

# Regulatory Issues with Connected Vehicles

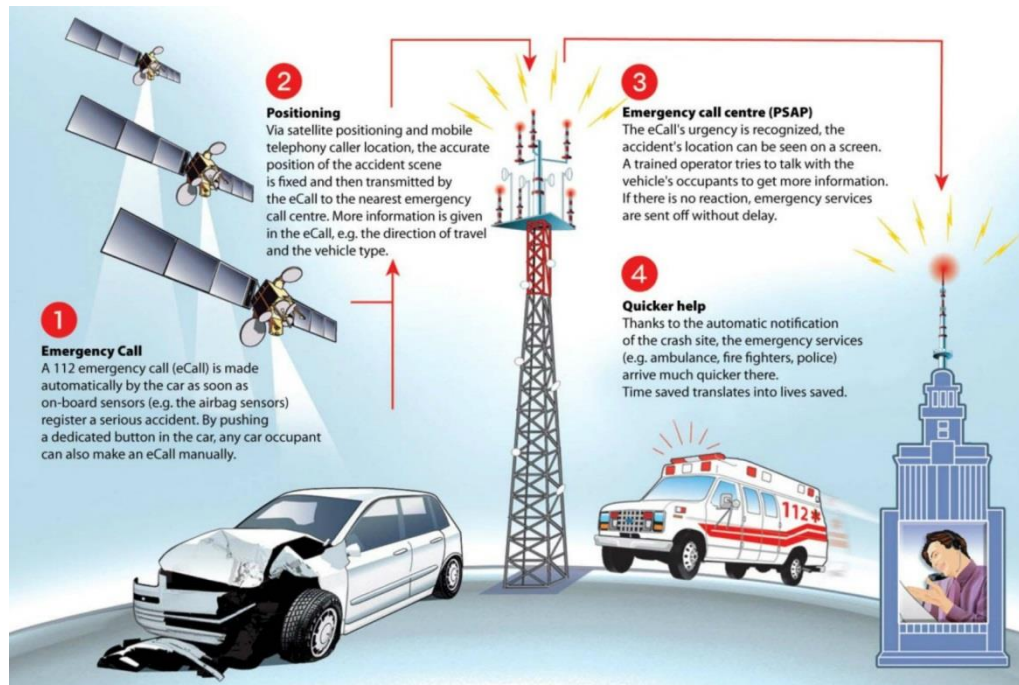
# Where it all started - the eCall

- In the EU Agenda from 2003 (Communication No. SEC(2003) 963) and from 2005 (Communication No. COM(2005) 431)
  - *Voluntary Implementation*
- **Directive 2010/40/EU - Framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other modes of transport**
- **Commission Delegated Regulation 305/2013 for the harmonized provision for an interoperable EU-wide eCall**
  - *Compulsory Implementation*
- Other Commission Delegated Regulations (for instance, over real time traffic information across the EU) and Decisions (for instance, on the deployment of the interoperable EU-wide eCall – 585/2014/EU)
- April 29, 2015: Regulation (EU) 2015/758 on type-approval requirements for the eCall in vehicle system based on 112 service (in force from 20 May 2015)
  - By **24 Dec 2015** MS to report to the Commission on deployment of PSAP infrastructure (585).
  - By **1 Oct 2017** eCall PSAP infrastructure to be operational
  - Starting **31 Mar 2018** all new types of vehicles to be equipped with 112 eCall
    - For existing types, eCall retrofitted on a voluntary basis

