

2017 HOUSE INDUSTRY, BUSINESS AND LABOR

HB 1394

2017 HOUSE STANDING COMMITTEE MINUTES

Industry, Business and Labor Committee Peace Garden Room, State Capitol

HB 1394

1/25/2017

27371

- ☐ Subcommittee
☐ Conference Committee

Committee Clerk Signature

Ellen LeTang

Explanation or reason for introduction of bill/resolution:

Autonomous vehicle data ownership.

Minutes:

Attachment 1, 2, 3

Vice Chairman Sukut: Opens the hearing of HB 1394.

Chairman Keiser~District 47 from Bismarck: Introduces HB 1394. I attend a conference KGBM & listened to testimony of autonomous vehicles. States need to figure out who owns the data collected that is happening with autonomous vehicle. This would have an effect on the insurance industry. We want to protect our customers. Who will own the information?

Attachment 1~hands out an amendment. This amendment gives the authority in advance.

I think it's important to catch up.

8:40

Rep Becker: My concern is with the consent of the owner; I could see if the dealer could have a check to give consent as part of the process of being to own an autonomous vehicle. That negates the entire bill, do you see that as a concern.

Chairman Keiser: With this legislation, we are preventing that. We could say with informed consent that you have the option not to do it. I think the intent is clear in the bill & is it's designed to avoid very thing, if we need to strengthen, I'm totally ok with that.

Rep Kasper: We had a bill in a past session that dealt with personal, confidential financial information that was run through House & Senate & was passed with a referral. The people of ND by 76% said that we do not want our confidential information shared. The problem I have with this bill is I don't see any penalty to the manufacturer or organization that collects the data, if they violate the terms of this bill. Is there a penalty elsewhere in statue of the violation?

Chairman Keiser: I'm not certain, but we could put a penalty in if we wish to do so.

Rep Kasper: Once the information is gathered, it's gone. I'm suspicious of personal data gathering by an outside entity. Do you have any concerns about that information could be used and stored?

Chairman Keiser: Reality is, with the autonomous, that information has to be collected & used to make it autonomous. Without that collections, there can't be any corrections when the vehicle is moving. If we are going to collect the data, the bill is trying to address the collection of the data that's done with is what the bill is trying to address.

Rep Kasper: Do you see any need once the date is collected & analyzed by the collector to keep that information for a long period of time, how do you see that?

Chairman Keiser: That is a two sided sword, we do want data collect to use for safety over a long period of time. The question is what should we do at this period of time.

Rep C Johnson: There are all kinds of vehicles, do you see it affecting different types of vehicles?

Chairman Keiser: The language is broad enough to cover that. If we need to expand it, I see no problem with that.

Vice Chairman Sukut: Anyone here to testify in support, opposition?

Leighton Yates~Manager: State Affairs: Attachment 2.

22:10

Rep Lefor: What about without consumer consent?

Yates: That information hasn't even begun collected at the moment, but the question should be now who owns the date but how to control the data. A lot of that information is zeros & ones, it means nothing to us but it helps the mechanical pieces of the motor. It has no information that would be applicable to any setting outside this vehicle's function. There are services like On Star, GPS or Emergency Services, you give consent by engaging them. There is no information sharing that I know of that's consensual?

Rep Lefor: What is your position, should we wait & be reactive rather than be proactive?

Yates: You should wait.

Rep Kasper: Page 2, 2nd paragraph, can you share some areas of undesirable data sharing that could be detrimental to the individual owning the vehicle obtained?

Yates: This is more for a third party requesting data & not really clarifying what the data is.

Rep Kasper: You are saying that the data, if used inappropriately could be used as a source of substantial, additional revenue to be envy? If they sold it, is there consent or not?

Yates: I'm sure there are some scenarios out there that a third party acting to that question. you have. This is so new; we need more time to identify who controls it.

Rep Kasper: You mentioned the recognition you received for your privacy statements & data, is that a written document you could share?

Yates: Yes, I can submit it to the committee but it's also our web site, autoalliance.org.

Rep Louser: When can we expect the industry to start selling fully automated vehicles?

Yates: The earliest to speak is 2021, but none of these are definitive.

Rep Boschee: In everyday, news breaches, ND citizens are very skeptical people, in the absent of the law on the state level, how would you encourage us to give confidence to our citizens that the information isn't being shared beyond the appropriate people.

Yates: I would refer back to the privately principles. The auto industry, not just Auto Alliance, the other members that we don't have in our association, they are committed to the data to be secured & aligned with our privacy principles.

Rep Boschee: Your organization has to makes sure data that shows up as consumer confidence.

Yates: I will refer back to our privacy principles & there are top watchdog agencies watching.

Tom Kelsch~Representing General Motors: Attachment 3.

35:00

Chairman Keiser: If I follow your argument to the extreme, we should never pass legislation because we are never in the final point. But the reality is that we do pass legislation & if something should develop, we introduce an amendment to the law. Is your argument, we should never pass legislation until we are to the final end of anything?

Kelsch: Certainly not. We need to know the level & definition of autonomous vehicle.

Rep Ruby: To address your one concern, it does mention in the bill on line 10, as a means to eliminate the human operator, are you considering possible as someone actually driving it, are you talking about a limited or complete function.

Kelsch: That is the question, we need to know the definition.

Chairman Keiser: On line 9-10, gives the definition of autonomous, anything that assists the diver of the vehicle.

Rep Ruby: We have a lot of protections on personal information in the law now & it hasn't been a problem for the industry, I'm wondering why is this different?

Kelsch: There are some protection there to balance the person's information. We don't know where this information is going, so it's too early to deal with the autonomous portion of information protection.

Rep Kasper: On line 7 of the bill, does GM agrees that the owner of the vehicle owns the data of the vehicle or the owner of the data is really the manufacturer who put the data gathering devices in the vehicle?

Kelsch: There is certainly some proprietary information in the systems that auto makers would say that we own that proprietary information. As far as some other data, we don't dispute that that the owner owns the data. All that broad definition of data, that that includes proprietary information of GM's, we wouldn't want that information released to other automobile manufacturers.

Rep Kasper: I'm confused. Data or information would not occur until the driver takes some action, that data gathering device is in there & to me, that's proprietary. That's not data, the data when an event occurs. Again, are you concerned that you want GM's to be able to own & control that data once it begins to be gather. I agree, you should protect your trade secrets on how you develop, but the data is another issue.

Kelsch: I would agree, the data, we are not talking about the data, we are talking about our method of collecting & providing that information would be our trade secret.

Chairman Keiser: Anyone else here to testify in opposition, neutral on HB 1394.

Jennifer Clark~Attorney at Legislative Council: One of the questions is, what does a motor vehicle mean. Title 39-01-01-46, there is a definition of motor vehicle. It's pretty broad definition.

Chairman Keiser: Would a closed autonomous tractor qualify?

Clark: I do believe that it is arguable that it would.

Rep C Johnson: Could strike that language & use any vehicle?

Clark: You can define it any way you want & should be done in this section.

Chairman Keiser: Closes the hearing on HB 1394. Committee members, what are your wishes.

Rep Becker: The question I have on whether we need to tighten up the content of the owner that it should be the expressed written of the owner.

Chairman Keiser: Further discussion.

Rep Boschee: Moves to adopt the language of the amendment.

Vice Chairman Sukut: Second.

Voice vote – Motion carried.

Rep Becker: Move for a Do Pass as Amended.

Chairman Keiser: Further discussion, what are the wishes of the committee?

Vice Chairman Sukut: Second.

Rep Kasper: I'm going to resist the motion; I think it's premature.

Rep Becker: I didn't feel the argument of the opposition was very strong but they made the best argument they could make. I support the motion.

Chairman Keiser: I do not support annual session but we could address this issue in one from now. This bill simply protects consumer rights. It will be two years before we meet to address the issue but we would change is in the future with an amendment.

Rep Kasper: I will oppose the motion but I will support it on the floor.

Roll call was taken for a Do Pass as Amended on HB 1394 with 9 yes, 5 no, 0 absent & Rep Lefor is the carrier.

PROPOSED AMENDMENTS TO HOUSE BILL NO. 1394

Page 1, line 6, replace "Exception" with "Exceptions"

Page 1, after line 15, insert:

- "3. A manufacturer, insurer, or seller of autonomous vehicles or autonomous vehicular technology may share, release, or distribute identifying or personalized information or data collected and stored by the autonomous vehicle, with the consent of the owner of the autonomous vehicle or by order of a court."

Renumber accordingly

Date: Jan 25, 2017Roll Call Vote #: 12017 HOUSE STANDING COMMITTEE
ROLL CALL VOTES
BILL/RESOLUTION NO. 1394

House _____ Industry, Business and Labor _____ Committee

☐ SubcommitteeAmendment LC# or
Description:17.0846.02002

Recommendation

☒ Adopt Amendment☐ Do Pass☐ Do Not Pass☐ Without Committee Recommendation☐ As Amended☐ Rerefer to Appropriations☐ Place on Consent Calendar

Other Actions

☐ Reconsider☐ _____

Motion Made By

Rep Boschee

Seconded By

Rep Sukut

Representatives	Yes	No	Representatives	Yes	No
Chairman Keiser			Rep Laning		
Vice Chairman Sukut			Rep Lefor		
Rep Beadle			Rep Louser		
Rep R Becker			Rep O'Brien		
Rep Bosch			Rep Ruby		
Rep C Johnson			Rep Boschee		
Rep Kasper			Rep Dobervich		

Total (Yes) _____ No _____

Absent _____

Floor

Assignment _____

If the vote is on an amendment, briefly indicate intent:

voice vote - motion carried

Date: Jan 25, 2017Roll Call Vote #: 2

2017 HOUSE STANDING COMMITTEE

ROLL CALL VOTES

BILL/RESOLUTION NO. HB 1394

House _____ Industry, Business and Labor _____ Committee

☐ SubcommitteeAmendment LC# or
Description: _____

Recommendation

☐ Adopt Amendment☒ Do Pass ☐ Do Not Pass☐ Without Committee Recommendation☒ As Amended☐ Rerefer to Appropriations☐ Place on Consent Calendar

Other Actions

☐ Reconsider☐ _____

Motion Made By _____

Seconded By _____

Representatives	Yes	No	Representatives	Yes	No
Chairman Keiser	X		Rep Laning	X	
Vice Chairman Sukut	X		Rep Lefor	X	
Rep Beadle		X	Rep Louser		X
Rep R Becker	X		Rep O'Brien		X
Rep Bosch		X	Rep Ruby	X	
Rep C Johnson	X		Rep Boschee	X	
Rep Kasper		X	Rep Dobervich	X	

Total (Yes) 9 No 5Absent 0Floor
Assignment Rep Lefor

REPORT OF STANDING COMMITTEE

HB 1394: Industry, Business and Labor Committee (Rep. Keiser, Chairman) recommends **AMENDMENTS AS FOLLOWS** and when so amended, recommends **DO PASS** (9 YEAS, 5 NAYS, 0 ABSENT AND NOT VOTING). HB 1394 was placed on the Sixth order on the calendar.

Page 1, line 6, replace "Exception" with "Exceptions"

Page 1, after line 15, insert:

"3. A manufacturer, insurer, or seller of autonomous vehicles or autonomous vehicular technology may share, release, or distribute identifying or personalized information or data collected and stored by the autonomous vehicle, with the consent of the owner of the autonomous vehicle or by order of a court."

Renumber accordingly

2017 SENATE TRANSPORTATION

HB 1394

2017 SENATE STANDING COMMITTEE MINUTES

Transportation Committee Lewis and Clark Room, State Capitol

HB 1394
3/23/2017
29629

- ☐ Subcommittee
☐ Conference Committee

Committee Clerk Signature

Mary Munder

Explanation or reason for introduction of bill/resolution:

Relating to autonomous vehicle data ownership.

Minutes:

Attachments #1-8

Chairman Laffen called hearing on HB 1394 to order.

Representative George Keiser: This bill deals with the ownership of information produced by autonomous vehicles. There are some implications that will come of that. Insurance will be one. Reality is, we in our vehicles create a tremendous amount of data. I think it is important that North Dakota Legislature set the policy here regarding this issue. The bill is short and simple.

(1The owner of the autonomous vehicle owns any data or information stored by the vehicle or gathered by the use of the vehicle for the purpose of this section. Autonomous vehicle means a motor vehicle using autonomous technology as a means to eliminate the human operator. We did have a clarification from Legislative Council. This definition would also apply to tractors in the field.

(2A manufacturer, insurer, or seller of these vehicles or the technology may share, release, or distribute non-identifying vehicle data collected and stored by the autonomous vehicles. Non-identifying means non-personalized information or data about the owner operator of the vehicle.

(3The manufacturer, insurer, or seller of an autonomous vehicle or the technology may share, release, or distribute identifying personal information or data, collected and stored by the vehicle, with the consent of the owner or by order of the court in case there is a legal proceeding.

