THE BROOKINGS INSTITUTION

WEBINAR

THE FUTURE OF CONNECTED CARS
SEVENTEENTH ANNUAL A. ALFRED TAUBMAN FORUM ON PUBLIC POLICY

Washington, D.C.

Tuesday, May 5, 2026

PANEL ONE: INNOVATION, CONNECTIVITY, AND INFRASTRUCTURE

MODERATOR: DARRELL M. WEST
Douglas Dillon Chair in Governmental Studies and Senior Fellow, Center for Technology Innovation (CTI), The Brookings Institution

MICHAEL GRAHAM
Vice Chairman, National Transportation Safety Board

ALEX WYGLINSKI
Associate Dean of Graduate Studies, Professor of Electrical and Computer Engineering, Worcester Polytechnic Institute

PANEL TWO: PRIVACY AND SECURITY

MODERATOR: DARRELL M. WEST
Douglas Dillon Chair in Governmental Studies and Senior Fellow, Center for Technology Innovation (CTI), The Brookings Institution

MARC SCRIBNER
Senior Transportation Policy Analyst, Reason Foundation

OMRI BEN-SHAHAR
Distinguished Service Professor of Law, University of Chicago Law School

* * * * *

WEST: Good afternoon. I'm Darrell West, a senior fellow in the Center for Technology Innovation at the Brookings Institution, and I'd like to welcome you to our seventeenth annual A. Alfred Taubman Forum. This forum was set up to cover different topics each year, and we are grateful to the late Mr. Taubman and the entire Taubman family for support over the years.

This year, our topic is the future of connected cars. It is an eventful time in the history of transportation. Both cars and trucks are being digitally connected through online sensors, safety devices, and entertainment systems. This situation offers a number of conveniences for drivers and passengers.

People can access digital resources when they're on the road and avail themselves of a range of entertainment options. At the same time, though, the ubiquitous connections raises questions about privacy, legal liability, and consumer protection. People worry about what happens with their data and what they will need to do in order to protect themselves.

To help us understand these issues, we have two panels. Our first panel features two distinguished guests. Michael Graham is the vice chairman of the National Transportation Safety Board. In that position, he deals with a wide range of transportation policy issues, including those involving cars and trucks.

Alex Wyglinski is the associate dean of graduate studies and a professor of electrical and computer engineering at the Worcester Polytechnic Institute, and he writes about issues related to connected cars.

And if you have questions for our panelists, you can email them to us at events@brookings.edu. That's events@brookings.edu.

So Michael, I'd like to start with you. You have considerable expertise on connected cars through your work at NTSB. So perhaps you could start with an overview of the current situation. How are cars being connected right now?

GRAHAM: Well, let me start by letting everybody know where the NTSB's interest is as far as connected vehicle technology goes, and we are purely in it for the potential imminent crash prevention of vehicles on the roads.

That's what we're looking at. So we don't look at other things that might make it very nice to have and down the road, but we're looking at it for preventing crashes and the vehicles talking to either each other, to the infrastructure, or vulnerable road users out there to prevent accidents in the future.

So where do we stand with that? Right now there's really no policy coming out of the Department of Transportation. There was one that was set up a few years ago. It's kind of been pulled down with the new administration. So we're really looking for leadership on the part of the Department of Transportation and to take a role in actually defining what the communication protocol will be.

For imminent crash prevention to happen we need part of the communication spectrum to send those signals from vehicle to vehicle. So we need a high reliability, low latency are

frequency range. And then the other part of that is we wanna make sure we don't get any interference within that frequency range.

We need the DOT to help with that, along with the FCC to protect that part of it. So, from the NTSB side, we're looking at it purely for crash prevention.

WEST: Okay. Thank you. So Alex, Michael was talking about the safety aspect of this, and we do know that there are systems where vehicles can communicate directly with one another and share information about navigational obstacles, traffic patterns, road conditions- And traffic signals. How does that work, and how does that affect driver safety?

WYGLINSKI: So that's a great question, and it's a, that's a good segue from, from, from Michael. So, so, a like, you know, over the, like, past two decades there has been a lot of research within the academic community, the electrical and computer engineering community, especially in terms of wireless connectivity and vehicle networks especially low latency communications, which is exactly what Michael mentioned.

So there were several candidates in terms of wireless technologies that could potentially s- fit that role in terms of vehicle-to-vehicle or V2V connectivity. But 5G communications, which is what a lot of folks use for, like, cellular access, right? Like our smartphones connect to the 5G network.

There is one mode in some of the latest releases of 5G called mode four or sidelink communications that enables direct vehicle-to-vehicle connectivity, and there's a requirement in terms of how much latency can be tolerated in that connection. Because, for instance, if you have something that's mission-critical, like, so for instance, like, you know, I'm here in New England, and there's this thing called deer, right? And they're on the road and everything like that. And the car ahead of you senses it but avoids the deer. It would be very convenient to have that, you know, warning message communicated to vehicles behind that vehicle indicating that there's such a op- you know, like, like, let's say, threat or a sort of critical situation up ahead for vehicles that might not be sensing it right away, right?

So there's a lot of experimentation. There's obviously a lot of theoretical research continues to be pursued, right, in terms of making this you know, technology even better, like decreasing the latency, making it more reliable. But there's also a lot of experimentation. So, like, my own background here at WPI, I have a lot of collaborators, I have a lot of grad students, undergraduate students, and we explore through actual experimentation in the lab, so a controlled environment, how can we bring that latency down?

How do we make it more reliable? How do we share that information so that, you know, wireless communication is yet another form of sensor modality in addition to your lidars, in addition to your radars, in addition to your vision systems with the, you know, critical, the critical goal of safety with respect to all drivers on the road.

WEST: No, it's great that you and your students are working to reduce that latency because transportation is one of those areas where we really need high-speed connections, and even some lag in the latency of those connections can prove to be very problematic.

So Michael, I know you're focused mainly on the safety aspect. What are the benefits that you see for consumers out of connected cars, specifically on the safety issue?

GRAHAM: You bet. There's a lot there like, like Alex was saying. You know, talking, if, if vehicles not just can talk to each other about something one vehicle's seen and another can't see, but pass that information on, the driver can react.

And what I would like to see too is maybe, and if they're not reacting, then they work with the sensor systems themselves to actually react, whether it's automatic emergency braking, things like that. Things we look at just like, most of your big cities all have connected intersections now. The infrastructure owner operators have really started the, putting the infrastructure in there for intersections and things like that with counties and cities.

There's a lot of information there. They track a lot of stuff, vulnerable road uner- users crossing streets and like that. And I would love to see, like Alex had said, something like if you're coming up on an intersection, there's vehicles in one lane, but the that are getting ready to turn right, maybe somebody decides to cross the intersection, they shouldn't be, but they're crossing anyway.

But that vehicle or that intersection can tell the vehicle approaching that cannot see the pedestrian or the scooter rider or the bike that's coming across, send that signal and notify the driver to do something. And if they don't react, then the sensor systems themselves would allow to a- automatically emergency brake.

So that's, that's the where we're focusing our attention out there. Or a large... W- we end up going to a lot of crashes where there's a traffic queue that has started on a highway or an interstate due to lane closures, maintenance, maybe previous crashes, and there's vehicles approaching, and they're not aware that there's stopped vehicles ahead.

Especially when we're talking tractor trucks with trailers and stuff like that. And those, when they don't see it, maybe the driver's fatigued for, distracted for whatever reason, and that truck plows in the back of that queue of vehicles. Unfortunately, normally we have a lot of fatalities, and it's, it's a really bad situation.

We would love to see a message sent to the driver, to the, the tractor truck that there's a queue ahead, you need to start slowing. And if they're not slowing, maybe the vehicle itself will start slowing because of that. So that's where we're focusing our attention from the NTSB.

WEST: Mm-hmm. No, it would be great to have prior notifications of those types of things when there's a traffic slowdown.

I know I've been in that situation before where you're kind of zooming along at 60 miles per hour, and then suddenly you have to brake because of a traffic issue So Alex, what do you see as the benefits of connected cars for consumers, either in the safety area or other aspects?

WYGLINSKI: Well, well, no, and that, that's exactly like the use case that Michael brought up.

That's exactly like one great use case, or like one great benefit for users is, is safety right now. Like, you know, for instance you know, like you, you can kind of infer from, let's say, various apps on your phone that might be connected to your car dashboard saying, "Oh, you

know, the highway's green at 60 miles per hour," and then all of a sudden like big blotch of red, right?

Like for, for several miles that might indicate that there's a problem or a blockage. But wouldn't it be great if, let's say, just like my car right now, so I just bought a car last year and it's wonderful. Like, you know, it has that like collision avoidance, it has blind spot detection, it has all these features.

But imagine in addition to that, it has like that like, you know, I would like to call that situational awareness that extends further than, let's say, tens of meters away. Like it could be ki- you know, miles away. Like it, it... And even like, you know, let's, if we take it up a notch, like let's say vehicles with autonomous or semi-autonomous functionality this could go into great things like, for instance, motion and pa- or path planning, right?

Like, so suppose I'm on the highway, I'm in like some sort of autonomous mode or, or whatnot, and then, and then all of a sudden it's like there, there's, let's say, a, a conflict. Like, you know, a semi is, is is damaged. It's causing you know, like, some sort of blockage on some highway, and then all of a sudden the f- the, the autonomous agent that's on the vehicle is saying, "We need to get off at this exit and here's like a rerouted path," automatically without any human intervention.

Or, you know, at a very least if, let's say, the situation gets complicated there's a graceful failure where the autonomous agent transfers ownership back to the, to the driver, but in a, in a time period that doesn't cause like, you know, any sort of like, you know, sort of dangerous situation. So I think for safety, connectivity is, is definitely one of kind of the key factors in, in, in supporting that safety aspect because it is essentially the sixth sense of, of a vehicle, right?

