

Morgan Lewis

CONNECTING THE CONNECTED CARS: FCC REGULATIONS AND SPECTRUM ISSUES

March 21, 2018

© 2018 Morgan, Lewis & Bockius LLP

Morgan Lewis Automotive Hour Webinar Series

Series of automotive industry focused webinars led by members of the Morgan Lewis global automotive team. The 10-part 2018 program is designed to provide a comprehensive overview on a variety of topics related to clients in the automotive industry.

Register now for upcoming sessions:

APRIL 18

The Autonomous Vehicle Regulatory Environment

MAY 17

Developing Licensing and Transaction Issues in the Age of Connected and Autonomous Vehicle Technology

JUNE 6

Supply Chain and Location Issues in an Evolving NAFTA Environment

SEPTEMBER 19

Labor and Employment from the Automotive Perspective

OCTOBER 17

Class Action Litigation from the Automotive Perspective

NOVEMBER 14

Automotive Finance: From Lending to Structured Finance

DECEMBER 12

Automotive Advertising & Marketing: Challenges Promoting Innovation with Evolving Technologies

Morgan Lewis

Table of Contents

Section 01 – Telecom, Media, and Technology Background

Section 02 – What Makes a Car “Connected”?

Section 03 – Who Regulates the “Connection”?

Section 04 – Recent Regulatory Developments

Section 05 – Critical Issues to Watch

Section 06 – Privacy and Data Security

Section 07 – Foreign Jurisdictions

Morgan Lewis

TMT: Who We Are

- Our lawyers have played a role in nearly every significant development in the communications industry in the past quarter century, in the United States and internationally.
- Our practice combines regulatory, corporate and transactional, dispute resolution, land use and legislative work.
- We are aggressive advocates for our clients in technically complex and contentious proceedings.
- We are nationally recognized for our experience in federal communications regulation.

SECTION 02

WHAT MAKES A CAR CONNECTED?



What Makes a Car “Connected”?

- Opinions diverge on the definition of a “connected” car.
- Our definition: The presence of devices in an automobile that use in-car telematics and other technologies that utilize connectivity, whether through dedicated short-range communications or over the internet, to provide location, diagnostics, or other information as well as to interface with other cars, homes, offices or infrastructure.
- Part of the “Internet of Things”
- Data collected and generated is part of “Big Data”
- The first *en masse* deployment of a connected car dates to 1996 and the General Motors/Hughes/EDS OnStar initiative. Two technologies involved.
 - Availability of civilian GPS signals enabled geolocation for vehicles in motion and at rest possible.
 - Availability of nationwide cellular networks facilitated data communications (telemetry and tele-command) and voice communications allowed OnStar personnel to communicate in real-time with drivers.

What Makes a Car “Connected”? (cont’d)

- First connected cars had some limitations. Connectivity constrained by cellular network’s footprint. Cellular voice and data services costly.
- Three fundamental wireless technologies provide the connectivity needed for contemporary motor vehicles.
- Satellite Navigation – GPS or other global satellite navigation signals needed to understand true position on Earth’s surface.
- Communications – Duplex communications needed for cars to appreciate their surroundings, make appropriate adjustments to reflect changes in traffic, accidents, etc..., and for telemetry/diagnostics.
- RADAR – Needed for collision avoidance and parking assistance.

What Makes a Car “Connected”? (cont’d)

- All of these wireless technologies require clean, know radiofrequency spectrum. Challenges face all three technologies.
- Wireless connectivity always a prerequisite to any meaningful level of autonomy.
- All autonomous cars are connected, but not every connected car is autonomous.
- Autonomous cars assume responsibility for driving functions.
- Society of Automotive Engineers (SAE) has developed automation standards adopted by
 - Level 0 = Zero autonomy
 - Level 5 = Vehicle is capable of performing all driving functions under all conditions

SECTION 03

WHO REGULATES THE CONNECTION?



Who Regulates the "Connection"?



U.S. Department
of Transportation



Federal
Communications
Commission



Who Regulates the "Connection"? (cont'd)

- The Department of Transportation (DOT) has authority to develop "national transportation policies and programs conducive to the provision of fast, safe, efficient, and convenient transportation at the lowest cost consistent therewith."
- National Highway Traffic Safety Administration (NHTSA), an operating administration within DOT, enjoys broad delegated authority to regulate U.S. highways and motor vehicles.
- Neither DOT nor NHTSA regulates wireless spectrum.
- Dept. of Commerce, National Telecommunications & Information Administration (NTIA) controls federal wireless spectrum allocations (DOT contributes to NTIA decisions through consensus driven Inter-department Radio Advisory Committee (IRAC)).

