Autonomous Vehicles:
Navigating the legal and regulatory issues of a driverless world
Table of Contents

Introduction
- SAE Levels
- Physical Ecosystem
- Strategic Partnerships

Legal Issues
- Regulatory
- Product Liability
- Cybersecurity and Data Privacy
- Intellectual Property

Case Study
- Keolis – AVs in Public Transportation
Introduction
Introduction

- **10 million** autonomous vehicles will hit the roads by 2020
- **In 10 years** fully autonomous vehicles will be the norm
- AVs will generate a **$7 trillion** annual revenue stream by 2050
- Widespread adoption of AVs could lead to a **90% reduction** in vehicle crashes

Sources:
https://www.cnbc.com/2017/06/01/the-7-trillion-promise-of-self-driving-vehicles.html
History of Autonomous Vehicles

- **1948** - Introduction of Cruise Control
- **1999** - FCC allocates 75 MHz of spectrum to Dedicated Short Range Communications
- **2007** - Teams create vehicles that self-navigate a 60-mile course as part of DARPA "Grand Challenge"
- **2009** - Google begins self-driving car project
- **2012** - Google's autonomous car passes a 14-mile driving test in Nevada
- **2009** - Google begins self-driving car project
- **2015** - Tesla releases its Auto-Pilot self-driving mode
- **2013** - Mercedes and Infiniti produce cars with radar sensors and some autonomous driving features
- **2013** - NHTSA releases initial policy on autonomous vehicles
- **2015** - Uber hires 40 Carnegie Mellon robotics researchers to work on autonomous vehicles; Ford begins testing its self-driving cars in CA, AZ, MI
- **2015** - Google's autonomous car passes a 14-mile driving test in Nevada
- **2016** - Major acquisitions and partnerships (GM and Cruise Automation; GM and Lyft; Toyota and Jaybridge Robotics; Uber and Volvo)
- **2016** - NHTSA issues guidelines for testing and deployment of autonomous vehicles
- **2016** - NHTSA issues revised safety guidelines for autonomous vehicles
SAE Levels of Automation

Source: https://www.nhtsa.gov/technology-innovation/automated-vehicles-safety
Basic Physical Ecosystem of an Autonomous Vehicle

- Global Positioning System (GPS)
- Light Detection and Ranging (LIDAR)
- Cameras (Video)
- Ultrasonic Sensors
- Central Computer
- Radar Sensors
- Dedicated Short-Range Communications-Based Receiver (not pictured)

Source: The Economist, “How does a self-driving car work?”
Key Physical Components of Autonomous Vehicles

• **Cameras** – Provide real-time obstacle detection to facilitate lane departure and track roadway information (like road signs).

• **Radar** – Radio waves detect short & long-range depth.

• **LIDAR** – Measures distance by illuminating target with pulsed laser light and measuring reflected pulses with sensors to create 3-D map of area.

• **GPS** – Triangulates position of car using satellites. Current GPS technology is limited to a certain distance. Advanced GPS is in development.

• **Ultrasonic Sensors** – Uses high-frequency sound waves and bounce-back to calculate distance. Best in close range.

• **Central Computer** – “Brain” of the vehicle. Receives information from various components and helps direct vehicle overall.

• **DRSC - Based Receiver** – Communications device permitting vehicle to communicate with other vehicles (V2V) using DSRC, a wireless communication standard that enables reliable data transmission in active safety applications. NHTSA has promoted the use of DSRC.
Companies Investing in Autonomous Vehicles

Vehicles operating in SAE levels of automation 1-3 are already in commercial use and many companies are investing further in developing highly and fully automated vehicles.
Strategic Partnerships
Recent Developments

• January 2017 – Keolis and NAVYA, in partnership with the city of Las Vegas, launched the first autonomous, fully electric shuttle to be deployed on a public roadway in the United States.

