RSAConference2017
San Francisco | February 13 – 17 | Moscone Center

SESSION ID: LAW-R11

LOOK MA, NO HANDS! RISK AND LIABILITIES IN THE ERA OF AUTONOMOUS VEHICLES

Francoise Gilbert
Shareholder
Greenberg Traurig, LLP
gilbertf@gtlaw.com
@francoisegilbrt
Silicon Valley, California, USA

Raffaele Zallone
Founder & Partner
Studio Legale Zallone
r.zallone@studiozallone.it
Milano, Italy

Connected Vehicles: How do They Work?

- Different kinds of possible automation, with different legal scenarios, related to several issues: liability, privacy, security
- Connected vehicles will use numerous connected devices (sensors, cameras, GPS navigation systems, etc.) to determine road and traffic conditions, identify obstacles, and drive to the chosen destination
- Numerous developments have occurred over the past few years, but R&D is ongoing. We can only infer from existing models what the future might bring
- The key point is that autonomous vehicles will record data for analysis to improve autonomous driving algorithm, and increase security and safety

Key Obstacles to the Development of Connected Vehicles

- Regulatory environment
  - Existing laws and regulations may not account for automated vehicles, and may not fully support the development, testing or operation of connected vehicles
- Support of the policy makers; or lack thereof
- Highly precise maps
- Limitation of cybersecurity risk to an acceptable level
- Allocation of liability when both humans and autopilots drive
- Availability of Insurance

Key Regulators / International

- United Nations Convention on Road Traffic
  - Vienna, November 8, 1968
  - Goal: facilitate international road traffic and increase road safety
  - Signed by numerous countries
  - Not signed by: US, China
  - Problem:
    - Article 8(1): Every moving vehicle shall have a driver
    - Article 8(5): Every driver shall at all times be able to control his vehicle
  - Amendment March 23, 2016
    - Article 8(5bis): Automatic technologies are now allowed when such systems can be overridden or switched off by the driver

Leading Actors / United States

- Department of Transportation NHTSA (National Highway Traffic Safety Security Administration)
- Department of Transportation ITS (Intelligent Transportation Systems)
- Federal Trade Commission: Internet of Things; Testimonial before Congress
- Federal Communications Commission: V2V communications
- States: laws, regulations
- US Auto Industry: Consumer Privacy Protection Principles
- Insurance Industry

Leading Actors / European Union

- **European Commission Initiatives**
  - Cooperative Intelligent Transport Systems (C-ITS) platform
  - Round Table on Connected and Automated Driving
  - C(2015) 6943: Decision setting up the High Level Group on the Competitiveness and Sustainable Growth of the Automotive Industry in the EU (Gear 2030) (October 19, 2015)
- **Declaration of Amsterdam (April 14, 2016)**
  - https://english.eu2016.nl/documents/publications/2016/04/14/declaration-of-amsterdam
  - Signed by Transportation Ministers of 28 EU member States.
  - Agreements on the steps necessary for the development of self-driving technology in the EU
  - EU Commission, EU member states and transportation industry pledged to draw up rules and regulations that will allow autonomous vehicles to be used on the roads.
  - Issues include: use of data, privacy and data protection, V2V and V2I communications, security

Leading Actors / European Union

- ACEA (European Automobile Manufacturers Association)
  - ACEA Principles of Data Protection In Relation to Connected Vehicles and Services
    - Transparency
    - Give customer choice
    - Always take data protection into account
    - Maintain data security
    - Process personal data in a proportionate manner

US Federal and State Laws, Regulations, Guidance

- Federal Laws/ Bill
  - Fixing America's Surface Transportation Act (FAST) (2015) (provides long-term funding for certain transportation infrastructure)
  - Autonomous Vehicle Privacy Protection Act – not enacted (2015)
- US DoT National Highway Traffic Safety Administration (NHTSA)
  - May 2013: Preliminary Statement of Policy Concerning Automated Vehicles
  - Sep. 2016: **Federal Automated Vehicles Policy – Accelerating the Next Revolution in Roadway Safety** (non-binding)
  - Oct. 2016: **Cybersecurity Best Practices for Modern Vehicles** (non-binding)
  - Dec. 2016: US DoT Notice of Proposed Rule Making regarding V2V communications on light vehicles

