavior. There's no-- there's nothing monitoring going on of the driver itself.

So they're looking at kind of behavior of the vehicle and inferring something. At same time, we've seen products and companies working on systems that are directly, either by camera or other means, there's companies talking about doing heart rate monitoring and some other technologies to help with driver or alertness. I don't know if any of those are shipping just yet. They may be. Nvidia certainly showed some systems, I think. Denso and some of the other OEMs are working on systems to do this.

So I think there's a little bit less that's in the market right now, but a lot of work going on in that area. And presumably, you do a better job, and I think in some cases, there are some things that consumers will want to have happen and it would probably make our car safer. Certainly doing away with distracted and drowsy driving, or even impaired driving, would be-- well, I heard the stat today, 10,000, something like 10,000 fatalities attributed drinking. So if we can deal with some of that through sensor technology, as long as it's transparent what's being monitored and what's happening with your data, which is what we usually advocate for, then I think it's acceptable.

MIKE LEGOWER: So I'd like to add, if anybody wants to jump in after any of these, just let us know and we'll be happy to let you have your say. So let me ask Jeremy, so Nat talked a little bit about V2V this morning, and we just wanted to get-- let the audience know and get some information about what information is contained in the basic safety message that's going to be sent via these DSRC channels. So could you-- do you have any-- could you enlighten us on that?

JEREMY GILLULA: Sure thing. So Carrie already talked about it a little bit. So these are messages sent out, broadcast by your car equipped with it. Obviously, right now, only very few models, I think, are. But of course the proposal by DOT is to eventually make that standard. And so it includes things like your GPS location, the path your vehicle's traveling, speed. It includes information about your vehicle's size.

So if you're-- from that, you may or may not be able to infer what the actual model of the vehicle is or the make. It also includes-- at least, or it will include, as proposed by DOT a unique cryptographic signature, so a unique identifier for your car. The idea is that these will rotate once every five minutes over the course of a week, and then you switch to a new one, a new set, basically every week. So it is a unique identifier but it's a rotating one.

But in addition to that, it would also include, for that signature, that cryptographic signature to be valid, it'll include who, basically, what entity assigned you that ID, which will presumably be either the manufacturer or some-- I mean, the system hasn't been decided yet. And so that would also be able to help someone who's receiving these messages determine what make or model you have.

Because presumably, a Volkswagen is going to get its signatures from-- or, its cryptographic signatures from a different place than, say, a Toyota, just because the companies are going to do it differently. That's, again, that's still a little hypothetical because that system hasn't really been worked out yet. So there's basically a lot of safety information and a lot of identifying information that will be broadcast, basically, once every tenth of a second.

CHRISTOPHER HILL: Can I just tack on to that? Because I think it's important to remember that for the federally sponsored connected vehicle program, NHTSA's proposed rule, the system was specifically designed with individual privacy and non-trackability in mind. So there's been a lot of protections put in place to ensure that you can't identify an individual vehicle or an individual driver.

And in fact, you're absolutely right that there's still a lot of uncertainty as to what this credential management system may look like. But I think the current thinking is that, again, it wouldn't allow you to get to the point of saying, I'm a Toyota a VW. At least, that's the federal government's position on how they would design this.

JEREMY GILLULA: So the-- so if you look at so Mitre actually. DOT hired Mitre to analyze the privacy and they determined that under various circumstances, well over-- the majority of cars could be individually tracked under this system.

It depends on the circumstances, what sort of coverage you have of the sensors that can receive this information. And so there are-- certainly they tried. We appreciate that they definitely put some effort into making it privacy-preserving. It's not there yet. Certainly the system as proposed would not protect privacy in any real meaningful way.

CHRISTOPHER HILL: I have to disagree, though, so--

JEREMY GILLULA: I mean, you look at Mitre's report, and that's what it says.

CHRISTOPHER HILL: You could look it a Booz Allen report that we did for NHTSA, and we would disagree with that position. So you know--

MIKE LEGOWER: I think Carrie--

CHRISTOPHER HILL: --there are differing positions on this, I think.

KATE WHITE: Absolutely. Steve?

STEVE BAYLESS: I just wanted to put this into perspective. What we're really talking about here is primarily vehicle-to-vehicle, but we're all sort of used to-- in general, connected cars have been around for a long time. There's a basically decade-old data ecosystem industry that we're all used to. When you use Google Maps, you can look exactly where all the traffic is. Most of that data is crowd-sourced from commercial vehicles, some of it from mobile devices, as well.

So the difference between that kind of connectivity and some of the privacy issues that are raised dealing with that kind of connectivity and the V2V connectivity are, in some cases, similar, in some cases, different. And I think one of the things-- the difference between knowing whether a particular road segment is red, yellow, green-- by the way, there was a huge debate over what constitutes red or yellow. I was part of that and I had to quit. So the--

[LAUGHTER]

But they finally decided what red means, and I think, actually, this is being driven by JD Powers and some of the folks that were looking at quality, vehicle quality. But overall, essentially, red, yellow, green doesn't tell you very much about-- we were talking about it tells you whether there's congestion on the road.

It tells you what to expect, might be able to route you around that congestion. But it doesn't tell you exactly what you would have to do that in that particular circumstance. It can predict, based upon massive historical data sets and analytics, what the congestion would be at that particular time of that particular day, given the weather conditions or whatever. But it can't really get you really discrete data. That's really the purpose of vehicle-to-vehicle is to get that level of discrete data that can actually help you make decisions on a second-by-second basis, literally.