Years ago we had the GLB case where they could share all your information with whomever, unless you opted out. This was very important information that they had, bank records, checking and saving accounts, very personal information and they could sell it to whomever. You had to formally fill out a request to 'not' have your information shared. Not many people did this, so we as a state fought the legislation and 72% of the people voted to 'not' let them get away with that. This bill models that as far as the opting out. I think my personal information should be mine and I should have the option to opt out of sharing it. I think this is the right thing to do and it is important to the citizens of the state of North Dakota.

Senator Casper: What information are we providing on our financial personal level?

Keiser: This will impact every citizen eventually. This information we provide is going to be used by insurance companies and riders in all levels. The key is to make sure we don't limit the industry.

Senator Clemens: I see a big difference between owning and sharing information. Could you just expand on that?

Keiser: The ownership is only for the data or information stored by the vehicle. So it is just a data and not the system. I paid for the system on my car but I don't own it. The system is creating the technology so they can use it or share it, as long as it is not my personal information.

Senator Casper: Do you have a difference of opinion between the auto manufacturers, the companies that are collecting that data, and the insurance companies?

Keiser: KPGM when they issued it said we have to be careful that it doesn't get too far down the road where they think they own everything including your personal information, and only they can share it with an insurance company.

Senator Casper: Can we legislate that the auto manufacturers can get the information but the insurance companies can't?

Keiser: Yes, I think we can. We did it before, with an opt in option similar to this.

Senator Rust: What is your opinion to inserting the language "owns any personal data and personal information" into the bill. Just putting the word personal before the word data and before the word information.

Keiser: I would have no objection.

Chairman Laffen: I know there is an organization called NCOIL, and you and several others are involved in it and they tried something like this and it didn't pass. Could you explain what they have done with this?

Keiser: My personal opinion and not speaking on behalf of NCOIL, but as a past president I understand it quite well. At every meeting at the end we try to identify emerging issues that need to be addressed on the insurance side and not on the personal information side. We had a discussion about that and they didn't table it, but it is an issue that still is alive, still an important issue with NCOIL, they are developing information right now. In terms of the personal information and the discussion at NCOIL, there is a general consensus that we need to protect that. On the insurance side we talked more about the implications of the autonomous vehicle. The projections on the emergency room volume could decrease 60-80% as a result of this. NCOIL is for helping the insurance side of it, but privacy on the personal side, it needs to be protected, despite what you may have heard.

Chairman Laffen: Questions? None. Further testimony in favor? Opposition to HB 1394?

(21:45) Leighton Yates, Alliance of Automobile Manufacturers: See attachment #1.

Chairman Laffen: (26:28) Could you define the industries address of data privacy to commitment? What does that really mean?

Leighton: Basically it is holding ourselves accountable for informing them of the personal data procedure and what is all put out there.

Senator Casper: What do you think of the legislation of sharing with the insurance company versus sharing with the manufacturer?

Leighton: Right now we share certain information about the vehicle with the manufacturers and insurance. They can plug in to see if it is running up to par. With the state there is also driver behavior information along with the data on how your vehicle is operating on a day to day basis.

Senator Casper: Can you testify whether or not the companies you represent are currently sharing the data that they are collecting on all of us with insurance companies?

Leighton: With insurance companies, if you have the third party partnerships on your vehicle, like On Star, Cirrus, etc., there is a disclosure on your vehicle or you can provide consent on your vehicle.

Senator Rust: Just what kind of information does it store? How do you respond to the general public fears that police or insurance companies can collect all this on you?

Leighton: Some of the types of personal data would be the location and/or driver behavior, all of those if they are collected by the manufacturer, it's either a disclosure on your vehicle, or in your owners-manual, or you provide consent to share that information. We make sure in our privacy principles that we explain to you what information is being used, how it is being used, and what the purposes are. Not all data will be personal, it will be vehicle information, too.

Chairman Laffen: Questions? None. Thank you. Continue with testimony in opposition.

Glenn Jackson, NDDOT: (31:53) See attachment #2.

Chairman Laffen: I am pretty sure we are going to like the study in HB 1202, it seemed to make sense for everybody. We could study this issue as a part of that as well. Is that something you would have the expertise for or would it fall to someone else. If we did this idea, I would prefer to keep this study with you. This is more a legal and insurance issue and if it all falls to you; could you figure it all out or find the expertise?

Glenn: I think the reason we went in the direction of HB 1202, was directing the department on making sure a study was done. There will be many cycles and we would have to have the attorney general, Insurance commissioner, Highway Patrol, etc. in the room so we can look at these specific issues and how they will affect ND drivers.

Chairman Laffen: Questions? None. Thank you. Further testimony in opposition to HB 1394?

Representative Emily O'Brien, District 42: (35:15) See attachment #3.

Chairman Laffen: If I were to ask any citizen in ND, that this bill would prevent your personal information from being shared, if you own an autonomous vehicle, 99.9% will say yes I want that law. Why should we vote against this?

Rep. O'Brien: From my personal opinion I think the definition is too broad for autonomous vehicles. It could be vehicles on the ground and in the air, so in flight who would own the data then? Where would the ownership lie?

Senator Clemens: When you are talking about autonomous vehicles it could mean a partially autonomous, right? Like you said we are all using vehicles already that are autonomous. Anti-skid system, tracking control, whatever, correct?

Rep. O'Brien: Yes.

Chairman Laffen: Questions? None. Thank you. Further testimony in opposition?

(43:08) Lacy Anderson, American Insurance Association: See attachment #4.

Chairman Laffen: There would be no problems studying it?

Lacy: No, there would be no issue.

Senator Casper: Is there a reason that the consumers would want the insurance companies to have this information?

Lacy: Yes, a certain amount they would want them to have but we are considering what is feasible for them to have.

Senator Casper: Why would the consumer want them to have this information?

Lacy: Part of it would be the ability to know the risks involved to underwrite it.

Chairman Laffen: Questions/ None. Thank you. Further testimony in opposition?

(46:54) Don Larson, Grand Sky Development Corporation: See attachment #5.

Chairman Laffen: Questions? None. Thank you. Further testimony in opposition? Students from Scranton, welcome.

(51:41) Jason Wetzel, Regional Director of Government Relations for General Motors: See attachment #6. This bill is not about just taking your hands off the wheel, diagnostic and sensing are also involved and insurances will sometimes plug in to see the driving record.

Chairman Laffen: There need to be rules someday and we are not there just yet.

Jason: There are a lot of discussions happening about these vehicles. There will be a dramatic decline in accidents and things of that nature and that's positive, but it is going to impact their industry, and I think they are aware of that and understand that. All the information you would need to address an accident is already in the vehicle. That technology is already there, It's not changing and it is going to record what it needs to record for the insurance companies and law enforcement.

Chairman Laffen: Questions? None. Further opposition testimony? Welcome back Carla.

(1:01:20) Carla Jacobs, Public Policy for Uber North Dakota: See attachment #7. We are urging you to vote for a Do Not Pass.

Senator Casper: Do you ever see the day when all vehicles will be autonomous? You could push a button and the vehicle would come pick you up and take you to work.

Carla: People's interest will determine this. Vehicles will still need to be serviced and the people that don't like to drive may look at this as an option.

Chairman Laffen: Questions? None. Thank you. Further opposition testimony?

(1:05:37) Marlo Anderson, with North Dakota Autonomous Vehicle: See attachment #8. We are a group of individuals in the state that are trying to advance this technology. Everyone is concerned about sharing the data. If you are in an autonomous vehicle, 'it' is taking you, so I don't understand the concern there and secondly when you are on a public road, that information should be accessible to be shared. If it is a foggy day and you are driving in front of me and have an accident, I want my car to know that, so I don't go barreling into you. I have had the opportunity to ride in a lot of these vehicles.

Chairman Laffen: Questions? None. Thank you. Further testimony in opposition? Neutral?
We will close the hearing on HB 1394. Discussion?

Senator Rust: I move a Do Not Pass on HB 1394.

Senator Casper: Seconded.

Chairman Laffen: Discussion?

Senator Casper: I think N.D. can be a key player in this, particularly in the transporting of commodities across the state. I don't think we should put roadblocks in the way of advancements. In the future there could be some issues with our privacy in the insurance industry but we are a long way from that.

Chairman Laffen: I agree with you and I think it will be looked at nationally, too. We have two years for them to make advancements.

Senator Rust: I echo the same feelings. In two years we may be looking at this again.

Roll Call taken: yeas-6, Nays-0, Absent-0. Motion carried.

Senator Rust will carry the bill.

Date: 3.23.17
Roll Call Vote #: 1

2017 SENATE STANDING COMMITTEE
ROLL CALL VOTES
BILL/RESOLUTION NO. "Enter Bill/Resolution No." HB 1394

Senate Transportation Committee

☐ Subcommittee

Amendment LC# or Description: _____

Recommendation: ☐ Adopt Amendment ☒ Do Pass ☐ Do Not Pass ☐ Without Committee Recommendation
☐ As Amended ☐ Rerefer to Appropriations
☐ Place on Consent Calendar

Other Actions: ☐ Reconsider ☐ _____

Motion Made By Rust Seconded By Casper

[illegible]

Total (Yes) 6 No 0

Absent 0

Floor Assignment Rust

If the vote is on an amendment, briefly indicate intent:

REPORT OF STANDING COMMITTEE

HB 1394, as engrossed: Transportation Committee (Sen. Laffen, Chairman)
recommends **DO NOT PASS** (6 YEAS, 0 NAYS, 0 ABSENT AND NOT VOTING).
Engrossed HB 1394 was placed on the Fourteenth order on the calendar.

2017 TESTIMONY

HB 1394

Jan 25, 2017

17.0846.02002
Title.

Prepared by the Legislative Council staff for
Representative Keiser
January 19, 2017

PROPOSED AMENDMENTS TO HOUSE BILL NO. 1394

Page 1, line 6, replace "Exception" with "Exceptions"

Page 1, after line 15, insert:

- "3. A manufacturer, insurer, or seller of autonomous vehicles or autonomous vehicular technology may share, release, or distribute identifying or personalized information or data collected and stored by the autonomous vehicle, with the consent of the owner of the autonomous vehicle or by order of a court."

Renumber accordingly



2

January 25, 2017

Hon. George Keiser, Chair
House Committee on Industry, Business and Labor
600 East Boulevard Ave.
Bismarck, ND 58505

Re: House Bill 1394 – Autonomous Vehicle Data Ownership

Dear Chairman Keiser:

On behalf of the Alliance of Automobile Manufacturers, I would like to thank you for the opportunity to express our concerns with House Bill 1394, legislation that raises a host of privacy and cybersecurity concerns, with little apparent benefit to North Dakota drivers. The Alliance is a trade association representing twelve of the world's leading car and light truck manufacturers, including BMW Group, FCA US LLC, Ford Motor Company, General Motors Company, Jaguar Land Rover, Mazda, Mercedes-Benz USA, Mitsubishi Motors, Porsche, Toyota, Volkswagen Group of America, and Volvo Car USA. Together, Alliance members account for roughly 77% of the cars and light duty trucks sold throughout the United States each year.

Automated Driving Systems (ADS) have the potential to revolutionize mobility, and dramatically reduce the 94% of accidents that the Federal government attributes to human error.¹ These systems use multiple redundant sensors to create a 360-degree field of view to guide the vehicle. They can react faster than a human driver to changing conditions, and have the capacity to eliminate many safety issues relating to driver distraction. Eventually, ADS have the potential to increase mobility for economically disadvantaged, blind, disabled, and elderly individuals who may be incapable of accessing or operating a conventional motor vehicle.

Mr. Chairman, you should be recognized and commended your foresight on this subject. At some point in the future – when fully automated vehicles are made available to consumers for private purchase – legislators will need to wrestle with a host of insurance and liability issues, but that day is not today. It is simply premature to consider how private passenger insurance will be impacted by this new technology, until we understand how the technology will be utilized.

Many believe the first uses for fully automated vehicles will not be in vehicles owned by private individuals, but in fleet or car-sharing application – imagine a college campus, military base, or airport. In these situations, we would not be talking about private passenger insurance at all, but likely self-insured entities. Given the development that is still necessary before individuals will be in a position to purchase a fully automated vehicle, there will be plenty of time to thoughtfully consider the issues raised in this legislation.

With that said, we see many concerns with the bill as drafted. First, it is unclear why this legislation is necessary at all, as an insurer can already collect and use data from a vehicle with a consumer's consent. There are countless advertisements on television of insurers who offer safe driving discounts, in exchange for allowing in the insurer to collect data from the vehicle and monitor driving behavior. We are aware of nothing in North Dakota law that would prohibit insurers from including such provisions for use and sharing in the contracts for these safe driving plug-in devices.