Like, because again, we have all these like sensor modalities. Having more information, like now there, there is a risk of too much information. But if, let's say, if that information that's shared from other vehicles or, let's say, of the road ahead is, is provided to the driver, provided to the vehicle, if it's making either semi-autonomous or autonomous decisions, it could, it could really help.

It could be a real game changer in terms of minimizing or at least reducing, you know, any sort of potential like accidents or any issues later down the road.

WEST: So Michael, we've talked a little bit about some of the possible benefits, but what are the risks for consumers with all these digital connections?

I mean, in one of your earlier answers you mentioned the possibility of distracted drivers, and of course there are many things that can distract drivers. But with all the digital connections, you know, like we have very elaborate entertainment systems. People can surf online, they can live stream movies.

I mean, all the things that you can do in your home now you can do in many modern vehicles. Are there risks for consumers by having all of these digital connections in their vehicle?

GRAHAM: Well, we already, we already have issues with that right now. We have a lot of distracted drivers on the road with just their phones alone.

You can't go... I can't drive anywhere, even just a mile to the, the metro station to go to work that I don't see at least one, if not multiple people working their phone while they're driving. And they don't even have to have forward collision warning systems on their cars and things like that.

So, it's, it's... it can get very complicated with all these mode- especially right now with the infotainment s- systems and things like that. It, it's driving distraction, and there's a lot of distracted drivers out there. I think you're gonna see a lot of work work is already being done on a lot of better driver monitoring systems out there.

We just did a board meeting on two Ford Blue Cruise crashes that happened on the interstate, and the limitations of just the forward collision warning systems that didn't even respond to two vehicles that were not moving on the road, and the vehicle was allowed to... was on an, a, a somewhat of an autonomous mode in level two and drove right into the back into these vehicles while both drivers were distracted.

So yeah, a lot of work needs to be done as to what's appropriate, what needs to be sent to the driver if they're distracted. A- you know, and if they don't respond, then what does the vehicle do in this case? So, y- distracted driving and driver monitoring systems I, I think are gonna be very important going forward.

Even when you talk about impairment and things like that, there's a lot of stuff coming out down the road. And how that's gonna be integrated, I, I don't think anybody knows quite yet.

WYGLINSKI: Yep.

WEST: Alex what do you see as the risks for consumers with all the digital connections?

WYGLINSKI: No, no, I think, like, definitely what, like Michael mentioned, like just to echo that, I think like there's a lot of this, there's a lot of information, there's a lot of distractions like, you know, either cell phones.

And imagine now if you outfit your car with like, let's say even more ways of like, you know, sort of like infotainment, right? Like, but I think, The risk also, and, and I'm gonna bring this up because I, I published a few papers and this is also cybersecurity as well. You know, because now what happens is you got a vehicle that's connected with the outside world, and whenever you have anything connected with the outside world, you're now opening yourself up to like, you know, let's say malicious users that can also compromise your vehicle security, right?

Several years ago, I published a journal paper and it was in collaboration with, with several researchers at University of Massachusetts Lowell, as well as University of New Hampshire, where we looked at this phenomenon called, like, phantom cars. So suppose that your vehicles on the road are all reporting to each other their GPS locations so that they have some sort of situational awareness saying like, you know, forget about, like, even blind spot detection, but you know every vehicle knows where every other vehicle is on the road.

Now, now the, the risk is what happens if one of the vehicles on the road, or let's say there's a malicious user off the side of the road, is feeding bogus information saying, "There's a vehicle right next to you," when in fact there's no vehicle, like the phantom car. Or misreports or distorts the reporting of a vehicle that is not in a location, but it puts it another location that creates a conflict, creates an accident.

So I, like, you know, from, from my world, right, like, you know, whenever there's, whenever there's, like, a wireless surface, wherever there's a way of people like, like a vehicle connecting with the outside world or anything connecting with the rest of the internet, that opens up to many different vulnerabilities.

Obviously, there's always a lot of current concerns in terms of like, you know, like things like user distraction and unintentional issues, right? Like even the reliability of those, like, vehicular connections, right? But then on top of it, there is the potential for also the, the malicious aspects that could also compromise road safety.

WEST: So Michael, Alex has mentioned some of these cybersecurity risks. How vulnerable are some of these connected cars to malicious actors phantom vehicle notifications or other things like that?

GRAHAM: Well, that's a good question. I, I don't think we have the expertise, or I do, I do. I don't have that expertise to say.

But we do know that any kind of false positives that Alex talked about can really negate any benefits of the systems out there. We have seen for years a lot of the, the heavy trucking industry pushing back on, like, forward collision warning systems because of all the false positives that have happened with onboard sensors.

Now the systems are getting better. As we have pointed out just recently with one of our board meetings, like I said with the Ford BlueCruise, is sensors are not perfect by any means, and they all have their limitations. So we need... There, a lot more work needs to be done in that area. The National Highway Tra- Traffic Safety Administration I think needs to really work for better performance standards when it comes to those onboard sensors, that they work a lot better at, at more realistic highway speeds and situations with different objects that a vehicle could come across down the road.

But I think that just goes to show you that with all the limitations of onboard sensors, that connected vehicle technology, vehicle-to-vehicle, vehicle-to-infrastructure, or vehicle to whatever vulnerable road users, can really help with the limitations of the onboard sensors and give them the information that they may not have.

And that's why we at the board and myself are very interested in connected vehicle technology.

WEST: So Alex, are there privacy concerns with these digital connections? Are there things people should be worried about?

WYGLINSKI: Well, un- unfortunately, that's not really my area of expertise in terms of privacy.

So I'm much more into, like, the actual connectivity, the physics of, like, the electromagnetic exchange. But I would imagine in terms of, you know, things like, you know, for instance, like sharing telemetry data between vehicles or the position of different vehicles and the like, you know, like, y- you know, you are sharing it with other vehicles, which means there is some level of trust that's occurring assuming that all vehicles on the road are assuming the same sort of ultimate objective, which is, like, s- a safe driving experience for everybody involved, right?

How, how else that information's used, you know, like, that, that again, like, you know, that- that's more of, like, you know, somebody in more of like a you know, sort of a, a, a, a trust or a cybersecurity type of perspective. Like, you know, if, let's say that information can be used by other entities to track somebody or track an individual.

But, but I think in terms of information exchange, like, you know, that, that, like there, there is a need of, let's say, like what, what Michael mentioned, like, you know, in addition to the sensors, and the sensors are absolutely not 100%. Like, you know, they, they, they're gonna do great. You know, like, people are investing a lot of money in great li- LiDAR systems, radar technology, vision systems, you know, and there's, there's backup, there's redundancies and such.

And then the connectivity further irons out any sort of bugs. If, let's say, there's a false positive. Like, let's say one sensor says, "I think there's a car in front of me," but the, all the other sensor modalities are saying, "No, I disagree," then there's an algorithm that would decide saying you know, the majority rule, we think that there's, there's no threat, there's no concern about what's ahead of us.

But however, like, you know, again, that, that information exchange, you don't... Like, you know, ultimately, where does that information stop? Like, you know, I, I, I, all I can say is that when there's an information exchange, like, you know, it's, it's done with one particular objective, but how else it's being used, like that, that's something that, you know, I, I think that, that would be a different expert altogether, right?

So.

WEST: Okay. Michael, what's your sense of the privacy concerns that can arise from these types of systems?

GRAHAM: You know, we really don't deal with that from the NTSB, but I totally understand where people are coming from. I mean, we've already seen this in the aviation community with all the tracking of aircraft through the various sensors that the, the FAA...

I mean, when you look at what's known as ADS-B data that, that's out there. Anybody can look it up online, and you can track just about everybody's airplane that is flying in the national airspace. That is very much a concern to a lot of different individuals that are concerned about their security and being tracked.

So there's a lot of moves for blocking all that stuff. So I can understand the concern when it comes to connected vehicle technology that, you know, people, you know, we, we like our privacy, and we should have our privacy if we don't wanna share something. So I, like Alex says, I, I don't have any expertise in that area.

I don't think we do from the board. But I totally understand it, and we do need to protect that.

WEST: So Michael, going back to something you mentioned earlier. You said that the Department of Transportation a few years ago had proposed some policies in terms of dealing with connected vehicles, but some of those ideas were put aside.

Could you just give us a sense of what those proposed policies were, and then what the situation is now?

GRAHAM: Sure. They, they were trying to come up with a path forward for connected vehicle technology. They- they've done a lot of research themselves and had some very good outcomes from their research on connected vehicle technologies when it comes to crash prevention and all and the systems worked very good.

But right now the, the industry is really it, I would say is, got the biggest group that's sitting on the sidelines right now, and that's the automobile manufacturers. And I'm not big into regulations personally, but that group definitely needs some regulatory certainty when it comes to putting these systems on their cars.

They're, you know, historically are not gonna put things on their car- unless they're mandated. So they are looking for some regulatory certainty when it comes there. Some of them are already been burned back in 2018 when everything was changed with the spectrum and the, and then eventually the sell off of part of the protected spectrum out there.

One manufacturer was already doing vehicle-to-vehicle work, and they've since turned those all off. Another one was getting... Another large manufacturer's getting ready to go ahead and go forward with some of that. And they got a letter back that just says, "Hey, we're... You know, don't do it." So they're...

If they don't see some regulatory certainty, we're not gonna see vehicles out there. We do, we do see some metropolitan area groups and counties doing connected vehicle technology out there, like snowplows and preeminence on intersections to where they can change the light when the snowplow is approaching so they can clear the roads quickly for those in the morning if there's snow.

Express buses, I know they're doing these down in Atlanta where they're changing the vehicle so the express buses can move through quickly and save a lot of time for the users out there. So, yeah, it's, They're the... We're-- They're gonna need some help out there. We need the DOT to take a lead role.

I don't think we're gonna see a lot of mandates right yet, but I think some voluntary help will get the industry moving. I know they're talking and speaking together, and they hadn't talked to each other for, like, six years before they put that out. So it's important the industry and the regulators are talking together.