And I think one of the things that-- it's-- so, generally, I think the auto industry has been very supportive of this. My industry association also includes not just the automakers but folks that manufacture traffic management systems, and the thing for traffic management systems is that, while typically 50% of congestion is reoccurring, the other 50% is usually traffic incidents, non-fatality crashes, fender benders, or it's just poor traffic management. It's just that they don't have enough data to sort of process vehicles through intersections fast enough. They don't have enough data to prevent crashes at intersections.

So the example that-- for example, knowing that a heavy vehicle is bearing down on the intersection, knowing the size of that vehicle and the weight of that vehicle, you can predict where that car is going to be able to brake in time. And so a really smart traffic signal can basically say, OK, I know this vehicle is bearing down. He's not going to make the intersection. He's not going be able to stop before the stop bar, so I'm going to hold the red for two seconds or for a second and a half so that he can actually stop.

So it's these kind of decisions that are getting made on a minute-by-minute basis. Is the privacy issue-- are there privacy issues that need to get addressed in looking at this level of discrete data? Of course. There are issues that have been addressed in the past, just dealing with sort of macroscopic traffic information, as well.

So I just want to put that in perspective, because there's a reason why we do want to share this level of data. There are issues related to being able to de-identify, obfuscate the data so that individuals are not being tracked, but it's something that I think the auto industry and DOT has been focusing on. Again, the standards were developed, the privacy requirements and the security requirements that were developed were the first requirements out of the chute before any technology was ever put out in the field.

JEREMY GILLULA: I feel like I should just point out that I'm-- as a privacy advocate, I'm not saying that we shouldn't have this sort of technology. What I'm saying is that there are other things that could be-- that there are ways to do it that could be privacy protected while still also enhancing safety.

So the example Steve gave, I don't need to know the exact length down to the inch of that heavy truck to know that it's a heavy truck bearing down on me. I don't need to know, necessarily, the

exact weight. You could bin these things into weight classes, into, you know-- but that sort of thing isn't part of the current specifications.

MIKE LEGOWER: So we have a whole panel on privacy.

JEREMY GILLULA: Yeah, sorry.

MIKE LEGOWER: I don't want to step on the toes of that panel much more. But moving on.

JAMES WILSON: One thing. I was going to say this earlier. Before this panel, we heard a number of suggestions. We're not sure that something will be recorded or information may not be stored, and it reminded me of a story from a different part of my professional career, where I ran the compliance program for a telecom company, one of the TWO big ones that wasn't AT&T, and we moved into a new headquarters.

And 250,000 employees, lots of stuff going on, and somebody very proudly said in passing conversation, a tech guy said, you'll be really interested to know that we have, with our new VOIP phone system, we have every phone call recorded. And I stopped for a minute and I thought, using my lawyer's not glass half empty, but my glass almost entirely and completely empty mentality.

I thought, wait a minute. We have every phone call recorded. The CEO makes a phone call to the Chief Counsel of the company, and that's recorded. And the guy says, yeah, that's fantastic, isn't it? And I'm thinking, OK, we've got subpoena compliance coming up and we've got this and we've got that going on.

And it sort of taught me, at that time, there wasn't a single person out of the 250,000 people in the company that had actually been tasked with thinking about that, apart from the guy that implemented the whole system. And no one had really taken that into account at all. Now, it took about an hour and a half before we turned the entire system off and changed things completely, but this is the sort of thing. There are all these different sorts of information that we're thinking about.

The data recorder that I've been told, one we're working on, will hold as many as 45 different types of information. I haven't actually asked anybody to delineate each one, but that's a lot of different sorts of information, and you're thinking those go to so many different buckets, where you've got one that's car performance, another one would be driver performance, a third one might be location or external factors. But you think of-- the car performance could be the braking or the speed, something like that. That bucket of information bleeds over into the driver performance.

It's one thing to know somebody is driving 70 miles an hour, but then, if you're thinking about the performance side of it, you're thinking, well, the guy's not supposed to be driving at 70 miles an hour in the school zone. And so all of these sorts of things are floating around with these different categories of information all being retained and all being subject to different usages and different needs and different demands, all of which can be incredibly helpful, but then present all

of these other types of issues that we'll talk about in the other panels, we'll no doubt be talking about as well.

KATE WHITE: So when we talk about all this data and we've now, thank you so much for giving us a sense of all of just the vast amount and type of data that we're talking about going forward. Who are some of those entities that will have access to this data to make it useful? Any one? Please.

STEPHEN PATTISON: Let me have a go, because I haven't spoken so far on this panel. So far, everything's been all right. I have a slightly different take on some of this stuff, but I think it does answer your question, Katherine, and I think it does pick up on James's point. And I'm looking at a world where there are going to be lots of connected and autonomous vehicles generating all kinds of data, some examples of which we've heard about already on this panel.

But it's easy in these debates to get sort of-- how do I put it? And I'm not suggesting that's happened to us, but it's easy to get dragged into a wealth of confusion and detail, which doesn't actually help us clarify what are the issues we really need to address if-- my view is that we need to work together to liberate this CAV market, right? Now, of course there are privacy concerns, and we need to get that right.

But I think, as responsible companies and responsible advocates, our aim is to try to find a way of dealing with the uncertainties and liberating these technologies to do good stuff for us. Essentially, to hold out the prospect of zero road deaths, or to hold out the prospect of much better and reliable traffic flows. So if we're going to look at it, and we're looking at what data is collected and who is going to be sharing it or using it.