Who Regulates the “Connection”? (cont’d)

- Federal Communications Commission (FCC) exclusively regulates non-federal spectrum resources (coordination through NTIA/IRAC needed when spectrum shared with federal uses).
- Any non-federal use of spectrum requires an FCC license (e.g., cellular networks) or authority under a blanket authorization (e.g., WiFi)
- Which agency regulates the wireless spectrum used for connected cars?
The FCC, with certain exceptions.
- Most of the technology involved in a contemporary car involves non-federal spectrum (e.g., cellular networks, DSRC V2V, RADAR)
- GPS and other satellite navigation networks are an important exception, the United States military flies the GPS satellite fleet and controls the navigation signals transmitting from the satellites, and the allocations these signals use involve federal spectrum.

SECTION 04

RECENT REGULATORY DEVELOPMENTS



GPS Interference

- Mobile satellite operators attempting to repurpose wireless spectrum adjacent to GPS signals that occupy the 1559-1610 MHz Global Navigation Satellite Service allocation.
- Original proposal would have blinded sensitive GPS receivers used to a “quiet neighborhood” for up to 20 kilometers from a base station.
- DOT and other federal-affiliated laboratories have undertaken painstaking tests over the last seven years to evaluate the full impact of this interference.
- Recent adjustments to the plan better protect GPS, but DOT has lingering concerns about “black swan” scenarios.
- Approval to repurpose at least some MSS L-band spectrum likely in 2018. Impact likely negligible for most car-based GPS receivers, but the older the GPS receiver, generally the more likely it will be to experience interference in the future.