US Federal and State Laws, Regulations, Guidance / 2

- State Laws
  - California
    - Two statutes
    - Autonomous Vehicle Testing Regulations (2014)
    - Draft Autonomous Vehicle Deployment Regulations
  - District of Columbia (1)
  - Florida (4)
  - Louisiana (1)
  - Michigan (6)
  - Nevada (3)
  - North Dakota (1)
  - Tennessee (3)
  - Utah (2)
- Pending Bills
  - at least 31 bills pending at the state level

US DoT NHTSA Federal Automated Vehicle Policy

- Non-binding evolutionary document
- Privacy
  - Great potential benefits of information sharing
  - However, should be data exchange should stripped of information that could identify the specific vehicle or user
  - Manufacturers must ensure that personal data is collected, recorded, shared and stored in accordance with applicable privacy and security agreements and notices
  - Manufacturers privacy policies and practices should entail:
    - Transparency
    - Choice
    - Respect for the Context
    - Minimization; De-identification; Retention
    - Data Security
    - Data Integrity and Access
    - Accountability

US DoT NHTSA Federal Automated Vehicle Policy

- Cybersecurity
  - Recommends that manufacturers and other concerned entities
    - Incorporate cybersecurity best practices from NIST, NHTSA, SAE, etc.
    - Document all security considerations
    - Share information about security threats between industry members
    - Consider adopting a vulnerability disclosure policy
- Model State Policy
  - Suggest that state regulators should retain their regulatory oversight regarding issues such as licensure or insurance requirements
  - Encourage states to work together to establish a coherent cohesive set of laws to facilitate the development and deployment of automated vehicles across the country.
  - As a condition for obtaining a permit for testing, manufacturers would be required to certify “accordance” with a 15-point checklist

Security of the Connected Vehicles

- Security of the product
- Security of the infrastructure
- Security of the data
  - vehicle data
  - personal data

Security of the Product

- Connected vehicles will need to be certified and meet the requirements defined by the relevant government and state agencies
- In Europe, the main requirements are related to emission standards, safety features (seat belts, air bags, braking systems, etc.) http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32009L0136&from=EN
- In the United States, the US Department of Transportation's National Highway Traffic Safety Administration is the primary regulator http://www.nhtsa.gov/About-NHTSA/Press-Releases/U.S.-Department-of-Transportation-Releases-Policy-on-Automated-Vehicle-Development

Security of the Product / 2

- The vehicle itself needs to be safe and protected from outside attacks
- The mechanical part of the operation of the vehicle is commanded by a processing unit, software and communication gear. Access to the vehicle can be through remote control or smartphone; a password must be inserted to start the engine
- Should these operations be carried out off-line or on-line? If on-line, where does the data go? To the manufacturer of the vehicle? To the manufacturer of the IT part of the vehicle? On whose network?
- If operated on-line, the breach of security devices is a data breach, and as such must be notified according to applicable laws
- For example, In the EU/EEA: http://eur-lex.europaegal-content/EN/TX.eu/lT/PDF/?uri=CELEX:32009L0136&from=EN

Security of the Product / 3

- The password and the access credentials must comply with predefined standards and must be changed periodically
- All devices used in a C/C system require attention: e.g. the sensors
- The sensors wave-length can be used to enter the system of the vehicle, hence causing a potential data breach: how will sensors be protected?
- No specific legal standards, but violation may result in data breach and liability for the producer

Security of the Network

- The vehicle will be connected with one or several networks
  - Which network?
  - Who will have access to the network?
- Who will be responsible for security?
  - Information in transit
  - Information in storage
- The manufacturer? Who is the manufacturer?

