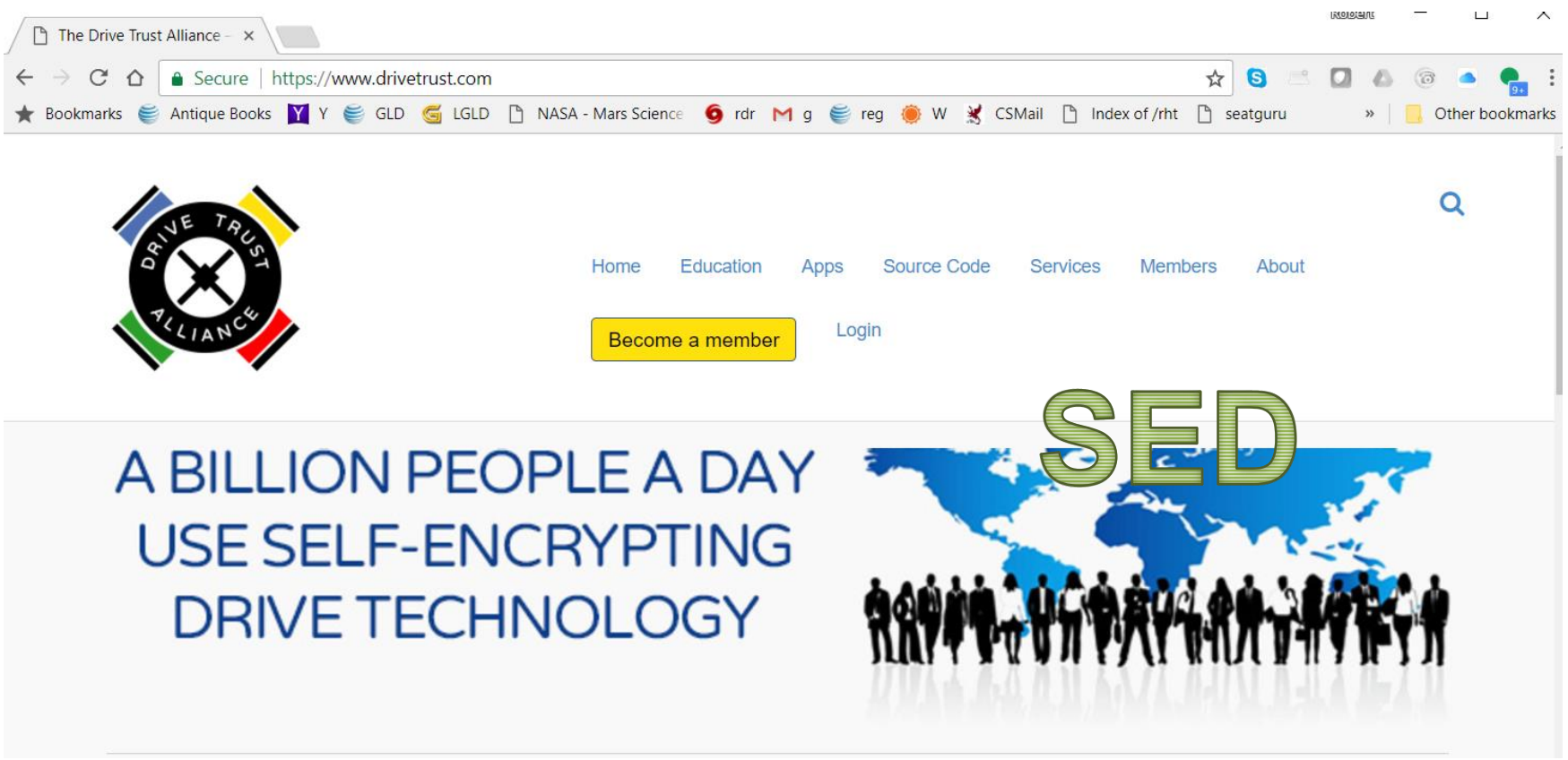

# Privacy "Invations" for Connected and Automated Vehicles

**Robert Thibadeau,Ph.D.**
School of Computer Science
Carnegie Mellon University
&
Chairman & CEO
Bright Plaza, Inc.. aka
Drive Trust Alliance (DTA)
**www.drivetrust.com**

Talk to AV17 Autonomous Vehicles Detroit
Thurs, Aug 26, 2017




**Every Non Volatile Memory Maker in World** makes Industry Standard Self-Encrypting Drives

Intel, Western Digital, Seagate, Micron, Samsung, SK Hynix, Toshiba, San Disk, etc. etc. etc.

