

# Speaking to Vehicular/IoT Technology Listening



Robert Thibadeau, Ph.D.  
School of Computer Science  
Carnegie Mellon University

&

Chairman & CEO  
Bright Plaza, Inc.. aka  
Drive Trust Alliance (DTA)

**[www.drivetrust.com](http://www.drivetrust.com)**

Talk to American Bar Assn Tech Committee  
RSA Conference-2017, San Francisco  
&  
Automotive Keynote  
Supply Chain Management Assurance <sup>1</sup>  
Spring Forum 2017, Washington DC

# Rules

- Temporary Lift of Chatham House Rule: We request attribution for this talk
  - Question Answering at end will not be taped
- Patent Pending on DTA Technology Privacy Technology and DTA-Micron Automotive Engineering Platform

# What's a Vehicle?

- **Highly Automated Vehicles (HAVs)**

- Land: Cars, Trucks, Rail, etc.

- Sea: Boats, Ships, Subs

- Air: Planes, Airships, Drones

- Space: Satellites, Space Ships

## **The same technical revolutions impact IoT**

Notably similar: *Smart Homes / Smart Buildings / Smart Campuses, Smart Cities...even IT and Cloud Societies*

# But...let's do cars today

## Automated Vehicle received views:

### 1. Feasible

Aircraft Proven Already

Watercraft Proven Already

Train Proven Already

Cars/Trucks believed Proven in Principle

### 2. Necessary : Relieve Traffic Congestion, Safety

### 3. Inevitable : ~2020 time frame, ubiquitous

by 2035

# *Received Vision of the Future*

We'll go **from buying cars to subscriptions to cars.**

Existential Example: Car/Truck Rental

Existential Changeover Example: Buy Software to Subscribe to Software  
(Microsoft, Cloud Computing)

**But, your subscription says, for example,**

- Type of car (Premium, Standard, Compact, Electric, Fuel Cell)
- Rights to call a car to you. (Every morning at 8AM, car is waiting at your house for you unless time changed or request cancelled, Every afternoon at 5PM, car is waiting where your morning pickup took you unless otherwise fetched.)
- Number of other people sharing car (0, 1, 2, 3?)

**Results of Automated Vehicle Adoption**

- More enjoyable travel experience
- Less congestion on roads (more efficient car utilization)
- Improved safety on roads
- Cost of ownership, one expense, tax advantage for civil result.
- Car Makers make more money!

# Sept 2016

## NHTSA HAV Guidelines



[https://one.nhtsa.gov/nhtsa/av/pdf/Federal Automated Vehicles Policy.pdf](https://one.nhtsa.gov/nhtsa/av/pdf/Federal_Automated_Vehicles_Policy.pdf)

Also with our comments at [www.drivetrust.com/](http://www.drivetrust.com/)

# THIS IS NOT A LEGAL DOCUMENT!

*IMHO:* It is a great framework out of which you can begin to think about legal issues

- Automotive **Industry accepted nomenclature** and Concepts
- Long life ... reasonably **good framework for tracking technology change** for the next 20 Years at least
- Check list for **areas of (safety) concern** as Vehicular Technology learns to speak to the world

And it is short and easy to read! Good for High School Classes

# Two Components Splashed Together

- **6 Levels of HAVs** (from nearly no automation to full automation) from SAE
- **10 Areas of Safety Concern** (mapped to different levels) from NHTSA

EOS (End of Story)

