JITI Safer Vehicle Seminar:
Advanced Automotive Safety Technologies

Policy Considerations for the Connected Vehicle

Scott J. McCormick
Connected Vehicle Trade Association
March 20, 2013

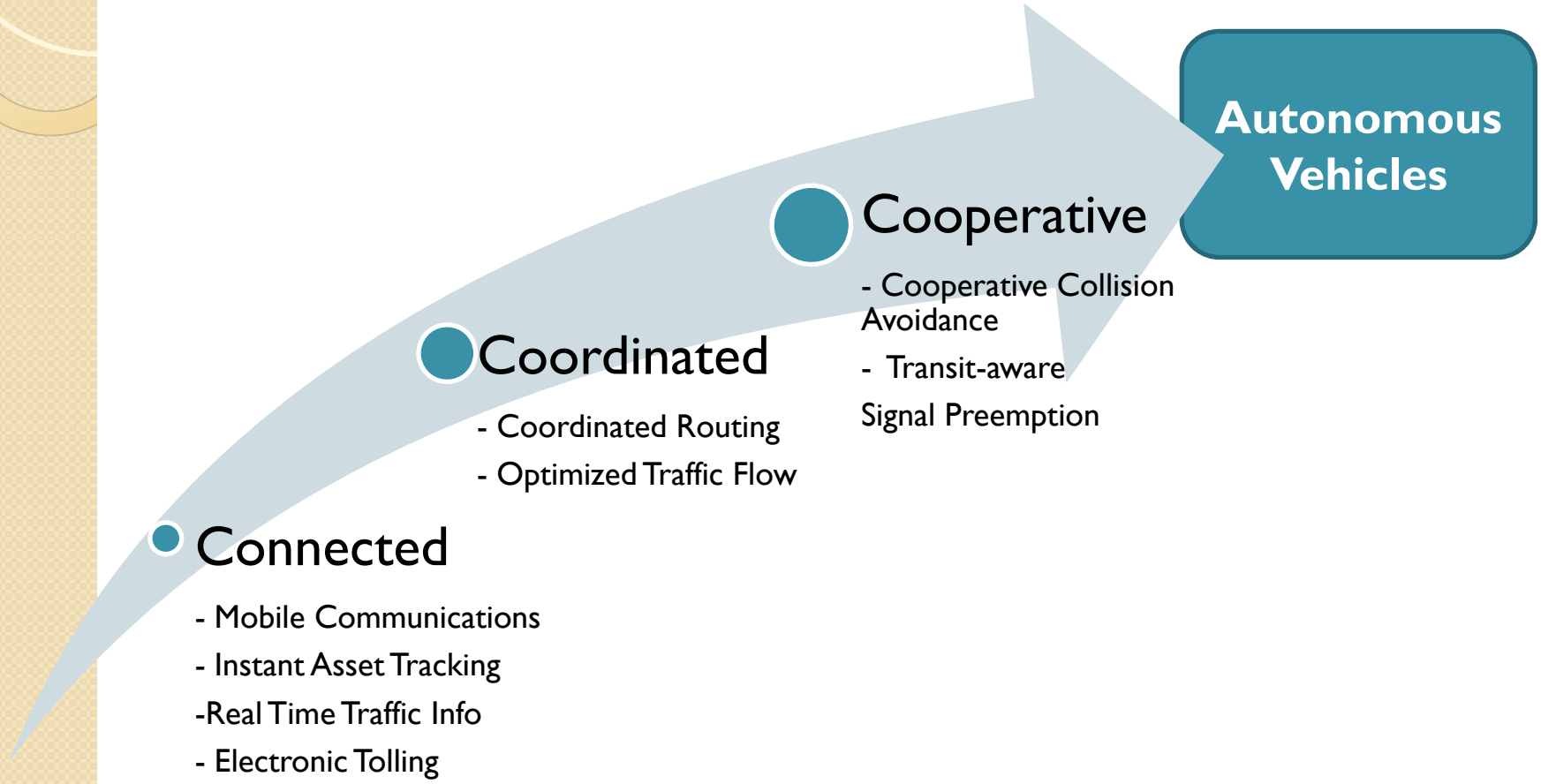
Scott J. McCormick, President
Connected Vehicle Trade Association