**100% of Google, Amazon, eBay, Facebook, etc. etc., Cloud data centers use Self-Encrypting Drives**

(Same use cases are for Automotive)

# Except… not SAE Drives…Yet

Bright Plaza, Inc.. aka

Drive Trust Alliance (DTA)

**www.drivetrust.com**

**Business is to increase Adoption to billions more people**

**For their Personal or Corporate Privacy Protection**

**We are the experts who know the Storage Device Makers**

**And how to get them to make SAE drives Self-Encrypting**

Talk to AV17 Autonomous Vehicles Detroit
Thurs, Aug 26, 2017

# 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

Also with our comments on Privacy Mistake (also at www.drivetrust.com/)

# NHTSA HAV Guidelines

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

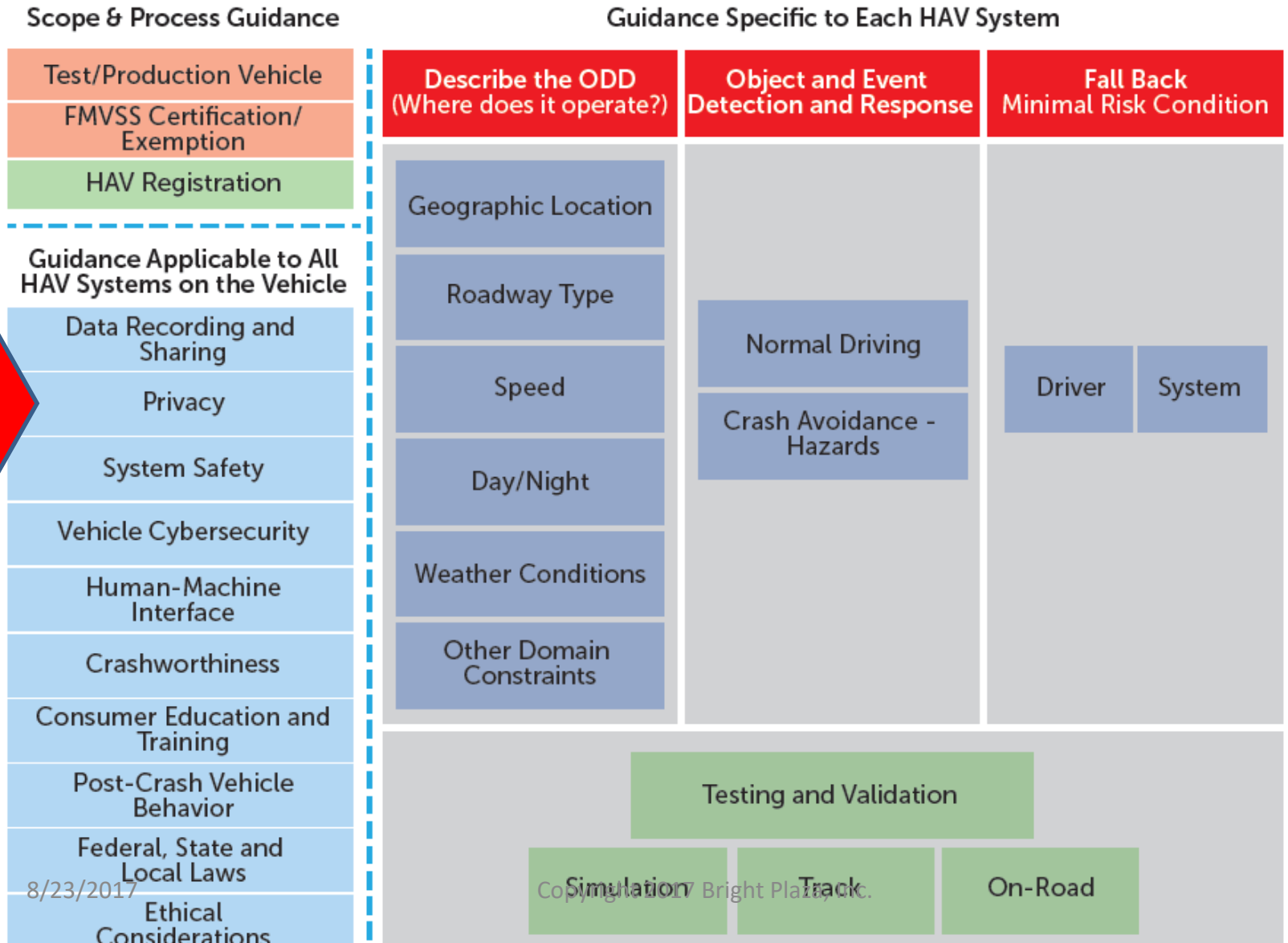
- **6 Levels of HAVs** (from nearly no automation to full automation) from SAE
- **10 Areas of Safety Concern** (mapped to different levels) from NHTSA