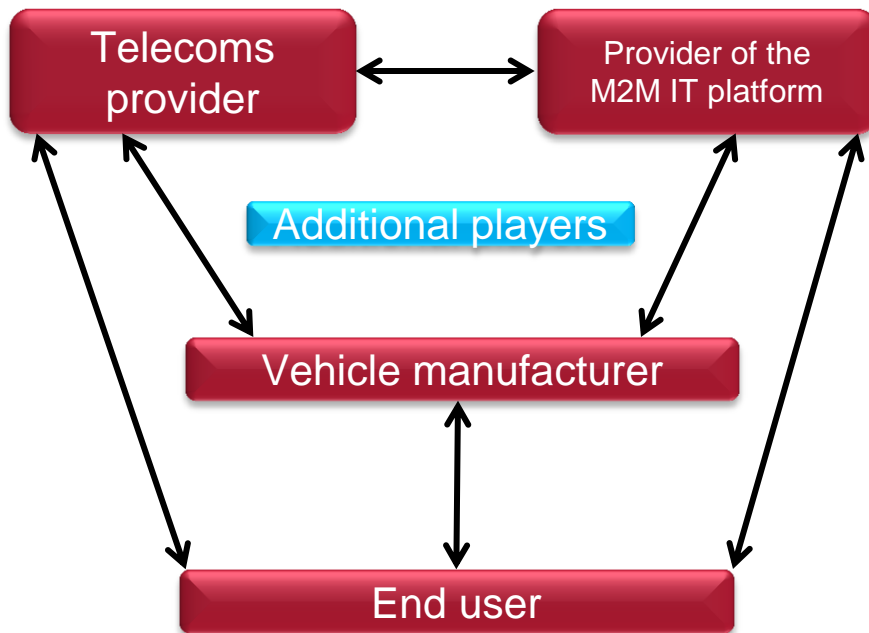


# What is an eCall?

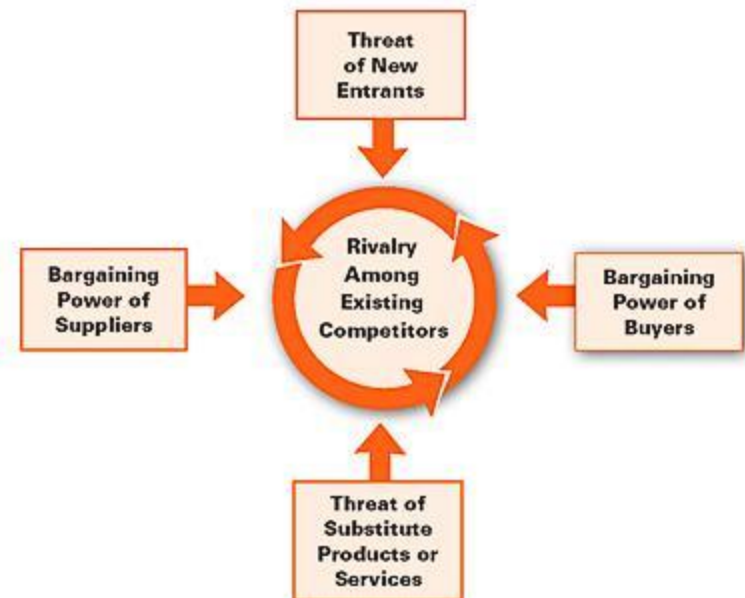
- An in-vehicle emergency call to 112
- Made automatically through sensor activation or manually
- Which carries a minimum set of data (MSD)
- Establishes an audio channel car ↔ PSAP
- Via public mobile wireless communications networks
- Mandatory on new models of cars / light vans from March 31, 2018