And i- their, their plan or their projection was for a very small percentage of new cars I'm talking like 6%. And we're not gonna see the benefits of connected vehicle technology, especially when it comes to imminent crash prevention, if we don't have a large majority of the vehicles talking to themselves or the infrastructure out, out there in, in the world.

WEST: By the way, I love that snowplow example of being able to change the traffic light when they're out, out plowing the roads. You can definitely see the advantage- Yeah ... of that in- Oh ... the same, in terms of passenger buses.

GRAHAM: Yeah. I, I'll tell you, I gotta give a shout-out to Macomb County just north of Detroit.

They're doing it up there, and they can clear all the roads in a couple hours quicker than they could in the past, get the roads clear before all the people hit the roads in the morning to go to work.

WEST: Yeah. You can definitely see the advantages of that. So Alex, what can drivers and passengers do to either protect their privacy or we also talked about some of the cybersecurity issues.

What can they do to protect their security situation in a world of connected vehicles?

WYGLINSKI: I mean, well, what it comes down to is not so much the, like, the users, right? Like the passengers and the, and the drivers. It really comes down to the development of the technology itself, right? Like, so, so I think it all has to be engineered at the beginning with the assumption that, like, you know, when, when, like, you know, whatever wireless technology you're using in order to interconnect the vehicles, whether it's some, some new release of 5G or whatnot to, to take into consideration the fact that there, there, there, there could be the potential for some sort of malicious user or some sort of entity out there that is trying to create some sort of disruption.

Now, now the critical aspect of this is that what ultimately works well is some sort of, like, sensor fusion, and that's very tricky. Sensor fusion is ver- a very tricky topic because now what you've got is you've got, like, you know, let's say through wireless connectivity, information from other vehicles, right?

And they might be different quality, different resolution. Like, let's say, like, let's say the information being exchanged is out of date. There's, like, latency or it's imperfect. It's missing some information. And then on the vehicle itself, it's, it potentially might have, like, you know, imperfect view of the outside world.

So it really comes down into obviously more research into creating platforms vehicles if you will, that can take not only the information that's shared by other vehicles to it through wireless connectivity, but also for instance the, the information coming from the vehicle itself, you know, its own lidar and/or optical, like, you know, vision system and/or radar.

There's even been, like, you know, some research studies, like, not by myself per se, but I've been reading up on it from other folks that are using, like, you know, roadside cameras, which is kind of an interesting concept. Like, you know, all those, like, roadside cameras that are along highways and incorporating that as yet another sort of sensor modality into the decision-making process for you know, identifying what the situational awareness is of these vehicles, right?

So, but, but there, but there is a caveat. Like, I, I do wanna emphasize the caveat, which is too much information is also not a good thing, right? So if, like, you have lidar, and lidar is a

massive amount of information, and then you have a radar system and optical systems, and then let's say the cars adjacent to you are also feeding their lidar InVision and/or radar information and then the camera on the side, what's gonna happen is, is that you're gonna hit a compu- a, a computing bottleneck, right?

Because that's a lot of information to take together to fuse and then make a decision And, and, and again, like the issue is low latency. It's gotta be low latency. So there's gotta be a trade-off somewhere. Like, you know, which data is gonna be the most useful in order to make that decision? Now but at the same time, having that data can also identify whether a network is being attacked.

Like, you know, the connected... So, so let's say you're getting connected information from one vehicle, and it's, it's not checking. It's not, it's not, it's not matching what your LIDAR and your vision and your radar and that other vehicle's sensor information being fed to you. You can then say, and th- this is very important, you can then identify that that vehicle or whoever's feeding that information to me is incorrect, it's potentially malicious, and then you can cut them out of the network as well.

So and that's another, that's another completely different area of research than to mine. There is, there is, like, in the Department of War space, they do talk about these distributed networks. They call it private 5G. And there, a few years ago there was this thing, and it's still going strong, called Zero Trust, where it's this assumption that anybody that's communicating with anybody else in the network is, like, you know, the premise of don't trust them until they're absolutely 100% validated, right?

And there, and that's its own, like, research space altogether. So there's a lot of activity that should be done, and should be done independent of the passenger and the driver, right? The technology should be able to filter out those, those malicious users and those threats against the network.

WEST: So Michael what do you think consumers can do to protect either their privacy or their cybersecurity situation?

GRAHAM: Well, f- I, I think that's a little outside my expertise, to be honest with you. I, I don't know what they're gonna be able to do with the, with the vehicles. I, I know there's some a- an agency out there that is looking very closely at that. So whatever performance standards may be set up for connected vehicle technology in the future, I know it has to go through that agency to make sure it's protected.

So I, I really, that's a little bit outside my expertise area. But I, I'm aware there's a group that will be looking at that. And, and like Alex said, there's a group that looks at issues with, with, between the military and the civilian side of the house to make sure there's no interference between frequencies and things like that in use.

WEST: Okay. We are starting to get some questions from our audience. So I'm going to start going through them. And those of you who are watching, if you'd like to submit any questions for our panelists, you can email them to us at events@brookings.edu. That's events@uh, brookings.edu. So one question that has come in is what types of infrastructure or facilities should public sector agencies install to insist with the connected car rollout?

Either one of you who'd like to jump in on that.

GRAHAM: Well, so as far as infrastructure goes like I said, a lot of the metropolitan areas already have put the infrastructure into their into their intersections out there. So a lot of them are already tracking not just what the lights are doing, but what the traffic's doing. I know a lot of them are looking at the different road users, not just, you know, whether they're walking, riding a scooter, a bike, things like that.

They're tracking a lot of information, but they're not... They're looking at it themselves, whether traffic gets backed up, do they need to change the lights? Do they need to get somebody out there to help with an accident? But so a lot of that's there. I think a lot of the infrastructure owners out there are kinda waiting for the vehicles to come along with their connected vehicle technology to be able to start talking to each other.

So like I said, the, the manufacturers have been on the sideline, and I understand why, but if we can get some certainty regulatory-wise, I think we're gonna have a lot of those start getting off the sideline and start getting into the game. And I think that provides a very promising future especially from the crash prevention side of the house.

WEST: Alex your thoughts on any infrastructure improvements that are needed?

WYGLINSKI: Yep. No, just echoing Michael. Like, you know, I think there's already quite a bit of infrastructure in places like, you know, like, like intersections, like, you know, let's say specific sections of highway and such that need additional observation and, and the like.

Definitely I think there needs, like, you know, from, from an auto manufacturer perspective and partnerships with, let's say cellular service providers, like, you know, so for instance, like going back to the example of that that collaborative journal paper that, that we were exploring- One of the reasons we, we looked at very importantly like, in, in that research in identifying where these phantom vehicles are located, we use those those side link channels for, for the 5G standard, right?

The mode four connections. And part of the reason for that is that as opposed to, let's say here's cellular service provider A and provider B and provider C, which are allocated different swaths of r- electromagnetic spectrum, like frequency bands to, to support their telecommunication networks, right?

Their cellular networks. The, the sidelink channels use, use the same frequency band and therefore allows for, it allows for, let's say, cars that might have different cellular service providers to, to interchange information with each other without having to force, let's say, different cellular service providers into the same frequency band.

And I think that's gonna be very important, that interoperability between vehicles, even if they have different service providers, even if it's different auto manufacturers to be able to connect with each other, right? I think earlier on in, in, in this, in, in this, in this this, this panel, like, you know, we were ta- we were talking also about like, you know, like, market penetration.

Like how many of these vehicles would be connected, right? And, and it's, you know, and like how long does somebody own a cell phone? It's like, you know, maybe six months to three years, right? How long does somebody own a vehicle? We're talking, you know, we have people that are like, you know, antique car enthusiasts that might have vehicles that, you know, they, it might not have any sort of embedded processing on board, right?

So, so, so I think the idea is this ability for like, you know, not, not infra- infrastructure from the sense of, you know, let's say installing equipment like r- roadside infrastructure like, you know, a vehicle to infrastructure, V to I or a vehicle, a vehicle to roadside or like, V to R. But also infrastructure from the sense of like all the different other stakeholders working together to at least increase the, the, the amount of inform- trusted information exchange between everybody.

Will it be perfect? Probably not, you know, because we'll have some folks that will insist on driving the antique vehicle without connectivity. But in those cases, and here's kind of the superpower of, of connectivity, multiple vehicles that are all sensing that one vehicle that's completely unconnected can then make the determination and share information amongst themselves saying, "That hole in air that we're detecting is not a hole in air.

There's an actual vehicle, it's just not communicating with anybody," right? And I think that's, that's gonna be really important. I think that's-- So from that standpoint, the infrastructure is a much broader definition. It's, it's across not only the, the what we, we have at the road, at the intersection, but also all the other stakeholders involved.

WEST: I think those are all terrific ideas. One thing I would add to the list is dynamic traffic lights. Like right now when the lights are switching from red to green, they do it on a fixed schedule irregardless of the amount of traffic coming in either direction. If we move towards dynamic traffic lights that basically change based on the flow of traffic at that particular intersection, I think that would make a huge differ- difference in traffic congestion.

We have a

GRAHAM: question- That's a good point. If I could add to that. Yeah, you know, we're, like I said, we're already seeing it with snow plows, buses, and emergency vehicles. Yeah. A lot of municipalities- That's right ... and counties are already doing it with, with the, the emergency vehicles out there to change the lights so they can get to wherever they need to as faster and, and that may save a life down the road.

So it is it's doable.

WEST: Yeah. No, I think that's an innovation that would make a big difference. You know, saving lives, as you mentioned, improving traffic flow, which would benefit all of us. So we have another question on this general topic of what the person refers to as data misuse, which the person in in that definition includes problems of bias, surveillance overreach, and discriminatory outcomes.

And so the question is: Given those problems of data misuse in any connected system, whether it's cars or anything else, what governance or technical safeguards can be built into connected vehicles to ensure the data are not misused, the consumers are proper- that their identity is properly protected, and the data security is maintained?