EOS (End of Story)

# 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



# 4 Privacy Invations

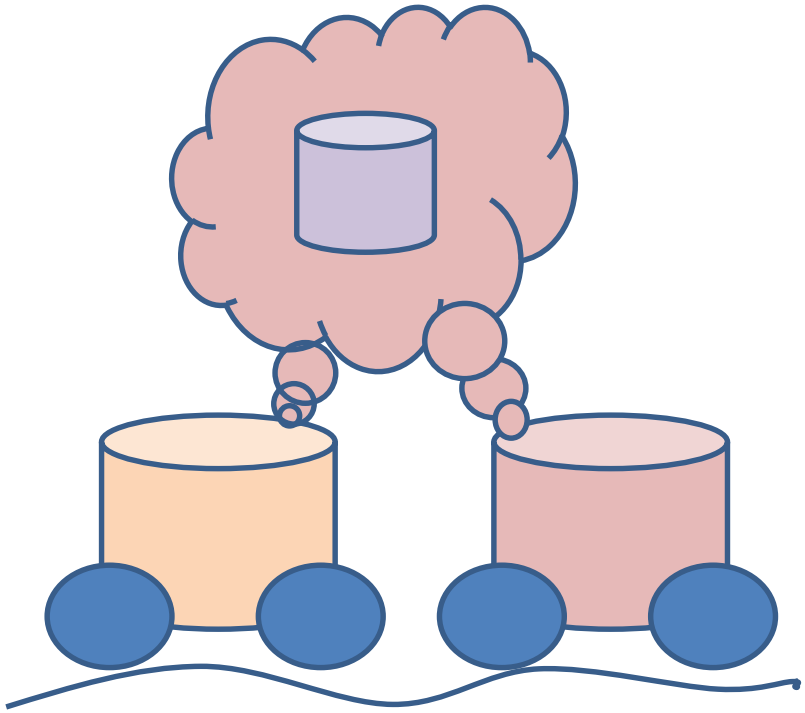
"Invation" = Invasion Invitations

Inside Car

Car to 'Road'

Car to Car

Car to Cloud



# HAV Privacy Design 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 Privacy comments on NTSHA HAV Guidelines 2016)
- When **cars can listen and understand** (people, roads, cars, and the cloud), ***and then act***, **privacy sensitive information becomes supersized too**.