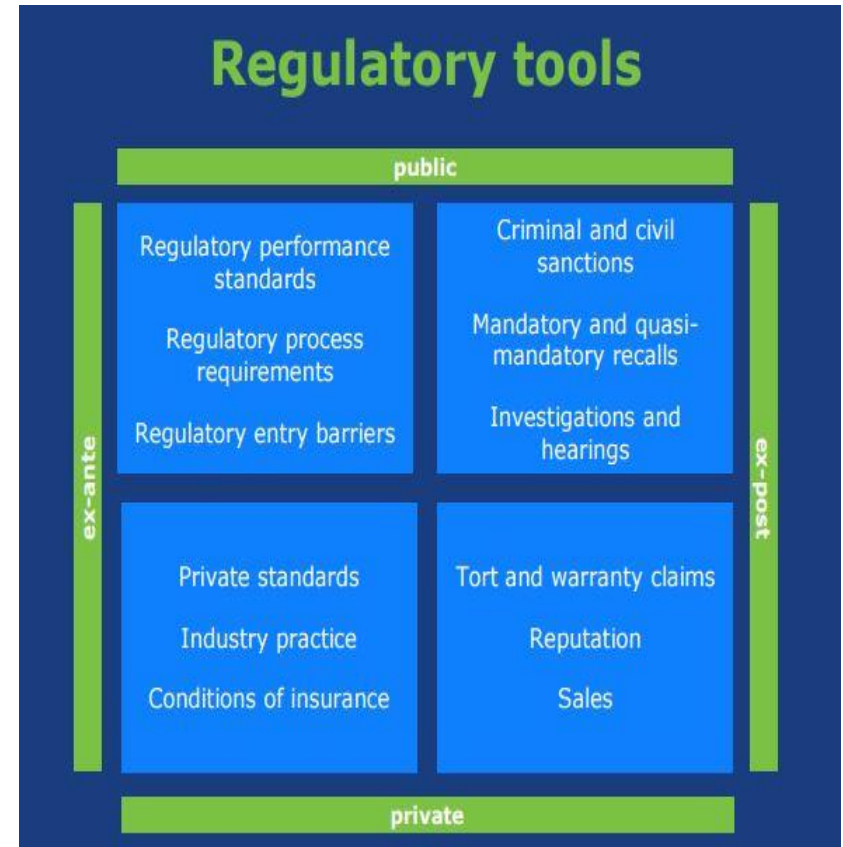
# The value chain



## The Five Forces That Shape Industry Competition



# Key legal issues



Source International Transport Forum - OECD

# Electronic communications and connectivity

- The structure of the contractual relationship between the IT provider and the MNO is essential for the purposes of TLC regulations
  - Different approaches around the EU as to what constitutes a public ECS
- Connected car as an ECS?
  - Connectivity provision and billing
  - Ownership of the SIM card
  - Flat fee v. consumption-based fee
  - From the MNO to the MVNO
- Possible restrictions on foreign IMSIs
- Permanent roaming for overcoming any restrictions on the use of extraterritorial E.164 / E.212 numbers? Global +88 → PSAP call back
- Insurance OBU obligation and interoperability issues
- Cybersecurity issues
- Interoperability
- Geo-positioning (Galileo and EGNOS)
- Standardization



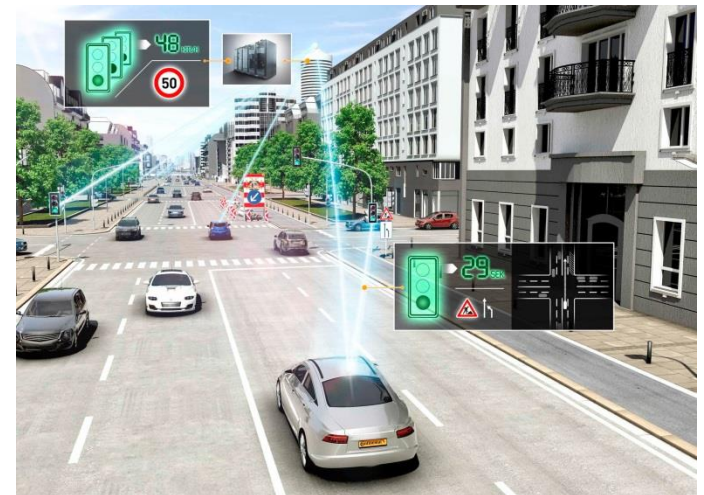
# Distracted driver regulations

- In-vehicle notices are not prohibited, if they do not:
  - impair the driver's attention (e.g., extensive information);
  - require the use of the driver's hands (e.g., messages opening or scrolling);
  - interfere with the hearing ability of the driver.
- Exceptions for vehicles belonging to Armed Forces, Police, Firefighters, Red Cross, Tax Police and State Forestry Corps;
- Rules also applicable to written notices which would be displayed on the OBU?
  - Yes, by way of analogy?