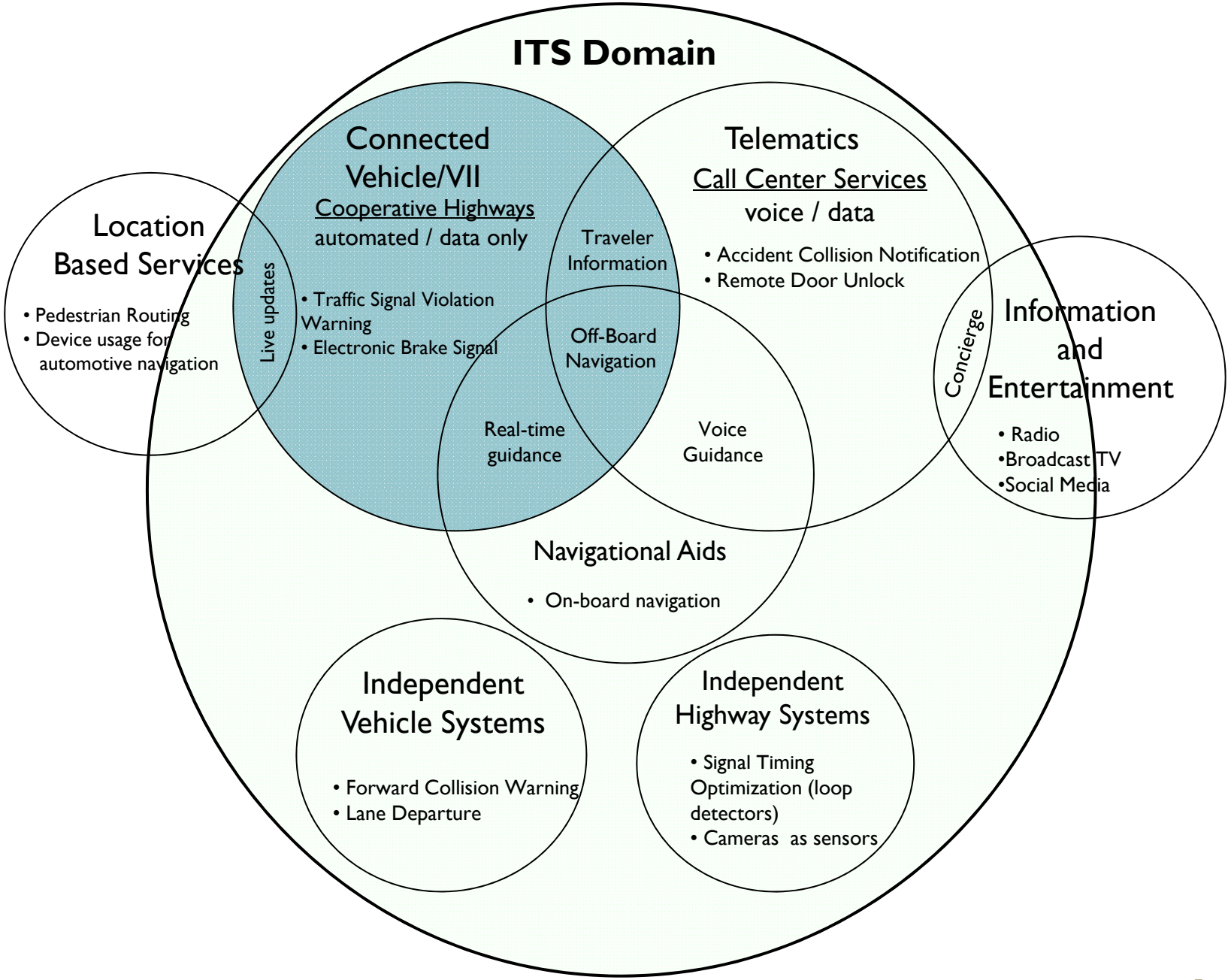
- Scott has degrees in Mathematics, Mechanical and Aerospace Engineering, a Master's in Business Administration, and Doctoral Research in Artificial Intelligence.
- Prior to being the President of the Connected Vehicle Trade Association, Scott was the Executive Director of the Automotive Multimedia Interface Collaboration, a nonprofit research organization of the world's largest automakers.
- Scott is a former Advisor to the United States National Science Foundation and the Industrial Sector Representative to the US Federal Laboratories Technology Transfer Consortium.
- He is as a Member of the Steering Committee to the Joint Commercial-Military Technology Transfer Committee
- He is a member of Advisory Board of University of California, Berkeley's Transportation Sustainability Research Center (TSRC).
- In March 2012, Scott was appointed by the United States Congress to advise the Secretary of Transportation on matters relating to the study, development, and implementation of Intelligent Transportation Systems.

