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

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 fi

So why would one want to access that information? So you can think about things like your

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 a

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-

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

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

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

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

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 at staas N 0-2(s)dust10(r)-

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 Cour

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

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

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

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.

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 mark

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 cdautake sarin(nf)3(or)3(m)-2(a)4(t s)-1(a)4(ra)4(sobt)-2ci

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]