WYGLINSKI: I mean, I, I'll, I'll jump in. I think, I think at least from my perspective, and, and again, I'm... I like to joke with like, some colleagues of mine, like I'm just a humble engineer, right? But, but the idea is the, like, you know, when, when we design a system and such, it, it really is gonna be dependent on what the ultimate like sort of objective is.

And in the case of, let's say, a connected vehicle network and such it's, it's again, it's about the situation awareness. The, the number, the big one being who's around me, right? And who's... Like, you know, so for instance, like, you know, we've done quite a bit of research here at WPI graduated a few PhD students a couple of years ago, where you know, the number one case, the use case that like, you know, like we- connectivity is gonna be really great at is when you're trying to do a lane change, right?

You're in the slow lane, you're trying to pass, let's say, that semi-trailer that's in the right lane, right? And so you go into the left lane, and then here comes this other vehicle that's booming along. And, you know, like, what's the situational awareness of that vehicle changing the lane, as well as that vehicle that's booming along going like much faster than, let's say, the vehicle that's doing the lane change, right?

And so- Like, what information, what is the absolute minimum information that all the vehicles within, let's say, what- like, you know, whatever frequent- like, you know, transmission range you're thinking of. Like, half a mile, a mile, you know, whatever makes sense, right? Given the speed limit of the, of the vehicle, but not too much of a range that you kind of overwhelm all the vehicles with unnecessary information exchanges in order to keep everyone safe.

And the minimum is gonna be things like, for instance, the, the, like, the location and the intent and the speed, you know? So, so for instance, if this vehicle is, like, right now behind the semi, right? And it's, and the semi is going 55 miles per hour, and the vehicle behind it is 55 miles per hour, and it needs to go into the left lane, it's only gonna communicate to everybody around saying, "This is my intent.

This is my location. And then, and then I'm gonna accelerate at this speed," and then send that information to, let's say, that other vehicle that might be half a mile away, but approaching really quickly, let's say 65 or maybe 70 miles per hour. Now, of course, there's gonna be issues of, for instance, the identity of that vehicle.

How do you distinguish one vehicle from another vehicle and such? You know, and, and, like, what would make sense? Like, is it gonna be the VIN? Maybe, maybe not. Like, you know. But may- we could also learn something from, let's say for instance, cellular technology. Cell phones are not identified by their cell phone number.

Like, you know, here's my cell phone number, it's 10 digits, that's that person. You know, they have something called an IMSI, or specifically for a cell phone, it's an IMEI, right? But in a cell phone network, usually because, you know, that, that's kind of like a really kind of serious amount of information that's being disclosed there- usually what happens in a cellular network, you have, like, a temporary ID that happen, that you are assigned within a cell until you go into the next cell in a cellular network.

Perhaps a model like that could protect things like the privacy of an individual as they're driving along so that, you know, you prot- you protect the profis identity of the individual, but you still provide the vital information that keeps that individual safe when they're doing kind of somewhat of a n- a risky move, right?

And I would consider, like, a high-risk move changing from one lane in a highway to another, right? And again, that's just kind of a very simplistic viewpoint, but to me, I'm kind of a

minimalist. And it also goes back to the point I made earlier, too much information doesn't necessarily mean better either.

So, you know, keep it minimal. Perhaps have a temporary ID type of of, of mechanism so that the identity of the vehicle or the driver is, like, you know, first of all, it's not by name, it's not by VIN, but it's something that says, "In this stretch of road, we have these vehicles with unique identifiers performing this action, and here's its location," such that everybody's able to drive safely.

WEST: Well, I love your lane-changing example since I grew up with the old-fashioned technology of the turn signal as an indicator of, you changing lanes or making a turn. But of course today nobody uses their turn signal, so some type of more automated approach might actually turn out to be safer.

Michael, any of your thoughts on ways to prevent data misuse?

GRAHAM: I'm sorry, I lost you for a minute. It looks like I lost my internet and I came back. So, no, I, I really don't. That's kind of, out- outside our expertise area.

WEST: Okay. Another question is this individual prefers a less connected experience.

So basically is asking for advice on what can drivers do who actually want fewer connections, fewer digital connections, that is as opposed to greater ones. What are their options? Like, are they just restricted to driving old cars that don't have all these digital connections?

GRAHAM: You wanna take that first, Alex?

WYGLINSKI: Yeah. I'll, I'll, I'll, I'll give it a try. I think, I think the thing is that again, is kind of like outside of the ar- my area of expertise, but I think you know, I think, I think it really will depend on a lot of factors in terms of, let's say, what, how the, the, the vehicle, like, you know, what are the options that are so...

Like, well, okay, so let, let me take a, take it a step back. Like, let's say if something that's like, let's say, mandated. Like, let's say in the future there's a regulation that requires some level of, of connectivity in the future. It's, it's like, you know, something as a safety technology, the equivalent of airbags, the equivalent of like, let's say rear-facing cameras, the equivalent.

Well, well then that's gonna be kind of difficult to kind of like opt out of because that, that's required, right? But I think anything beyond that, right, like in terms of connectivity like, you know, like for instance, like, you know, taking my vehicle right now, you know, it has the option to, you know, have additional services, right?

I'm just don't wanna pay for them, so I opt out, right? I don't, I don't need like, you know, like never ending connectivity to the internet so that my seven-year-old in the back can continuously watch all these like kid shows and stuff. Like, you know, I, I'll just say, "No, no, thank you." And, and but, but let's say the basic connectivity that's like required, say, for my vehicle for safety purposes, I won't be able to opt out of, and you know, and there's a reason for that, right?

Like, you know, in terms of like keeping everyone on the road safe. So I would imagine in the future something of th- that nature. Like, you know, there, there might be some like tiers of, let's say, connectivity and like, I think just like the, what the, the person who was asking the question, they were kind of leaning towards that.

Like, you know, less connectivity. Maybe not no connectivity, but let's say the absolute minimum that keeps everyone safe, including the driver and everyone around them. But at the same time, let's say not have any of like, you know, the, the additional connectivity that, that may or may not be necessary for, for safety purposes.

WEST: So we have another question on the issue of electronic attacks on the infrastructure that supports connected cars. Person wants to know what are the possible risks in terms of an electronic attack on the infrastructure that supports these cars? What are the effects, and what can be done about that?

GRAHAM: Well, I'll take that first. I, I think what we're looking at is maybe with connected vehicle technology out there, if we lose the infrastructure, we're just not gonna have information, let's say, from an intersection. And I know a lot of these are pretty well-protected 'cause I've seen a lot of municipalities have, have put in the fiber optic cable there, and they will have the command centers with either in the county or, or the city to control a lot of this stuff.

Of course any of it could be attacked by you know, cyber issues. But I think what we'll just have is like Alex has said, we may just have, like if that vehicle's not there the other vehicles could talk to each other and say, "Hey, I, I have no information on the intersection up there." And hope- maybe that would be you know, a warning sign to the driver that, "Hey, you know, I need to be a little more cautious as- at this intersection," a- as they approach.

WYGLINSKI: No, exactly. Exactly what Michael mentioned. And I think, I think, and, and additionally, one big field of active research is also the detection of threats against the network. So let's say there's an electronic attack being, being like, you know, currently in progress against a part of infrastructure or against the vehicular traffic along a stretch of road, what would happen is like, like you know, like...

And, and it's cat and mouse, right? Because if it's like very, if it's very obvious, what would happen is the network would then, like somebody in the control center or somewhere is gonna say, "Hey, there's an issue happening here." Like you know, the, the, the traffic i- like there's somebody or something that, that is affecting, let's say, the connectivity between the vehicles, or is introducing data or information that does not correlate with, suppose, let's say, with the sensor information from multiple vehicles.

Or let's say the infrastructure itself is unable to connect with the vehicles on the road. That could signal to, let's say, repair crews or some sort of security or, or some- or somebody saying there's a problem here. Now, the cat and mouse, of course, in this research area is- a lot of, a lot of malicious users would also try to mask their intentions to make it look like it's a natural phenomenon, and then how do you catch those folks?

And it's just kind of like this cycle of, of like literally of cat and mouse. But again, this is an area of like active research in terms of identifying threats against these types of networks, given how important they are. But but, but, but the key thing is, is identifying the threats and,

and also the fact that there's enough redundancy and there's other forms of sensor modalities in the network, that helps a lot.

You know, it's like, you know, if, if everyone was just dependent on connectivity, that's one thing. But usually a lot of cars more and more, they're like, you know, equipped with visual sensors with like the lidar, with the radar and, and other forms of information that they're not just con- they're not just dependent on one form of information, and they can kind of like filter out anything that could look as bogus.

WEST: Okay, we have another question. Are there any policy or regulatory actions that need to be undertaken to protect consumers in a world of connected cars? Hmm.

GRAHAM: I, I'm, I'm not aware of any. Alex, do you

WYGLINSKI: know? No. No, I'm, I'm not. Sorry.

WEST: Okay. Someone has a question about fully autonomous vehicles as opposed to connected cars per se. And they're suggesting that autonomous vehicles will increase people's willingness to commute over longer distances. And so they want to know what cities should do to either encourage that or respond to that type of incentive.

WYGLINSKI: Hmm.

GRAHAM: Well, I... What I would say about this is connected I think when we look at autonomous vehicles, they're, they're... The ones we have out there right now are all using onboard sensors, and there's... That creates issues as you see a lot of these that are being deployed right now are in what I would cl- classify as more of a closed course area.

There's certain things that they don't do. One of the toughest things for an autonomous vehicle to do is merge. You know, with the onboard sensors, if somebody s- starts slowing down and waves them in, autonomous vehicles don't alway- can't always pick that up. So, I think to have truly And this is my opinion, truly safe autonomous vehicles out there, we need connected vehicle technology.

We need to be, these vehicles need to talk to the infrastructure and other vehicles to be able to merge or know what's happening up ahead because of the limitations on onboard sensors. This is just a, a, another redundancy, like Alex had said, that just makes it safer and decreases the risk of having an autonomous vehicle.

So I, I fully support connected vehicle tech- technology, especially when it comes to autonomous vehicles.