¹ See National Motor Vehicle Crash Causation Survey (NMVCCS)

Automakers have gone to great length to inform consumers what data is collected from a vehicle, and how that data is utilized. These efforts have been highly praised by privacy watchdog groups. In 2014, automakers developed a set of Privacy Principles that recognize technologies and services in automobiles are increasingly designed to enhance vehicle safety, improve vehicle performance, and augment the driving experience. Many of these technologies and services rely upon information generated by vehicle systems. The Principles have a strong lineage based on the FTC's Fair Information Practice Principles. With signatures from all Alliance members, they represent an industry wide commitment to responsible stewardship of the information collected to provide vehicle services.

Second, the legislation fails to utilize terms in a clearly defined and technically actionable manner. The term "autonomous vehicle," as defined, would not allow for clear delineation between existing technologies and future automated driving systems. As result, there would be confusion in determining whether a vehicle is, or is not, subject to the legislation. Even more concerning, the term "data" is not defined in any way in the bill. Vehicles generate stunning amounts of data, given the dozens of individual sensors now found on everyday vehicles. This data generation will grow exponentially when automated driving systems are deployed. The undefined scope of data in the bill as drafted could allow for misinterpretation and could ultimately result in a consumer's vehicle data being susceptible to undesired data sharing. Additionally, much of this data, even if it is "stored" or "gathered" in the vehicle, may not be retrievable in any sort of usable format. Declaring ownership of information, when a vehicle may not have the technical ability to deliver such information anywhere off the vehicle, will lead to consumer confusion.

While adjustments to state insurance and liability laws may be necessary at some point in the future as a result of the deployment of automated vehicle technology, we see no reason to rush such consideration of this data portion in piecemeal fashion, particularly when the industry has already addressed data privacy for all vehicles through commitments to its consumers. A targeted bill considered in a vacuum will do little to address the range of issues that may need to be addressed. We would recommend, instead, taking the time to have a thoughtful dialog on the subject, at a time when the changes to the insurance and legal marketplace are in better focus.

We thank you for the opportunity to express our concerns, and would welcome the opportunity to meet with you, the committee, or any interested parties to further discuss the concerns that led to your filing of this legislation.

Sincerely,



Leighton Yates
Manager, State Affairs

Cc: House Committee on Industry, Business and Labor

Jan 25, 2017

HB 1394

3

Chairman Keiser and members of the House Industry Business and Labor Committee, my name is Thomas D. Kelsch. I am appearing today on behalf of General Motors in opposition to HB 1394. General Motors is opposed to HB 1394 for the following reasons:

- HB 1394 is a solution to a problem that does not exist, and could have a chilling effect upon autonomous vehicle development with ramifications beyond North Dakota.
- The bill attempts to predict marketplace dynamics well before fully automated vehicles are owned by the general public. Automated vehicle technology is still in its early stages and requires more testing and learnings by automakers. Consumer ownership of fully automated vehicles is not imminent, and there is little reason to rush to make sweeping changes before we have a solid understanding of how the technology will be developed and deployed.
- The existing legal framework for vehicle data is appropriate for autonomous vehicles. NDCC 51-07-28 already provides for access to event data recorders. There is no evidence that change is needed, and any effort to the contrary would unnecessarily raise significant consumer concerns and could impede the development of autonomous vehicles.
- Indeed, HB 1394's data ownership rights could equate to broad and unfettered data access for autonomous vehicles. This fails to account for the potentially significant cybersecurity concerns created by potentially mandating public wide access into safety critical vehicle systems for data.
- Moreover, autonomous vehicle development and ultimately deployment relies upon secure storage and transmission of data. This bill could threaten that important assumption necessary to move this technology forward. It would also put at risk automaker proprietary information.
- HB 1394 is not ripe to solve any existing consumer issue. Instead, it raises significant concerns that could threaten autonomous vehicle development and its potentially dramatic safety benefits on North Dakota roadways.
- For these reasons General Motors urges this committee to recommend a **"Do Not Pass"** for HB 1394.



Attachment # 1 pg 1
HB 1394 3-23-17

March 23, 2017

Hon. Lonnie J. Laffen, Chair
Senate Committee on Transportation
600 East Boulevard Ave.
Bismarck, ND 58505

Re: Oppose House Bill 1394 – Autonomous Vehicle Data Ownership

Dear Chairman Laffen:

On behalf of the Alliance of Automobile Manufacturers, I would like to thank you for the opportunity to express our concerns with House Bill 1394, legislation that raises a host of privacy and cybersecurity concerns, with little apparent benefit to North Dakota drivers. The Alliance is a trade association representing twelve of the world's leading car and light truck manufacturers, including BMW Group, FCA US LLC, Ford Motor Company, General Motors Company, Jaguar Land Rover, Mazda, Mercedes-Benz USA, Mitsubishi Motors, Porsche, Toyota, Volkswagen Group of America, and Volvo Car USA. Together, Alliance members account for roughly 77% of the cars and light duty trucks sold throughout the United States each year.

Automated Driving Systems (ADS) have the potential to revolutionize mobility, and dramatically reduce the 94% of accidents that the Federal government attributes to human error.¹ These systems use multiple redundant sensors to create a 360-degree field of view to guide the vehicle. They can react faster than a human driver to changing conditions, and have the capacity to eliminate many safety issues relating to driver distraction. Eventually, ADS have the potential to increase mobility for economically disadvantaged, blind, disabled, and elderly individuals who may be incapable of accessing or operating a conventional motor vehicle.

As I have stated previously before your House counterparts, at some point in the future – when fully automated vehicles are made available to consumers for private purchase – legislators will need to wrestle with a host of insurance and liability issues, but that day is not today. It is simply premature to consider how private passenger insurance will be impacted by this new technology, until we understand how the technology will be utilized.

Many believe the first uses for fully automated vehicles will not be in vehicles owned by private individuals, but in fleet or car-sharing application – imagine a college campus, military base, or airport. In these situations, we would not be talking about private passenger insurance at all, but likely self-insured entities. Given the development that is still necessary before individuals will be in a position to purchase a fully automated vehicle, there will be plenty of time to thoughtfully consider the issues raised in this legislation.

With that said, we see many concerns with the bill as drafted. First, it is unclear why this legislation is necessary at all, as an insurer can already collect and use data from a vehicle with a consumer's consent. There are countless advertisements on television of insurers who offer safe driving discounts, in exchange for allowing in the insurer to collect data from the vehicle and monitor driving behavior. We are aware of nothing in North Dakota law that would prohibit insurers from including such provisions for use and sharing in the contracts for these safe driving plug-in devices.

¹ See National Motor Vehicle Crash Causation Survey (NMVCCS)

Attachment #1 pg. 2

HB 1394 3-23-17

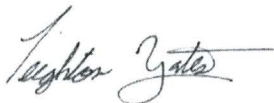
Automakers have gone to great length to inform consumers what data is collected from a vehicle, and how that data is utilized. In 2014, automakers developed a set of Privacy Principles that recognizes technologies and services in automobiles are increasingly designed to enhance vehicle safety, improve vehicle performance, and augment the driving experience. Many of these technologies and services rely upon information generated by vehicle systems. These efforts have been highly praised by privacy watchdog groups and have a strong lineage based on the Federal Trade Commission's (FTC) Fair Information Practice Principles. With signatures from all Alliance members, they represent an industry wide commitment to responsible stewardship of the information collected to provide vehicle services. These principles are enforceable under section 5 of the Federal Trade Commission Act and because all of our members have made themselves subject to this enforcement, we believe there isn't a current need for additional laws/regulations. Simply put, by publicly committing to these principles, Alliance members become accountable not only to their customers, but also to state and federal regulators.

Second, the legislation fails to utilize terms in a clearly defined and technically actionable manner. The term "autonomous vehicle," as defined, would not allow for clear delineation between existing technologies and future automated driving systems. As result, there would be confusion in determining whether a vehicle is, or is not, subject to the legislation. Even more concerning, the term "data" is not defined in any way in the bill. Vehicles generate stunning amounts of data, given the dozens of individual sensors now found on everyday vehicles. This data generation will grow exponentially when automated driving systems are deployed. The undefined scope of data in the bill as drafted could allow for misinterpretation and could ultimately result in a consumer's vehicle data being susceptible to undesired data sharing. Additionally, much of this data, even if it is "stored" or "gathered" in the vehicle, may not be retrievable in any sort of usable format. Declaring ownership of information, when a vehicle may not have the technical ability to deliver such information anywhere off the vehicle, will lead to consumer confusion.

While adjustments to state insurance and liability laws may be necessary at some point in the future as a result of the deployment of automated vehicle technology, we see no reason to rush such consideration of this data portion in piecemeal fashion, particularly when the industry has already addressed data privacy for all vehicles through commitments to its consumers. A targeted bill considered in a vacuum will do little to address the range of issues that may need to be addressed. We would recommend, instead, taking the time to have a thoughtful dialog on the subject, at a time when the changes to the insurance and legal marketplace are in better focus.

We thank you for the opportunity to express our opposition to HB 1394, and would welcome the opportunity to meet with you and the committee to further discuss any concerns or answer any questions. We appreciate your time and consideration.

Sincerely,



Leighton Yates
Manager, State Government Affairs

Cc: Senate Committee on Transportation

Frequently Asked Questions (FAQs) on Automotive Privacy

1. Why did the auto industry develop Privacy Principles for vehicles?

Automakers take great pride in providing our customers with safe, reliable products, including data privacy and data security. The Privacy Principles acknowledge that technologies and services in automobiles are increasingly designed to enhance vehicle safety, improve vehicle performance and augment the driving experience, and many of these technologies and services rely upon information generated by vehicle systems. Sometimes, that information includes the precise location of vehicles or how drivers operate their vehicles. The Principles represent a unified commitment to responsible stewardship of the information collected to provide vehicle services.

2. What are these technologies and services, and why are they useful?

As new vehicle technologies and services emerge, the goal of automakers is to continue enhancing benefits to customers while respecting their privacy. Technologies and services available today enable greater road safety through connectivity. Automatic crash notification calls help assist vehicle occupants when needed. Alerts about traffic conditions help reduce congestion. Electronic security or smartphone applications help locate lost or stolen vehicles. These features and more are important to automotive customers, and providing them in a transparent way is important to automakers.

3. How do the Privacy Principles compare to efforts in other industries and government?

Automakers are among the first industries to develop Privacy Principles to address consumer concerns about what data we collect, how we use it, and when/why data is shared. These Privacy Principles have a strong lineage, building on Fair Information Practice Principles, Federal Trade Commission (FTC) guidance, the White House Consumer Privacy Bill of Rights and the guidance of privacy advocates.

4. What should consumers do to stay informed about their privacy in automobiles?

First, check with the automaker: Within a vehicle, internal computers are constantly communicating with each other to operate the vehicle, and automakers work hard to safeguard this in-vehicle computer network to preserve the integrity of safety critical systems. However, not all data needed to operate a vehicle is stored or transmitted. Privacy policies associated with the vehicle system are available to consumers, and automakers encourage their customers to review them. Automakers may provide customer notices through a variety of methods, including online, owner's manuals, paper or electronic registration forms and user agreements, and/or in-vehicle displays. Consumers will also find information on how to delete certain data they stored on their vehicles.

Second, always ask about privacy policies and practices of relevant providers, including:

- **Wireless carriers:** Many of our customers pair their mobile devices with vehicle-integrated systems, so we urge customers to check the privacy policies of their wireless carriers prior to pairing their device.
- **Mobile app providers:** When customers pair their mobile devices with vehicle systems, they may access mobile apps and websites that have their own policies for customer review.

Third, always ask who wants vehicle data and why: Many data miners, retailers and service providers want access to consumer vehicle data. For example, insurance companies seek access to vehicle data for setting individual premium rates. Some insurance companies only want mileage driven per year, while others may want much more information, such as driving behaviors like hard braking and accelerations, or even GPS locations of travel. The FTC and White House have raised concerns about discriminatory “redlining” services, the practice of denying services or charging more for them for particular groups based on race, sex or where people live and travel. Consumers are rightly concerned about sharing vehicle data with a company that may share that information with business affiliates for any number of reasons, including sales and marketing. This could potentially allow many people to access consumer vehicle data without prior authorization. Several states have passed laws limiting the extent to which insurers can require consumers to allow access to their vehicle data. Under the automotive Privacy Principles, consumers must consent to providing insurers with vehicle data.

5. What types of information are generated, transmitted, retained, or shared in an auto today?

Today, different types of data are generated, transmitted, retained or shared for different purposes:

Data generated in an auto, but not transmitted outside the vehicle, that is necessary for the operation of the vehicle: Within a car, computer systems constantly exchange data to ensure the smooth operation of the vehicle. From steering to braking, crash avoidance, and acceleration, dozens of onboard computers simultaneously share information as consumers travel down the highway. This data is not transmitted outside, or retained in the long-term computer memory, of the vehicle -- unless it is part of a subscription service, in which case owner consent is required under the Principles.

Data transmitted outside of the vehicle: Certain functions can require the transmission of data outside the vehicle. For example, automatic crash notification systems transmit data so that emergency responders can be directed to crash scenes with information on the nature of the crash. Diagnostics systems may transmit data outside the car to identify potential maintenance issues.