• January 2018 – Toyota announces “e-Palette” concept vehicle which is a fully electric autonomous vehicle that can be customized by a partner for applications such as food deliveries (Pizza Hut), ride-sharing (Uber), or store fronts (Amazon).

• January 2018 – Udelv, a Bay Area tech company, completed the first delivery of goods by a self-driving car when it delivered groceries in San Mateo.

• February 2018 – Hyundai announced that a fleet of its fuel cell electric cars made a successful fully automated trip from Seoul to Pyeongchang. This is the first time a Level 4 car has been operated with fuel cell electric cars.
Legal Issues Around Autonomous Vehicles

- Regulations
- Liability
  - Personal Injury
  - Cybersecurity and data breaches
  - Intellectual property ownership
Federal and State Regulations
Federal Regulation of Autonomous Vehicles

Federal Motor Vehicle Safety Standards

- The National Highway Traffic Safety Administration (NHTSA) within the Department of Transportation (DOT) specifies minimum safety performance requirements for motor vehicles and equipment. Automakers must certify compliance before selling vehicles.

- Fully autonomous vehicles (and some highly autonomous vehicles) would not meet current Federal Motor Vehicle Safety Standards (FMVSS) (i.e., if manufacturers seek to design vehicles without mirrors, bumpers, braking pedals, and other features required by the FMVSS).

- NHTSA can approve a limited number of exemptions from the FMVSSs.

- NHTSA also can approve importation of autonomous vehicles that do not meet FMVSSs for testing, subject to conditions.
Federal Regulation of Autonomous Vehicles


• Guidance identifies 12 safety elements: (1) system safety; (2) operational design domain; (3) object and event detection and response; (4) fallback (minimal risk condition); (5) validation methods; (6) human machine interface; (7) vehicle cybersecurity; (8) crashworthiness; (9) post-crash ADS behavior; (10) data recording; (11) consumer education and training; and (12) federal state and local laws.

• Recommends that entities involved in ADS testing and deployment demonstrate how they address the 12 safety elements by publishing a Voluntary Safety Self-Assessment.
Federal Regulation of Autonomous Vehicles

• NHTSA, the Federal Highway Administration (FHWA), and the Federal Transit Administration (FTA) have sought comments related to autonomous vehicles
  • NHTSA requested comments on regulatory barriers to Automated Safety Technologies, and testing and compliance certification
  • FHWA requested comments on what is needed to accommodate ADS technologies and maximizing their potential benefits in the transportation network
  • FTA requested comments on current and near-future status of automated transit buses and related technologies, with the goal of informing FTA’s efforts to promote development of ADS in the public transit sector
• Deadline for filing all comments was March 5, 2018
Federal Legislation Governing Autonomous Vehicles

• Congressional efforts underway to amend current law regarding regulation of autonomous vehicles

• House and Senate bills have similar objectives:
  • Authorize NHTSA to issue more exemptions from FMVSSs (up to 100,000 vehicles per year within three years after enactment)
  • Require NHTSA to update FMVSSs to accommodate autonomous vehicles;
  • Require mandatory safety assessment reporting of the elements similar to those in DOT’s voluntary safety assessment report
  • Include cybersecurity and privacy requirements
  • Preempt state regulation of safety but preserve state role to regulate licensing, registration, insurance, and other traditionally state functions

• House passed its bill in late 2017

• Senate bill is on hold while senators work through issues regarding privacy, cybersecurity and safety
State Laws Governing Autonomous Vehicles


- 10 additional states have executive orders in place issued by their governors relating to autonomous vehicles (Arizona, Delaware, Hawaii, Idaho, Maine, Massachusetts, Minnesota, Ohio, Washington, and Wisconsin).

- Arizona, California, Florida, Michigan, and Nevada have been most active.

Product Liability
Liability for Autonomous Vehicle Accidents

• Will courts treat autonomous vehicles as drivers and apply a negligence standard or as sophisticated technology and apply a product liability standard?