WYGLINSKI: Yep. Yep. No, just jumping in, like exactly what Michael said. I think like the, the more information, especially with, especially with the you know, like it's just another form of information that goes into decision-making process with the autonomy.

And like, you know, if you look at how like, LIDAR or vision systems or radar work, it, it, the sensor modality, like the sensor information goes as far as, let's say, what it, like the first car, right? And then behind it, it doesn't know how many cars are behind it or the cars in front of it and such. So, so it's very limited.

But wireless is kind of like that, like it goes beyond, let's say, just the physical kind of environs, if you will, of like the cars around you. It could... And let's say for instance, you're in like you know, in a, in a downtown part of a very built up city and you're at an intersection that doesn't provide you much much of like a sort of like situational awareness, at least from a vision standpoint of the c- traffic that's crossing, right?

But it doesn't matter with wireless because the wireless information just like sort of permeates through the, through the air and it, it's not blocked by buildings at le- at least at the frequencies we're talking about. So you could tell that a car is approaching even if you don't see it, right, and the LIDAR doesn't see it and the radar doesn't see it and the vision system doesn't see it, and you have enough information.

Or let's say the, the wireless relay, the wireless equipment that's in that, that intersection, right? The, the, the stoplight. So wireless is like, is, is great because it gives even more information, the more lead time, the more sort of awareness to that autonomous agent so it can make the best possible decision

WEST: So I have one more question for each of you, and then we're going to move to our second panel.

There's a question that has come in about what is happening in other countries. So we know connected cars are not just a US phenomenon, but there are a number of nations around the world that are experimenting and rolling these vehicles out. So, what the person wanted to ask, and I'm going to kind of paraphrase what was a long question on this, is which other countries appear to be making progress on tackling the issues that we've talked about here?

Are there particular countries that seem to be doing a good job or-- And then I'll just kind of add my own footnote to this. Are there lessons that could be learned from the experience of other countries?

GRAHAM: I'll, I'll go ahead and start it off there. Absolutely. I, I will tell you, the US actually is pretty far behind on a lot of this already. The European New Car Assessment programs are, are far ahead of the US when it comes to not just the forward collision warning s-on-board sensor systems and the performance required of their cars to get top safety ratings but they are in China.

And a lot of those between China and the European, European Union they are moving far ahead on trying to establish connected vehicle technology on their new cars. And that's like I talked about earlier, you know, how do we get the manufacturers on board? They're looking for some regulatory certainty, but how do we incentivize it?

Maybe not just by regulation, but maybe by our New Car Assessment Program, which is kind of-- has fallen far behind the rest of the world. Incentivize it there as a top safety pick on some of this technology. I think we'll get a lot more manufacturers to put it in 'cause some people really buy vehicles when it comes to being top safety picks.

And if they have to if they have these technologies or need these technologies to get top safety picks, I think that's a great way to incentivize the industry to start producing these.

WEST: Alex, we'll give you the last word on this. What do you see happening in other countries? Are there lessons we can learn?

Are there other countries that are doing a particularly good job at

WYGLINSKI: this? So, okay, so from a research standpoint, so, one of the many sort of like non-- like, you know, additional hats that I wear so like many-- like, you know, my professional community, the Institute of Electrical and Electronics Engineers.

So I was the president of the Vehicular Technology Society, which this is its, like- You know, one of the main things, connected vehicles, right? And so I was president in 2018 and 2019, and there was a, there's a lot of research activity done globally. China's one of them, and Europe in pr- as well. Like, you know, but other countries in, in addition to them.

But there is definitely a big research push in terms of connectivity, also connected and connected and autonomous vehicle technology. So combining the two, so not only just, like, connecting information, but connecting it and then feeding into the autonomous decision-making. I think, I think in terms of publications that I'm seeing from the US, like, y- you know, if that's, if that's a quantitative metric, it, it, it is a little bit behind compared to other parts of, of, like, you know, the world where there's been extensive research into this domain.

But at the same time I would say just, like, being the academic that I am, right, there is a lot of information exchange, right? Like, you have these international venues. Like, so for instance, like the IEEE Vehicular Technology Society has this biennial conference called the Vehicular Technology Conference where we bring together, like, you know, 800 to 1,000 people twice a year from all parts of the world to exchange information and kind of build upon all the knowledge that everyone's generating.

But, but yeah, I would say, like, you know, in terms of where papers are originating on this topic, it's, it's definitely global. I think it's a little bit more beyond, like, the United States in terms of, like, research activities into the cutting edge in this domain.

WEST: No, I think it is important. Certainly many other countries are putting a lot of effort into connecting their cars building the infrastructure.

And as Michael suggested there's a lot going on in Europe. Of course, there are many major car manufacturers are located out there, and their governments are kind of working to both improve connectivity but also think about some of the issues that we've discussed. And then Michael briefly mentioned China, which of course is a juggernaut in the automotive area for a lot of different reasons.

But I think it's good for people in the United States to pay attention to what is going on elsewhere. So Michael and Alex, I wanna thank you for sharing your thoughts with us. Both of you raised a number of fascinating points. And we appreciate you taking the time to join us.

GRAHAM: Thanks for having me. Thank you, Darrell.

WEST: Thank you. Okay. We are now going to move to our second panel. So on the first panel we had several discussions of issues related to privacy, some of the challenges that

the connected vehicle space faces on the privacy front. We mentioned issues of cybersecurity we're gonna continue discussing those things, but then also add some other elements in terms of legal liability issues.

What happens in a world of connected cars when there, when legal issues arise, there are accidents or fatalities that take place. And then of course, the role of insurance companies in the connected car space. That's kind of an intri- interesting element that we didn't discuss in our first panel but we will look at in our second panel.

So our second panel features two very distinguished experts. Marc Scribner is a senior transportation policy analyst at The Reason Foundation, and he's written extensively on issues related to connected vehicles. And Omri Ben-Shahar is the distinguished service professor of law at the University of Chicago Law School, and he also has written on the legal issues of connected cars.

So, Omri, I'm gonna start with you. And basically how do you see the privacy situation in regard to connected cars, and what wor- what worries should drivers have on this front?

BEN-SHAHAR: Yeah. Well, I see the privacy issues as ones that largely suffocate the development and the some of the applications of connection and of tracking of cars and how people drive.

In the area that technology emerged from the use it was introduced by auto insurance companies, you know, tracking how people drive. Before cars were connected, they introduced devices that allow, that would broadcast to the insurers how cars are driven. And on the basis of these, of this data that was collected, insurers would price the the premiums and in- the policies.

These raised privacy issues. This was called the Big Brother Is in the Car with You and led to regulations in var- of various types in various states. Some of it, most of it was ultimately relaxed, but some, in some places it is still, it, it stifles or entirely chokes the use of this kind of technology.

The main ground for that is, of course, privacy, and we can talk through this panel about the, the effects of this. What are the downsides of stifling the introduction and the use of tracking of drivers by mostly state law.

WEST: Okay. Thank you. Marc, I'm gonna bring you into this conversation.

What privacy concerns do you see? Are there things that drivers should be worried about in terms of protecting their privacy through connected cars?

SCRIBNER: Yeah, thanks. And it, it definitely depends on the application of, of where those specific privacy concerns arise. You know, insurance is one, and that has a long history, and it's still being played out before state insurance commissions.

But automakers also have quite a bit of experience in, in this now through their infotainment systems. And automakers generally concede that the vehicle data that's generated are owned by the vehicle owners or lessees. But they have user agreements that allow automakers access to read and write that data.

So what automakers have, have learned in this experience is that ensuring customer trust through robust privacy principles and security protections is viewed as critical to maintaining, Well, first establishing, but then maintaining that continued user consent for data sharing. So I think establishing trust from the outset is critical.

But obviously with all of this data, and we're gonna see more and more of it generated and collected these privacy concerns are going to continue to manifest, and I don't know if there is a a simple fix to all of this. I think we're going to continue dealing with them on a case-by-case basis as technology evolves.

WEST: Well, Omri let me put that question to you. What should drivers do to protect their privacy? Are there steps either they should undertake? Are there regulatory or policy actions that

BEN-SHAHAR: we should think about? Yeah. I, I think the basic question is to understand first what are people's privacy concerns.

Once we understand that, we can also ask how to protect that. And I don't think that the privacy concerns that arise in driving in the use of connected cars or tr- being tracked as a driver are heightened relative to other privacy concerns. This is a quite a generic issue in the data economy.

I think people have heightened privacy concerns when they engage in some applications online that require very sensitive things like DNA, like type of browsing that is done, and people care about privacy. But by and large, people are splashing their data on, in applications in a way that at least raises a question to what extent these privacy concerns that are so central in our lawmaking- kind of conversation are really part of the everyday concerns of people.

I think people are concerned about various things, but they can't resist the upsides, the benefits of data technologies. In the area of connected cars, the i- issue might be, or tracking of drivers might be a bit plays out a little bit differently. On one hand, the, the, the main thing that can be seen when people are being tracked is their location.

Their location they already, most people already know that it's being tracked because they are happy to use navigation, say, maps and navigation devices that gets them there one minute faster. So, the, the extent of the privacy concern is questionable and empirically very hard to verify. The assumption that it exists could be grounds for some kind of action, but so far, at least in the US, it is subject, entirely subject to contracting.

People can give up their data. And as Marc immediately said i- in opening his remarks there are contracts that regulate that, and in many contexts people click, "I agree," when they purchase a car, for example, a smart car, without fully recognizing what it is that will be tracked and for what purpose.

In the insurance context, which I hope we'll talk more about because it is very... there are a lot of things to say there, people have to enroll in a way that changes their insurance policy, changes their priva- So they are-- This is one of these rare moments where the click, "I agree," is not a thoughtless kind of thing that you do endless times a day, but a, a major transaction that you enter into with ups and downs.

Downside may be giving up data, the upside, getting better premium, and many other things that that are to be spoken about.