What are the Fundamental Issues?

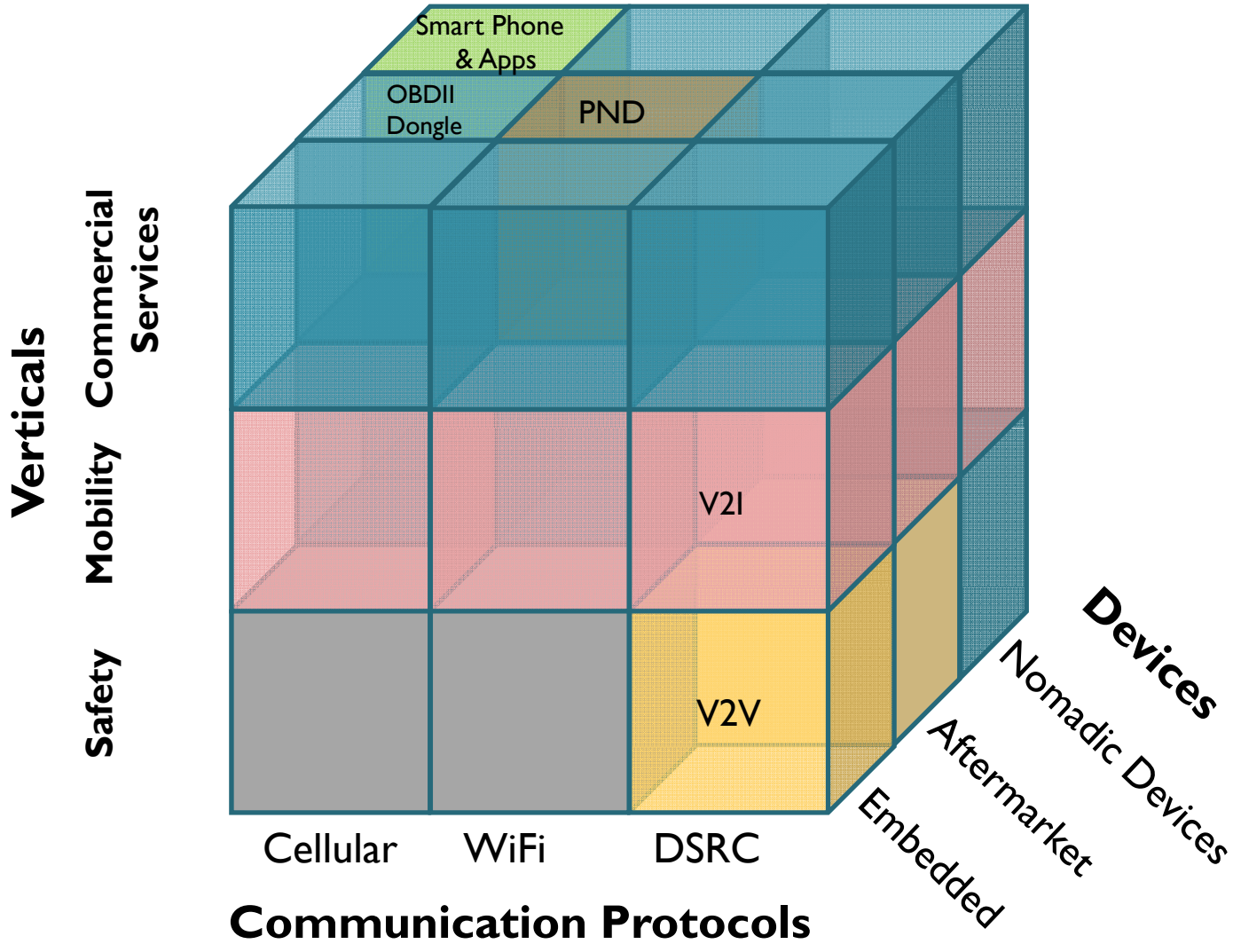
- The Ecosystem
- Government Policy and Regulation
- Distraction
- Liability
- Privacy
- Data Ownership
- Addenda
  - Security
  - Spectrum Use