• How will liability be apportioned?
  • Fleet Operator/Service Providers
  • Vehicle manufacturers
  • Technology companies/software manufacturers
  • Local government’s responsible for maintaining infrastructure
Florida, Michigan, Nevada and the District of Columbia shield manufacturers from liability for damages resulting from third party conversion of vehicle into autonomous vehicle, except where damages are caused by defect present in vehicle as originally manufactured.
Managing Liability Among Parties

• Warranties and indemnifications should clearly define scope, responsibility and liability
• Responsibility for maintenance, repairs and updates should be defined
• Liability between automaker, technology company and vehicle owner/operator should be defined
• Responsibility for compliance with federal, state and local laws and regulations should be defined
Cybersecurity
Potential Attack Gateways

- Electrical Control Units (ECUs)
  - Airbag, Advanced Driver Assistant System, Engine, Steering & Brakes, etc.
- On-Board Diagnostics (OBD) II Diagnostic Port
- Dedicated Short-Range Communications-Based Receiver
- USB Ports
- Passive Keyless Entry/ Remote Key
- Remote Link Type App
- Tire Pressure Monitoring System (TPMS)

Explanation of Key Attack Gateways

• **Electronic Control Units (ECUs)** – ECUs are embedded systems that control one or more electrical systems or subsystems within a vehicle and are connected via an internal network. They control systems like the engine and transmission, steering and brakes, infotainment, lighting, etc. Risks arise when access to ECUs (usually peripheral ECUs like an infotainment system) are breached and malicious actors are able to access certain ECUs or the whole network. Vehicles today have up to 100 ECUs onboard.

• **OBD II Diagnostic Port** – Every car manufactured after 1996 and sold in the U.S. must have an OBD II installed. The port was originally mandated to permit monitoring of emissions, etc. It is increasingly used to facilitate non-diagnostic features like enabling Wi-Fi, or enabling an insurance company to track usage through attachment of a “dongle” to the port. These ports can provide a means of access for attackers into an otherwise secure system.

• **DSRC-Based Receivers** – DSRC is being promoted as a means of encouraging V2V and vehicle-to-infrastructure (V2I) communications. The short-wave communications can be subject to spoofing and other attacks. There’s now a push to move to more advanced 5G-based communications.
Common Security Vulnerabilities

- **Software Glitches** – Connected vehicles today contain more than 100 million lines of code. More code means more opportunity for bugs and mistakes. Glitches, even when inadvertent, can be exploited.

- **No Single Source of Knowledge of or Control Over Source Code** – Software for different components of connected vehicles is being written by different developers, installed by different supplies, and no one source has knowledge of or control over the source code.

- **Increase Use of Apps Leave Vulnerabilities** – Consumers are using an increasing number of smartphone apps to interface with their connected cars and help run certain functions. Researchers have already demonstrated weaknesses in some of these apps. Likely to see spread in use of malware.

- **Need for Constant Updates May be Overlooked** – With the increased use of connected features comes an increased need for continuous updates to fix glitches and help protect vehicles. There is a risk these updates could be overlooked or that malicious actors could infect routine updates.
Cybersecurity Threats and Concerns

• The same types of attacks that are possible in any connected device are generally possible in connected vehicles once access is gained.

• For example – Denial-of-service (DoS) attacks (e.g., utilizing the Controller Area Network (CAN) Bus system), remote access and control (e.g., the 2015 Jeep event), man-in-the-middle (MiM) attacks, etc.

• The difference between attacks like these against common IoT devices and attacks within a connected or autonomous vehicle is the likelihood for increased risk to life and property in the vehicle context.

Source: CNN: Jeep remotely carjacked, shut down on highway

The 2015 white hat attack on a Jeep Cherokee led to the recall of 1.4 million vehicles and highlighted risks.
Consumers Desire and Fear Connectivity

In 2014, McKinsey conducted a survey of 2,000 new-car buyers in Brazil, China, Germany, and the U.S. about connected car issues. The survey remains interesting for the disjoint it highlights between consumer desire for connectivity and consumer fear of the possibility of attacks as a result of that connectivity.