WEST: Yeah, we will definitely come back to this insurance question in a few minutes. But... And I love that example that you gave of the maps because I think maps illustrate my personal love-hate relationship with personal data in the sense that, you know, we all love the mapping features in our cars.

You know, we can't really navigate. Like, I actually grew up reading maps. It's much easier to have this digital tool that tells me where to go which corner to turn on, and so on. But at the same time, you know, you worry about the use of that information particularly the location aspects of it.

But Marc, I wanna pose that same question to you. What should consumers do to protect their privacy?

SCRIBNER: Well, I think that the types of data it, it really matters. And we're talking about geolocation data. That's viewed by consumers as more sensitive, but it's also viewed by regulators as highly sensitive.

And the Federal Trade Commission, for ins- instance, has analogized automotive geolocation data to mobile phone geolocation data. So subjecting it to heightened scrutiny on the, the uses of those data. And states have taken a similar tact. They've you know, fleshing out exactly what or how this data can be used and what are the, you know, the minimization, retention, et cetera, principles involved.

And they've done some of that through, through enforcement actions against individual firms who were found to be engaged in a, an unfair practice. So, you know, the existing consumer protection laws right now are, are... Even though we don't have, say, a national comprehensive Data Privacy Act existing consumer protection laws are doing a lot of heavy lifting.

And that you know, body of law is being fleshed out both at the state and at the federal level just through these case-by-case actions.

WEST: So Omri, you mentioned the issue of insurance companies a little while ago, so I do wanna delve into that topic. What are the insurance issues in the area of connected cars?

What are the things that people should worry about

BEN-SHAHAR: there? Yeah. It's, it's actually a very interesting issue, notwithstanding the fact that it has to do with auto insurance. Just the title might me- anesthetize many of our listeners. But it, it turns out that that technology that was introduced maybe 25 years ago by an insurance company, by progressive.com, and has later been adopted by many insurers, has major effects on highway safety.

When people that enroll in this program, it's a completely opt-in and about 22 to 25% of a market penetration. When people opt into this program, they are no longer paying insurance premiums the way they used to, the way possibly, Darrell, you pay. Namely rated by their income, their, their, their p- past ex- driver's experience and record.

Maybe their loca- the location of their home credit score, the demographic rating which is by the way known and b- thought to be by many states to be totally unfair towards marginalized communities. Instead, they're rated by how they drive. The applications, the devices record sharp turns, sharp brakes driving s- speeding at night, things like that.

And based on massive data that insurers have as to what factors correlate or even cause accidents like excessive speeding or lane change, abrupt lane changes they give each policyholder a safety score that changes continuously as they drive, and based on that score, they charge a premium. Now, many people start this program realize, "Oh, gee, we are charging...

We're being... We have low safety scores." But over time, and studies have shown that really quickly, sometimes within 30 to 60 days, they learn to drive differently. The result is a phenomenal reduction in fatal accidents, in car accidents in general, but in fatal accidents more specifically. And studies that were done based on, on massive data put this effect at the order, the vicinity of 30% reduction in fatal accidents.

Now, we don't have it with us anymore, the experts from the NTSB and... But there's nothing like this in the history of automotive safety. S- the things like seat belts or airbags have been hailed as important innovations in highway safety. They're expensive, and they have not been shown to have that massive effect.

Here you have a technology that requires no infrastructure, no investment. It's just data, but it changes how people drive. People want to drive better because they get premium discounts, because their devices show them what they're doing wrong, because they feel that they are being observed, and something in their brain changes.

Less impulsive, more what we call system one. And less system one, more system two. All of that translates to a great benefit for individuals and for others. And that is the question that I think we have to put on the scale. Privacy on the one hand, less fatalities on the other hand, and ask states like California that prohibit, outright prohibit this technology, how many lives are lost every year?

I've calculated, I can tell you in a minute, if this tech- when this technology is banned. A- and that is the big question that we have to ask, I think, on every privacy restriction on a data technology that is known to create such a, a important social benefit

WEST: No, that's a great point. So, Marc, how do you see insurance companies using information?

Are there things that we should be concerned about?

SCRIBNER: Well, I think you know, everything Omri just said is, is very important for people to internalize. And, and specifically that state, you know, the insurance markets are regulated at the state level. So it is individual insurance commissions or legislatures that are making this call.

And I think the, the data absolutely show, the research absolutely shows that this technology aligns individual driver incentives in a great way to promote much safer outcomes, and it's

something that, that ought to be embraced by the insurance regulators. But you know, it is, it's very unfortunate that we don't have that uniform support.

But the, you know, these kinds of applications, public benefit applications of vehicle technologies, we heard, you know, the, the previous panel talked a lot about V2X, vehicle to everything communications that transmit safety information. But there's also non-safety potential applications as well for public benefit, road usage charging as well.

And in these cases, yes, the integrity of this data is vitally important. The security of that, especially when, when geolocation data is involved, vitally important. But I do share Omri's concern that sometimes these nebulous privacy concerns are raised without really considering the other side of the equation these, these potentially massive benefits.

WEST: So I'd like to move a little bit beyond privacy to the issue of cybersecurity. On our previous panel, we talked a little bit about malicious uses data breaches foreign actor intrusions into the world of connected vehicles. How much should consumers be worried about this? Are there things we should do to safeguard that kind of

BEN-SHAHAR: information?

Omri? I have to admit that I am not too familiar with the cybersecurity issues relating to driving data and to connected cars. These, many of the breaches, the major breaches that have occurred have to do with financial data, like the leak- the spill of the, all the financial files of 140 million Americans by Equifax.

These are at the forefront of data security issues. One thing that has, usually does not come up in the discussion of this is the recognition that against most of the types of fraud that occur when this data reaches the wrong hands, people are insured. So the data, the losses are occasionally the losses, there is a great loss that is con- centered on an individual, a type of identity theft that ruins lives.

But on the overall scale of the epidemic of data leaks and data security breaches the type of credit card frauds and other types of fraud, people are insured by, mostly by federal law and and other plans. So again, the harm occurs at the social level. When you have an insurance scheme, that means that collectively we pay through various s- systems for the coverage against these ki- types of financial frauds.

And we have to think about it not so much as a private affront, but as a social epidemic. And the, and try to figure out whether part-- that cost, again, is put that on the scale of the downside. In the context of connected cars, which is what we're talking about I'm not all that familiar with the types of breaches that have occurred and what is the social loss that resulted.

I know that there is a potential, potential concerns with hacking into, for example, the algorithms of autonomous vehicles, what have... And all of these things are part of how the system has to be designed. That's exactly what regulators should be concerned once the scheme is put into place and it has some vulnerabilities that could harm society as a whole.

That these need, these, the, the standard for safety has to be elevated.

WEST: So Marc, your thoughts on cybersecurity risks and potential threats from

SCRIBNER: hacking. Yeah. And, and, you know, there, cybersecurity risk is can take many forms here. But to give a I think going back to the previous panel talking about potential interactions between vehicle connectivity and automation, this was a, a major part of the discussion around the 2017 proposed rule from the National Highway Traffic Safety Administration on vehicle-to-vehicle communications.

If you look back at that proposed rule- There were a number of, of deficiencies there, which I think explains in large part why it didn't move forward. But one of them was where... The place where they should have discussed had regulatory text for the secure credential management system, which is the, the system that manages the cryptographic keys that would secure these basic safety messages that would be moving between cars and, and roadside equipment.

They, in that proposed rule, just left a m- massive bracketed gap, in essence saying, "We'll figure this out by the time we get to the final rule stage." Now, that's not a very good legal position to be in as a regulator. You're supposed to provide notice. But it also, it gets at an issue that I think explains why the autonomous vehicle industry back then and still today, I believe, has largely opposed these kind of approaches to vehicle connectivity.

As was alluded to in the previous panel, they are very concerned about expanding the attack surface that this, you know, potentially forced connectivity would bring on their technologies. And these technologies, you know, the- they, they control the entire dynamic driving task. A human being, if, if, if that person is in the vehicle, may not have even an ability to intervene.

So they're very concerned about you know, spoofing and other sort of malicious data that might be ingested by their automated driving systems. And back in 2017 when this was last proposed they were not confident in the approach that was laid out by regulators. We will see if this is again proposed in the future, if their minds have been changed.

But that's where they, they came down the last time this was seriously considered. And it was... A lot of it was cybersecurity concerns that, that brought down that proposal.

WEST: Are there any policy or regulatory actions that you feel need to be undertaken in order to protect consumers? Omri, I'll start with you on

BEN-SHAHAR: that.

So, you know, I'm looking at applications that people enroll into. It seems that there is... We talked already about the insurance aspect. A couple of years ago there was, you know, a scandal was re- for example, reported in, in the media when it turned out that unbeknownst to many buy- new car buyers, their cars were connected and companies like GM and others were collecting their data and using it for whatever uses, Probably mostly benign.

Nobody died from this, but people felt an affront that it is in pa- in part privacy and in part just being, you know, undignified by not being told what you're doing, and why don't we get to enjoy the benefits of the data that you're selling? The coupons that flash on our device, say for for Dunkin' Donuts why is the law- automaker getting this value?

The, My, my thought at that time was that this is giving this kind of activity by automakers, enrolling people into tracking without people's affirmative knowledge, is giving a ba- bad rap for technology that has done so much for reducing highway fatalities by auto insurers. And it has become one of these examples of a bad technology, tracking people, a privacy nightmare.

I think that we, the, what, the, what happens here is the use of technology or infiltration of that technology into people's devices, into people's cars, without their knowledge and without respecting their ability to opt in or to opt out that is is key. So what lawmakers have to make sure is that when we have something like this that is so prominent in people's life, it's not those endless cookie consents that pop up numerous times a day on your device, but how your car is driven regularly and to where, and that someone knows it, and it's not just your insurer to whom you handed that information, but other parties, and who knows to with whom it is shared.

That cannot that cannot happen. Those things need to be sanctioned and in part because, as I said, they are doing great harm to the otherwise the good uses of that technology.

WEST: So Marc, your thoughts on whether there needs to be any policy or regulatory actions undertaken.