So the way I think about this is, first of all, I'm thinking-- and I don't say I've got the answers, but it's a suggestion to think of it in terms of categories. So the first thing I'm thinking is, I'm focusing on vehicle-generated data. So let's separate vehicle-generated data from the data that's on your mobile phone, you happen to be sitting in a vehicle, or the data from some app that's linked to that mobile phone. So it's vehicle-generated data.

Then the next broad category is vehicle-generated data that is somehow used or usable to identify the user of that vehicle. Sometimes I say user, sometimes I say registered keeper of the vehicle, but I think in the future, we're looking a long way into the future, now. People will actually own-- fewer people will own vehicles and more people will be using vehicles from time to time.

So there's data that's linked to the vehicle identification number, however that's described, which could be attributed to the individual who's using the vehicle. And that's, obviously, kind of the most sensitive category of data. That will fall under personal data protection regulation and law, and is something which, in a nutshell, shouldn't be shared with anyone without the user's permission, roughly.

Now, alongside that, there are other categories of data, which I think are, to some degree, sensitive, too. And the category here is, is there data generated by this car which is brand-

sensitive? Is it sensitive to the manufacture of the car? Does it have IP relevance, intellectual property relevance? Does it tell you something about the performance of the vehicle, which is of interest to a competitor or someone like that?

And then there is the category-- I'll come onto that second category in a minute-- then, there's the category which is actually not brand-sensitive data. So it's not sensitive data at all, and it's not linked to an individual. So start with that. You've got data, I think, about road conditions, right?

So you've got data which you can collect from your car, from a car, about potholes in the road. It's already been done through a mobile app that was trialed in Boston a couple of years ago. But actually, there's no reason why it couldn't be done through vehicle-generated data, and it tells you where the potholes are. There's data about if suddenly a group of cars are putting on their hazard warning lights, that kind of tells you something about what's happening to the traffic flow.

Now, this kind of data anonymized-- doesn't have to be anonymized because it's not linked to a vehicle identification number of any sort-- can be extremely useful to public authorities, managing traffic flows, repairing roads, and so on and so forth. No reason why that shouldn't be shared between the companies collecting the data and the local authorities, on the basis of some sort of agreement, which outlines the terms under which it's going to be shared.

There may be a second category of this not very sensitive data, which is shared not necessarily with traffic management authorities or highways agencies, but is shared with other companies that might want to use anonymized data of this sort to offer different services. So data about either ambient temperature inside the vehicle and stuff like that, which might be of use to other companies offering different solutions. And again, is there a reason why that shouldn't be shared between the companies that collect it and the companies that are interested in it, on the basis of a sort of mutual agreement?

So then you come into that category which is of brand-sensitive data. And here, I think, again, you've got two aspects of brand-sensitive data. One is this, is it really IP sensitive? Does it really-- is it really sensitive data about the manufacturer's design of the vehicle? And that's hugely sensitive, in terms of brand value. That should be protected. It's up to the manufacturer to decide whether they want to share it with anyone, and the terms on which they do want to share it. Again it's collected on an anonymized basis.

And then there is, finally, the second area of brand-sensitive data, which is data not about the-- if you like the overall design and performance of the vehicle, but about the individual components. And the individual components of the car, as everybody knows, there's a huge number of individual components, all made by different people.

That's also a very interesting vehicle-generated data, which is brand differentiated. No brand wants it to be widely known that their fuel injection pumps are actually not working as well as someone else's fuel injection pumps. They want to share that with the fuel injection pump manufacturer, so that, with luck, they can improve the design of fuel injection pumps.

So the car company collects it, they share it with the fuel injection pump manufacturer on the basis of some sort of confidentiality agreement. So I think if we think about it in this way-- and I'm not just saying this is the only way-- bur we think about in this way, we can envisage a structure of categorizing data of different legal arrangements underpinning the sharing of that data, which will help liberate the connected and autonomous vehicles for us.

There's one last category and I'm not sure I have the answer to this, and it's basically pre- and post-crash data. What are going to be the rules around sharing pre- and post-crash data? And I think pre- and post-crash data could fall into any one of those sensitive categories. It could be sensitive in terms of the user, the driver of the vehicle who did something wrong. It could be sensitive in terms of the components malfunctioning. It could be sensitive in terms of the overall brand design.

So you've got sensitive data there, which I think we do need to think quite carefully about how we make it more publicly available in the event of a crash. So anyway, I'm not sure if that really did answer the question, but I wanted to set out a slightly-- a way of thinking about this thing, which I think might be helpful. Thank you.

STEVE BAYLESS: So--

MIKE LEGOWER: Did you have something?

STEVE BAYLESS: I was just going to say that there's a good example of a lot of freight carriers now apply analytics in individual components. So they'll be able to tell you when a part is going to fail before it fails. And is that proprietary data? Probably, it is, to that supplier or that OEM. But it also includes the driver. It includes how the driver is performing, as well. And so that also is-- that shades it as well, because drivers might be sensitive to how they're being tracked in, terms of their driver performance.

JEREMY GILLULA: I also just want to say, Stephen alluded to this a little bit about the pre- and post-crash, the sort of shadow-- or, not shadow, but the background to all of this is that any data collected could conceivably be-- and also, James also alluded to this-- the subject of a subpoena. Law enforcement could say they want it with a warrant, any information that's collected.