# Where's the Data? Inside CAR

 = Machine Learning /AI

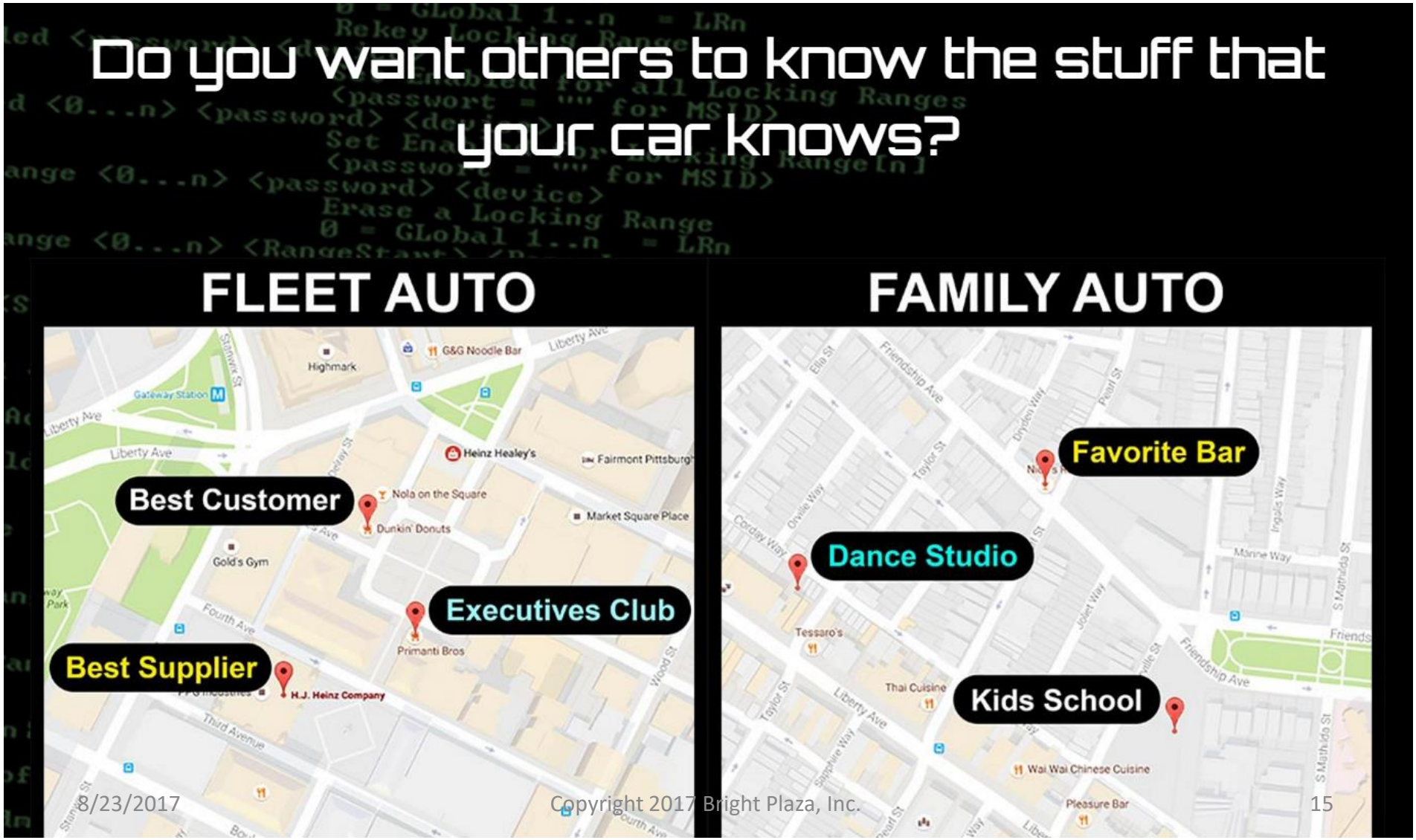
- ADAS (Advanced Driver Assist System)
  - GPS (Locations)
  - Infotainment
  - Human Interactions
  - Automated Vehicle Systems (e.g., Cars ahead, Behind, Beside, MPG, EV History)
  - Video – Audio Recording
- Trackers (Insurance)
- Engine (Mileage, Wear, Power)
- Black Box (Law, Accidents, Insurance)
- Smart Sensors (Raindrop, Predictive Road Slickness)
- Network Logs