SCRIBNER: Well, when it comes to the, the commercial applications of this, and I would include insurance in that y- you know, I think having clarity and ideally uniformity across the country so clear standards that everyone is aware of and that everyone can follow.

That's where you go state by state, particularly on privacy you're going to get dramatically different approaches, and I don't think that is very helpful for your typical consumer. Now when it comes to government systems, I think people have, Stronger concerns when it is the government that may be collecting or at least perceived to be collecting sensitive information.

To give the example of, of road usage charging, which the idea there is to, is to charge to tax by the mile rather than by the gallon of fuel consumed, so a replacement for the fuel tax. But the, the best versions of that technology make use of location data. That way you can track when you're driving on non-public roads, on private property, or you're driving out of state.

And potentially you can charge, you know, varying rates based on different roadway and traffic characteristics. But you know, people have been very nervous about the idea that location information is going to be collected in order to bill you for your, for your road use. So what some states have done, and I think this has been led by Oregon, they probably have the, the best example here.

They adopted a mix of data minimization, retention, and access rules. So for the location data, they made sure that it's only collected and processed by a third-party account manager, not the government agencies that really only care about the revenue to pay for, for roads. They have retention policies that specify that that data that's collected, location data that's collected must be destroyed within 30 days following the conclusion of a billing period.

And then for that brief period while those location data exists, they have c- very rigid access rules. So those data are exempt from disclosure to public records requests and subpoenas

issued in civil actions. So divorce proceedings, insurance proceedings are not going to have access to that road usage charge location information.

When it comes to criminal law enforcement it does provide... Oregon does provide an exception there, the lone exception but it requires that law enforcement seek a warrant in order to obtain that information. And this was written in consultation with, with privacy advocates, and I think that's the approach with, with especially government data, is to bring the, the stakeholders together and hammer out these solutions, recognizing that the public is going to be more concerned about sensitive data that's collected by the government than perhaps they will from a value-added commercial service.

WEST: So we're starting to get some questions from our audience. And again, just to remind people, if you have questions for our panelists, you can email us at events@brookings.edu. That's events@brookings.edu. So, excuse me. There's a question that has come in. It's kind of a long question, but I'm gonna try and summarize it here.

The question is- Can you comment on the future of connected vehicles reporting information to government agencies? And some of the examples the person gives is on the use of roads aggregated tele- telemetry data electric vehicle charging numbers, safety metrics and so on. And then the question is: What is the information the government needs to have in order to make effective use of connected vehicles and to make use of these vehicles safer and more efficient?

BEN-SHAHAR: Yeah. Yeah I think that this continues very well on the previous question that you posed there. You know, I, I view-- I recognize the heightened concerns that people m- would have with the government getting access to some of the location data. But we also have to ask what is the public interest in this area?

After all, using roads is a very public behavior. Roads are public. And a- and it also affects other people. When you have people drive in a d- in dangerous ways, they're affecting others. And so, we'd like to have the government, the data reach the hands of the government in order to serve purposes that we think and we can support, like road safety, like, solving crimes, finding the cars, you know, checking location of cars.

That is done very often in order to advance law enforcement against, you know, various crimes, not just road safety. I'd like the government to have that kind of information. And I'd like to make sure that it is not also used incidentally or purposely for other goals. For example, like enforcing, enforcing so- various prohibitions of, say, visiting abortion clinics.

It's not-- these are areas of core privacy concerns where we would like to have a different might, might wanna have a different rule as to the data in the hands of the government. The uses of these data, in the-- in other words, in the hands of the government, and not just for the applications that I mentioned, but for various other things telematics and da- data technology that could advance various road improvements, traffic rule improvements so as to reduce vulnerabilities of different kinds are, are great uses.

And therefore I think that having a one-size-fits-all government should be out or government should be suspected is maybe a little bit too crude to serve the social interest.

WEST: Marc, your thoughts on that?

SCRIBNER: Yeah, I think it, it, it will depend on the application. But in general, I think the government you know, for, for whatever purpose it is seeking these data it should, it should state what that purpose is.

'Cause a lot of it, in terms of the data that they need to perform their, their core government functions, a lot of things... Say you're a, a state department of transportation. You don't really care about the precise geolocation information there. What you do care about is, is aggregate traffic flows.

So getting a data set, you know, anonymized that gives aggregate counts by time of day in order for them to make better roadway investment decisions examine, you know, potential high hazard, you know, safety r- risk or areas of concern a- along the roadway. That I think is, you know, you know, I, I think you could accomplish that without giving up all of this personally identifiable information that will, will be, you know, potentially generated by the, the vehicle.

So data minimization and clearly stating what you're, you're after. Similar principles that are applied in, in states with, you know, more, more robust privacy frameworks apply to the private sector. I think, you know, the government has legitimate uses for these data, but it, it also doesn't need every granular detail in order to carry out its core functions.

WEST: So there's another question. I'm gonna ask this person's question, and then I'm gonna add something onto it. The question is, how can local and state governments take advantage of connected vehicle data to improve their own transportation safety and system performance? And what I'd like to add onto that is kind of an example.

What I've heard in other contexts is connected cars basically provide all this information that could actually help local governments improve their mass transit systems, you know, where the bus lines should be. Like, there's just a wealth of private sector information that actually would be valuable for transportation planning purposes.

So, their question is basically saying, like, are there ways in which local and state governments can take advantage of connected car data to improve their own transportation systems?

SCRIBNER: Well, I think one was w- the one you just mentioned in terms of mass transit. Transit signal priority is increasingly being deployed with, with buses outfitted and, and, and, you know, special traffic signals that can adjust the phases in order to give those, those buses priority over, over- private car traffic.

But when it comes to certain other applications, I think near term, you're, you're probably still gonna be reliant on in-road equipment loop detectors and the like that are doing traffic counts. And the reason is, it's not that the, y- you know, connected vehicle technology is necessarily bad, but for the, the reasons that were laid out in the previous panel it's not being widely deployed.

It will take a long time for a sufficient number of vehicles to be out there to really generate the kinds of safety benefits people are after, but also to give you an adequate representation of use of the road network. So people right now are holding onto their vehicles on average more than 12 years.

And it's gonna take some time before I think we get some of the, the V2- V2X applications out there and widely distributed in order to realize some of those benefits that the, the, the government could, could potentially get out of that technology.

WEST: Omri, any thoughts on your part?

BEN-SHAHAR: Well, I'm kind of a a very futuristic thought.

You might think it's a little crazy, but here it is. Why should, you know, the way people drive is subject to the law, rules and laws that are one size fits all. We all have to drive the same speed limit on a particular road. We have to all to abide in the same rules. But if people have different skills, create different risks, have different experiences that are all tracked and recorded, and we know that people vary along these things, and we pro- probably by now have the technology to identify and to profile people according to this where connected cars give us the opportunity to communicate to people personalized or individualized commands.

In fact, in a work that I did, a book that I wrote a few years ago called Personalized Law, I imagine that reality and the, the road, laws of the road is a good place to start. You wake up in the morning, and today, based on the data that the algorithm has, you're told that when you, when you... I drive on Lake Shore Drive from Hyde Park to downtown Chicago, I'm not subject to the one size fits all 45 m- miles per hour speed limit.

But today and based on a factor there, I have to drive slower. And Marc probably can drive faster, and this could also change day by day and can be communicated on the dashboard in a connected car. Reasons, the main reasons historically that the law shied away from more personalized commands had to do with information.

These problems are largely being resolved, and the way to communicate these types of commands is probably something that we will increasingly begin to incorporate. So I said this is a bit crazy and kind of futuristic at this moment, but at the speed in which things are happening and car technology is changing it provides us at least an opportunity to think about these kinds of improvements.

SCRIBNER: Kind of building on that you know, from the perspective of infrastructure owner/operators, one of the, the best applications of autonomous vehicles would absolutely need connected vehicle technology, and that's, it's, it's to leverage platooning of these vehicles in a, in a cooperative context. So you could imagine you have...

We have managed lanes today, the HOT lanes express toll lanes. Imagine a dedicated lane where you could move a fleet of autonomous vehicles packed very closely together at 80 miles an hour down an urban interstate. That's the kind of benefit. I mean, the capacity benefits would be enormous in terms of person throughput.

So that is, I think, the kind of benefit that longer term could really get the, the, the government sector excited about some of these applications. Not, you know, safety obviously is a, a, a, a, an, a, a critical benefit here, but there are efficiency benefits that we could realize with the right combination of technologies.

WEST: No, I think that's a very good point. And, you know, we all hate traffic congestion, and I think when I was growing up, the rule was you should always stay at least 10 feet

behind the car ahead of you per 10 miles per hour or s- something like that. And people don't realize with autonomous vehicles and the collision avoidance systems, we can actually compress that distance.

Like we need more time to stop at high speeds. Autonomous vehicles don't need the same distance. So I think you're exactly right. We can develop much more efficient systems. And Omri, I love your idea about personalized transportation, like we're used to hearing about personalized medicine, personalized learning systems.

There could be ways to personalize our transportation needs and uses in ways that would benefit us personally as well as other people around us. There's a question about- Connected vehicles ways to think about connected vehicles as part of a broader system shaped by technology, policy, and public behavior.

And the specific question is, what do our panelists see as the greatest friction points emerging across technology, policy, and public behavior, and how might those frictions be resolved, or how might they influence the long-term success of connected cars?

BEN-SHAHAR: Marc, do you wanna go first?

SCRIBNER: Sure. I can name my, my kind of biggest concern in this, this arena, and that is the the, the kind of the geopolitical considerations that have, that have entered the picture on this. So I in, It, it went into effect last year but during the tail end of the, the Biden administration the Commerce Department's Bureau of Industry and Security issued a a final rule that restricts the import and sale of, of certain connected vehicles that contain any software designed, developed, manufactured, or supplied by a person or, you know, an entity controlled by or, or subject to foreign entities of concern.