Data transmitted into and out of the vehicle: While basic navigation systems are only receivers for directions coming into the car, enhanced navigation systems both transmit and receive data from outside the vehicle so drivers can learn about traffic conditions and get directions. Trip information may be retained for convenient access to previously accessed destinations. For greater convenience, vehicles can also transmit and receive data so consumers can remotely monitor where their car is, remotely start their car, obtain vehicle diagnostics reports and access on-board information services.

Data generation that is required by law: Certain vehicle data is required by law, such as data pertaining to emissions controls, on-board tire pressure sensors, and gauges. The government requires that event data recorders (also known as "EDRs") monitor critical information about the vehicles in which they are installed, but this information is only stored for seconds at a time and constantly overwritten -- unless there is a crash and then the data (immediately prior to and after the crash) is recorded for use in analyzing the performance of the vehicle's safety systems.

Data that is shared: Technical data regarding such matters as warranty or safety is shared with authorized dealers, who also share this information with automakers. Some information may also be shared for marketing purposes, but only with express, affirmative consent by the vehicle owner or registered user.

6. What data does a consumer own or control in an automobile?

Increased Internet use and smartphones have raised many questions about data and ownership. For instance, a consumer owns a smartphone but not the proprietary system and data that make the smartphone work. As autos evolved into complex computer systems that generate, store and analyze data, similar questions arose about data ownership related to vehicles. Here are the answers:

- **EDR data:** Automakers affirm they obtain vehicle owner consent in order to retrieve EDR data.
- **Infotainment data:** Consumers can control the type of information they enter into the infotainment system, such as music and contact lists.
- **Personal subscription information:** Consumers can control identifying information, including name, address, credit card numbers, telephone numbers and email addresses.
- **Technical data:** Automakers reserve the right to use technical data that is stored in, and relates to the functioning of, the vehicle.

7. What data can consumers review?

Data from contract or subscription-based services: Some vehicle systems and third-party providers allow vehicle owners and registered users to access historical data from a variety of subscription-based services, including roadside assistance, navigation, automatic crash notification, entertainment, and concierge services.

Data from in-vehicle diagnostics: Some data may be accessed by consumers via password-protected websites, report emails, and mobile applications, as well as on-board reporting systems or embedded touch screens. This data includes diagnostics and vehicle information on emissions controls, tire pressure, oil life, upcoming service needs and brake life. Driver behavior information can include vehicle speed, safety belt use and information about braking habits.

8. Why can't consumers access all the data generated in an automobile?

Consumer privacy and safety may be threatened or corrupted when unauthorized individuals access certain vehicle information. That is why it is important to safeguard vehicle information. There are also practical considerations. A home computer has an operating system comprised of millions of lines of codes that are not meaningful to most users. Likewise, a vehicle processes

Attachment #1 pg. 6

NB 1394 3.23.17

substantial amounts of data necessary for its functioning but not associated with the owner or registered user.

9. Can a consumer decide to turn off the information flow within a vehicle?

On home computers or smartphones, consumers can tell online advertisers and retailers that they want to avoid “tracking cookies” that retain Internet browsing information. By contrast, automobiles rely on the on-board network of computers to function, and these systems cannot be turned off and still allow the vehicle to operate. However, vehicle owners and registered users have access to a variety of subscription-based services offered by manufacturers and third-party providers. Owners and lessees can opt out of subscription-based services or choose not to contract with certain vendors who seek access to various types of data.

10. Can consumers decide which third parties receive their data?

In many instances, consumers have a choice. For instance, owners and registered users can direct vehicle health reports and forward emails to their repairer of choice. If data is collected or transmitted by an automaker or third party, owners and registered users are informed of the collection of required data either at the point of sale or at the point of lease via the owner’s manual or through various service subscriptions upon registration or contract. Data is not tracked or shared without such disclosure. Examples of the types of data that consumers can share with third parties include:

- Information necessary to diagnose and repair vehicles.
- Vehicle “health data” such as emissions controls, tire pressure, oil life.
- Driver behavior information such as average speed or engine throttle.
- Subscription-based information and service options such as geolocation, navigation, automatic crash notification, and road-side assistance.

11. How do automakers address sensitive personal consumer information?

The most sensitive types of consumer information relate to geolocation (where the vehicle goes), driver behavior (such as vehicle speed or use of safety belts) and biometrics (physical or biological characteristics that identify a person). For each of these categories, the Privacy Principles require clear and prominent notices about the collection of such information, the purposes for which it is collected, and the types of entities with which the information may be shared.

12. Who has agreed to these Principles?

A list of automakers that have signed onto the Consumer Privacy Principles may be found at www.AutomotivePrivacy.com. When participating automakers work with third-party service providers, automakers commit to taking steps to ensure that these providers adhere to the Principles as well. Regarding automobile dealers, they are franchisees and independent businesses not controlled by automakers, and thus the Privacy Principles do not apply directly to dealers. However, automakers and their dealers have been working together to protect customer privacy and will work to implement the Principles, as well as ensure that customer information is protected throughout the vehicle purchase and ownership periods.

13. When do these Principles go into effect?

Participating automakers commit to meet or exceed the commitments contained in the Principles for new vehicles manufactured no later than Model Year 2017 (which may begin as early as January 2, 2016), and for Vehicle Technologies and Services subscriptions initiated or renewed on or after January 2, 2016. While adherence to the Principles does not require engineering changes in vehicles, if automakers make engineering changes they agree to comply no later than Model Year 2018.

14. To whom are automakers accountable?

Participating automakers agree to meet or exceed these Privacy Principles. By publicly committing to this set of Privacy Principles, participating members become accountable not only to their customers, but also to state and federal regulators.

15. What else are automakers doing to enhance privacy and data security?

Privacy is a priority for all automakers. As vehicles become increasingly interconnected, both data protection and data privacy need to be considered from the earliest stages of product development; in other words, "Privacy is by Design." All automakers today have technical and organizational security measures in place to protect customer data against manipulation, loss, destruction and access by unauthorized parties. And, automakers are working to establish a voluntary automobile industry sector information sharing and analysis center or comparable program for collecting and sharing information about existing or potential cyber-related threats and vulnerabilities in motor vehicle electronics or associated in-vehicle networks.

Attachment #1 pg. 8

HB 1394 3.23-17

ALLIANCE OF AUTOMOBILE MANUFACTURERS, INC.
ASSOCIATION OF GLOBAL AUTOMAKERS, INC.

Consumer Privacy Protection Principles

PRIVACY PRINCIPLES FOR VEHICLE
TECHNOLOGIES AND SERVICES

November 12, 2014

CONSUMER PRIVACY PROTECTION PRINCIPLES

**PRIVACY PRINCIPLES FOR
VEHICLE TECHNOLOGIES AND SERVICES**

I. INTRODUCTION

The automotive industry is developing innovative technologies and services that promise to deliver substantial benefits and enhance the driving experience. These technologies and services may assist in enhancing safety, reducing the environmental impacts of vehicles, diagnosing vehicle malfunctions, calling for emergency assistance, detecting and preventing vehicle theft, reducing traffic congestion, improving vehicle efficiency and performance, delivering navigation services, providing valuable information services, and more. The Alliance of Automobile Manufacturers, the Association of Global Automakers, and their members are excited about the benefits offered by today's vehicle technologies and services and look forward to expanding the array of innovative technologies and services offered to consumers.

Many of these technologies and services are based upon information obtained from a variety of vehicle systems and involve the collection of information about a vehicle's location or a driver's use of a vehicle. Consumer trust is essential to the success of vehicle technologies and services. The Alliance, Global Automakers, and their members understand that consumers want to know how these vehicle technologies and services can deliver benefits to them while respecting their privacy.

Privacy is important to consumers, and it is important to us. That is why the Alliance and Global Automakers have issued these Privacy Principles ("Principles"). The Principles provide an approach to customer privacy that members can choose to adopt when offering innovative vehicle technologies and services. Each member has made an independent decision about whether to adopt the Principles, and other companies may choose to adopt them as well. We provide a list of those companies that have adopted the Principles in the Appendix, and they are referred to as "Participating Members."

The Principles apply to the collection, use, and sharing of [Covered Information](#) in association with [Vehicle Technologies and Services](#) available on cars and light trucks sold or leased to individual consumers for personal use in the United States.

ALLIANCE OF AUTOMOBILE MANUFACTURERS, INC.
ASSOCIATION OF GLOBAL AUTOMAKERS

Attachment #1 pg 10
NB1394
3-23-17

CONSUMER PRIVACY PROTECTION PRINCIPLES

The Principles are subject to change over time. When they do change, the Alliance and Global Automakers will post the updated Principles at www.automotiveprivacy.com and <https://www.globalautomakers.org/topic/privacy>. The Principles are not intended to replace inconsistent or conflicting applicable laws and regulations, where they exist. So, the Principles should be interpreted as subject to and superseded by applicable laws and regulations. Participating Members may implement the Principles in different ways, reflecting differences in technologies and other factors. And Participating Members may choose to incorporate into their privacy programs elements that are not addressed in the Principles and are free to take additional privacy steps. But regardless of how Participating Members design their privacy programs and implement the Principles, Participating Members affirm the following fundamentals, as detailed in the relevant sections that follow:

- **Transparency:** Participating Members commit to providing [Owners](#) and [Registered Users](#) with ready access to clear, meaningful notices about the Participating Member's collection, use, and sharing of [Covered Information](#).
- **Choice:** Participating Members commit to offering [Owners](#) and [Registered Users](#) with certain choices regarding the collection, use, and sharing of [Covered Information](#).
- **Respect for Context:** Participating Members commit to using and sharing [Covered Information](#) in ways that are consistent with the context in which the [Covered Information](#) was collected, taking account of the likely impact on [Owners](#) and [Registered Users](#).
- **Data Minimization, De-Identification & Retention:** Participating Members commit to collecting [Covered Information](#) only as needed for legitimate business purposes. Participating Members commit to retaining [Covered Information](#) no longer than they determine necessary for legitimate business purposes.
- **Data Security:** Participating Members commit to implementing reasonable measures to protect [Covered Information](#) against loss and unauthorized access or use.

CONSUMER PRIVACY PROTECTION PRINCIPLES

- **Integrity & Access:** Participating Members commit to implementing reasonable measures to maintain the accuracy of [Covered Information](#) and commit to giving [Owners](#) and [Registered Users](#) reasonable means to review and correct [Personal Subscription Information](#).
- **Accountability:** Participating Members commit to taking reasonable steps to ensure that they and other entities that receive [Covered Information](#) adhere to the Principles.

The application of these fundamental principles is described in more detail in the sections that follow.

II. APPLICABILITY

The Principles apply to the collection, use, and sharing of [Covered Information](#) in association with [Vehicle Technologies and Services](#) available on cars and light trucks sold or leased to individual consumers for personal use in the United States.

Participating Members are listed in the Appendix.

Each Participating Member commits to complying with the Principles for new vehicles manufactured no later than Model Year 2017 (which may begin as early as January 2, 2016) and for [Vehicle Technologies and Services](#) subscriptions that are initiated or renewed on or after January 2, 2016. To the extent practicable, each Participating Member commits to implementing the Principles for [Covered Information](#) collected from vehicles manufactured before January 2, 2016. If compliance with the Principles involves a vehicle engineering change, each Participating Member commits to complying with the Principles as soon as practicable, but by no later than vehicle Model Year 2018.

Some Participating Members may work with [Third-party Service Providers](#) to provide some or all of their [Vehicle Technologies and Services](#). When doing so, Participating Members commit to taking reasonable steps to ensure that [Third-party Service Providers](#) adhere to the Principles in providing [Vehicle Technologies and Services](#) that involve the collection, use, or sharing of [Covered Information](#). Businesses other than [Third-party Service Providers](#) may provide [Owners](#) and [Registered Users](#) with apps or other offerings that involve the collection of information from vehicles. Participating

ALLIANCE OF AUTOMOBILE MANUFACTURERS, INC.
ASSOCIATION OF GLOBAL AUTOMAKERS

Attachment #1 pg. 12
HB1394 3-23-17

CONSUMER PRIVACY PROTECTION PRINCIPLES

Members will encourage those businesses to respect the privacy of [Owners](#) and [Registered Users](#) and will take reasonable steps to provide those businesses with an opportunity to provide [Owners](#) and [Registered Users](#) with information about the businesses' privacy practices.

However, the Principles directly apply only to Participating Members. The Principles do not apply directly to vehicle dealerships that are not owned by Participating Members.

III. SCOPE OF THE PRINCIPLES AND DEFINITIONS

The Principles provide a framework for Participating Members to embrace when collecting, using, and sharing [Covered Information](#). The following defined terms are used in the Principles. Together, the definitions describe the scope of the Principles.

Affirmative Consent: An [Owner's](#) or [Registered User's](#) clear action performed in response to a clear, meaningful, and prominent notice disclosing the collection, use, and sharing of [Covered Information](#).