GPS Interference

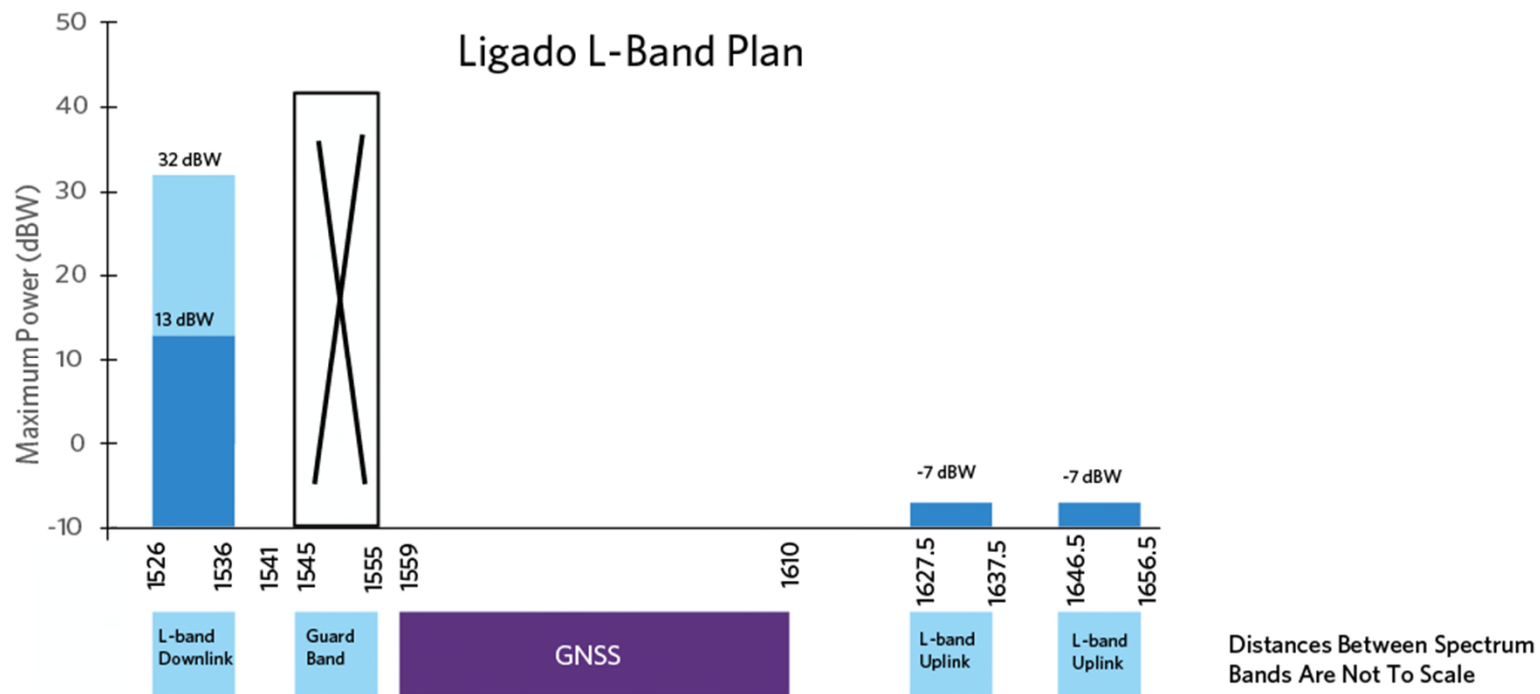


Chart: Ligado ex parte in Feb 2018

DSRC Under Siege

- In 1999 FCC allocated 5.85-5.925 GHz for Dedicated Short Range Communications (DSRC) Services; enables short- to medium-range high throughput, duplex data transmission.
- Supports Vehicle-2-Vehicle (V2V), Vehicle-to-Infrastructure (V2I) and Vehicle-to-Pedestrian (V2P) communications (collectively, V2X).



DSRC Under Siege (cont'd)

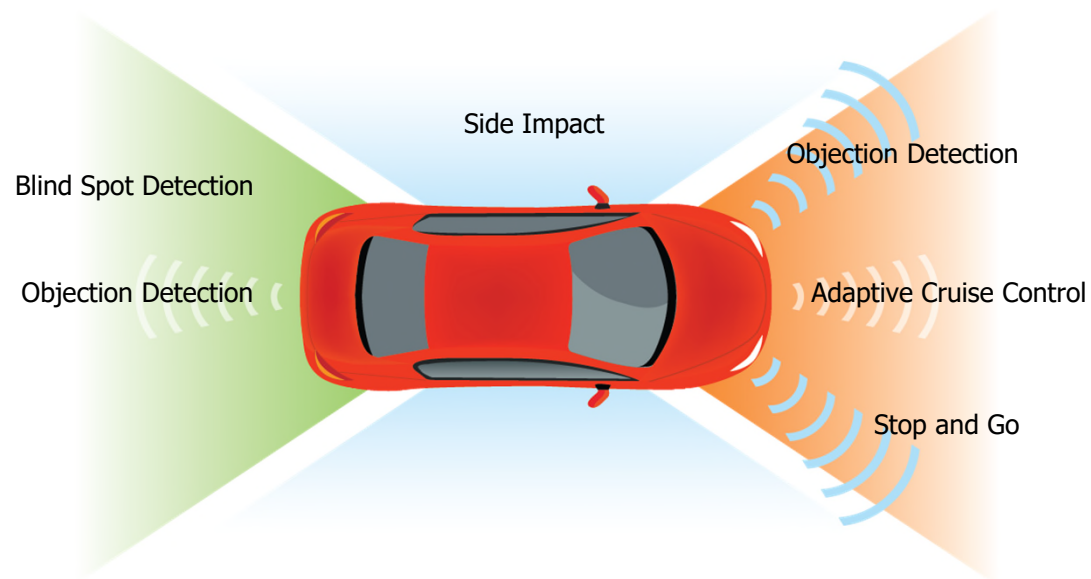
- Standards to support DSRC slow to develop (IEEE 802.11p finally adopted in 2010) leaving the band underutilized and vulnerable to arguments it lies fallow.
- As a result, in 2013 FCC proposed unlicensed services share the lower 45 MHz of the band. Contentious and as of Q1 2018 parties working to develop industry-led sharing solution – prototype testing underway led by FCC in collaboration with DOT and NTIA.
- Auto manufacturers began building 802.11p DSRC-enabled cars *en masse* in 2016/2017, but outcome for the band remains unclear, and co-channel and adjacent interference represent a potential threat if FCC opens the lower 45 MHz for shared use.

DSRC Under Siege (cont'd)

- In early 2018, automobile manufacturers and component suppliers that favor 802.11p DSRC-based service fighting a two front war.
- Unlicensed, high-tech interests want shared use of the 5825-5950 MHz band for themselves.
- Cellular interests also now making arguments that their networks are better capable of supporting V2X communications relative to 802.11p.
- Situation remains dynamic, but FCC wants parties to share spectrum when feasible.

RADAR Consolidation

- RADAR, a radio-determination system using pulsed emissions for comparison of reference points, enables applications such as forward collision avoidance, cross-traffic alert, adaptive cruise control previously spread over numerous wireless spectrum allocations.