- 13% of car buyers are no longer prepared to even consider a new vehicle without Internet access.

- More than ¼ of car buyers now prioritize connectivity over features like engine power and fuel efficiency.

- 45% of U.S. car buyers are reluctant to use car-related connected services because they want to keep their privacy.

- 43% of U.S. car buyers are afraid that people can hack into their cars and manipulate the systems if the car is connected to the Internet.

Key Regulator – Dept. of Transportation and National Highway Traffic Safety Administration

• The key regulator with regard to cybersecurity and safety concerns is NHTSA

• NHTSA has incorporated the National Institute of Standards and Technology’s (NIST) Cybersecurity Framework as part of the multi-layered approach it recommends for vehicle cybersecurity

• NHTSA works closely with the Federal Trade Commission (FTC) on issues related to consumer privacy in connected and autonomous vehicles, but its mandate is safety
Litigation Risks – Cybersecurity

• Car manufacturers that release vehicles later found to contain defects and cybersecurity vulnerabilities, along with the suppliers that provide flawed subparts, could face significant lawsuits in the U.S. and elsewhere.
  
  • In 2015, after Chrysler recalled the Jeep Grand Cherokee to fix a flaw highlighted in the dramatic hack of the vehicle, the company and Harman International, maker of the flawed Uconnect dashboard computer, faced a high-stakes consumer lawsuit.
  
  • The recent flurry of lawsuits against Apple, Intel, and others in connection with allegations that they sold defective products containing the Meltdown and Spectre flaws, could be a foretaste of similar actions that could be brought in connection with later-discovered weaknesses within internal networks and systems.

• Manufacturers or suppliers that fail to push timely updates may face regulatory enforcement actions or consumer lawsuits.
  
  • In 2016, Dutch regulators sued Samsung over a lack of consistent updates to its Android-powered phones. The regulator contended that Samsung should be responsible for pushing updates two years after the sale of a phone. There is a possibility similar reasoning could be applied to connected vehicle features.
Key Cybersecurity Takeaways

• **Provide Multi-layered protection** – Beginning at level of individual ECUs, moving up a level to include software to protect vehicle’s internal network by examining all network communications, and building in mechanisms to stop attacks from advancing within network.

• **Defend against externally-facing potential gateways** – Ensure weakest links in car’s security are viewed as potential threats and defenses are built into system. This is particularly true to infotainment or similar externally-facing mechanisms that are developed or utilized by multiple external entities.

• **Ensure vendors and suppliers have strong security** – Connected and autonomous vehicles are made up of subparts and subsystems. It is critical to review and monitor vendor and supplier policies and practices.

• **Promote timely updates** – Companies should push timely and effective fixes as soon as problems are identified.
Data Privacy
Privacy Concerns

“GPS monitoring generates a precise, comprehensive record of a person’s public movements that reflects a wealth of detail about her familial, political, profession, religious, and sexual associations. . . . I would take these attributes . . . into account when considering the existence of a reasonable societal expectation of privacy in the sum of one’s public movements.”

“[I]t may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties. This approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying on mundane tasks.”

Multiple Players are Collecting Data from Multiple Points Within Connected and Autonomous Vehicles

Today's connected technologies are making transportation safer and more convenient. Many new features are enabled by the collection and processing of data. Cars are becoming part of a trusted mobile ecosystem that ensures data flows between a network of carmakers, vendors, and others to support individuals' safety, logistics, entertainment, and security needs. This visual represents devices that may be employed in today's connected cars, as single vehicles will have all of these features but most new vehicles have some. Much connected car data is protected by technical controls, laws, self-regulatory commitments, privacy policies, and other emerging mechanisms or controls.
Common Data Privacy Vulnerabilities

- **Data related to vehicle journeys** – Car makers, app developers, on-board assistance systems, etc. collect data regarding movements of vehicle. Length of time data is kept, who has access to it, and whether consumer has right to opt-out are key issues.