Law enforcement could come to you and say they want it and they may not have a warrant, and then it's, what is the policy of the company? Most companies, I think, I've just been looking their policies, say they will they share it. There has to be legal process for them to share it with law enforcement, which is the right way to do it. But when data is collected, it can be gotten other ways.

MIKE LEGOWER: So Stephen, you mentioned a bunch of categories of data that you felt you didn't see a problem with sharing them, there. It's totally fine to share those types of data, which raises the interesting question, it seems like a lot of the data collected from automated vehicles and via the vehicle-to-vehicle communication would be beneficial to share. It would be beneficial to the public to share.

So automated vehicle learning data would help all automated vehicles become safer, so that raises the interesting question is, should there be some data that there are requirements to share with various entities? And I'll open that up to the panel. Yeah, go ahead.

JAMES WILSON: Well, I think on this point, the greater good it is certainly easily answered, in that you want to share information to get to a systemic solution to a problem. But we're going to have, and we will soon feel the clash between, the greater good and the specifics of the case. And you take, for example, a warning light that comes on in a car that's perhaps storing some information about a potential malfunction.

And you look at it. I know this with my car. It tells me and my tires are under-inflated, and that's just the default position. The manufacturer says, yeah, that light's always on. Costs a lot of money to fix it. Leave it on.

But you think about that. You think that sort of light goes on and you get a little habituated to that sort of thing, and you want that information going back to a manufacturer to sort out the tire problem. So that's a greater good. But on the specific, I look at that light and I get into an accident and the insurance company obtains that information says, well, we can't pay out in this case, because this fellow was driving with the warning light on for the last two weeks, three weeks, month, or whatever.

And so you want the greater good to be satisfied by everything that Stephen said with the sharing and dissemination and use of information. And then we're going to get down to the micro side of it, which is the owner or the user of the vehicle might say, well, I don't want that particular type of information shared for a specific case. And these are going to be-- these are big ticket decisions that have to be made legislatively, in many cases, and they're the sorts of things we're going to be grappling with for the, well, near term, long term.

MIKE LEGOWER: There might be a variety of opinions on this, but how detrimental to the development and implementation of connected and automated vehicles would be to have various federal state and local rules mandating the collection and sharing of certain information generated by these vehicles?

JEREMY GILLULA: I mean, I was going to say, I think it depends on the information, a lot. That's hugely dependent. Sharing the type of information, perhaps, in a more privacy protective way, that is, in the basic safety messages, hugely beneficial, and that's a-- that will eventually be a mandate. But then, there will be other things where mandating sharing might not be helpful at all.

BRIAN MARKWALTER: Yes, I agree, and I think to Stephen's point earlier, clearly to the extent you can share anonymized data about some condition that's happening on the road that's widespread, I don't think there'd be much argument with that. I think we'd like to see some consistency so that as you drive around, it's not one thing in one locality another thing in another locality.

I think where there is some sensitivity about sharing data is the hard work that's going on-- I'll put this in the future bucket, but around autonomous vehicles and the research that's going on by companies and discussions about sharing that data. So we just need to be careful that we don't disincentivize really hard research and machine learning and collecting information by mandate that that has to be shared. So that one, we do need to be careful about. But we're starting to have that conversation. That's really for vehicles that we're not going to experience just yet, as Nat pointed out.

CARRIE MORTON: I'll maybe add to that. If you think about 35,000 annual fatalities, that's unacceptable. That's a big reason we're here talking about the importance of connectivity and automation is the safety benefit.

But if you turn that statistic on its head, one fatality per 100 million miles, developers are looking for a needle in a haystack, and how we validate that is a huge challenge, and I think the industry is starting to think about how can we anonymously share data that has nothing to do with a driver, but more about these edge case scenarios, so that we can accelerate evaluation of these technologies. Because statistically speaking, we can't drive each of these control-- each vehicle with a specific control algorithm for 100-- or, a billion miles, for example, to validate the technology.

So if we can find a way that protects the investment in innovation from these companies that the companies have made, and at the same time, share these unique scenarios to compile, let's just say, a database, if you will, that can help to simulate and validate these technologies so that we know that they're safe, as safe as a human, possibly, maybe safer. I think that's really an important place that we should focus on sharing data.

KATE WHITE: How challenging is anonymization when it comes to this data? Is it proving to be one of the big stumbling blocks for these technology-- developing these technologies and having people comfortable with it, or do you think it's not that big of a deal? And--

[CHATTER]

BRIAN MARKWALTER: So I was just-- let me tag on something to what you were saying. I do have a lot of confidence in the industry and the engineering community. I participate in engineering conferences where you see a lot of peer-reviewed work being done. So I can see that there will be papers and data presented on these edge cases.

And I think the industry has kind of learned how to share. We've seen other cases in computer vision and other areas where there are just big databases that are out there, and the academic and R&D community uses them. That's not answering your question.

But I do think trying to make that happen from the top down at the regulatory structure is going to be pretty challenging. Just, I don't know-- the industry generally knows how to work that information among its developers, and it somehow finds its way into the development process.

CHRISTOPHER HILL: Just to respond to your specific question, I'm referring back to the, I'd say the federally sponsored V2V and V2I programs. What was being talked about earlier is being done. There is a large data environment being built to gather this broadcast connected vehicle data, largely intended to make it available to highway agencies so they can develop better responses to operational problems on the highways, or to make it available to researchers.