And really the focus was on China. Now the, the software restrictions are going into effect. They took effect this year. The hardware restrictions take effect in 2029. And notably, those hardware restrictions, at least for the time being, exclude sensors supporting autonomous driving, so the, the LiDAR radar cameras, et cetera.

And then the the unidirectional communications equipment. So think radio receivers your GPS receiver, your satellite radio, and certain things like that. But this is ra- you know, China has been very competitive on devel- developing these components and, and as well as cars. And I think a breakdown in, in international cooperation is really going to potentially put this these technologies at risk.

So I hope that... I, I understand there may be legitimate national security concerns with some of these technologies, but I think that our, our regulators, our lawmakers need to be, be very careful that we aren't slowing down technology that could greatly benefit consumers and then the, the public at large, especially through the, the safety applications.

BEN-SHAHAR: Yeah. In, in, in the spirit of the kind of the invitation from this- Question to look a little bit broadly and that way Marc also po- kind of expanded the, the lens. I'll say, you know, we various social activities that have been forever governed by human or by small data have led to a lot of distortions and a lot of harm.

You know, there are more than 40,000 fatalities in the roads. There are hundreds of thousands of people dying in hospitals because of medical care that is not poorly delivered and, or poor diagnosis. There are millions of people that are in in, you know, the problem of human and sex trafficking.

Very hard for police to resolve because people disappear. I'm giving examples of areas where data technologies can lead to breakthroughs, massive breakthroughs in improvement, taking humans out of the loop and replacing them with a algorithmic science and AI. And not only AI, you know, but various ways to explore, find patterns, and deliver better outcomes.

In the roads, it's by tracking how people drive, connected cars. In, in the area of medic- of medicine, it is allowing machine learning te- te- models to learn to, to make diagnosis and deliver re- prescriptions for, But for that they need a lot of data. They need to be trained on various millions of past charts, something that rules like HIPAA don't allow.

In the area of human trafficking can have identify people, and hundreds of thousands of people have been rescued through facial recognition technology. Something that is at the sanctum sanctorum of data privacy protection, and outright prohibited in the great parts of the world. So all of these questions need to be put for us, you know, in this new reality.

How much are we willing to ride the good benefits that these technologies are providing with guardrails on the edge, but without generic suspicion that everything that runs on data inv- evokes some kind of privacy nightmare, and that everything needs to... We need to impose a moratoria until we're sure that these systems are perfect.

WEST: I think both of you have made great points on that question. Poor- thanks for sharing your views. There's a question I'd like to ask that I also asked on the first panel, and that is your view about how other countries are handling these types of issues with connected cars. Are there particular countries you think are doing a good job?

Are there lessons from abroad that might inform how we all should be thinking about connected vehicles?

SCRIBNER: Well, I think i- in, in Europe they've, they've taken an accelerated approach, but they, they, you know, they've selected- They, they went down the DRC pathway, and they did have strong support from major automaker Volkswagen in that. So maybe that was-- that helped them a lot, so they were able to you know, deploy a whole roadway network enabled roadway network in Austria and Germany.

So, you know, I think they've, they've learned lessons. They are as the US both due to inaction and also FCC action on the radio spectrum issue has decided to, to go down the, the C-V2X path similar to, to what China has decided. But yeah, I think looking at where, you know, they've done a good job of finding near-term applications, especially government and commercial applications where you can you know, potentially get this technology on the road quicker and realizing those benefits, not waiting for the entire fleet to turn over in, you know, over, over a couple decades.

So I think there are lessons that the US can learn. I think but, you know, where we are today in terms of automakers not equipping their vehicles with the necessary radios I think that needs to be addressed first. Whether that's private or public, we'll see.

WEST: Omri, any thoughts on your part?

BEN-SHAHAR: I'm not sure I have a lot to add. My-- From the perspective that I see, I, I'm kind of concerned about the speed by which European lawmakers feel that confidence to regulate data technologies. It starts with GDPR about eight years ago, and a whole barrage of enactments at the EU level, the Digital Markets Act, the Digital Service Act, the, the data, the AI Act, now the Data Fairness Act.

Before even it's clear what these technologies are, what are the downsides and what are the upsides, typically from the perspective of some kind of a vague sense of consumer privacy concern, we have this bombardment of enactments that stifle pr- pr-progress, data technologies in the co- in the continent, in the European continent.

And it is not by chance that they don't have data, big data technology breakthroughs in the continent. The main thing that they do is fine American companies or Chinese companies for what they regard as an offense. And maybe it's important to be very, you know, hence be, be very concerned- With the downsides.

But the level, the speed and breadth of the prohibitions that they enact seem for me to be, in general, counterproductive.

WEST: I'm curious what type of infrastructure improvements each of you think would be necessary in order to move us into this world of connected cars so we can get the advantages while hopefully minimizing any disadvantages.

BEN-SHAHAR: I would just... You know, I, I know I'm not a, an expert on the infrastructure. I usually study the legal questions of what are the harms and benefits that justify some kind of legal engineering rather than technological engineering. But I live in the s- south side of Chicago, 10 miles from here. When I go on the expressway on the toll road you move from Illinois to Indiana.

In Illinois, you have devices that record you as, you know, every 30 miles, and you don't have to stop to pay toll. In Indiana, you have to go through gates and stand in line. And even if you have a device like an E-ZPass, you have to stand for it to be re- It is... The technology is just not there. And so long lines on the highway of people standing in line to pay cash or something for the, that is a, a technology breakthrough that everybody... You know, it could be replaced by tech- a tech- the technology that we have in Illinois. It's this... I know it's a silly example, and we're talking about much more advanced digital technology, but so much more can be done with that eye that views us at a t- at a level in the Illinois expressways.

It could, as Marc suggested before, tax us for using roads based on miles. Especially for electric vehicles where you can't tax at the pump, you'll tax on the expressway. These are important innovations that could lead to less distortions in types of activities.

WEST: Marc, any- Let me- ... infrastructure improvements do you think would be necessary?

SCRIBNER: Well, I, I think before we, we consider making any infrastructure improvements, I think we need to figure out who is going to pay for them. That was... If you go back to that 2017 National Highway Traffic Safety Administration proposed rule on vehicle-to-vehicle

communications, the, th- that, that called for, that framework called for about 20,000 roadside equipment units to be deployed throughout the national highway system.

You know, those roadside equipment, th- those DSRC boxes ran, you know, several thousand dollars with a, with a te- five to 10-year life cycle. But- The National Hig- Highway Traffic Safety Administration isn't going to fund a nationwide roadside equipment network. Was that going to be, I, which I don't think they have the legal authority to do it, but would, would, would that have been an unfunded mandate on the state departments of transportation?

I'm not sure they would have liked that. And, you know, but get, answering these, these questions early on before we decide to make major investments, I think will, will save people a lot of a, a lot of heartache. Because, you know, some of those communities that did decide to purchase DSRC boxes states and, and communities well, the FCC decided that they're sunsetting DSRC use in the 5.9 gigahertz band.

So those, those, they were, they're gonna have to either replace all their equipment with retrofit or replace with connected vehicle or, sorry cellular vehicle to everything technology if they wanna continue using those types of applications. So we just need to make some decisions on just standards, payment responsibility basics like that, I think, before moving ahead with major infrastructure investments.

WEST: Yeah. But a last question for each of you. Kind of thinking two to three years down the road, what do you think the world of connected vehicles is going to look like? And will we be happy with what we see though?

BEN-SHAHAR: I have to admit that this is not necessarily a question that I've given a lot of thought to. I've looked more at the questions that surround the introduction of autonomous vehicles. And maybe this is a moment to touch on that issue, type of connected cars, but a much more interesting type and interesting questions talking about level four connected vehicles without a driver.

And w- in the next three years, we will probably see, three years from now, we will probably see more of these, and we will be living through a period that, for better or worse, we can call the messy middle. Before all cars are autonomous, which might happen at some point in the future, we'll have the roads have to be shared By very efficient, very good, and very safe autonomous vehicles, and very unsafe or to some degree, less safe human-driven vehicles.

And there might be collisions that we'll have to figure out, the law will have to figure out how to resolve. On the one hand, there is the, might be the negligence of the driver. On the other hand, there might be some products liability issue, some problem with the design of the algorithm. And we will have fascinating trolley problems.

Namely, how to... Who decides how an autonomous vehicle is programmed when it has to make a tragic choice? It cannot avoid an accident, but it needs to determine who will get injured, and it can do so instantaneously, but it needs to be given some guidance. What lives to save, what kind of harms to I think that three years from now, we will have to address these issues to a greater extent because of the introduction into the public roads of autonomous vehicles.

WEST: Marc, your thoughts on the situation down the road.

SCRIBNER: Yeah. When, when it comes to vehicle-to-everything communication, I think in three years the, the picture won't look that much different than it does today. So very marginal penetration and maybe we'll have a commitment from, from automakers and a path forward from national regulators, but I don't think much in terms of deployment.

But to Omri's point, you know, on autonomous vehicles, we, th- they are, we have all forms of, or all sorts of connections. They're connected you know, to the cloud both because they need to communicate with their, the robotaxis, and trucks need to communicate with command centers. But also they, they collect so much data that they need to offload it.

There's not enough compute on board the, these vehicles for them to do everything independently. So, we're also, I think, gonna see more more wireless software updates that may or may not, and we'll see if Congress decides to change it, on the s- sort of through vehicle recalls. But I think we're gonna see increasing connectivity of certain types as we have for the last, you know, s- couple decades.

But you know, some of these, these purely safety-focused more or less vehicle-to-everything communications I don't think are gonna change all that much in the near term.

WEST: Well, we are out of time, but Omri and Marc, I wanna thank you for sharing your views. Both of you did a tremendous job.

Lots of provocative ideas that I think give all of us a lot to think about. And for those of you who tuned in we appreciate your interest in our discussions. And if you're interested in learning more, at Brookings we write regularly about connected cars and digital technology in general.

You can check out our work on our TechTank blog as well as our TechTank podcast. So thank you very much for tuning in.