- **Data on consumer habits and preferences** – Data ranging from music preferences, news and radio selections, and other features is being used to target consumers. How this is done and whether consent is obtained will dictate potential ramifications.

- **Data from or related to children** – Collection, use, and storage of children’s data is governed by special rules which should be considered.

- **Differences in regulations between markets** – Privacy regulations vary widely by region and market. For example, the EU is set to implement its groundbreaking data privacy and protection law, the GDPR, this May. The law includes a broad definition of personal information and strict requirements for consent and use and protection of such data. Companies working in the European market need to be prepared.
Key Regulator – FTC

- The FTC has authority to bring actions against companies or individuals that engage in unfair or deceptive acts or practices, including those involving vehicle data privacy and security. The agency uses law enforcement, policy initiatives, and consumer and business education to accomplish its mission.

- As the primary agency with authority over consumer privacy, the FTC has ongoing efforts related to protecting the privacy of consumers who use connected devices, which includes connected vehicles.

- For example, the FTC could use its enforcement authority in appropriate circumstances to bring an action against an automaker that uses a consumer’s data in a way that violates the manufacturer’s stated privacy policies. We have as yet to see the FTC focus on in-vehicle privacy protections, although this may be a coming development.

- The NHTSA released a streamlined version of its automated vehicle policy framework in the fall of 2017. That revised policy does not address privacy issues, leaving governance of privacy in this field largely to the FTC.

- FTC and NHTSA held a joint workshop in June 2017 concerning connected cars, with a particular focus on privacy issues.
Litigation Risks – Data Privacy

• Breach of vehicles’ systems that store consumer data, or breach of manufacturers’ systems containing such data, and the subsequent release of sensitive information may trigger notification obligations under state data breach notification laws and could, in some circumstances, lead to private lawsuits in some states.

• Collection and use of consumer behavior data to facilitate additional marketing efforts could also lead to lawsuits where that data is collected and used in this manner without consent and without informing consumers.

• Data on vehicle location and tracking could lead to increase requests from U.S. or other law enforcement agencies for assistance in locating or tracking suspects in criminal cases. Companies’ responses to such requests could lead to consumer distrust of such tracking features, or could lead to conflicts with law enforcement similar to those taking place regarding iPhone access.
Key Privacy Takeaways

- **Build privacy protections into system designs** – Consumer privacy protection should be considered at each stage of system development and implementation.

- **Obtain consent** – Collection of some forms of consumer information is improper absent consent. Build mechanisms into systems to obtain consent and update consent as necessary.

- **Recognize that children pose special risks** – Collection, storage, and use of children’s data is protected by the Children’s Online Privacy Protection Rule (COPPA) and other laws and regulations.

- **Limit collection of sensitive information** – Collect only such information as necessary and protect what is collected. Do not collect personally identifiable information if not necessary for business purpose.

- **Plan for and be ready to notify consumers in the event of an incident** – Best protection against costly consumer litigation is timely and accurate notification, and having proper policies and procedures in place.
Protecting Intellectual Property
• Industry traditionally occupied by OEMs for 100+ years now includes IP-conscious tech companies

• One obvious way to protect is through patents, but there are some considerations before doing so – is invention hardware or software related?

• Software centric technology companies working with OEMs are leading to increased joint ventures and strategic partnerships

• Give away patents? Tesla has made available limited open source patent pool for electric vehicles
Who Filed the Most Patents?