# Family or Corporate 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?

# GPS Memory…

from www.drivetrust.com/autoerase



# Family and Corporation Privacy Technology
## (just like an iPhone or Google's Data Centers)

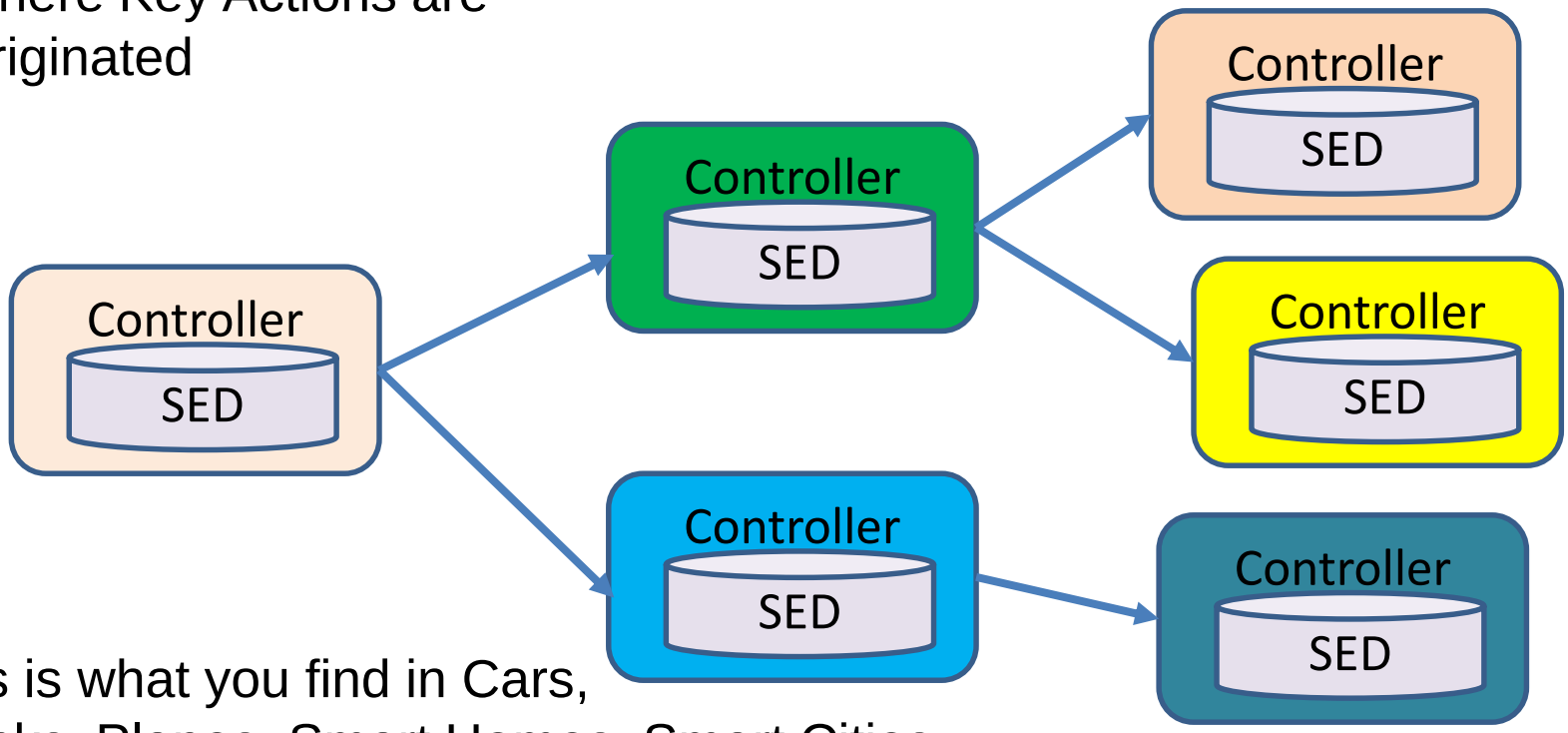
- **Your car web site should let you sell or repurpose your car by cryptographically erasing** all current user/passenger knowledge.
- **If your car crashes, nobody should be able to get the data off of it without your permission** – even by removing the memory
- **Your car 'key' should unlock your user data and all the current passenger user data.** Like the iPhone – Hardware Encryption Locked/Unlocked
- **Your car web site should let you download your last car's knowledge** from your old car while preserving the privacy of that knowledge.