# Telecoms and data protection

- Road safety related minimum universal traffic information free of charge to users
- Systems for a nominal value
- Telecoms-specific data retention obligations
  - Invoicing or interconnection purposes
    - 6 months
  - Crime detection purposes
    - 24 months for voice traffic
    - 12 months for Internet data traffic
    - 30 days for unsuccessful calls
    - The content of the communications may not be retained





# Telecoms and data protection (cont'ed)

## Position of the EU on eCall

- eCall processing of personal data must comply with all EU Directives on data protection (including Directives 95/46 and 2002/58)
  - Notice & consent generally needed to process personal data
  - Express written consent for “sensitive” data
- Personal data:
  - not to be retained longer than necessary for the emergency situations and to be fully deleted as soon as they are no longer necessary for such purpose
  - not to be available outside the 112-based eCall in-vehicle system (iVS) to any entities before the eCall is triggered
- MSD sent by the 112 eCall iVS to include only minimum information such as:
  - Vehicle identification and propulsion
  - Time stamp
  - Vehicle location
  - Vehicle direction
  - Recent Locations
  - No. of passengers



# Telecoms and data protection (cont'ed)

- No additional data to be transmitted by the 112 eCall iVS
- MSD must be stored in such a way as to make its full and permanent deletion possible
- Only retention of last 3 locations OK if strictly necessary to specify the current location and the direction of travel at the time of the event
- Privacy enhancing technologies to be embedded in the 112 eCall iVS to provide privacy protection and necessary safeguards to prevent surveillance and misuse



# Manufacturers to ensure that:

- 112 eCall iVS system be not traceable or subject to constant tracking
- In the internal memory of 112 eCall iVS data be automatically/continuously removed
- 112 eCall iVS and TPS eCall exchange no personal data.
- Non-use of TPS eCall or refusal of the data subject to give consent for TPS eCall processing must not affect 112 eCall iVS
- Clear/comprehensive info in owner's manual re data processing through 112 eCall iVS:
  - reference to the legal basis for the processing
  - 112 eCall iVS is activated by default
  - arrangements for data processing performed by 112 eCall iVS
  - specific purpose of eCall processing, only for emergency situations of the “severe accident”
  - types of data collected/processed and recipients of data
  - time limit for the retention of data in 112 eCall iVS
  - no constant tracking of the vehicle
  - data subjects' rights including service responsible contact
  - necessary additional information re traceability, tracking and processing of personal data for TPS eCall to be subject to explicit consent → separate info in owner's manual

*“eCall - Do you have any concerns for your privacy? You shouldn't ...”*

(Source: EU Digital Agenda)