RADAR Consolidation (cont'd)

- RADAR enables applications such as forward collision avoidance, cross-traffic alert, adaptive cruise control previously spread over numerous wireless spectrum allocations.
- In 2017 FCC made the decision to consolidate vehicular RADAR in the 76-81 GHz band.
 - Unlicensed vehicular RADAR phased out of 16.2-17.7 GHz and 46.7-46.9 GHz.
 - Unlicensed wideband and ultrawideband vehicular RADAR phased out of 23.12-23.29 GHz and 22-29 GHz.
- Vehicular RADAR in 76-81 GHz now under Part 95 licensed-by-rule framework
- Hard transition deadlines out of other RADAR band may present problems for servicing certain older vehicle.

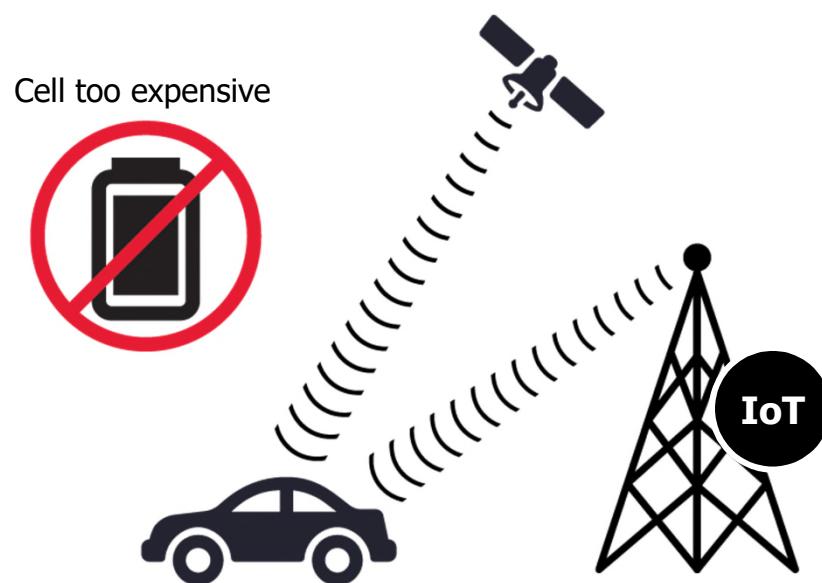
SECTION 05

REGULATORY ISSUES TO WATCH



Issues to Watch – Long-Range Communications

- Connected *and* autonomous cars require communications with greater range.
 - DSRC supports short- to medium-range communications only.
 - Cellular prohibitively expensive, particularly for narrow-band telemetry communications.
- Various technologies jockeying to fill this void.
 - Satellite-based narrowband services viable; Big LEO operator Globalstar just announced automotive initiative.
 - Terrestrial IOT deployment in UHF/VHF another option.



Issues to Watch – High Precision GPS Coming

- Augmented satellite navigation signals coming from Galileo and other alternative GNSS satellite operators.
- Will give the driver navigation precision to within millimeters.
- Foreign GNSS systems need permission to serve U.S. first.
- New receivers likely to be expensive, complex, and susceptible to overload interference.

Issues to Watch – Broadband Satellite

- In-motion broadband communications coming from non-geostationary super constellation.
- Antennas no longer concave dishes with distinct feeds.
- New designs will be flat, passive phased arrays that adjust antenna gain dynamically without moving parts. Gimbal mounts not required.
- Will integrate seamlessly with automotive roof.
- Will enabled duplex broadband connectivity in remote, underserved areas; also viable for DTH TV.

SECTION 06

PRIVACY AND DATA SECURITY



Type of Data Collected by Connected Cars

Connected Car Services (from Edmunds)

- Automatic Collision Notification
- Remote Horn and Lights
- Concierge Services
- Roadside Assistance
- Crisis Assistance
- Sports and News Information
- Dealer Service Contact
- Stock Information
- Destination Information and Guidance
- Stolen Vehicle Tracking
- Emergency Services
- Text Message Display
- Fuel/Price Finder
- Traffic Information
- Hands-Free Calling
- Vehicle Alarm Notification
- Local Search
- Vehicle Alerts and Diagnostics
- Location Sharing
- Vehicle Location
- Remote Door Lock and Unlock
- Weather Information

Other Forms of Data Collection by Cars/Disclosure Obligations

- Long Standing Data Collection Technologies
 - On-Board Diagnostics
 - Event-Based Recorders
 - Driver Consent for Insurance Purposes
- Some State Laws Address Disclosure of Information
 - 17 States have laws addressing the disclosure of Event-Based Recorders
 - (1) with owner's written consent; (2) court order; (3) emergency investigation; (4) emergency medical care; (5) medical and vehicle safety research; (6) to diagnose, service, or repair the vehicle; (7) probable cause of an offense.