And certainly, there was work that had to be done to anonymize that data, and I certainly wouldn't say it was a trivial exercise to do that. We were very much involved in that work. But certainly, there's ways using data analytics and other tools to be able to do that to protect the privacy. So certainly, on the V2V side, I'd say I wouldn't underestimate the challenges, but certainly, they're all challenges that can be addressed.

When we start to move into the automated vehicle space, I think we have a whole new set of challenges. We're not talking about starting with largely anonymized broadcast data, we're talking about other sorts of data, and I think we have a new set of challenges there that I don't think, necessarily, anyone has taken on yet.

STEPHEN PATTISON: Just let me cover a couple ones. I think you asked about anonymization. And I think-- I always say this about Internet of Things type things. The technology can help secure the data from unauthorized interference, but, currently, the technology cannot guarantee that anonymized data will stay anonymized. On the contrary, generally speaking, if you've got enough computing power and you really want to do it, you can probably re-identify data that was given to you on the basis that it made anonymized.

So there is one area where I think we do need to think carefully, and it applies not just to CAVs, but applies across the board in this new technology era. It's how can we create proper sanctions for those who seek to re-identify data which has been entrusted to them on the basis that it be kept anonymous. And I don't think there's an easy technological answer to it.

I wanted to make another point, if I may, about-- I've written down liability, and I can't, honestly, remember, now, what prompted the thought, but it was something which, I think, Katherine said up there. In some of this stuff about the drive-- I can use the word drive in this context-- the drive towards safer connected and autonomous vehicles will focus on the issue of liability. And up to point, we have legal systems which are very good at passing liability along the chain to whoever is genuinely liable for a fault or an accident.

I'm looking way ahead now, because people have mentioned it. If you get to a pure AI, Artificial Intelligence system, liability issues become a bit murkier, to say the least. Because A-- and here, brief parenthesis, I'm distinguishing between machine learning and artificial intelligence machine learning.

To put it very crudely, I see as a computer taking in lots of data and drawing patterns out of that particular data which it applies to a new situation. And there, you can more or less see, if the thing goes wrong, you can more or less see, well, that was why it went wrong, because we failed to put in this bit of data.

I mean, sorry. Anecdote, there's a famous example of this about computers being trained to spot fraudulent names, right? So when you feed in a load of regular names, and it says, right, now I've got a rough idea of the regular names. I'll spot the irregular names and we'll assume they're fraudulent. That's fine until you get a community that comes from a particular group popping up with unusual names, and then it suddenly looks as though the system is discriminating unfairly against those.

That's a machine learning problem, and actually once you've identified it, you can fix it. Artificial intelligence takes that machine learning habit of pattern recognition essentially further and further, to such a point that I don't think anyone right now would guarantee that in an artificial intelligence environment, we can be 101% confident that we know how an artificial intelligence computer has actually reached the conclusions it has.

So if you-- if we get to the world where AI is running connected and autonomous vehicles-- and I think we're a long way from that, I think. We can go a long way with machine learning. If we get into an AI world, it becomes quite difficult, actually, when you get to liability. A, you've got the question of can the person who started the robot share the algorithm on which it runs, the AI device, on which it runs.

Are we willing to do that? In what circumstances they are willing to do that? What happens if-- and then, the question of, well, actually, we didn't design this AI system to make this mistake, we designed it in a different way that the thing is now making its own judgments in some way. And it has, presumably, made a mistake. So this issue of liability, I think, we'll come up against time and again as we advance this kind of technological revolution.

JAMES WILSON: Maybe-- well, to make a brief point, following up on Stephen's point about the legal system being good at doing certain things. It is, except sometimes it isn't. I was at a patent meeting yesterday at NAFTA negotiations in Canada and somebody was talking about patent enforcement in the Eastern District of Texas. This is a sinkhole of misery when it comes to patent enforcement.

Supreme Court recently hopefully sorted that problem out, but there are issues like that where we're going to have elements coming up where our legal system is lagging in its ability to cope with all of these new issues coming up. And I think that's where the legislative involvement is going to be critically important, trying to sort out some of these issues up front, so that we don't get into the liability morass that will harm all of the innovation that everybody here is promoting.

MIKE LEGOWER: So I want to pivot this conversation a little bit to data ownership. So when we're talking about the data that's being generated and collected by these vehicles, who is it that owns that data, currently? Who is it that owns that data in the future, or who will own that data in the future? And what if it's traveling over a public network, as is envisioned in many of these technologies, does that change the ownership issues at all? Anyone care to comment?

JEREMY GILLULA: I mean, I'll jump in. And if someone up here wants to correct me, I would love to be wrong. But my presumption and everything I've read to date suggests that it is the manufacturer, if you're talking about a personally owned vehicle, that it would be the

manufacturer or whatever third party the manufacturer contracts with to make their system or run their system that owns the data.

And there, I'm talking about data that is collected on the vehicle and then transmitted off of it. I'm not talking about what's in the event data recorder that is only looked at in the case of a crash or something like that. In terms of transmission over public networks, encryption in transit is easy and is essentially a solved problem, and so that's really not an issue. You start to make sure you do it right, but it's not a technically challenging thing these days.

MIKE LEGOWER: So some of the transmission of this data is going to be subject to very, very serious time constraints, right? Does encryption poses a bigger problem in that?

JEREMY GILLULA: I mean, encryption can introduce delays, but there are also ways to do the encryption in hardware that will introduce very minimal delays. So I don't think-- I mean, again it depends on the specifics of the type of data. But I don't think that-- I mean, we we've also made very large strides, particularly in the last decade, on doing encryption very quickly, very efficiently. So I don't think it should be an issue.