# FTC / NHTSA
# Privacy Workshop
# Washington DC, June 28, 2017

NADA Video

# Car compute storage is a Supply Chain "thing" (or try "mess")

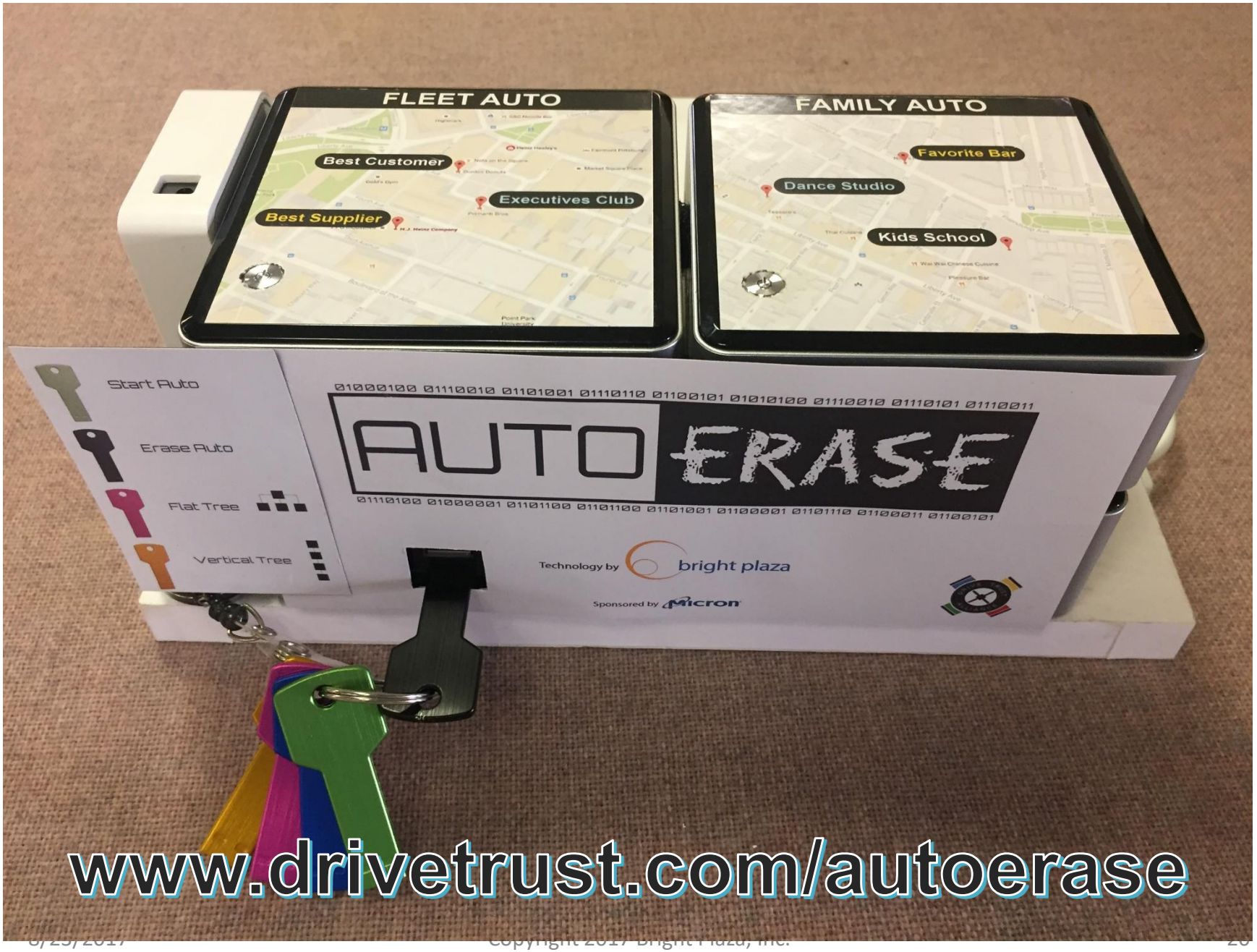
One or More Roots Where Key Actions are Originated




This is what you find in Cars, Trucks, Planes, Smart Homes, Smart Cities, Robots, etc etc etc.

# 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.
  - No new technology – SEDs are already selling in the many millions – There needs to be new glue/intranet key technology
  - 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



# 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.

# A Bit of Flash Info

- Current Automotive Flash is almost exclusively JEDEC e.MMC (e.g., SD cards are this).
- Next generation is called JEDEC UFS (Universal Flash Storage.)
  - REQUIRED to support TrustedComputingGroup.org Commands already, but NOT Yet SED Commands
  - We can work with you to sneak this in (and we believe there need to be some Flash Memory firmware tweaks to make it work well.)

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

**And we can help get the flash memory makers to provide the technology**

# Thanks!

rht@drivetrust.com