# From the past...

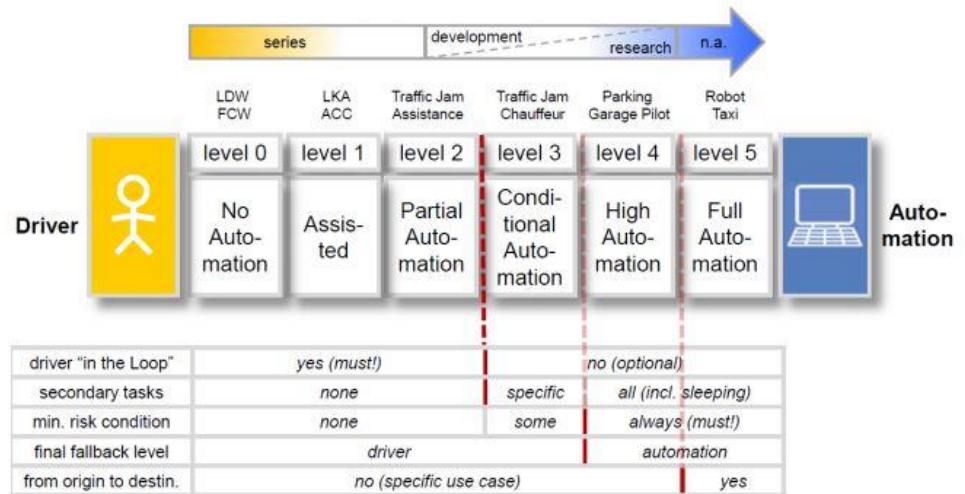


# ...to the Future

How the car connects to the outside world



FT



## Meanwhile in Mexico...

- New telecoms law includes provisions for MNOs, MVNOs and OTT application providers (connected cars?):
  - Lawful intercept and real-time monitoring
  - Data collection obligations (12 months)
  - Resale contract transparency
  - Permanent roaming permitted



# Meanwhile in Mexico...

- Mexico City enacted new Transportation Regulations
  - New regime for app transportation providers
    - Includes 1.5% profit-sharing
  - Prohibition on driver distractors
    - GPS and displays may only be manipulated when car stopped



# Privacy and Security Issues

# Scope of Regulated Data

- Data privacy laws regulate the collection, use, storage, disclosure, and other processing of “personally identifiable information” or “PII”
  - **What?** Name and other “identifiers,” and any other data that can be linked with the identified or identifiable person (incl., e.g., UDID, cookie data, and IP address)
  - **Who?** Employees, consumers, contractors, patients, insureds, corporate customer contacts, supplier contacts, website visitors, business partner contacts, end users, and other individuals.
- Two approaches to regulation globally:
  - United States: Sector-specific (HIPAA/HITECH, GLBA/FCRA, and the like) and data-specific (SSNs, bank account, credit/debit card numbers)
  - European Union/Mexico/Canada: Omnibus privacy laws applicable to all PII, regardless of sector, category of individual, or type of PII; EU tends to lead the rest of the non-US world



# Covered Entities

- Role of “processor” vs. “controller”
- Local compliance issues
  - Notice/consent
  - Legitimacy/proportionality
  - Information security
  - Sensitive PII requirements
  - Data protection filings/ consultations with data protection officers
- “Downstream” privacy issues
  - Information security and breach notification
  - Contract terms with service provider – “new” EC Model Processor Contract
  - Permits subcontracting
  - Key “formalities”

# Cross-Border Transfer Restrictions

- Key example: “Adequacy” requirement for ex-EU data transfers
- Solutions:
  - Consent
  - Model contracts
  - Binding corporate rules
- ***On October 6, 2015, the ECJ invalidated the Safe Harbor framework***

# Non-US Data Breach Notice Duties

# Expanding Global Breach Notification Laws

- Alberta (Canada), Austria, Chile, Denmark, Germany, Greece, Mexico, Norway, Portugal, Qatar, Russia, and more...



# International Examples

- **Mexico** (*Data Protection Law (“DPL”)*)
  - *Scope:* breaches to the security of personal data that affect data subjects in a material manner
  - *Timing:* “immediately”
  - *Recipients:* Data subjects and the Mexican Institute for Access to Information and Personal Data (“IFAI”)
- **Canada** (Personal Information Protection and Electronic Documents Act)
  - **NEW:** *June 18, 2015 (not yet in force, waiting on implementing regs)*
  - *Scope:* unauthorised access to or disclosure of the personal information where a reasonable person would consider that there exists a risk of significant harm to an individual as a result
  - *Recipient:* Office of the Privacy Commissioner and data subjects

# National Implementations of the Data Protection Directive (95/46/EC)

- **Germany** (Section 42(a) of the Federal Data Protection Act)
  - *Scope:* sensitive data, professional privilege data, criminal records, bank accounts, credit card accounts, telecommunications data
  - *Timing:* “without undue delay”
  - *Recipients:* data subjects and competent regulatory agency
- **Austria** (Section 24 of the Federal Data Protection Act)
  - *Scope:* serious misuse of data if the data subjects might be harmed.
  - *Timing:* “without undue delay”
  - *Recipient:* data subjects
- **Norway:**
  - *Scope:* unauthorized disclosures of personal data
  - *Timing:* as soon as possible
  - *Recipient:* the Norwegian Data Inspectorate