Automakers are the leaders in autonomous vehicle related patents

Who Leads the Autonomous Driving Patent Race?
Number of worldwide patent filings related to autonomous driving (January 2010–July 2017)

- Bosch: 958
- Audi: 516
- Continental: 439
- Ford: 402
- GM: 380
- BMW: 370
- Toyota: 362
- Volkswagen: 343
- Daimler: 339
- Google: 338

Based on a total of 5,839 patent filings related to autonomous driving
identified and analyzed by the Cologne Institute for Economic Research
Sources: Cologne Institute for Economic Research, WIPO
Who Owns the Most Patents?

- Toyota is the global leader in the number of autonomous vehicle patents with more than 1,400 patents

<table>
<thead>
<tr>
<th>Ranking</th>
<th>Company</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Toyota</td>
</tr>
<tr>
<td>2</td>
<td>Robert Bosch GmbH</td>
</tr>
<tr>
<td>3</td>
<td>Denso Corp.</td>
</tr>
<tr>
<td>4</td>
<td>Hyundai Motor Corp.</td>
</tr>
<tr>
<td>5</td>
<td>General Motors</td>
</tr>
</tbody>
</table>

- Google is the tech company with the most autonomous vehicle patents, but ranks 26th when compared to all companies with autonomous vehicle patents

Areas of Innovation

Figure 1B: Self-Driving Inventions across the Three Main Categories (2010 – 2015, projected)

Source: Thomson Reuters 2016 State of Self-Driving Automotive Innovation
Areas of Innovation

• **Autonomous Driving**: Navigating a vehicle without human input from passengers using sensory (LIDAR), control, and navigation equipment that responds to the environment when traveling.

• **Driver Assistance**: Enhances vehicle systems for safety and improved driving when the driver is in control. Technology includes blind-spot detection, pedestrian detection, lane-departure warnings, intelligent braking, traffic-sign recognition, automatic braking, and adaptive cruise control.

• **Telematics**: Includes telecommunications, vehicular technologies, road transportation, road safety, electrical engineering (sensors, instrumentation, wireless communications, etc.), computer science (multimedia, Internet, etc.), GPS technology, DSRC, V2V, and V2I.

Source: https://www.herrmanandherrman.com/blog/vehicle-vehicle-communication/
Key Technology Areas

• **Artificial Intelligence (AI)** – In order for the AV to operate in a full range of environments with millions of changing aspects that will need to be accounted for, it will require AI, which will allow the base level software to be developed and tested with a self-learning capability.

• **GPS** – These global positioning systems will be a critical link for AV to determine their location as they move.

• **Dedicated short range communications (DSRC)** – The ability for vehicles to communicate with each other (“vehicle-to-vehicle” or “V2V”) and infrastructure (“vehicle-to-infrastructure” or “V2I”).

• **LIDAR** – LIDAR is a radar system that emits a laser in a pattern similar to a rotating radar, only in more discrete and densely-spaced increments. The reflected laser light is used to provide the AV information on the distance for each discrete laser emission.
Sample Autonomous Vehicle Patents

- U.S. Patent No. 9,475,491
  - Titled: Lane Changing for Autonomous Vehicles
  - Directed to a method for changing travel lanes by identifying and accepting a target gap between a pair of vehicles in an adjacent travel lane.

- U.S. Patent No. 9,244,462
  - Titled: Vehicle Trajectory Planning for Autonomous Vehicles
  - Relates to a method for describing the current the state and a goal state of the autonomous vehicle and determining a vehicle trajectory from the current state to the goal state.

- U.S. Patent No. 9,428,163
  - Titled: Autonomous Vehicle Emergency Braking Method
  - Describes a method for autonomous emergency braking in a to avoid or reduce the severity of an accident by measuring the speed of the vehicle during autonomous emergency braking and determining vehicle speed independent of the wheel rotational speeds of the vehicle.
Patent Litigation

• Patent infringement suits
  • Most from non-practicing entities and not true competitor lawsuits
  • Seeing both at the district court level and IPRs recently

• Examples of recent AV related patent suits
  • Quanergy Sys., Inc. v. Velodyne Lidar Inc. (N.D. Cal.)
  • Collision Avoidance Technologies v. Ford Motor Company (E.D. Tex.)
Future Areas of Litigation

- Lawsuits will likely increase once there is a robust autonomous vehicle market to support them.