Other Potential Datasets and Data Flows

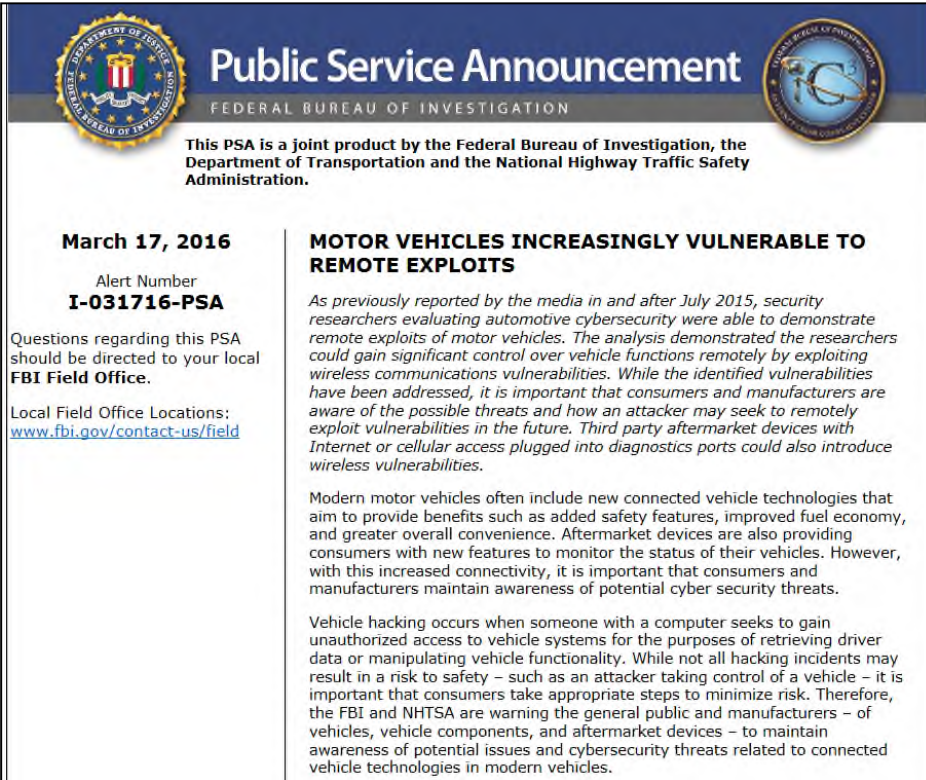
- Vehicle diagnostic and performance information can be automatically sent to manufacturers to improve safety and performance. With connectivity, diagnostic and vehicle performance information.
- Potentially allow for sending information to insurers about drivers habits (opt-in/out?)
- Driver biometrics (stress levels, drowsiness, drunk driving, serious health events, etc.)
- Behavioral data (seatbelt use, frequency of hard-braking, rates of acceleration, frequency of violating speed limits, etc.)
- Phone contact lists (if downloaded to vehicle)
- Name, address, billing information uploaded to manufacturer/third party for subscription services
- City planning: improving targeting road repair, planning for growth (e.g., smart cities), improving safety, reducing congestion, increasing fuel efficiency
- Performance of automated-vehicle systems and related event data (see NHTSA automated vehicle policy)

Increasing Risks and Vulnerabilities

- Automotive Networks
 - Electronic Control Units (ECUs)
 - ~100 ECUs
 - 100+ million lines of code
 - Wireless: Wi-Fi, Bluetooth, radio frequency, cellular networks
 - Wired: USB, CD/DVD, and SD cards
- Increasing Connectivity and Communications
 - Vehicle-to-Infrastructure (V2I)
 - Vehicle-to-Vehicle (V2V)
- Third Party Applications
- Ability for Remote Compromise and Interaction
 - Control and access features
 - Obtain information

FBI NHTSA Announcement

- “Vehicle hacking occurs when someone with a computer seeks to gain unauthorized access to vehicle systems for the purposes of retrieving driver data or manipulating vehicle functionality. ”



Public Service Announcement
FEDERAL BUREAU OF INVESTIGATION

This PSA is a joint product by the Federal Bureau of Investigation, the Department of Transportation and the National Highway Traffic Safety Administration.