STEPHEN PATTISON: Can I perhaps-- let me just pick up on that last point. But I'd say I agree, really. I mean, it won't be encryption that accounts for a significant delay. I mean, this-- more important-- and this is a sensitive issue, I know, is whether the communication system is based on, essentially, 5G or whether it's going to be based on DSRC, where right now, the speed of those is probably going to be quite different. But I originally was going to say something about data ownership. Only to say, I'm sure James would say this but he's too polite to say it.

Every time I-- and like you, oh, I love to use the phrase data ownership. You know, who owns the data? And I nearly always get a lawyer put their hands up and say, no, no, the law does not recognize data ownership. Generally speaking, what the law recognizes is a data subject, a data controller, and a data processor, and that's what we'll be looking at here, I think.

And I think the data controller is, well, obviously, is going to be the company that's collecting the data, which I'm assuming, that-- we could argue this-- I'm assuming it's actually going to be the vehicle manufacturer, in most cases. I'm assuming we have a system where vehicle manufacturer is collecting the data and then deciding which data to process and how.

But data processing may be done by someone else. So the data subject is the car, if it's got a personally identifiable number attached to it. It's the person driving the car as well. And the data controller is the company that has collected the data and decides what to do with it.

BRIAN MARKWALTER: I would--

STEPHEN PATTISON: But James may have a view on that.

BRIAN MARKWALTER: I was just going to jump in here and reemphasize something Stephen said earlier, and that's that we're going to have a structural change in the ownership model for vehicles, we need to keep in mind as we do this. I think most people expect that as we shift

highly automated vehicles, there's also going to be a shift towards mobility as a service. There's more urbanization. It's just going to make sense. We know how much idle time cars have to today.

So I think with that, there's just going to be inherent difference in what consumers expect and how we think about ownership. It's not your car, so you're going to want certain services to happen, but then that's it. It's somebody else's vehicle to begin with.

JAMES WILSON: Well, I do have a very strong view, and I'll keep that to myself. But I think the critical component here is this is not something to be left to the fine print. It's something we really need to address upfront, and not sort of tiptoe into it backwards, and not really understand where we are. Because it's not that this is entirely unique, but we are going to a new place with new technologies and so many unanticipated consequences.

And so much of it's good, but when it comes to ownership of data, it's the sort of thing that I think we do need to attend to up front, as much as we can, given that we don't know half of what will be in place in five years or 10 years. But I think this is one of the places where it really-- we want to free innovation and not interfere with innovation, but this is the sort of intellectual thing we can think about up front.

KATE WHITE: So sort of to bring it to the consumer. Today, how are consumers being made aware of what their car can do and what information is being collected? And going forward, how do we think consumers will be informed?

CHRISTOPHER HILL: If I could again speak to sort of the federal program, the V2V, V2I program, I mean, truthfully, I think the average consumer has very little interest in what data flows and where it flows to. I think if you have a very sophisticated consumer, there are ways in which they can quite easily find that information. That program was built around a whole set of standards. There's a whole reference implementation architecture that exists that if you want to look it up, you can see exactly how vehicle flows from the vehicle to the other components of the network.

But as I say, I'm not sure that's something that consumers, at least in that program, are particularly concerned about. We conducted some public acceptance market research for DOT, and the overwhelming response was that people seemed to be very unconcerned about the data flow. In fact, they acknowledged that in many situations in their lives, they're being tracked, and as long as they're getting some benefit from the service, that they didn't really care where the data went. What they did care about was protecting personal privacy and information that was sensitive. But as I say, I think in that program, we may be making more of an issue than it really needs to be.

KATE WHITE: I was wondering-- Carrie, in Ann Arbor right now, you actually have a pilot where people have volunteered to sort of participate and have their V2V communication. How have you informed that consumers participating in that pilot?

CARRIE MORTON: All right, so as a university, we're also following institutional review board process. I've been volunteered. My vehicle's connected, so come and talk to me. And I think, while we haven't taken a formal survey, the sentiment we get is that they're excited to see the potential and the safety benefits. And there isn't a specific concern around the safety.

And when we've asked them if we were able to provide you additional benefit by sharing this data, it's the same as all of the other applications we download on our iPhone and check the box without even reading. If it's really-- it as Chris said, it's if there-- if it's going to provide them a benefit that's worth the trade of, they seem very comfortable with that. We see potential for this exact transaction when you consider trying to speed the deployment of these technologies using retrofit devices.

If you can have a third party, for example, who provides or offsets the cost of adding V2V to an existing vehicle, perhaps your '66 Mustang, that a third party could take advantage of some of the data coming off of it, but at the same time, providing a benefit to that consumer who's chosen to retrofit that technology on their vehicle.

So, so far, we don't see a lot of concern. And especially, I will just add, this technology only has a range of 1,000 feet. Or, sorry, 1,000 meters, in the best case. So the type of privacy concerns aren't much different than other technologies that are out there. If I wanted to take a camera and follow a vehicle and get its license plate, I can also find a lot of information there as well.

STEVE BAYLESS: I just want to add one thing to what Carrie had said, is that the benefits usually differ across different road user categories, and so one of the things we've heard a lot is the use for pedestrians and motorcyclists, because there are no occupant protection or crash-worthiness features in motorcycles or bicycles or even with pedestrians. So usually, it's a no-brainer for them. For other types of consumers, it's hard to tell, and you only-- the only way you can find out, I think, is by doing the research.