Comment Period Over on September 2016 Draft



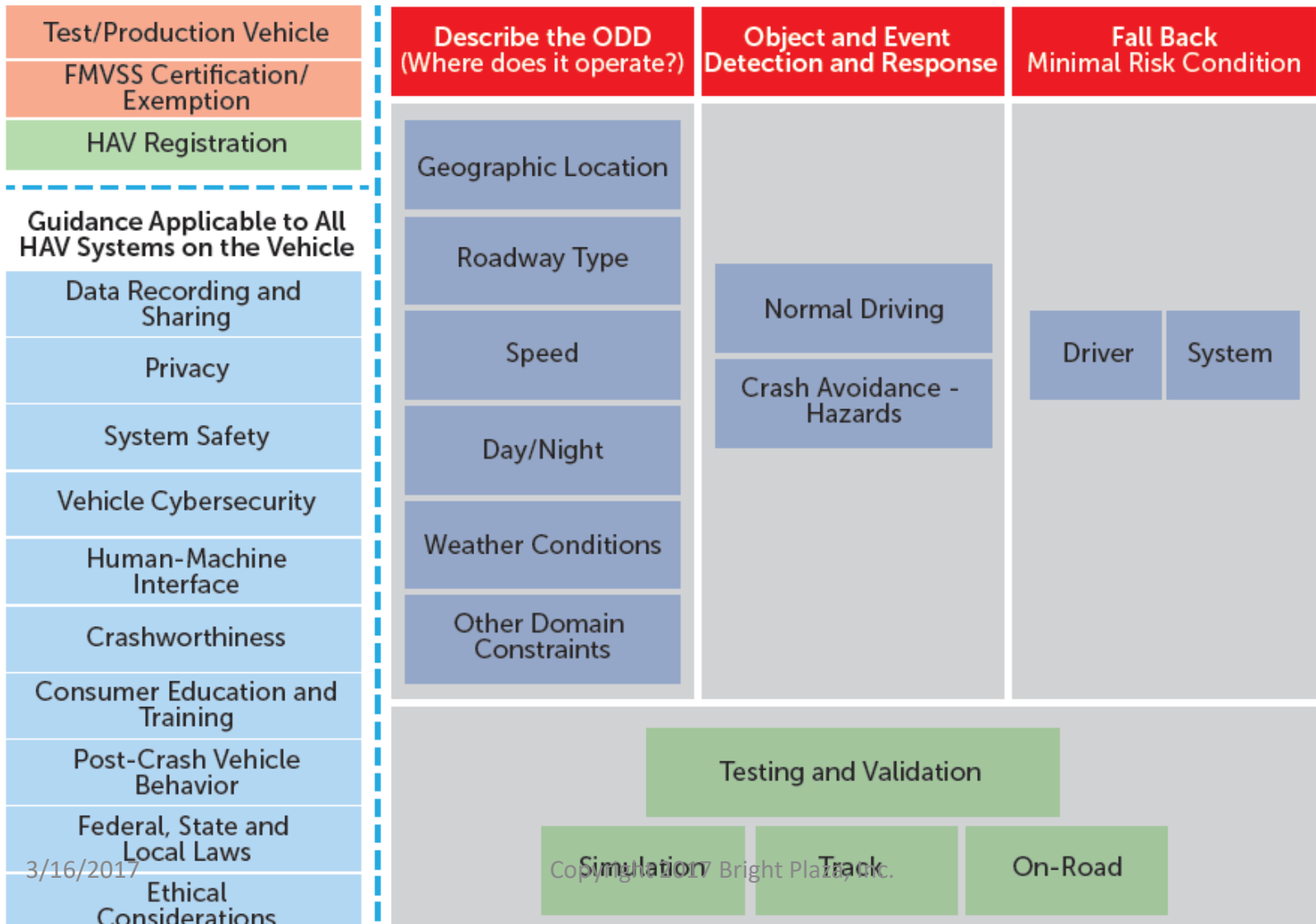
# 6 HAV Levels

- 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.