March 17, 2016
Alert Number
I-031716-PSA

Questions regarding this PSA should be directed to your local **FBI Field Office**.
Local Field Office Locations:
www.fbi.gov/contact-us/field

MOTOR VEHICLES INCREASINGLY VULNERABLE TO REMOTE EXPLOITS

As previously reported by the media in and after July 2015, security researchers evaluating automotive cybersecurity were able to demonstrate remote exploits of motor vehicles. The analysis demonstrated the researchers could gain significant control over vehicle functions remotely by exploiting wireless communications vulnerabilities. While the identified vulnerabilities have been addressed, it is important that consumers and manufacturers are aware of the possible threats and how an attacker may seek to remotely exploit vulnerabilities in the future. Third party aftermarket devices with Internet or cellular access plugged into diagnostics ports could also introduce wireless vulnerabilities.

Modern motor vehicles often include new connected vehicle technologies that aim to provide benefits such as added safety features, improved fuel economy, and greater overall convenience. Aftermarket devices are also providing consumers with new features to monitor the status of their vehicles. However, with this increased connectivity, it is important that consumers and manufacturers maintain awareness of potential cyber security threats.

Vehicle hacking occurs when someone with a computer seeks to gain unauthorized access to vehicle systems for the purposes of retrieving driver data or manipulating vehicle functionality. While not all hacking incidents may result in a risk to safety – such as an attacker taking control of a vehicle – it is important that consumers take appropriate steps to minimize risk. Therefore, the FBI and NHTSA are warning the general public and manufacturers – of vehicles, vehicle components, and aftermarket devices – to maintain awareness of potential issues and cybersecurity threats related to connected vehicle technologies in modern vehicles.

Federal Communications Commission

- Spectrum Frontiers Order – July, 2016
- Fifth Generation (5G) Wireless Network and Device Security Notice of Inquiry – December, 2016
- Restoring Internet Freedom (also referred to as Network Neutrality) – January, 2018
 - Reclassification of Broadband Internet Access Services
 - Recent 9th Circuit Decision in *FTC v. AT&T Mobility*
- Communications, Security, Reliability and Interoperability Council (CSRIC)

Federal Trade Commission

- FTC – Self-appointed enforcer of privacy and data security obligations
- Connected Cars – Viewed as part of the “Internet of Things”
- IoT refers to things “such as devices or sensors . . . that connect, communicate or transmit information with or between each other through the internet.”
Internet of Things, FTC Staff Report, January, 2015
- FTC’s jurisdiction limited to devices that are sold to or used by consumers.
- Big Data: A Tool for Inclusion or Exclusion, FTC Staff Report, January, 2016
- January, 2018 – FTC releases “Key Takeaways Report” following joint workshop with National Highway Traffic Safety Administration (NHTSA) held in June, 2017.

FTC Key Takeaways from Joint Workshop

- Connected Cars collect data ranging from aggregate to sensitive personal data.
- Aggregate information can be used for traffic management.
- Non-sensitive personal data – used to measure specific performance of a particular car.
- Sensitive data – biometric data for authentication purposes and real-time geolocation data.
- Unexpected use of collected data.
- Addressing privacy concerns is important to gain consumer acceptance.
- Different kinds of collected data will require different forms of consumer consent.

FTC Key Takeaways from Joint Workshop (cont'd)

- Connected and autonomous vehicles will have cybersecurity risks and vulnerabilities that can be exploited. Panelists identified some best practices for addressing some of the risks, including the following:
- Information sharing with groups such as the Auto-ISAC, the International Organization for Standardization and the Society of Automotive Engineers could limit the extent to which vulnerabilities can be exploited.
- Network design opportunities could be useful to protect safety-critical functions if they are segregated from other functions controlled through the network.
- Disclose newly discovered vulnerabilities during development and after sale to mitigate such risks.

NHTSA Cybersecurity Guidance



The screenshot shows the NHTSA website header with the logo and navigation links: Ratings, Recalls, Risky Driving, Road Safety, Equipment, and T. Below the header is a news article titled "U.S. DOT issues Federal guidance to the automotive industry for improving motor vehicle cybersecurity". The article includes a "Share:" section with icons for Facebook, Twitter, LinkedIn, and Email. The date is "October 24, 2016 | Washington, DC" and the text states: "Guidance covers cybersecurity best practices for all motor vehicles, individuals and organizations manufacturing and designing vehicle systems and software".