## National Implementations of the Data Protection Directive (95/46/EC)

- **NEW: Amendment to the Dutch Personal Data Protection Act**
  - Effective January 1, 2016
  - *Scope:* personal data breach if the data breach is likely to have adverse consequences to the privacy of the individual
  - *Timing:* “without undue delay”
  - *Recipients:* data subjects and competent regulatory agency

## Expect Changes in Europe...

### – Draft EC Data Regulation (Articles 31 and 32)

- As initially drafted, would provoke a tidal wave of notifications
- *Scope*: a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed
- *Timing*: within 24 hours of becoming “aware” of an issue
- *Recipient*: supervisory authorities
  
- **June 17, 2015**, Article 29 Working Party recommended different thresholds for notification, e.g., *when breach is likely to adversely affect the privacy of the data subject.*
- More revisions coming on this...
- Final regulation expected *2016 or 2017...*



# Regulatory Issues with automated driving and autonomous cars

# Baby you can drive my car

[https://www.youtube.com/watch?v=H0jJAPvN2ul&feature=player\\_detailpage](https://www.youtube.com/watch?v=H0jJAPvN2ul&feature=player_detailpage)



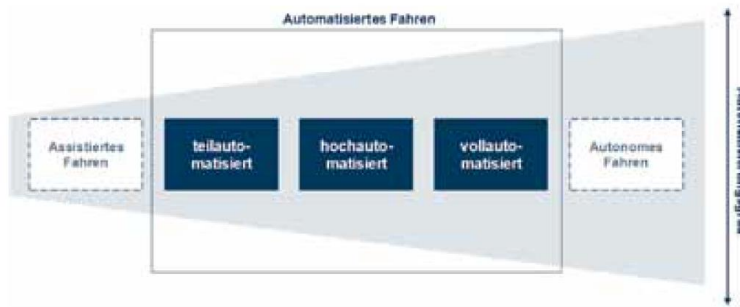


Die  
Bundesregierung


# Strategie automatisiertes und vernetztes Fahren

**Leitanbieter bleiben, Leitmarkt werden, Regelbetrieb einleiten**

# “Strategy automated and connected Driving”

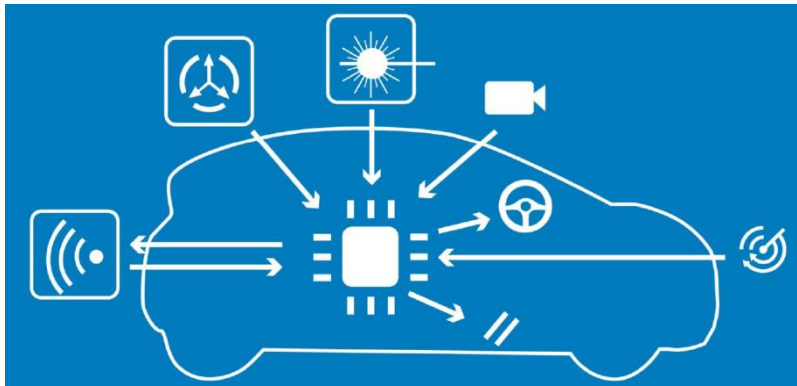


© ZF Friedrichshafen AG

- Potential
  - Goals
  - Action list
  - Implementation
-  Die Bundesregierung



# Regulatory challenges: EU



## European Roadmap Smart Systems for Automated Driving

- Vienna Convention on Road Traffic
- Type approval requirements
- UNECE Regulations
- National road traffic laws