# 10 Areas of 'Safety' Concern

## Scope & Process Guidance

## Guidance Specific to Each HAV System



# 4 Data Communications Systems

Inside Car

Car to 'Road'

Car to Car

Car to Cloud

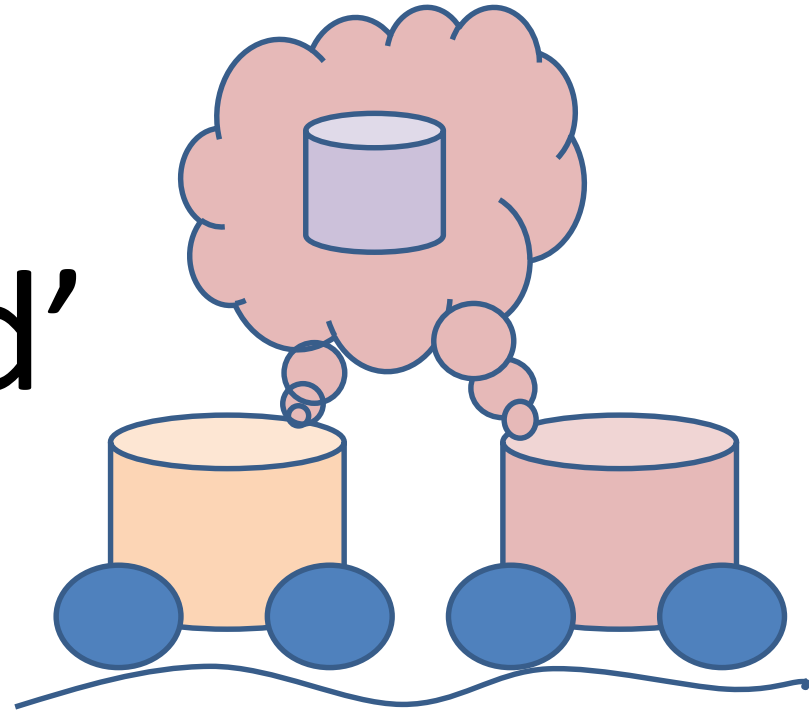
# Privacy



# 4 Privacy Invations

“Invation” = Invasion Invitations

Inside Car  
Car to ‘Road’  
Car to Car  
Car to Cloud



# Where's the Data? Inside CAR



= Machine Learning /AI



ADAS (Advanced Driver Assist System)



- GPS (Locations)



- Infotainment



- Human Interactions



- Automated Vehicle Systems (e.g., Cars ahead, Behind, Beside, MPG, EV History)



- Video – Audio Recording



Trackers (Insurance)



Engine (Mileage, Wear, Power)



Black Box (Law, Accidents, Insurance)



Smart Sensors (Raindrop, Predictive Road Slickness)



Network Logs



# GPS Memory...

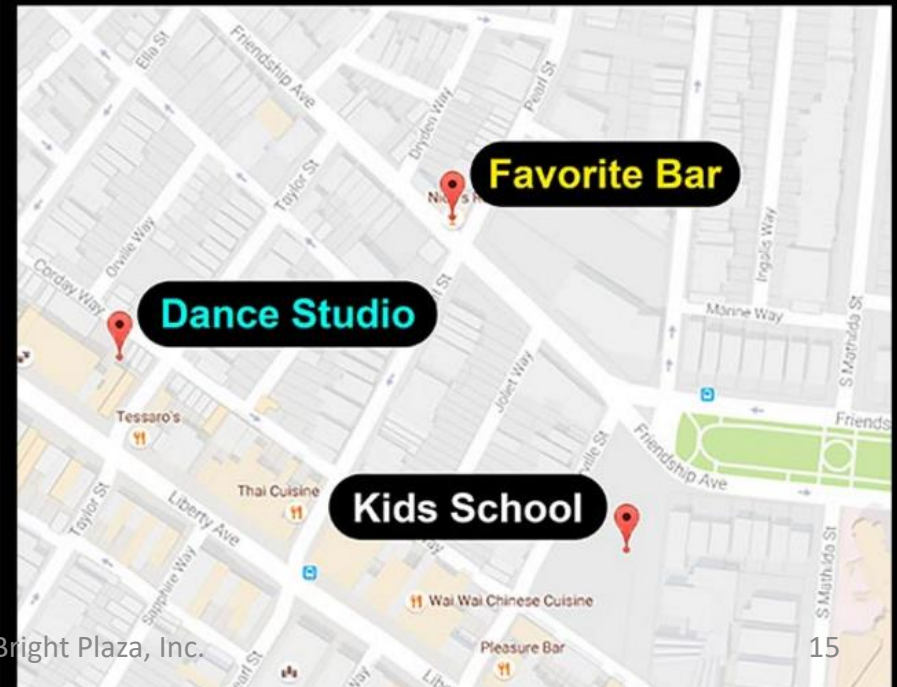
from [www.drivetrust.com/autoerase](http://www.drivetrust.com/autoerase)