United States Department of Transportation

NHTSA
NATIONAL HIGHWAY TRAFFIC SAFETY ADMINISTRATION

Ratings Recalls Risky Driving Road Safety Equipment T

← NEWS

U.S. DOT issues Federal guidance to the automotive industry for improving motor vehicle cybersecurity

Share: [f](#) [t](#) [in](#) [✉](#)

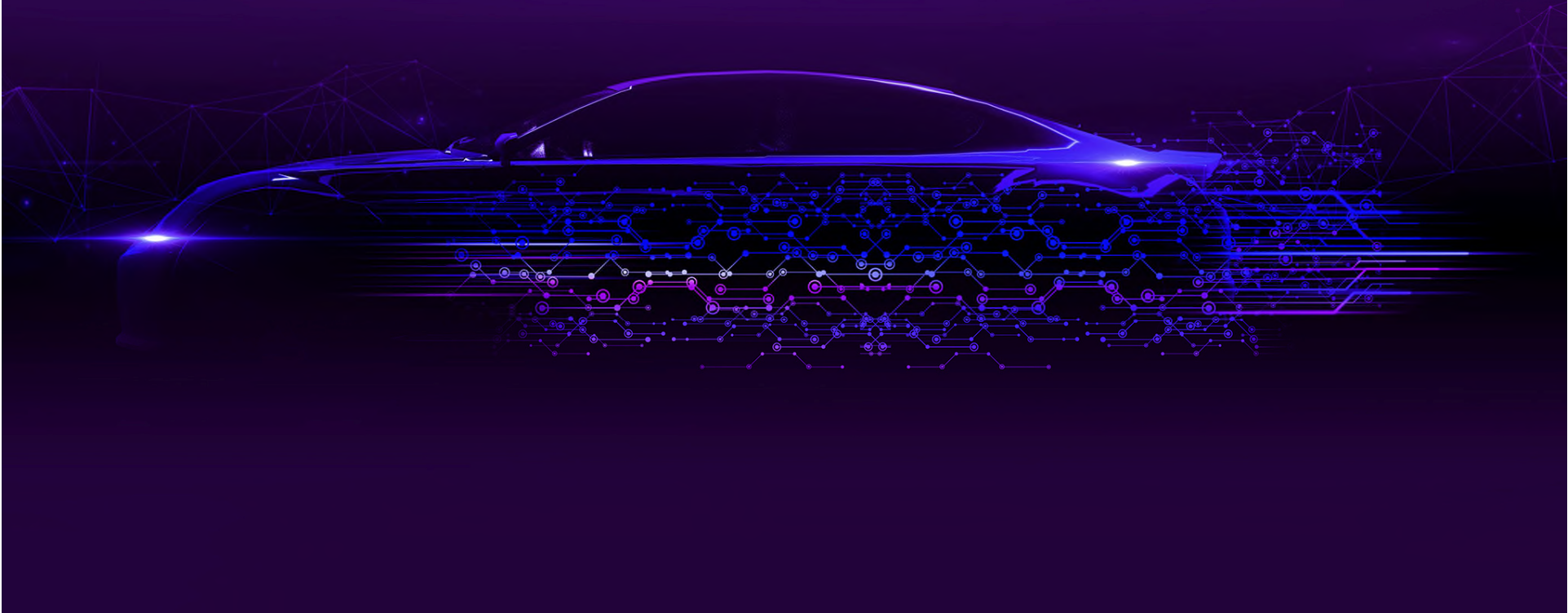
October 24, 2016 | Washington, DC

Guidance covers cybersecurity best practices for all motor vehicles, individuals and organizations manufacturing and designing vehicle systems and software