Biometrics: [Covered Information](#) about an [Owner's](#) or [Registered User's](#) physical or biological characteristics that serves to identify the person.

Covered Information: 1) [Identifiable Information](#) that vehicles collect, generate, record, or store in an electronic form that is retrieved from the vehicles by or on behalf of a Participating Member in connection with [Vehicle Technologies and Services](#); or 2) [Personal Subscription Information](#) provided by individuals subscribing or registering for [Vehicle Technologies and Services](#).

Exclusion from Covered Information: If Participating Members collect [Covered Information](#) and then alter or combine the information so that the information can no longer reasonably be linked to the vehicle from which the information was retrieved, the [Owner](#) of that vehicle, or any other individual, the information is no longer [Covered Information](#). If Participating Members attempt to link the information to specific, identified individuals or vehicles or share the information without prohibiting the recipients from attempting such linking, the information becomes [Covered Information](#).

Attachment #1 pg 13
NB 1394 3.23.17

ALLIANCE OF AUTOMOBILE MANUFACTURERS, INC.
ASSOCIATION OF GLOBAL AUTOMAKERS
CONSUMER PRIVACY PROTECTION PRINCIPLES

Driver Behavior Information: [Covered Information](#) about how a person drives a vehicle. Examples are vehicle speed, seat belt use, and information about braking habits. This does not include information that is used only for safety, diagnostics, warranty, maintenance, or compliance purposes.

Geolocation Information: [Covered Information](#) about the precise geographic location of a vehicle.

Identifiable Information: Information that is linked or reasonably linkable to i) the vehicle from which the information was retrieved, ii) the [Owner](#) of that vehicle, or iii) the [Registered User](#) using [Vehicle Technologies and Services](#) associated with the vehicle from which the information was retrieved.

Owners: Those individuals who have legal title to a vehicle that receives or is equipped with [Vehicle Technologies and Services](#) that use [Covered Information](#); those entitled to possession of such a vehicle, like purchasers under an agreement (for example, a vehicle loan where the vehicle is collateral); and those entitled to possession of such a vehicle as lessees pursuant to a written lease agreement that, at its inception, is for a period of more than three months. The term "Owners" does not include lienholders and lenders.

Personal Subscription Information: Information that individuals provide during the subscription or registration process that on its own or in combination with other information can identify a person, such as a name, address, credit card number, telephone number, or email address.

Registered User: An individual other than an [Owner](#) who registers with, and provides [Personal Subscription Information](#) to, a Participating Member in order to receive [Vehicle Technologies and Services](#) that use [Covered Information](#).

Third-party Service Providers: Companies unaffiliated with Participating Members that receive [Covered Information](#) when conducting business on behalf of a Participating Member.

Vehicle Technologies and Services: Technologies and services provided by, made available through, or offered on behalf of Participating Members that involve the

ALLIANCE OF AUTOMOBILE MANUFACTURERS, INC.
ASSOCIATION OF GLOBAL AUTOMAKERS

Attachment # pg. 15
HB 1394 3.23.17

CONSUMER PRIVACY PROTECTION PRINCIPLES

collection, use, or sharing of information that is collected, generated, recorded, or stored by a vehicle.

IV. SPECIFIC PRINCIPLES

1. TRANSPARENCY

Participating Members commit to providing [Owners](#) and [Registered Users](#) with ready access to clear, meaningful notices about the Participating Member's collection, use, and sharing of [Covered Information](#).

Participating Members commit to providing notices in a manner that enables [Owners](#) and [Registered Users](#) to make informed decisions.

How Participating Members may provide notices: Participating Members may make notices available in a variety of ways. Depending on the nature of the [Vehicle Technologies and Services](#) and the circumstances in which they are offered, different mechanisms may be reasonable to provide [Owners](#) and [Registered Users](#) with ready access to clear, meaningful notices about the [Covered Information](#) that Participating Members collect, use, and share. There is no one-size-fits-all approach. Among the various ways Participating Members may choose to provide notices are in owners' manuals, on paper or electronic registration forms and user agreements, or on in-vehicle displays. At a minimum, Participating Members commit to making information regarding the collection, use, and sharing of [Covered Information](#) publicly available via online web portals.

When Participating Members may provide notices: Participating Members commit to taking reasonable steps to provide [Owners](#) and [Registered Users](#) with ready access to clear, meaningful notices prior to initial collections of [Covered Information](#). Notices need not be provided prior to every instance of collection where addressed by prior notices.

Content of notices: Participating Members commit to designing the notices so that they provide [Owners](#) and [Registered Users](#) with clear, meaningful information about the following:

ALLIANCE OF AUTOMOBILE MANUFACTURERS, INC.
ASSOCIATION OF GLOBAL AUTOMAKERS

CONSUMER PRIVACY PROTECTION PRINCIPLES

Attachment # 1 pg. 15
HB 1394
3.23.17

- the types of [Covered Information](#) that will be collected;
- the purposes for which that [Covered Information](#) is collected;
- the types of entities with which the [Covered Information](#) may be shared;
- the deletion or de-identification of [Covered Information](#);
- the choices [Owners](#) and [Registered Users](#) may have regarding [Covered Information](#);
- whether and how [Owners](#) and [Registered Users](#) may access any [Covered Information](#); and
- where [Owners](#) and [Registered Users](#) may direct questions about the collection, use, and sharing of [Covered Information](#).

Notices regarding the collection of [Geolocation Information](#), [Biometrics](#), and [Driver Behavior Information](#): When Participating Members collect, use, or share [Geolocation Information](#), [Biometrics](#), or [Driver Behavior Information](#), Participating Members commit to providing clear, meaningful, and prominent notices about the collection of such information, the purposes for which it is collected, and the types of entities with which the information may be shared. Please see the Choice section below for information about the Principles' [Affirmative Consent](#) conditions if Participating Members use [Geolocation Information](#), [Biometrics](#), or [Driver Behavior Information](#) as a basis for marketing or share such information with unaffiliated third parties for their own purposes.

Changing notices: Participating Members commit to taking reasonable steps to alert [Owners](#) and [Registered Users](#) prior to changing the collection, use, or sharing practices associated with [Covered Information](#) in ways that have a material impact on [Owners](#) or [Registered Users](#). If the new practices involve using [Covered Information](#) in a materially different manner than claimed when the [Covered Information](#) was collected, Participating Members commit to obtaining [Affirmative Consent](#) from [Owners](#) and [Registered Users](#) to the new practices.

ALLIANCE OF AUTOMOBILE MANUFACTURERS, INC.

ASSOCIATION OF GLOBAL AUTOMAKERS

CONSUMER PRIVACY PROTECTION PRINCIPLES

Attachment #1 pg. 16
HB1394 3-23-17

2. CHOICE

Participating Members commit to offering Owners and Registered Users with certain choices regarding the collection, use, and sharing of Covered Information.

Certain safety, operations, compliance, and warranty information may be collected by necessity without choice.

When Participating Members provide notices consistent with the Transparency principle, an Owner's or Registered User's acceptance and use of Vehicle Technologies and Services constitutes consent to the associated information practices, subject to the Affirmative Consent provisions below.

Participating Members understand that the sharing and use of Geolocation Information, Biometrics, and Driver Behavior Information can raise concerns in some situations, therefore Participating Members also commit to obtaining Affirmative Consent expeditiously for the following practices:

- using Geolocation Information, Biometrics, or Driver Behavior Information as a basis for marketing; and
- sharing Geolocation Information, Biometrics, or Driver Behavior Information with unaffiliated third parties for their own purposes, including marketing.

Affirmative Consent is not required, however, when Geolocation Information, Biometrics, or Driver Behavior Information is used or shared

- as reasonably necessary to protect the safety, property, or rights of Participating Members, Owners, Registered Users, drivers, passengers, or others (this includes sharing information with emergency service providers);
- only for safety, operations, compliance, or warranty purposes;
- for internal research or product development;

Attachment #1 pg 17
HB1394
3.23.17

ALLIANCE OF AUTOMOBILE MANUFACTURERS, INC.
ASSOCIATION OF GLOBAL AUTOMAKERS
CONSUMER PRIVACY PROTECTION PRINCIPLES

- as reasonably necessary to facilitate a corporate merger, acquisition, or sale involving a Participating Member's business;
- as reasonably necessary to comply with a lawful government request, regulatory requirement, legal order, or similar obligation, which, in the case of requests or demands from governmental entities for [Geolocation Information](#), must be in the form of a warrant or court order, absent exigent circumstances or applicable statutory authority; and
- to assist in the location or recovery of a vehicle reasonably identified as stolen.

Participating Members also need not obtain [Affirmative Consent](#) when sharing [Geolocation Information](#), [Biometrics](#), or [Driver Behavior Information](#) with [Third-party Service Providers](#) that assist in providing [Vehicle Technologies and Services](#) if those parties are not permitted to use that information for their independent use and the sharing is consistent with the notices that Participating Members have provided.

Participating Members may obtain [Affirmative Consent](#) at the time of vehicle purchase or lease, when registering for a service, or at another time.

3. RESPECT FOR CONTEXT

Participating Members commit to using and sharing [Covered Information](#) in ways that are consistent with the context in which the [Covered Information](#) was collected, taking account of the likely impact on [Owners](#) and [Registered Users](#).

The context of collection: Various factors will determine the context of collection, including the notices offered to [Owners](#) and [Registered Users](#), the permissions that they have provided, their reasonable expectations, and how the use or sharing will likely impact them.

- When Participating Members present clear, meaningful notices about how [Covered Information](#) will be used and shared, that use and sharing is consistent with the context of collection.

Attachment #1 pg. 18
NB1394
3.23.17

ALLIANCE OF AUTOMOBILE MANUFACTURERS, INC.
ASSOCIATION OF GLOBAL AUTOMAKERS
CONSUMER PRIVACY PROTECTION PRINCIPLES

- Participating Members commit to making reasonable and responsible use of [Covered Information](#) and may share that information as reasonable for those uses. Reasonable and responsible practices may vary over time as business practices and consumer expectations evolve.

The following examples illustrate some of the reasonable and responsible ways in which Participating Members may use or share [Covered Information](#) consistent with the context of collecting that information, taking into account the likely impact on [Owners](#) and [Registered Users](#). The list is not meant to be exhaustive.

- Using or sharing [Covered Information](#) as reasonably necessary to provide requested or subscribed services;
- Using or sharing [Covered Information](#) to respond to a possible emergency or other situation requiring urgent attention;
- Using or sharing [Covered Information](#) to conduct research or analysis for vehicles or [Vehicle Technologies and Services](#);
- Using or sharing [Covered Information](#) to diagnose or troubleshoot vehicle systems;
- Using or sharing [Covered Information](#) as reasonably necessary to facilitate a corporate merger, acquisition, or sale involving a Participating Member's business;
- Sharing [Covered Information](#) for operational purposes with affiliated companies that are clearly associated with the Participating Member or with the [Vehicle Technologies and Services](#) from which the [Covered Information](#) was collected or derived;
- Using or sharing [Covered Information](#) to prevent fraud and criminal activity, or to safeguard [Covered Information](#) associated with [Owners](#) or their vehicles;
- Using or sharing [Covered Information](#) to improve products and services or develop new offerings associated with [Vehicle Technologies and Services](#), vehicles, vehicle safety, security, or transportation infrastructure;
- Using [Covered Information](#) to provide [Owners](#) or [Registered Users](#) with information about goods and services that may be of interest to them;
- Sharing [Covered Information](#) as reasonably necessary to comply with a lawful government request, regulatory requirement, legal order, or similar obligation, which in the case of requests or demands from governmental

ALLIANCE OF AUTOMOBILE MANUFACTURERS, INC.
ASSOCIATION OF GLOBAL AUTOMAKERS

Attachment #1, pg. 19

HB 1394

3.23.17

CONSUMER PRIVACY PROTECTION PRINCIPLES

entities for [Geolocation Information](#), must be in the form of a warrant or court order, absent exigent circumstances or applicable statutory authority; and

- Using or sharing [Covered Information](#) to protect the safety, property, or rights of [Owners](#), Participating Members, or others.

4. DATA MINIMIZATION, DE-IDENTIFICATION & RETENTION

Participating Members commit to collecting [Covered Information](#) only as needed for legitimate business purposes. Participating Members commit to retaining [Covered Information](#) no longer than they determine necessary for legitimate business purposes.

5. DATA SECURITY

Participating Members commit to implementing reasonable measures to protect [Covered Information](#) against loss and unauthorized access or use.

Reasonable measures to protect [Covered Information](#): Reasonable measures include standard industry practices. Those practices evolve over time and in reaction to evolving threats and identified vulnerabilities.

6. INTEGRITY & ACCESS

Participating Members commit to implementing reasonable measures to maintain the accuracy of [Covered Information](#) and commit to offering [Owners](#) and [Registered Users](#) reasonable means to review and correct [Personal Subscription Information](#).

Participating Members may provide the means to review and correct [Personal Subscription Information](#) in a variety of ways, including but not limited to web portals, mobile applications, or in-vehicle tools.