Evolution to Autonomous Vehicles





Connected Vehicle Ecosystem



Government Policy and Regulation

- The regulatory challenges presented by connected vehicle technologies are unique and unprecedented in the highway vehicle context.
- The two DOT agencies principally involved in regulating vehicle safety are the National Highway Transportation Safety Administration (NHTSA) and the Federal Motor Carrier Safety Administration (FMCSA).
- NHTSA's broad enforcement authority, including recall authority, extends to vehicles in use, the agency regulates the safety of new vehicles and original equipment through its rulemaking authority, primarily mandatory Federal Motor Vehicle Safety Standards (FMVSS)
- FMCSA is authorized to prescribe commercial vehicle usage requirements, including vehicle operator requirements (e.g., hours of operation, substance abuse requirements, etc.).

Distraction

- States that enacted no-texting laws saw the incidence of crashes increase (largely due to below-the-dash texting)
- Outlawing all cell phone use is a non-starter:
  - Talking to the person next to you is just as distracting as a phone call.
  - Most OEMs are looking at tethering phones as a 'carry-in' transceiver
- The HMI of the vehicle is diametrically opposite the user interface of the phone

Distraction Policy and Regulation

- A policy is a principle or rule to guide decisions and achieve rational outcomes.
- Laws already exist to punish driving behavior (crashes, speeding, failure to yield, reckless endangerment, drunk driving, etc.)
- Penalties for distracted driving must scale against the severity of the incident as existing laws do for driving behavior.
- Currently the average fine for littering is four times the fine for texting while driving.

Liability Overview

- Generally governed by state law; vary widely – claims, defenses, evidentiary rules differ
- Strict liability – relies on existence of defect
- Negligence – exercise of due care
- Failure to warn – may be strict liability or negligence
- Breach of implied warranty (fitness, merchantability)
- All of the above impact connected vehicles.

Liability Issues

- Major vehicle safety technologies typically have been available and in use on new vehicles – sometimes for years - before they have become mandatory safety standards.
- Therefore, the decision, whether by Congress or DOT, to require these systems has essentially been aimed at taking a proven safety technology and expanding its existing use across the new vehicle fleet.
- The decision to regulate connected vehicle technologies presents a contrasting situation in which the regulatory decision likely will be based on proof-of-concept and pilot projects, rather than incorporating a safety technology already in use into a mandatory standard.

Key Liability Policy/Legal Questions:

- Adequacy of existing laws to address potential failures?
  - Federal Tort Claims Act, State Laws
- Guidance from existing cases of warning system or navigational failures?
  - Motor vehicles, aviation, rail/transit, maritime
  - Expanded experience base
- Protections based on governmental linkage (e.g., immunities, indemnification, limitations of actions/remedies, etc.)?
- Rather than building a Policy and Regulation framework based on data ownership, we would be better served by building one based on authority, rights, and responsibilities.