JEREMY GILLULA: So I just wanted, because we've talked a little bit about the V2V stuff, I also just wanted to throw in some other connected car things. And if someone from Volkswagen or GM is on a panel later, it would be great if they would correct me, again, if I'm wrong, because I'm just reading their privacy policies. And their privacy policies say, the way we'll inform you of what-- you know, if we decide to change what we're collecting, is we'll just put up a new privacy policy.

That's at least what-- they may do other stuff, but in terms of what they've bound themselves to do, by saying, this is the promise we make to you as a consumer, in some sort of official fashion, they've basically said, you just have to keep checking our privacy policy page to see if something's changed.

MIKE LEGOWER: So we have a little under 15 minutes left, and I think we promised to open up to questions from the audience. So if anybody has a question out in the audience, you can just raise up your comment card and somebody will come around to collect it and bring it up to the front. We do have one to start off with. So this question is about small auto repair shops and how they're going to be able to maintain and repair vehicles in the future that are going to be

sophisticated, in terms of their data collection and connectivity capabilities. Does anybody care to comment on that?

BRIAN MARKWALTER: So I will, and not because I want to turn this into a right to repair discussion--

[LAUGHTER]

--which we don't want to have. But I think we do have to think, today, about, at least in the ownership model, how consumers will upgrade and repair their cars in the future. We know we want connected and especially automated vehicles to be secure. And I think part of that, we're going to have to-- we need to start working now on some sort of tiered access.

There's clearly systems that need to be to be highly protected, but we do need a way-- we know consumers will, once they own a car, they're going to want to update and modify and do things. We need to be able to empower consumers to do that and maintain the functional safety of the vehicle over time. So I don't have an exact answer, but that conversation needs to continue.

CARRIE MORTON: I would just add, I think we have an example. When it comes to emissions regulation, we have onboard diagnostics. The vehicles are continually diagnosing themselves. It's done in a standard way. There's a standard protocol that repair technicians can plug into the vehicle, and it doesn't have to be an OEM technician. It could also be an independent technician, because the technology is standardized. And I think that's a really good example.

I can tell when my oxygen sensor has failed and needs to be repaired, but I don't know all of the control algorithms that diagnosed and got us there. So there's a perfect balance. And I think it's also important to note that for the safe operation of these vehicles, there needs to be some level of sharing, because if I'm-- I'll just pick an insurance company.

If I'm Allstate and I'm having your car repaired, how do I know that those automated systems are fully repaired and that you're safe to be back on the roadway? It's in the best interest of the person repairing the vehicle and insuring the vehicle and the driver to have those systems in place.

STEPHEN PATTISON: Can I-- I may make a slightly different point on this. I do-- but we're straying a bit into the cybersecurity discussion, so don't tell me off, because I knew Katherine's extremely strict on this. But there is a point here, which is, to put it very briefly so we don't stray into it. The lifecycle of a car is probably 10 or 12 years. The lifecycle of the software that's going to be running a lot of this connectivity is probably 12 or 18 months, right? Before there's a bug in it and someone discovers it.

So we've got to have an answer to the whose responsibility is it to identify bugs and then ensure the cars-- or, those bugs are fixed in cars? Now, online, generally speaking, we're used to over the air upgrades, so we don't have to do it ourselves. And I suspect that's the way we're going to have to go with connected cars. Because connected cars are only safe if everybody's using good

connectivity for their cars. It only takes a few people not to do that much for the system, suddenly, to fail.

So I think we're going to have to be looking at over the air upgrades. And I think I'm not going to intervene on the privacy thing, but I think privacy is important. But I think when consumers buy a connected car I think you're right. They'll be less bothered about the privacy, but they will be very bothered about the security, much more bothered about the security of their connected car than they are bothered about the security of their connected phone, actually. And they'll want to know whose responsibility is it to upgrade the software in this car.

And yes, we can say, we'll send around a message that tells you there's something wrong. Please drop in to a repair shop and get it repaired. But I'm not convinced that the most reliable way of doing it.

KATE WHITE: So we've touched a little bit on the fact that there will be attractive to some secondary uses of the data. Do you think that in order to incentivize the technology, to really-- so that it will be implemented faster, especially as we move away from cars being, probably, sold directly to consumers, that it will be necessary for people to be open to the fact that there will be-- there will need to be a to monetize the data? Do you think that's inevitable or not? Oh, no one wants to touch it.

[LAUGHTER]

STEVE BAYLESS: I'll try to answer it. I mean, if you look at, for example, windshield wiper data. When the windshield wipers are activated, it's probably raining. Now, does the consumer think that, well, I want to sign a-- I want to opt out, or I want to opt in to share this data with the National Weather Service? Generally, no. It's usually taken care of by the OEM or by whatever service provider, supplier that they're using.

And again, I think it goes back to this issue, is the different-- what the data is useful for and where the data should flow to where it's most useful. So that the weather guys get the weather data, but the auto guys get their auto data as well. So I'm not sure if that answers your question, but I think there is some extent in a vehicle, and the uses really can never necessarily be assumed, or the utility of any particular data set can't necessarily be assumed. You just have to let people work those issues out.

KATE WHITE: Right here.

MIKE LEGOWER: Oh, OK.

KATE WHITE: Sorry, so here's a question from the audience. We keep hearing about manufacturers collecting vehicle repair status information to share with their dealers, yet dealers only perform a third of the service today. How does the aftermarket that performs the rest of the service obtain the same information? OK.