Participating Members commit to exploring additional means of providing [Owners](#) and [Registered Users](#) with reasonable access to [Covered Information](#), taking into account potential security and privacy issues.

ALLIANCE OF AUTOMOBILE MANUFACTURERS, INC.
ASSOCIATION OF GLOBAL AUTOMAKERS

CONSUMER PRIVACY PROTECTION PRINCIPLES

Attachment #1 pg 20
HB1394 3.23.17

7. ACCOUNTABILITY:

- *Participating Members commit to taking reasonable steps to ensure that they and other entities that receive [Covered Information](#) adhere to the Principles.*

Accountability mechanisms that Participating Members may implement:

Participating Members commit to implementing reasonable policies, procedures, and practices to help ensure adherence to the Principles. Participating Members may implement training programs for employees and other personnel that handle [Covered Information](#). Participating Members may consider creating internal privacy review boards to evaluate and approve new technologies and services involving [Covered Information](#). Participating Members should make available reporting mechanisms for consumers to report concerns to Participating Members. Participating Members also commit to taking reasonable steps to ensure that [Third-party Service Providers](#) adhere to the Principles in providing [Vehicle Technologies and Services](#) that involve the collection, use, or sharing of [Covered Information](#).

V. CONTACT INFORMATION

ALLIANCE OF AUTOMOBILE
MANUFACTURERS

803 7TH STREET, N.W., SUITE 300
WASHINGTON, DC 20001
TEL: (202) 326-5500

GLOBAL AUTOMAKERS

1050 K ST., NW SUITE 650
WASHINGTON, DC 20001
TEL: (202) 650-5555

**ALLIANCE OF AUTOMOBILE MANUFACTURERS, INC.
ASSOCIATION OF GLOBAL AUTOMAKERS**

CONSUMER PRIVACY PROTECTION PRINCIPLES

Attachment #1, pg 21
HB 1394
3-23-17

**Appendix
Participating Members**

AMERICAN HONDA MOTOR CO., INC.

ASTON MARTIN LAGONDA OF NORTH AMERICA, INC.

BMW OF NORTH AMERICA, LLC

CHRYSLER GROUP LLC

FERRARI NORTH AMERICA

FORD MOTOR COMPANY

GENERAL MOTORS LLC

HYUNDAI MOTOR AMERICA

KIA MOTORS AMERICA

MASERATI NORTH AMERICA, INC.

MAZDA NORTH AMERICAN OPERATIONS

MERCEDES-BENZ USA, LLC

MITSUBISHI MOTORS NORTH AMERICA, INC.

NISSAN NORTH AMERICA, INC.

PORSCHE CARS NORTH AMERICA

SUBARU OF AMERICA, INC.

TOYOTA MOTOR SALES, USA

VOLKSWAGEN GROUP OF AMERICA, INC.

VOLVO CAR GROUP

**North Dakota Department of Transportation
Glenn Jackson, Director, Driver's License Division
House Bill 1394**

Mr. Chairman, members of the committee, I am Glenn Jackson, Director, Driver's License Division of the North Dakota Department of Transportation (DOT). Thank you for giving me the opportunity to address you today.

HB1394 establishes specific rules for vehicle manufacturers regarding privacy of data in autonomous vehicles. The NDDOT opposes this bill. We believe that establishing specific rules before the technology is even commercially available may prevent industry from shifting possible testing or operation to North Dakota, as they could be viewed as too rigid for their needs. As a result of our consultation with multiple stakeholders, we support HB1202 as the vehicle for autonomous technology management.

Recent guidance from the US Department of Transportation, the Governor's Highway Safety Administration, The American Association of Motor Vehicle Administrators, and others all agree on the need for vigilance by the states, but also caution not to create too many rules too soon.

We agree a focus must be placed on information privacy. Focus will also need to be placed on data-sharing, law enforcement engagement with autonomous vehicles, operator requirements, how the laws apply to vehicles when a driver is not operating the vehicle, and many other issues. This technology is moving quickly and it behooves us to be vigilant and stay abreast of current capabilities. However, it also is important for us not to put specific rules in place before we understand fully how these processes are best regulated.

Mr. Chairman that concludes my testimony, I would be happy to answer any questions.

HB 1394- Autonomous Vehicle Data Ownership
Emily O'Brien, Representative, District 42

Mr. Chairman & Members of the Committee,

I appreciate the sponsors intent of HB 1394 relating to Autonomous Vehicle Data Ownership. I personally work closely with many different Unmanned Aerial Vehicles as an Entrepreneur Coach, and I believe that we are pre-mature in this field. For autonomous vehicles to move from concept and testing to part of everyday reality, a comprehensive regulatory framework must be in place- a framework that, to date, has been conspicuously absent. **That is why I am OPPOSED to House Bill 1394.** Federally, the United States government has merely called for research on the impact autonomous vehicles will have on the transportation system and released a framework to classify the technology used in autonomous vehicles. At the state level, only a handful of states have passed legislation related to autonomous vehicles- in 2016, 20 states introduced legislation. 16 states introduced legislation in 2015, up from 12 states in 2014, nine states and D.C. in 2013 and six states in 2012. Eleven states- Alabama, California, Florida, Louisiana, Michigan, Nevada, North Dakota, Pennsylvania, Tennessee, Utah and Virginia and Washington D.C. have passed legislation related to autonomous vehicles. Governors in Arizona and Massachusetts issued executive orders related to autonomous vehicles. The legislation that exists primarily relates to the testing of autonomous vehicles. The current states statutes are not identical- they have different requirements for the testing and operation of autonomous vehicles. Since 2013, only two federal bills have been introduced that touch upon autonomous vehicles, and only one has become law. On December 4, 2015, the "Surface Transportation Reauthorization and Reform Act of 2015" was signed into law as Public Law 114-94. This Act modestly calls for grants for autonomous vehicle research. Thus far, the agent of change has not been Congress but, rather, the Department of Transportation and, specifically, the National Highway Traffic Safety Administration (NHTSA). In 2013, the US Department of Transportation- through the NHTSA- issued its Preliminary Statement of Policy Concerning Automated Vehicles- attached you will see the NHTSA framework classifying five "levels" of autonomous capability. Current state regulations are almost universally aimed at manufacturers and the testing process. These regulations also tend to be aspirational, as they target level 3 and level 4 autonomous vehicles- vehicles that for the most part are only now beginning to be developed. Because much level 3 and level 4 autonomous vehicle technology is unknown and, to any extent known, constantly being updated, these regulations are mainly focused on future risk prevention. Current regulations target manufacturers, not consumers. With that being said, state regulator agencies and legislatures must be careful when regulation for the general public. In the NHTSA Policy, the NHTSA noted "because Level 4 automated systems are not yet in existence and the technical specifications for Level 3 automated systems are still in flux, the agency believes that regulation of the technical performance of automated vehicles is premature at this time." Both state and federal governments run a real risk of stifling technological innovation by trying to regulate too far into the future. In Section 1, Subsection 1,

of HB 1394, it states that "autonomous vehicle" means a motor vehicle using autonomous technology, as a means to eliminate the human operator. In North Dakota Century Code 39.01.01-46 the definition of Motor Vehicle- includes every vehicle that is self-propelled, every vehicle that is propelled by electric power obtained from overhead trolley wires, but not operated upon rails, and for purposes of motor vehicle registration, title registration, and operator's licenses, motorized bicycles. The term does not include a snowmobile as defined in Section 36-24-01. The bill attempts to predict marketplace dynamics before fully automated vehicles are owned by the general public- and could impact not only current vehicles that have autonomous features like automatic brights, breaking system, vibrating seats, etc. on the road, but unmanned vehicles in the air, autonomous tractors in the field and soon to be autonomous vehicles on the road. In Subsection 2 it states "a manufacturer, insurer, or seller of autonomous vehicles or autonomous vehicular technology may share, release, or distribute nonidentifying aggregate vehicle data collected and stored by the autonomous vehicle- I believe that this could have unintended consequences on the owners, operators, and autonomous vehicle. In Subsection 3, a manufacturer, insurer, or seller of autonomous vehicles or autonomous vehicular technology may share, release, or distribute identifying or personalized information or data collected and stored by the autonomous vehicle, with the consent of the owner of the autonomous vehicle or by order of a court. The Drivers' Privacy Protection Act, other federal statutes including the Electronic Communications Privacy Act and the Federal Communications Act could apply to certain aspects of autonomous vehicle data and communications. Additionally, 47 states and the District of Columbia have enacted laws applicable to personal information. While these laws are generally applicable to data breaches, many also include requirements for safeguarding personal information. Although these laws provide from some protections of various personal information, because of the type of data involved, the manner of collection, or the entity collection the data, some or all of these protections may or may not be applicable to autonomous vehicles. Perhaps the most fundamental question that needs to be considered is how the collection and sharing of location data impacts the concept of an individual's "reasonable expectation of privacy," which impacts both protections afforded by Fourth Amendment and the applicability of privacy interests in tort law. Another factor that complicates the reasonable expectation of privacy issue is the potential that location data from autonomous cars would be shared with third parties, including the manufacturer or other service providers. That concludes my testimony, I will take any questions you may have.

Level	Description
Level 0: No automation	The driver is in complete and sole control of the primary vehicle controls (brake, steering, throttle, and motive power) at all times, and is solely responsible for monitoring the roadway and safe operation of all vehicle controls.
Level 1: Function-specific automation	Automation at this level involves one or more specific control functions; if multiple functions are automated, they operate independently of each other. The driver has overall control, and is solely responsible for safe operation, but can choose to cede limited authority over a primary control (as in adaptive cruise control), the vehicle can automatically assume limited authority over a primary control (as in electronic stability control), or the automated system can provide added control to aid the driver in certain normal driving or crash-imminent situations (e.g., dynamic brake support in emergencies).
Level 2: Combined-function automation	This level involves automation of at least two primary control functions designed to work in unison to relieve the driver of controlling those functions. The driver is still responsible for monitoring the roadway and safe operation, and is expected to be available to take control at all times and on short notice (e.g. adaptive cruise control and automated steering working together to guide the car's movements).
Level 3: Limited self-driving automation	Vehicles at this level of automation enable the driver to cede full control of all safety-critical functions under certain traffic or environmental conditions, and in those conditions to rely heavily on the vehicle to monitor for changes in those conditions requiring transition back to driver control. The driver is expected to be available for occasional control, but with sufficiently comfortable transition time.
Level 4: Full self-driving automation	The vehicle is designed to perform all safety-critical driving functions and monitor road-way conditions for an entire trip.

<http://www.nortonrosefulbright.com/knowledge/publications/141954/autonomous-vehicles-the-legal-landscape-in-the-us>

Attachment #4 pg1
HB 1394 3.23.17
Lacy Anderson

AUTONOMOUS VEHICLES: ROAD SAFETY AND INSURANCE
An issues brief of the American Insurance Association

As with the public at large, the American Insurance Association, our members and the property-casualty insurance industry are all following developments for potential autonomous vehicles with great interest. By autonomous or driverless vehicles we mean vehicles that can operate with no or virtually no human control. As these technologies develop there are important things for the public, private sector and public policy decision makers to keep in mind.

Insurers do, of course, support these innovations in a number of ways. Such innovations are built upon and continue to build upon automotive safety advances and technologies that insurers have long championed. AIA and our industry have strongly advocated auto safety and technological improvement through the decades including the founding of Insurance Institute for Highway Safety. Also, insurers may well insure the companies developing autonomous vehicle technologies if not, at this time, the finished products as used by consumers. With this experience insurers offer a few important reminders as this technology develops and policy makers consider how to regulate it.

First and foremost, before operating on the public roads autonomous vehicles simply must meet all federal and state safety requirements. That means everything from passenger restraints to crash worthiness to "driver" reliability. Ironically, might one argue that a driverless vehicle have to pass state-mandated driving courses just like residents? One would think so as those tests are, of course, a linchpin for safe operation with a driver-operated vehicle.

Second, as autonomous vehicles will use a host of communication streams in real time, such systems must be hardened against potential cyber-attack. With telematics, dedicated short-range communications, vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I) and more there are myriad avenues for unscrupulous actors to make vehicular attacks or system wide ones. The media has already reported such incidents. At the same token, while nefarious attacks must be anticipated and prevented, appropriate, permissive data access should be preserved. Manufacturers, individuals, insurers and more should all be able to use data from systems to improve products, services and prices.

Third, autonomous vehicles are entirely untested as ready-for-consumer-market products. Such vehicles have no experience whatsoever operating autonomously and carrying consumers on the roads or highways. It is effectively impossible to precisely rate and underwrite this risk as the technology is in the infancy of its use. Thus, in some ways this is similar to dawn of the automobile when there were no insurance coverage mandates for decades. Consequently, insurers must not be forced to cover or even offer coverage for autonomous vehicles for the foreseeable future.