Data Ownership

- A typical car can generate up to an exabyte of data a year (1 billion gigabytes)
- Almost all of the data is used by the car's internal systems for engine management, steering and braking, command and control of subsystems, etc.
- Event triggered data management is also a major concern for OEMs.
- Very little of the data is attributable to your travels, driving behavior or other personal information.
- Isolating useful data to extract knowledge from is a monumental task.
- Transaction data has dual ownership.

Data Ownership Policy Issues

- Automakers differ widely on what data the vehicle owner have rights too.
- Consumers vary even more widely on what information they do or don't want.
- Accessibility to the data is difficult, may void warranties, and is not generally human-readable.
- The raw data is rarely useful, although the derived knowledge can be.
- The issue isn't "How do we keep data from bad people," it's "How do we keep people from doing bad things with data?"

Privacy

- U.S. Federal Trade Commission (FTC) published the Fair Information Principles in 1995 which provided a set of non-binding governing principles for the commercial use of personal information.
  - While not mandating policy, these principles provided guidance on how to draft privacy policy.
- Privacy, at both the Federal level and the State levels, is regulated by specific industry and type of use:
  - Banking Information, Credit Card transactions, phone records, HIPPA, internet usage, etc.

Privacy Policy and Regulation Issues

- There are a number of fundamental questions that must be answered first:
  - What data?
  - Who owns it?
  - What about meta data?
  - How will you handle dual ownership?
  - Should a car owner have rights to 'see' car data he doesn't have rights to (OEM data like diagnostics, performance, etc.)?
  - Why should my car have a different privacy policy and regulation than my phone or internet connection, cable or marine radio?

Conclusion

- To maximize the potential of USDOT's Connected Vehicle program and achieve an optimal ITS ecosystem that supports safety, mobility, increased transportation efficiency, and environmental applications, we must have a clear and implementable ITS privacy and security strategy which harnesses both connected and autonomous technologies.
- Our ITS strategy must include technical and policy solutions, namely a fully secured connected vehicle network and adequate consumer privacy protections that evoke trust from drivers and passengers traveling on U.S. roads and highways.

