Autonomous Vehicles

“Law of Autonomous Vehicles” Isaac Asimov robot laws paraphrased for autos
Auto will not injure a human or through inaction, allow a human to come to harm.
Auto must obey the orders (steering and braking) given to it by humans, except where such orders would conflict with the First law.
Auto must protect its own existence (avoid potholes) as long as such protection would not conflict with the First or Second law.

Details Behind the Laws

Do you avoid a small ball in the lane, resulting in traffic jam? (yes)
Do you avoid a small ball in the lane, causing traffic jam, if there was a human chasing the ball? Would you sideswipe a car to avoid a human? (yes)
Would you hit a (populated) school bus under any circumstance? (maybe)

Self-Driving Cars

Utopian view
- Save lives (1.3 million die every year in manual driving)
- 4D’s of human folly: drunk, drugged, distracted, drowsy driving
- Eliminate car ownership
- Increase mobility and access
- Save money
- Make transportation personalized, efficient, and reliable

Dystopian view
- Eliminate jobs in the transportation sector
- Failure (even if much rarer) may not depend on factors that are human interpretable or under human control
- Artificial intelligence systems may be biased in ways that do not coincide with social norms or be ethically grounded
- Security

Self-Driving Cars: Grain of Salt

- Our intuition about what is hard or easy for AI is flawed
- Carefully differentiate between:
  - Doubtful: Promises for future vehicles (in 2+ years)
  - Skeptical: Promises for future vehicles (in 1 year)
  - Possible: Actively testing vehicles on public roads at scale
  - Real: Available for consumer purchase today
- Rodney Brooks prediction in “My Dated Predictions”:
  2032: A driverless “taxi” service in a major US city with arbitrary pick and drop off locations, even in a restricted geographical area.
  2045: The majority of US cities have the majority of their downtown under such rules.

Beyond Traditional Levels: Two AI Systems

- Starting point:
  - All cars are manually controlled until the AI system shows itself to be available and is elected to be turned on by the human.
- A1: Human-Centered Autonomy
  - Definition: AI is not fully responsible
  - Notes:
    - No teleoperation
    - No 10-second rule: It’s allowed to ask for human help, but not guaranteed to ever receive it.
    - Arrive to a safe destination or safe harbor.
    - Allow the human to take over when they choose to.
- A2: Full Autonomy
  - Definition: AI is fully responsible
  - Notes:
    - No teleoperation

Two Paths to an Autonomous Future

Human-centered Autonomy
Localization and Mapping: Where am I?
Scene Understanding: Where/who/what/why of everyone else?
Movement Planning: How do I get from A to B?
Human-Robot Interaction: What is the physical and mental state of the driver?
Communicate: How do I convey intent to the driver and to the world?

Full Autonomy
Localization and Mapping: Where am I?
Scene Understanding: Where/who/what/why of everyone else?
Movement Planning: How do I get from A to B?
Human-Robot Interaction: What is the physical and mental state of the driver?
Communicate: How do I convey intent to the driver and to the world?

Notable Progress

Full autonomy (A2)
Waymo
Uber
GM Cruise
NuTonomy
OptimusRide
Zenuity
Voyage
...

Human-centered autonomy (A1)
Tesla Autopilot - Model S/X
Volvo Pilot Assist - S90/XC90/XC60/V90
Audi Traffic Jam Assist - A8
Mercedes-Benz Drive Pilot Assist - E-Class
Cadillac Super Cruise - CT6
Comma.ai openpilot
...

Self-Driving Cars: Personal Robotics View

*First wide reaching and profound integration of personal robots in society.
  * Wide reaching: 1 billion cars on the road.
  * Profound: Human gives control of his/her life directly to robot.
  * Personal: One-on-one relationship of communication, collaboration, understanding and trust.

Introduction (2017 predictions)

* 10 million autonomous vehicles will hit the roads by 2020
  – Reality: In a talk at the Uber Elevate Summit in Washington, D.C., today, U.S. Department of Transportation Secretary Elaine Chao shared a total overall figure for ongoing testing of autonomous vehicles on U.S. roads: More than 1,400 self-driving cars, trucks and other vehicles are currently in testing by more than 80 companies across 36 U.S. states, plus DC itself.
* 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

History of Autonomous Vehicles

SAE Levels of Automation

Source: https://www.tc. wv.edu/technology-innovation/autonomous-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)

How much computing power?

- The Georgia Institute of Technology Porsche Cayenne:
  - Seven dual-core 2.13Ghz processors with 2GB of RAM required to make sense of the data collected by the cars' instruments.
  - Some cars run as many as 17 processors to dispense the computing load.

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.

Hardware Comparison

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
  - [Image of various companies logos]

Recent Developments

- January 2017—Koelis 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 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 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.

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

Product Liability: State Laws

- 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.

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 or Control Over Source Code–Software for different components of connected vehicles is being written by different developers, installed by different suppliers, 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.

Potential Attack Gateways

- Electronic 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 WiFi 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.
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.

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

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 foreshadow 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.

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.
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 increased 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.

Patents

- 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?

- Toyota is the global leader in the number of autonomous vehicle patents with more than 1,400 patents.
- Google is the tech company with the most autonomous vehicle patents, but ranks 26th when compared to all companies with autonomous vehicle patents.

- Source: https://www.reuters.com/article/us-tech-ces-autos/automakers-not-silicon-valley-lead-in-driverless-car-patents-study-idUSKBN0UJ1UD20160105
- The 2016 State of Self-Driving Innovation, Thomson Reuters.

Who Owns the Most Patents?

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

- 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 telecommunication, 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 range 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 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 – 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

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

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

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 ArmaShuttle 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
Case Study - Keolis

A self-driving shuttle in Las Vegas got into an accident on its first day of service

Surprise: it was the human's fault

A Las Vegas-based self-driving shuttle service celebrated its launch day by getting into an accident with a human driver; the shuttle hit the front end of a large delivery truck as the human driver pulled out into the street from a loading bay.

The shuttle did what it was supposed to do, in that it's sensors registered the truck and the shuttle stopped to avoid the accident. Unfortunately the delivery truck did not stop and grazed the front fender of the shuttle.