Fourth, to permit a viable private insurance market to develop for autonomous vehicles insurers must be permitted the maximum freedom in rating, underwriting and insuring this technological advancement. This must even include the ability to exclude coverage for such vehicles entirely as some companies may not be in a position to insure a completely untried entrant to the consumer automotive marketplace.

AIA, our member and industry are excited about the potential of autonomous vehicles. As this technology is only now developing, public policy decision makers must very carefully consider their actions before passing laws that could suppress the innovation, endanger consumers or harm insurance market competition.

Testimony to the Senate Transportation Committee
Chairman Lonnie Laffen
Tom Swoyer
Grand Sky Development

Attachment #5 pg. 1
HB 1394 3.23.17
Don Larson

HOUSE BILL 1394

Mr. Chairman and members of the committee, my name is Tom Swoyer and I am the President of Grand Sky Development Company. As most of you know, Grand Sky is the name of a development park operating under an enhanced use lease that Grand Forks County arranged with the U.S. Air Force. It is a one of a kind asset for the State of North Dakota

We are currently home to two of the largest aerospace companies in the world, both of whom are focused on developing unmanned systems in North Dakota. Those companies are Northrop Grumman and General Atomics. Together, these companies are investing over \$50M in facilities at Grand Sky where they will create high-quality jobs focused on researching, developing, training and testing unmanned aircraft. These two companies are just the tip of the iceberg, and I am working every to bring more of these types of companies to North Dakota.

I am here today to testify in opposition to House Bill 1394. While this bill was conceived with good intentions, its practical effect will create confusion and uncertainty and will ultimately "slam on the brakes" of a growing industry in our state. There are numerous problems with how we define "owner", how we define "autonomous" and how we define "operations." Specifically, our industry is moving towards a model where leased vehicles or co-op owned and operated vehicles will become more common. How will we determine who the owner of a leased vehicle is? We further compound this issue with the fact that the most popular unmanned systems in the US right now are built and offered by Chinese, French and other foreign manufacturers.

Attachment #5 pg 2
HB 1394 3.23.17

The word "autonomous" also creates problems because we are not defining the degree of autonomy. Some farm equipment can operate in some form of an autonomous mode as well as existing automobiles that have automatic braking and lane keeping technologies. In my world autonomy is a very carefully used word. While many unmanned aircraft have some form of "autonomous" capabilities, there are still many functions which can be overridden by an operator or pilot.

Finally, the way we define "operations" causes us concern. If one of my customers contracts us to take photos of their farm under a contract, a leasing company may own the aircraft, and I may own the contract to take the photo but the farmer will certainly want to own photo itself so that no one goes off and sells it.

These are just a few examples of how a well-intentioned piece of legislation can have far reaching negative consequences on an entire industry. My world revolves around unmanned aircraft and very soon to be autonomous aircraft. It may not seem immediately obvious that self-driving cars have much to do with unmanned aircraft but this legislation creates links that can't be undone. Also, the convergence of automobile technologies with aircraft technologies is happening at a furious pace and small unmanned aircraft launched from ground vehicles will soon be commonplace. Where does a car end and an aircraft begin?

In conclusion, I oppose this legislation because of the unintended negative consequences that will clearly result if it is passed. The unmanned aircraft industry is growing rapidly in North Dakota and we seek to avoid regulation that will unintentionally curtail its growth.

Attachment #6 pg. 1
HB 1394 3.23.17

General Motors Testimony: HB 1394
North Dakota Senate Transportation Committee
Thursday, March 23, 2017

Good afternoon Chair Laffen and members of the Senate Transportation Committee. My name is Jason Wetzel and I am Regional Director of Government Relations for General Motors.

I appreciate the opportunity to comment on House Bill 1394, relating to autonomous vehicle (AV) data ownership.

As originally proposed, the legislation sponsored by Rep. Keiser allows manufacturers, insurers, or sellers of AVs or AV technology to share, release, or distribute non-identifying aggregate vehicle data collected by AVs. An amendment to the bill added in the House also allows manufacturers, insurers and sellers to share, release or distribute personalized consumer data with the consumer's written consent.

There are several issues created by this legislation. The bill attempts to predict marketplace dynamics well before fully automated vehicles are owned by the general public. AV technology is still in its early stages and requires much more testing and learnings by automakers before it can reach mainstream production. Consumer ownership of fully automated vehicles (Level 5) is not imminent and there is little reason to rush to make sweeping changes before we have a solid understanding of how the technology will be developed and deployed. One issue with the bill is that it does not distinguish between the five levels of autonomy recognized by the industry and outlined by the National Highway Traffic Safety Administration (NHTSA) in the Federal Automated Vehicles Policy. As written, the bill equates Level 5, which is a fully autonomous vehicle that does not have a steering wheel, with the Level 2 or Level 1 platforms, which respectively have two or a single form of technology aiding the human driver with the safe operation of the vehicle such as forward collision alerts or lane departure warnings.

In any event, the existing legal framework that addresses vehicle data access is appropriate for AVs. To supplement that point, it's worth noting that most automobile manufacturers, including GM, install event data recorders (EDRs) in their vehicles. EDRs are regulated under Federal Motor Vehicle Safety Standard 563. An EDR is a function on the Sensing and Diagnostic Module (SDM) that records vehicle data including speed, seatbelt use, brake use, and change in velocity five seconds before, during, and after a crash or near-crash event. The SDM is the module that "tells" the airbag to fire when crash or near-crash conditions are met. Consent from the vehicle owner must be obtained to access EDR data unless one of the limited exceptions is met such as for emergency response, service and repair, and official government request. Manufacturers are required to disclose the presence and recording capability of an EDR in owners' manuals. Some insurance companies may also enter into agreements with insureds to install aftermarket recording devices that plug into the dashboard to record vehicle data about an insured's driving for potential discounts. These products are independent from manufacturers' EDRs.

There is no evidence that regulation of AV data is yet needed. Any effort to proceed with such premature regulation would unnecessarily raise significant consumer concerns and could impede the development of AVs. This is due, in part, because the bill seems to associate EDRs with the

Attachment # 6 pg 2

HB 1394 3-23-17

technology platforms supporting AV deployment and development, and proposes to provide equal access to both – despite AV technology being much more complex.

In fact, HB 1394's data ownership rights could equate to broad and unfettered data access to AV data. This construct fails to account for the potentially significant cybersecurity concerns created by potentially mandating public wide access to safety critical vehicle systems for data. These are not systems being designed for open access by third parties. Moreover, AV development and ultimately deployment relies upon secure storage and transmission of vehicle data to connected vehicle networks. This bill could threaten that important imperative necessary to move this technology forward.

This bill may also impede upon proprietary information developed by technology companies and automakers. The measure states that the owner of an AV owns any data or information stored by the AV or gathered by the use of the AV. It does not draw a distinction between data generated by the AV and the software installed to make the vehicle function and operate. When you purchase a smart phone for example, you do not own the licensed software that enables the phone to operate. You own the phone, your texts, emails, and all of your personal information, but not the copyrighted proprietary software. More simply put -- you don't own the recipe for secret sauce when you buy a Big Mac. This bill likens access to ownership in a way that could impact autonomous technologies such as the unmanned aircraft system (UAS) industry advancing in North Dakota.

Fully autonomous vehicles will generate countless lines of code as they operate. HB 1394 would treat incomprehensible lines of 1s and 0s as if it is information that is easy to access and decode, and for some reason – share with third parties.

Mr. Chairman and members of the committee, HB 1394 is not ripe to solve any existing consumer issue. Instead, it raises significant concerns that could threaten AV development and its potentially dramatic safety benefits on North Dakota roadways. For that reason, I respectfully request that you oppose HB 1394.

**TechNet Written Testimony on HB 1394 to the North Dakota Senate
Transportation Committee**

Attachment 6 pg 2
HB 1394 3.23.17

Thursday, March 23, 2017

Chair Laffen and members of the Senate Transportation Committee, Joanie Deutsch, Executive Director for TechNet, writing in opposition to House Bill 1394.

I appreciate the opportunity to comment on House Bill 1394, relating to autonomous vehicle data ownership. This legislation is concerning and would likely have a chilling effect upon autonomous vehicle development with ramifications well beyond North Dakota.

If you are not familiar with TechNet, we represent over 70 of the nation's leading tech companies. Our diverse membership includes dynamic startups to the most iconic companies on the planet. Also included in our membership are leaders in autonomous vehicle development, including Waymo (formerly the Google Self Driving Car Project), General Motors, Uber, and Lyft. We are the national, bipartisan network of technology companies that promotes the growth of the innovation economy. A full membership list is available on our website, here: <http://www.technet.org/leaders/member-companies/>.

Automated vehicle technology is still in its early stages and consumer ownership of fully automated vehicles is not imminent, as the vehicles continue to be tested in company-owned fleets. HB 1394 attempts to predict marketplace dynamics well before fully automated vehicles are owned by the general public. As such there is little reason for North Dakota to rush to make sweeping changes with respect to its current law regarding recording devices on motor vehicles before there is a solid understanding of how autonomous technology will be commercially deployed.

The existing legal framework for recorded data in motor vehicles is appropriate for autonomous vehicles and a change in law is not needed. Moreover, HB 1394 does not solve any existing consumer issue. Instead, it raises considerable safety concerns that could threaten autonomous vehicle development and its perhaps dramatic safety benefits on North Dakota roadways.

Autonomous vehicle systems are proprietary and will generate significant amounts of safety-critical data, and manufacturers spend significant resources to develop this technology. Free use of the data underlying these systems by the insurance industry would be unprecedented and halt the development, testing, and deployment of this life-saving technology in North Dakota.

The bill's data ownership rights could equate to broad and unfettered access to data stored by autonomous vehicles. This construct fails to account for the potentially significant cybersecurity concerns created by possibly mandating public wide access into safety critical vehicle systems for data.

Attachment #6 pg. 4

HB 1394 3.23.17

Autonomous vehicle development and ultimately deployment relies upon secure storage and transmission of data for the safe operation of the vehicles. This bill could threaten that important assumption necessary to move this technology forward. It would also put at risk automaker proprietary information.

For these reasons and more, I urge you to vote no on HB 1394.

Thank you.

Attachment # 7 pg 1

North Dakota Senate Transportation Committee
March 23, 2017 -- HB 1394
Uber Technologies Written Testimony

Good morning Chairman Laffen and Members of the Transportation Committee, my name is Carla Jacobs. I am the head of Public Policy for Uber North Dakota. Thank you for the opportunity to testify today on HB 1394.

As you know from this committee's work in 2015, Uber is a ridesharing app that connects passengers with drivers at the push of a button. This technology has enabled Uber to improve mobility and the quality of life for people living in and around Fargo since 2015 and in Bismark and Grand Forks more recently. In these cities, riders have access to safe and reliable transportation and drivers have access to flexible earning opportunities.

Seven years ago, the idea that you could push a button and get a ride was unthinkable. Today ridesharing is a reality in over 70 countries across the globe. Ridesharing came to North Dakota in 2015 and since then we have seen that things change for the better because people can get an affordable, safe, and reliable ride across town.

North Dakota was one of the first states to pass regulations for ridesharing, and since that time, many other states have looked to this model for their own state regulations. North Dakota has helped pave the way for innovation in transportation.

And now we're looking toward the future of transportation and seeing that self-driving cars can make cities and towns safer, cleaner, more efficient and more affordable. Uber is equipped with one of the strongest self-driving engineering groups in the world, the practical experience that comes from running ride-sharing and delivery services in hundreds of cities, world-class manufacturing partners like Volvo, and the intelligence that comes from doing 1.2 billion miles on the road every month.

The benefits of autonomous vehicle technologies are clear.

- In 2016, over 40,000 Americans died as a result of car crashes and 94% of those crashes are due to human error.
- This technology will allow for increased mobility for individuals with disabilities and result in longer independence for aging populations
- We will see continued improvement to DUI rates across the country

North Dakota can position itself to continue to be a leader and create open doors for innovation- it has done so with ridesharing, unmanned aircrafts and can do so with self driving technology.

Many companies, including Uber, are currently identifying where they will test and operate AVs and HB 1394 creates roadblocks for emerging technology.

The bill before you today creates significant concerns about data ownership, data privacy, and proprietary data.

The bill would regulate ownership of and access to the data collected by autonomous vehicles without acknowledging that there may be significant changes to the way autonomous vehicles are owned and operated compared with the traditional motor vehicle owner operator model used today.

Since the first autonomous vehicles available for purchase by early adapting customers will be more expensive, it's likely we will see a shared use model with networks like Uber or large fleet operators. Because of this potential change, establishing requirements solely in-line with the traditional vehicle owner operator model and giving full control over data collected when the owner is not necessarily the one in the vehicle or using the vehicle, is not logical and may prove to be confusing and concerning.

Additionally, appropriate data sharing for insurance purposes in North Dakota is already accomplished through private contracts between insurance companies and their customers and already addressed by existing law for event data recorders. There is no need for special legislation in this area in the context of autonomous vehicles.