BRIAN MARKWALTER: So I don't know, and I don't know that that's a problem that needs to be solved. I've seen-- it may be even the founder of Waze was working on something. So I think the markets can work in this area, where somebody empowers consumers to share, aggregate and share information. So there are ways around that. I don't think it's an obligation of the automotive OEM or their dealerships to share information. But I also believe that if it's available and can be aggregated and there's a financial benefit, then somebody will do it.

JEREMY GILLULA: So in terms of that, I think it's enlightening to look at other scenarios where the same sort of thing has happened. If you look at smartphones, it's very difficult, particularly in certain brands of smartphones, for a third party to repair it. It's almost designed in a way that only the OEM can repair it.

And so there, that's a case where there has been no legislation. There's been no regulation. There's been no mandates. And we've seen where the market has gone. Whether that's good or bad, I'm not going to say. It's not my place to take because I'm a technologist, not a-- I don't even know who would judge that sort of thing. But we have seen other examples, just in other industries. Now, a car is not a smartphone. I'm not saying that. So--

MIKE LEGOWER: So here's another question from the audience. What is being done about selling your highly automated vehicle in 2024 and the new owner being able to find out everything your car knows and has learned about you and your family? So essentially, what are the processes for accessing, deleting, modifying the data on highly automated cars, highly automated vehicles in the future? Is any thought being given to that?

CHRISTOPHER HILL: I mean, I think this is a fascinating topic, and I think we heard from one of the earlier presentations about the rental car industry and the ability to delete information that your rental car has picked up as a result of you going in with your smartphone or whatever.

I don't think there's been concerted research done on this particular issue of how you would deal with this in a highly automated vehicle, but I think there's already some thought being given to it in other scenarios, and I could see that being kind of extrapolated to automated vehicles.

And I think there would be a strong desire and expectation to be able to easily delete that information. That being said, I certainly know there are cases where law enforcement agencies have been able to go in and look at telematics systems in existing vehicles and even where information has been theoretically deleted to be able to reconstruct that, so it goes back to an earlier comment. Anybody who's willing to invest enough time and energy in trying to find the information is probably going to be able to do it. But I think it's something we're going to have to consider in the future.

JAMES WILSON: And I think this may take us, again, to legislative issues, where you certainly would like to know the delineation of what can be deleted and what can be kept. There are certain things, just as we now want accurate information on an odometer to be retained, there are certain things that, legislatively, from a public policy perspective, we might want to maintain the structural integrity of the car, the number of miles driven, a couple of metrics like, that to pass to

the next owner. But there are other things that I think from a public policy perspective, we would want to say, enough is enough. That information does not continue to exist.

BRIAN MARKWALTER: Yeah, it's not a perfect analogy, but there are, even today, in the connected home area, there are groups working on-- I think, maybe the National Association of Realtors and others have put out some recommended practices on trying to make sure if you sell a house and there's a home system that goes with it, that that is cleaned and made available for the next purchaser.

MIKE LEGOWER: Do you want to select from your favorite questions there?

KATE WHITE: Yeah, so here's a question. So several members of the panel have cited research that consumers are not concerned when their data is shared, and the concern-- and this is because privacy policies are not transparent about what data is shared and with whom and how extensive it is. For example, the role of data brokers have in obtaining this information.

Should there be a requirement that the details of personal data sharing be provided so consumers can make an informed choice? And I think just rest assured that if you feel uncomfortable answering this question, I think the next panel or the third panel of the day will definitely get to this one, but--

STEPHEN PATTISON: I won't be here for the next panel. So I'm going to say now what I think on the subject. So I'm lucky. I mean, the short answer is-- I'm not going to answer the question. You can read through terms of conditions and it tells you that stuff, but actually, nobody reads through terms and conditions. So I do think there is an issue here, actually.

And I think it may be the case right now that people are not-- don't seem to be terribly bothered about data sharing. But I do think in future, this whole industry is going to be driven by data sharing and data use, and I think consumers will want to know less who's got their data but much more what use are they putting it to. And that's my first point. I think there's a kind of assumption that people are interested in who's got it, but actually, the not interested in who's got it. They're interested in what they're doing with it.

My second point is I do think consumers will eventually demand much more clarity and simplicity about what's in the terms and conditions. I'm not saying that T's and C's will be replaced, but I think consumers will want a snapshot of how their data is going to be used. My third and final point is I think it's actually perfectly possible to break down data usage into half a dozen or eight categories of data usage, which I think would give consumers much greater transparency of how their data is going to be used, and much greater confidence about allowing their data to be monetized.

JEREMY GILLULA: The other thing I would add is the danger of inferring this sort of thing from customer surveys. What's good for people on average may not be good for the person who is worried about, oh, because my location data was shared, now you know that cop in my whatever town can extort money out of me because I went to some place that my local community doesn't like, or something like that. I mean, that's happened before, right? That's not

a hypothetical; it's happened. And so you always have to design privacy for the sort of most vulnerable population, and not for the population as a whole. And it can be done, right? That's It takes a little more thought, is all.

KATE WHITE: Well, I see we have run out of time. And I wanted to thank all of our panelists so much for participating today. This has been a wonderful conversation, and we look forward to having more of them. And for the audience, we're going to-- we'll break for lunch, and the cafeteria in this building will be open. It's right around the corner there. Or you're free to leave for lunch L'Enfant Plaza has a food court. But you will have to come back through security when you come back for the afternoon. So with that, thank you very much.

[APPLAUSE]

[MUSIC PLAYING]