# Regulatory Challenges: USA

## Autonomous Vehicles



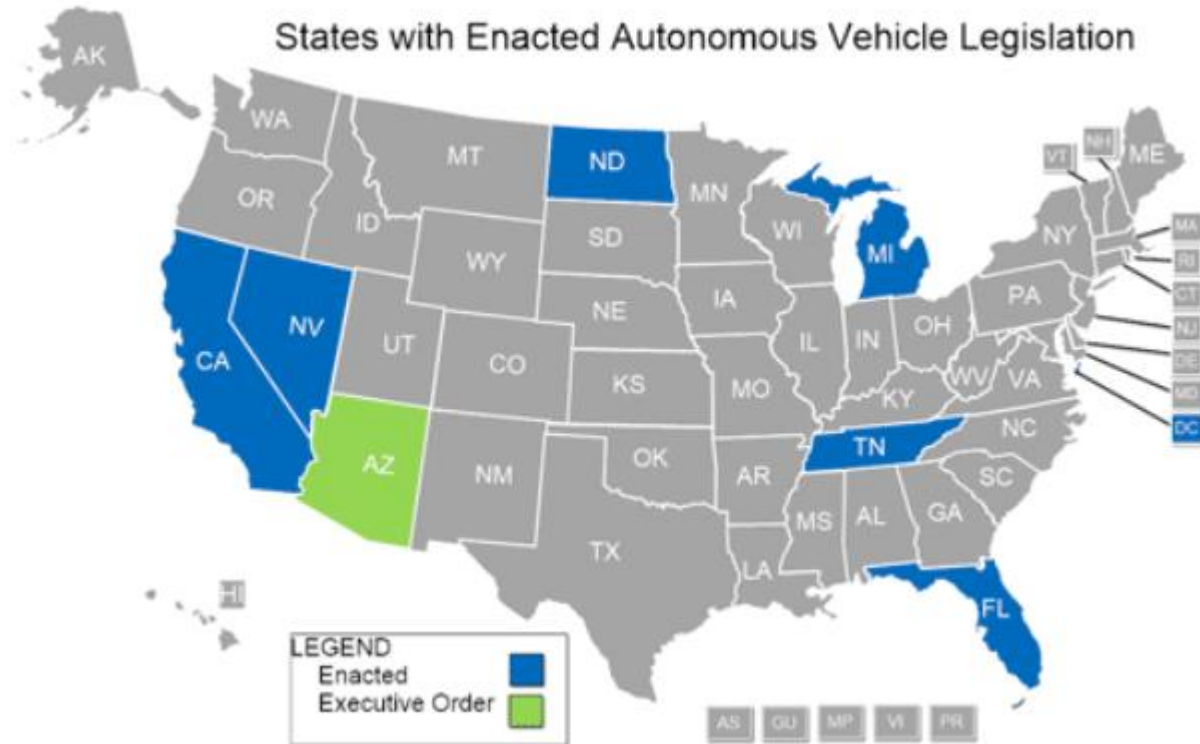
Many people consider autonomous vehicles to be a significant part of the future of the automotive industry.

As the technology for autonomous vehicles continues to develop, it may be necessary for state and

municipal governments to address the potential impacts of these vehicles on the road.

Sixteen states introduced legislation related to autonomous vehicles in 2015, up from 12 states in 2014, nine states and D.C. in 2013, and six states in 2012.

# Regulatory challenges: USA



Nevada was the first state to authorize the operation of autonomous vehicles in 2011. Since then, five other states—California, Florida, Michigan, North Dakota and Tennessee—and Washington D.C. have passed legislation related to autonomous vehicles. Arizona's governor issued an executive order related to autonomous vehicles.

<http://www.ncsl.org/research/transportation/autonomous-vehicles-legislation.aspx#Enacted>  
Autonomous Vehicle Legislation



“Those are the kinds of projects that will advance this technology, and let us daydream about spending our retirement being whisked around in a sleek sedan with spinning seats and hardwood floors.”

Alex Davies in WIRED.





# Thank You