Furthermore, the type and amount of data collected by AV systems to make the systems work is significant and yet the bill does not make clear what types of "identifying and personalized" information can be shared, nor does it stipulate an individual's privacy should be protected by third parties.

Lastly, because we are early in the development of this technology, companies are working to innovate to create the best hardware and software needed to advance self driving technology. This bill could require that data related to these proprietary systems be shared and distributed creating an anticompetitive landscape that will stifle innovation and prevent self driving benefits from coming to North Dakota.

In summary, it is too early to regulate a solution to a problem that we can't yet fully define for an industry whose future is still being developed.

We appreciate the work that the committee has done on this issue to date and look forward to working with you on future efforts related to self driving technology. However, the current language creates significant challenges and we urge a Do Not Pass recommendation on this bill.

The following are excerpts from the Federal Automated Vehicles Policy

Marlo Anderson

For DOT, the excitement around highly automated vehicles (HAVs) starts with safety. Two numbers exemplify the need. First, 35,092 people died on U.S. roadways in 2015 alone. Second, 94 percent of crashes can be tied to a human choice or error.

Model State Policy

Today, a motorist can drive across state lines without a worry more complicated than, "did the speed limit change?" The integration of HAVs should not change that ability. Similarly, a manufacturer should be able to focus on developing a single HAV fleet rather than 50 different versions to meet individual state requirements. State governments play an important role in facilitating HAVs, ensuring they are safely deployed, and promoting their life-saving benefits. The Model State Policy confirms that States retain their traditional responsibilities for vehicle licensing and registration, traffic laws and enforcement, and motor vehicle insurance and liability regimes. Since 2014, DOT has partnered with the American Association of Motor Vehicle Administrators (AAMVA) to explore HAV policies. This collaboration was one of the bases for the Model State Policy framework presented here and identifies where new issues fit within the existing federal/state structure. The shared objective is to ensure the establishment of a consistent national framework rather than a patchwork of incompatible laws.

Note on "Levels of Automation"

There are multiple definitions for various levels of automation and for some time there has been need for standardization to aid clarity and consistency. Therefore, this Policy adopts the SAE International (SAE) definitions for levels of automation. The SAE definitions divide vehicles into levels based on "who does what, when."⁴ Generally:

- At SAE Level 0, the human driver does everything;
- At SAE Level 1, an automated system on the vehicle can sometimes assist the human driver conduct some parts of the driving task;
- At SAE Level 2, an automated system on the vehicle can actually conduct some parts of the driving task, while the human continues to monitor the driving environment and performs the rest of the driving task;
- At SAE Level 3, an automated system can both actually conduct some parts of the driving task and monitor the driving environment in some instances, but the human driver must be ready to take back control when the automated system requests;
- At SAE Level 4, an automated system can conduct the driving task and monitor the driving environment, and the human need not take back control, but the automated system can operate only in certain environments and under certain conditions; and

- At SAE Level 5, the automated system can perform all driving tasks, under all conditions that a human driver could perform them.

Privacy

The Department and the Administration strongly believe in protecting individuals' right to privacy. This is exemplified by the White House Consumer Privacy Bill of Rights and the Federal Trade Commission's privacy guidance. In November 2014, the Alliance of Automobile Manufacturers and the Association of Global Automakers published Privacy Principles for Vehicle Technologies and Services. Given these available resources, HAV manufacturers and other entities, either individually or as an industry, should take steps to protect consumer privacy. Manufacturers' privacy policies and practices should ensure:

- a. Transparency: provide consumers with accessible, clear, meaningful data privacy and security notices/agreements which should incorporate the baseline protections outlined in the White House Consumer Privacy Bill of Rights and explain how Entities collect, use, share, secure, audit, and destroy data generated by, or retrieved from, their vehicles;
- b. Choice: offer vehicle owners choices regarding the collection, use, sharing, retention, and deconstruction of data, including geolocation, biometric, and driver behavior data that could be reasonably linkable to them personally (i.e., personal data);
- c. Respect for Context: use data collected from production HAVs only in ways that are consistent with the purposes for which the data originally was collected (as explained in applicable data privacy notice/agreements);
- d. Minimization, De-Identification and Retention: collect and retain only for as long as necessary the minimum amount of personal data required to achieve legitimate business purposes, and take steps to de-identify sensitive data where practical, in accordance with applicable data privacy notices/agreements and principles;
- e. Data Security: implement measures to protect data that are commensurate with the harm that would result from loss or unauthorized disclosure of the data;
- f. Integrity and Access: implement measures to maintain the accuracy of personal data and permit vehicle operators and owners to review and correct such information when it is collected in a Federal Automated Vehicles Policy 20 way that directly or reasonably links the data to a specific vehicle or person; and
- g. Accountability: take reasonable steps, through such activities as evaluation and auditing of privacy and data protections in its approach and practices, to ensure that the entities that collect or receive consumers' data comply with applicable data privacy and security agreements/notices.

System Safety

Manufacturers and other entities should follow a robust design and validation process based on a systems-engineering approach with the goal of designing HAV systems free of unreasonable safety risks. This process should encompass designing the intended functions such that the vehicle will be placed in a safe state even when there are electrical, electronic, or mechanical malfunctions or software errors.

The overall process should adopt and follow industry standards, such as the functional safety process standard for road vehicles, and collectively cover the entire design domain of the vehicle. Manufacturers and other entities should follow guidance, best practices, design principles, and standards developed by established standards organizations such as International Standards Organization (ISO) and SAE International, as well as standards and processes available from other industries such as aviation, space, and the military (e.g., the U.S. Department of Defense standard practice on system safety), as they are relevant and applicable. See NHTSA's June 2016 report, "Assessment of Safety Standards for Automotive Electronic Control Systems," for an evaluation of the strengths and limitations of such standards, which the Agency believes could support the future development of a robust functional safety approach for automotive electronic control systems.

The process should include a hazard analysis and safety risk assessment step for the HAV system, the overall vehicle design into which it is being integrated, and when applicable, the broader transportation system. The process should describe design redundancies and safety strategies for handling cases of HAV system malfunctions. The process should place significant emphasis on software development, verification and validation. The software development process should be well-planned, well-controlled, and well-documented to detect and correct unexpected results from software development and changes. Thorough and measurable software testing should complement a structured and documented software development process. The automotive industry should monitor the evolution, implementation, and safety assessment of Artificial Intelligence (AI), machine learning, and other relevant software technologies and algorithms to improve the effectiveness and safety of HAVs.

Design decisions should be linked to the assessed risks that could impact safety-critical system functionality. Design safety considerations should include, but not be limited to, design architecture, sensor, actuator, and communication failure; potential software errors; reliability; potential inadequate control and undesirable control actions; potential collisions with environmental objects and other road users, potential collisions that could be caused by actions of the HAV system; leaving the roadway, loss of traction or stability, and violation of traffic laws and deviations from normal (expected) driving practices.

All design decisions should be tested, validated, and verified as individual subsystems and as part of the entire vehicle architecture. The entire process should be fully documented and all, changes, design choices, analyses, associated testing and data should be fully traceable.

Vehicle Cybersecurity

Manufacturers and other entities should follow a robust product development process based on a systems-engineering approach to minimize risks to safety, including those due to cybersecurity threats and vulnerabilities. This process should include systematic and ongoing safety risk assessment for the HAV system, the overall vehicle design into which it is being integrated, and when applicable, the broader transportation ecosystem.

The identification, protection, detection, response, and recovery functions should be used to enable risk management decisions, address risks and threats, and enable quick response to and learning from cybersecurity events. While this is an evolving area and more research is necessary before proposing a regulatory standard, entities are encouraged to design their HAV systems following established best practices for cyber physical vehicle systems. In particular, entities should consider and incorporate guidance, best practices, and design principles published by National Institute for Standards and Technology (NIST), NHTSA, SAE International, the Alliance of Automobile Manufacturers, the Association of Global Automakers, the Automotive Information Sharing and Analysis Center (ISAC) and other relevant organizations.

The entire process of incorporating cybersecurity considerations should be fully documented and all actions, changes, design choices, analyses, associated testing and data should be traceable within a robust document version control environment.

As with safety data, industry sharing on cybersecurity is important. Each industry member should not have to experience the same cyber vulnerabilities in order to learn Federal Automated Vehicles Policy from them. That is the purpose of the Auto-ISAC, to promote group learning. To that end entities should report any and all discovered vulnerabilities from field incidents, internal testing, or external security research to the Auto-ISAC as soon as possible, regardless of membership. Entities involved with HAVs should consider adopting a vulnerability disclosure policy.

Human Machine Interface

Understanding the interaction between the vehicle and the driver (commonly referred to as "human machine interface (HMI)") has always played an important role in the automotive design process. New complexity is introduced as HAVs take on driving functions, in part because the vehicle must be capable of accurately conveying information to the human driver regarding intentions and vehicle performance. This is particularly true of SAE Level 3 systems in which human drivers are expected to return to the task of monitoring and be available to take over driving responsibilities, but drivers' ability to do so is limited by humans' capacity for staying alert when disengaged from the driving task.

Manufacturers and other entities should consider whether it is reasonable and appropriate to incorporate driver engagement monitoring to Level 3 HAV systems. Furthermore, manufacturers and other entities should consider how HAVs will signal intentions to the environment around the vehicle, including pedestrians, bicyclists, and other vehicles. Manufacturers and other entities should have a documented process for the assessment, testing, and validation of the vehicle HMI. Considerations should be made for the human driver, operator, occupant(s), and external actors with whom the HAV may have interactions

(other vehicles, pedestrians, etc.). HMI design should also consider the need to communicate information to pedestrians, conventional vehicles, and automated vehicles regarding the HAV's state of operation relevant to the circumstance (e.g., whether the HAV system identified a pedestrian at an intersection and is yielding).

Given the rapidly evolving nature of this area and ongoing research, manufacturers and other entities should consider and apply the guidance, best practices, and design principles published by SAE International, ISO, NHTSA, American National Standards Institute (ANSI), the International Commission on Illumination (CIE) and other relevant organizations.

At a minimum, indicators should be capable of informing the human operator or occupant that the HAV system is:

1. Functioning properly;
2. Currently engaged in automated driving mode;
3. Currently "unavailable" for automated driving;
4. Experiencing a malfunction with the HAV system; and
5. Requesting control transition from the HAV system to the operator.

In fully automated vehicles, manufacturers and other entities should design their HMI to accommodate people with disabilities (e.g., through visual, auditory, and haptic displays). In designs where an HAV is intended to operate without a human driver or occupant, the remote dispatcher or central control authority should be able to know the status of the HAV at all times. Examples of these may include automated delivery vehicles, last mile special purpose ground drones, and automated maintenance vehicles.

The entire 126 page document can be found at:

<https://www.transportation.gov/AV/federal-automated-vehicles-policy-september-2016>



**Statement of
Ford Motor Company**

**State of North Dakota
Senate Committee on Transportation
Hearing on**

**"HB 1202 and HB 1394, Relating to the Operation and Regulation of Autonomous Vehicles and
Autonomous Vehicle Data Ownership, Respectively"**

March 23, 2017

Ford appreciates North Dakota's interest in issues related to automated vehicles. As a general matter, we strongly believe that if a state wishes to pursue legislative or regulatory action with respect to such vehicles, that action should be premised upon removing impediments to their safe testing and deployment.

With respect to HB 1202, we are grateful for the attentiveness of the Legislature, Department of Transportation, and Department of Commerce to the views of Ford and other stakeholders. We support adoption of the amendment requiring that the Department of Transportation study automated vehicles and report back to the Legislature. We thank Senator Ruby, the Governor, and the Department of Transportation for their positive engagement on this matter and stand ready to provide our assistance moving forward.

Additionally, Ford regrets that it opposes HB 1394 in its current form. We believe there is no need at this time to address data sharing related to automated vehicles, particularly because these vehicles are not yet deployed, and data sharing could compromise sensitive intellectual property and other confidential business information. Instead, we feel it is more appropriate for auto insurers and automated vehicle developers to engage in discussions to improve their mutual understanding of the types of data generated by new technologies, the value of such data to adjusting insurance claims or properly pricing underwriting vehicles, and the feasibility and usefulness of sharing such data, as well as the implications for consumer privacy, vehicle security, and confidential business information raised in all cases. We would welcome your leadership in facilitating such cooperative conversations, which are critical to developing sound public policy.

Ford Motor Company believes automated vehicles have significant potential to improve safety and mobility. Our company, in partnership with ARGO AI, is hard at work to achieve the goal of deploying a Society of Automotive Engineers (SAE) Level Four vehicle without a steering wheel or accelerator and brake pedals for commercial applications in limited geo-fenced areas in 2021. This is challenging work, whose success can be aided by having the right policies in place to facilitate, rather than impede, innovation.

We are grateful for the opportunity to provide our views on HB 1202 and HB 1394 today. We hope to continue working collaboratively with the Legislature in helping craft reasonable policies that ensure a safe, competitive future for automated vehicles.