Scott McCormick

51037 Weston Drive

Plymouth, Michigan USA 48170

Bus: +1.734.354.0546

Fax: +1.734.446.0326

Cell: +1.734.730.8665

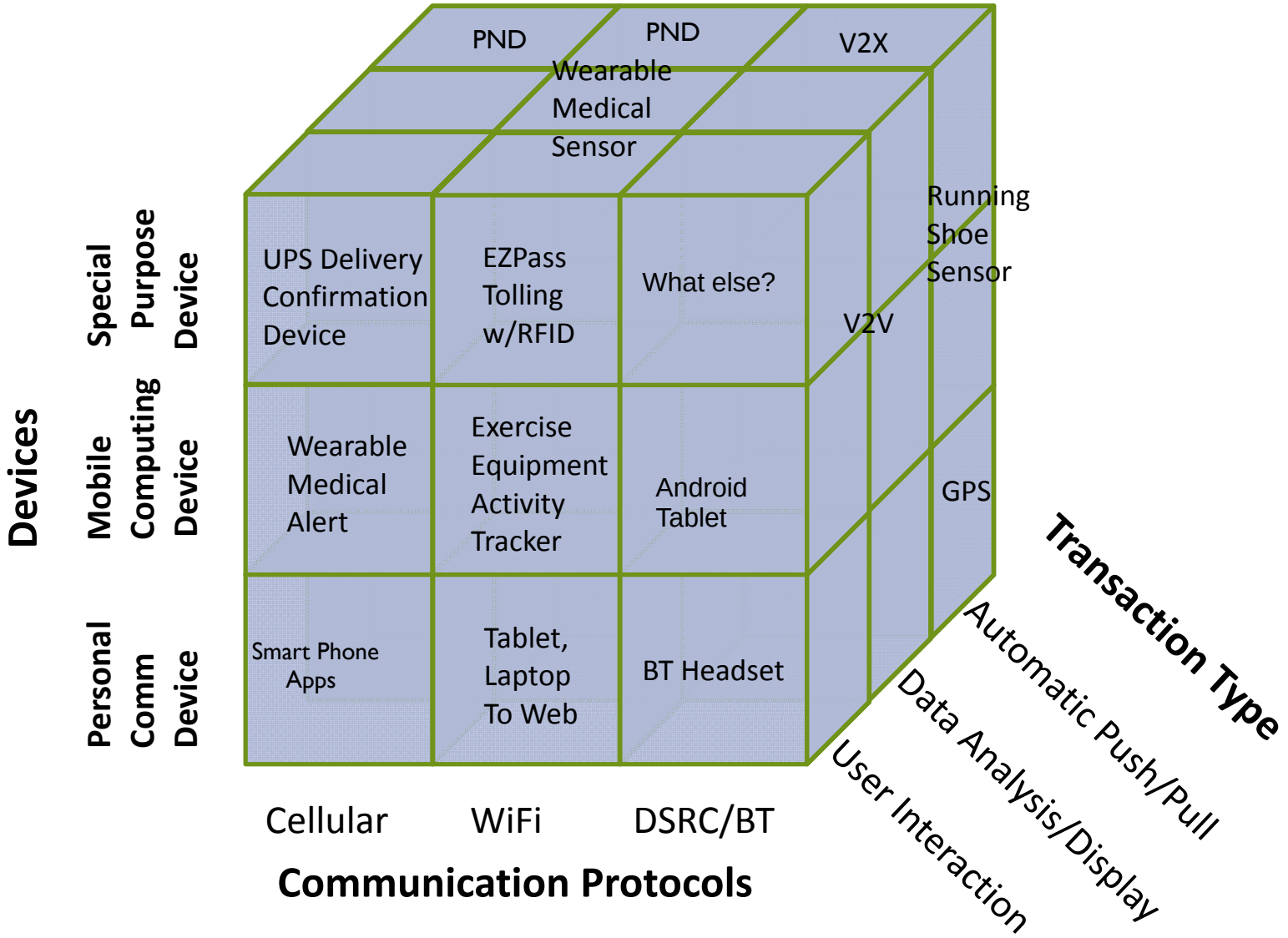
Skype: scott.j.mccormick1

sjm@connectedvehicle.org

www.connectedvehicle.org

ADDENDA

Mobile Ecosystem



Security

- The auto industry and federal government have spent years and millions designing protection for the DSRC communication link from the car to the world.
- There is a major program now with NHTSA and the US DOT/Volpe Center to address Cybersecurity of Automotive Safety-Critical Electronic Control Systems (CYBER).
- Without the internet analogy of server-side security, there is a huge risk with any near term in-vehicle deployment of apps.

Security Issues

- UC San Diego inserted malware on a CD.
  - This was put it in a car with a cell connection, and infected it.
  - It then infected other cars in its directory.
  - The researchers were then able to control the infected vehicle's functions via a cell phone, remotely.
- With the advent of third part apps and downloadable content, a fundamental concern now is how to protect the vehicle's data, apps and content from corruption, unapproved access and malicious intent.

Spectrum Use

- At present, Dedicated Short Range Communication (DSRC) is the only viable communication protocol for vehicle safety messages.
- The FCC is considering reevaluating use of that spectrum for unlicensed WiFi devices.
- LTE and 4G are now being tested to see if the latency is low enough to accommodate safety messages.
- The US DOT Safety Pilot is determining the viability of the DSRC spectrum for vehicular use.
- Research is needed to see if other licensed forms of WiFi devices can cooperatively share the spectrum.

What I think will happen

- Distraction – Too many special interests for a broad regulation, so the punishment should fit the crime.
- Liability – OEMs will protect themselves, existing laws are adequate.
- Data Ownership – OEMs will decide who gets what, but can't prevent others from getting it.
- Privacy – We give up a lot of privacy to use a cell phone, because we place a high value proposition on it. The real question should be are we giving up any more data, and how can it be used?
- Security – We can penalize bad behavior, but will never solve the problem.
- Spectrum Use – Groundswell of objections to sharing DSRC with unlicensed devices will protect the spectrum for the time being.