- The automaker and tech company partnerships will limit the extent some companies get accused.

- The area of patent innovation with the least amount of patents filed are in telematics and is an area likely to be litigated.
Protecting IP – Patents

• Defense Strategies
  • Participate in joint defense groups where possible
  • *Inter partes* reviews (like in Quanergy and CAT case)
  • Potential Section 101 motion for patent ineligibility
  • Assess potential exposure/damages early on

• Licensing Patents
  • Increase standard-essential patent licensing campaigns for connected cars
  • Potential for standard-essential patents in autonomous vehicles but technology is still developing
Protecting IP – Trade Secrets

• Intellectual property for autonomous vehicles may be protected as a trade secret

• Trade secret protection applies to “information including a formula, pattern, compilation, program, device, method, technique, or process”

• DTSA now provides federal cause of action for misappropriation of trade secrets

• Trade Secrets v. Patents
  • Trade secrets can remain a secret and will not be published like patents
  • Trade secrets are protected at time of conception
  • Patents are limited to a 20 year term and trade secrets can last until they become public
  • Trade secrets may require joint venture agreements to keep confidentiality
  • Trade secrets not as appealing for technology that can be reverse engineered
Protecting IP – Trade Secrets

• **Waymo v. Uber Case**
  - Waymo sued Uber for trade secret misappropriation alleging that former engineer took 14K documents
  - Alleged that after Uber acquired the Otto, it used more than 100 trade secrets to develop its Lidar solution

• Case settled in February 2018 for $245 million or .34 percent equity in Uber
Protecting IP – Trade Secrets

• Take reasonable precautions to maintain secrecy
  • Confidentiality agreements
  • Non-disclosure agreements
  • Non-compete agreements or clauses in employment agreements
  • Clearly identify and define trade secrets and continue training employees
  • Stay current and revisit!

• Manage employees
  • Manage access to sensitive information
  • Keep detailed procedures when onboarding and offboarding employees
  • Conduct exit interviews and ask employee to return equipment and files
Insurance Considerations
Autonomous car data vs. human data

In 2020, the average autonomous car may process 4,000 gigabytes of data per day, while the average internet user will process 1.5 gigabytes. That means...

1 autonomous car = 2,666 internet users
WHO PAYS WHEN A DRIVERLESS CAR CRASHES?

- Is the driver liable?
- Is the car manufacturer liable?

DATA
- What was the time and location of the crash?
- Who was in control, the driver or the car?
Case Study
Autonomous Vehicles in Public Transportation

Public transportation agencies are showing interest in incorporating autonomous vehicles into their service, and looking at pilot programs using AVs

- Use of AVs for “micro-transit” or “last mile” service could reduce costs and expand accessibility
- Reduction in costs – maintenance is less expensive and operators may be unnecessary
- Safety benefits
- Driver/operator jobs will be impacted; operators will need to be retrained to become “computer technicians
  - ADA compliance requirements means on-bus presence of an operator probably cannot be eliminated
- Infrastructure maintenance and interactivity with vehicles
  - Traffic lights and vehicles must talk to each other and roads must be pothole free
Case Study – Keolis
Case Study – Keolis

• Keolis Pilot Project in Las Vegas
• Las Vegas and Nevada are leading the way in legislative and regulatory changes to facilitate the introduction of autonomous and connected vehicles
• Keolis operates Navya-supplied Arma Shuttle that seats up to 8 passengers, 6 days a week up to 8 hours a day, in traffic, in a pilot sponsored by AAA
• Finalizing agreements highlighted range of issues, including roles and responsibilities of the parties, regulatory requirements, intellectual property, cybersecurity, vehicle maintenance, vehicle attendant roles and responsibilities and risk management
Thank You!