Security of the Network / 2

- Who defines the level of security of the network?
- Who is the entity responsible for it?
- The network is made of (a) the vehicles and its devices; (b) the network itself; and (c) the service points: hence there are several possible entrance points to be safeguarded from potential attacks
- How are all these parts of the infrastructure going to be protected? Who will set the standards for their security?
- When/if the vehicle breaks down, the user will be directed to a service point
- Who and what will be connected within the networks, so that data can be downloaded and the computer reset
- How are the service points going to be protected?

Security of the Network / 3

- The network will be only as safe as its weakest point
  - Where is the weakest point when everything is so tightly intertwined?
- Perfect storm
  - Internet of things
  - Ransomware
  - Unknown threats
- How to ensure 100% security 100% of the time
  - FAA operation as a guidance?
- Ethical issues

Security of the Data

- Connected vehicles send and receive information, including personal data
- Personal data will be collected and stored (for future reference and to assess liability)
- By whom?
- Who will be the “data controller”?
- Where will the data be stored? In the cloud? Who will be responsible for this data?
- The answer to these questions will determine applicable laws and forum as well as the entity responsible for fulfilling data protection obligations

US DoT NHTSA Best Practices (Dec. 2016)

- NHTSA's Cybersecurity Best Practices for Modern Vehicles
- Recommend:
  - Identify risks and analyze threats
  - Protect against those threats
  - Detect attacks
  - Respond to attacks
  - Recover from attacks
- Layered approach
  - Limiting the likelihood of an attack
  - Ensuring that even after an attack, the vehicle is still able to perform vital functions

Protection of the Data

- ***Vehicle to vehicle communications***
  - Vehicle ID
  - Sensors
  - Crash avoidance feature
- ***Manufacturer to vehicle communications***
  - Car condition
  - Software updates
- ***Remote functionality***
  - Interaction between vehicle and smart phone
  - GPS
- ***Telematics / Infotainment***
  - Screen in the vehicle
  - Preferred radio station
- ***Operational data***
  - Potholes
  - Traffic condition
  - Weather condition
- ***Car condition***
  - Geolocation
  - Driving speed
- ***Driver to Vehicle communications***
  - Biometric data (voice commands)
  - Car condition (flat tire)
  - Driving patterns
  - Speed
  - Braking frequency
- ***Parental control***
  - Geofencing
  - Speed limit
- ***Introduced by user***
  - Phone address book
  - Calendar
  - Websearches

Privacy Issues / European Union

- The most likely scenario is that vehicle to vehicle interaction will be available when the new GDPR come in force in Europe (May 27, 2018) http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN
- This implies several obligations on the part of the data controller:
  - Due information notice to be given to user (GDPR Sec. 13 & 14)
  - Users have right of access / right to be forgotten and portability (GDPR Sec 15-20)
  - Controller required to perform an impact assessment (GDPR Sec. 35) and appoint a DPO (GDPR Sec. 37-39)
  - Controller required to implement procedures to identify/notify data breach (GDPR Sec. 33-34)
  - Will security breach is a connected vehicle require notification to the competent DPA (GDPR Sec. 36)
  - Fines (GDPR Sec. 83)

Privacy Issues / United States

- **Federal Automated Vehicles Policy – Accelerating the Next Revolution in Roadway Safety**
- **Consumer Privacy Protection Principles for Vehicle Technologies and Services (2014)**
  - Transparency
  - Choice
  - Respect for context
  - Data Minimization; de-identification, and retention
  - Data Security
  - Integrity and access
  - Accountability
- **Consumer Protection laws**
  - Federal Trade Commission (Sect. 5 of FTC Act)
  - States: Unfair and Deceptive Practices Act

Questions?

Francoise Gilbert

gilbertf@gtlaw.com

Greenberg Traurig

Silicon Valley, CA (USA)

Raffaele Zallone

r.zallone@studiozallone.it

Studio Zallone

Milano (Italy)