Do you want others to know the stuff that  
your car knows?

## FLEET AUTO



## FAMILY AUTO





# Other Family Use Cases

- HAV 3+ that can Listen to your voice can listen to passenger voices, so must recognize who is talking (your 13 year old screaming “STOP!”)
- Do you really want the person who buys your car to be able to find out what happened in the back seat, and who it happened with, for the last 10 years?



# What's in the Cloud

**WOW!**

- **All Cars today** have Cryptographic Certificates (X.509) that **ID the car** and **ID the manufacturer** (software updates).
- **Plaintext Data in the Cloud** needs to be enough to provide network applications, with real-time and historical data:
  - Advertisements (upsells, like Ludicrous Mode)
  - App Stores (upsells)
  - Manufacturer Monitoring (to improve your experience...)
  - Legal Records (Insurance Proof)
- **Car Restore Functionality**
  - New Car gets old car's brains about you, your family or you, your company

# Thibadeau's HAV Laws

- A Car is a **Supersized Smart Phone that carries you**, instead of you carrying it.
  - HAV Privacy is vastly more an issue than a lawyer writing a privacy policy. (See [www.drivetrust.com](http://www.drivetrust.com) Privacy comments on NHTSA HAV Guidelines 2016)
- When **cars can listen and understand** (people, roads, cars, and the cloud), ***and then act***, **privacy sensitive information becomes supersized too.**

# Thibadeau's Family and Corporation Privacy Technology

- **Your car 'key' should unlock your user data and all the current passenger user data.** Like the iPhone – Hardware Encryption Locked/Unlocked
- **Your car web site should let you sell or repurpose your car by cryptographically erasing** all current user/passenger knowledge.
- **Your car web site should let you download your last car's knowledge** from your old car while preserving the privacy of that knowledge.

# DTA Comments on NHTSA Privacy Policy

***Repurposing a Vehicle*** – When a vehicle is repurposed, all individual or organizational data about owners, drivers and passengers should be cryptographically erased, like the iPhone.

***Multiple Drivers*** – In a vehicle with multiple drivers, only the personal information of the person driving, and the people riding, should have their data cryptographically unlocked for reading and writing, like the iPhone.

***Central Management Privacy Assurance*** – A remote, cloud privacy manager is essential. This way the HAV can be proven to have been protected even if it is stolen or otherwise lost, like the iPhone.

# Supply Chain Assurance Proposed Requirement

- Self-Encrypting Drives (Non-Volatile Storage Devices) should be required for Supply Chain Assurance.
  - Industry Standard Interface to Device Required (Trusted Computing Group, Storage Workgroup, Opal, Enterprise, or other approved Standard.
  - Encryption in Industry Standard Self-Protecting Hardware simplifies assurance immensely
  - Allows law enforcement a known device where privacy sensitive data is protected
  - Already all Smart phones...but proprietary interfaces

A Car is a **Supersized Smart Phone**  
**that carries you**, instead of you  
carrying it.

...and all that implies...

“Speaking to Vehicular/IoT Technology  
Listening” Robert Thibadeau, 2016

**Thank You!**

[rht@drivetrust.com](mailto:rht@drivetrust.com)