Morgan Lewis

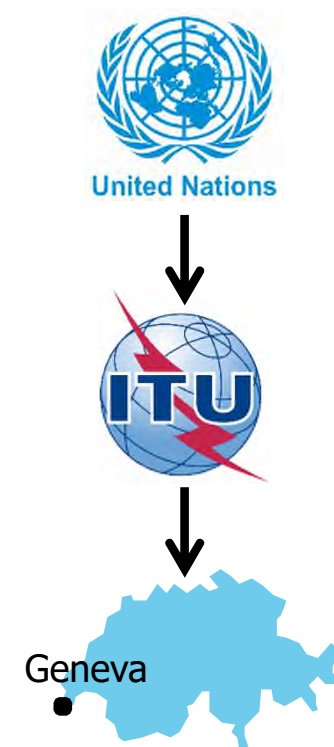
SECTION 07

INTERNATIONAL ISSUES



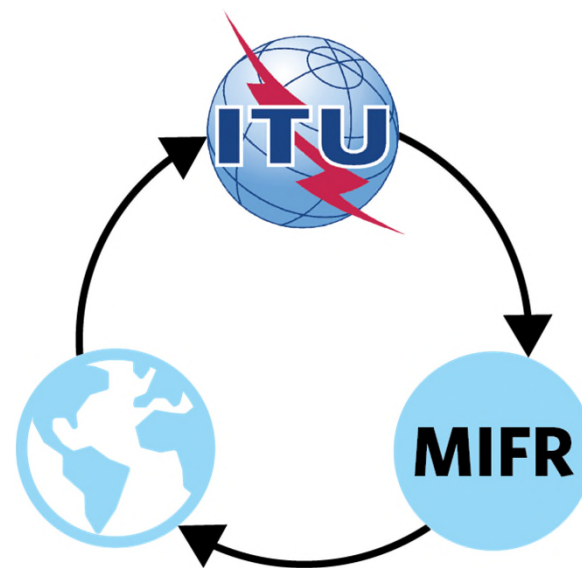
The ITU

- The International Telecommunication Union (ITU) is the UN-affiliated agency for information and communication technologies (ICTs).
 - 193 member countries
 - HQ in Geneva; 12 regional offices
- Founded on the principle of international cooperation between governments (Member States) and the private sector (Sector Members, Associates and Academia).
- The ITU allocates global radio spectrum and satellite orbits and develops the technical standards that ensure that networks and technologies seamlessly interconnect.



ITU: Spectrum Coordination

- Coordination of access to spectrum depends on international cooperation.
 - TV broadcasts over the same frequency all over the world.
 - Cell phone roaming across borders (*e.g.*, harmonized GSM bands)
- International frequency registration
 - Countries provide the ITU, via registration, spectrum use information to gain international protections and coordination assistance.
 - Registration to the Master International Frequency Register (MIFR) means receiving international recognition in accordance with the Provisions of Article-8 of the ITU-R Radio Regulations.



The ITU and ITS Communications Standards

- The ITU is developing a Collaboration on Communications Standards for Intelligent Transport Systems (“ITS”).
- The Collaboration intends to provide a global forum for the creation of an internationally accepted, *globally harmonized* ITS communication standards by (i) promoting and cross-referencing existing standards where appropriate, (ii) modifying and extending existing standards; or (iii) developing new standards where necessary, with the goal of enabling the rapid deployment of fully *interoperable* ITS communication-related products and services in the global marketplace,
- Collaboration is formed by ITU Members, ITU Sector and Associate Members (*e.g.*, car manufacturers, telecommunications carriers and telecom equipment manufacturers) and Standards Development Organizations (*e.g.*, ETSI).
- Standards will be mandatory after publication by the ITU.
- Collaboration holds regular meetings (most recent coinciding with Geneva Auto Show March 2018).

Example of ITU Work: Automotive Radar

- At the World Radiocommunication Conference (WRC-15), the ITU allocated radio-frequency spectrum for the operation of short-range high-resolution automotive radar to the 79 GHz frequency band. Previously several countries were allowing use of the band for vehicular radar applications.
- The allocation of the 79 GHz frequency band provides a globally harmonized regulatory framework for automotive radar to prevent collisions.
- Intent to use of the band is on an unlicensed, non-exclusive basis across borders, while protecting interference to other users of the band (*e.g.*, radioastronomy).
- Due to spectrum regulations and standards, the use of the 24 GHz UWB band for vehicle radar applications will be phased out by the year 2022 in both Europe and the U.S. ITU fully supports this transition and consolidation into the 79 GHz band.

European Union

- The European Commission Decision on Intelligent Transport Systems in the 5.9 GHz band was developed in co-operation with the Member States and was adopted by the Commission in August 2008.
- The Decision harmonizes the conditions for use of the 5875-5905 MHz frequency band for safety related applications of ITS on a license free, non-exclusive basis.
- Increasing vehicle safety and cutting road deaths are major goals of EU transport policy with two fronts:
 - ITS
 - Short-range radar systems



EU eCall Initiative

- Regulation (EU) 2015/758 43 requires all new cars be equipped eCall from April 2018.
- In the event of a serious accident, eCall automatically dials 112, Europe's single emergency number.
- It communicates the vehicle's exact location to emergency services, the time of incident and the direction of travel (most important on motorways), even if the driver is unconscious or unable to make a phone call.
- An eCall can also be triggered manually by pushing a button in the car, for example by a witness of a serious accident.
- Section 6 of the Regulation lays down specific provisions related to the privacy of the personal data of the users (*i.e.*, owners of the car) of the eCall system.

National Regulations to Consider

- Telecommunications Regulations (Spectrum Allocation and Licensing)
- Automotive, Traffic, and Road Regulations
- Data Protection and Privacy Regulations
- Consumer Protection Regulations

Germany

Connected cars in Germany could be subject to:

- German Communications Act, and other telecommunications regulations. Germany follows EU rules on spectrum allocation
- Germany Federal Data Protection Act and resolutions
- General Data Protection Regulation (GDPR), EU-wide privacy regulation that becomes effective in May 2018
- German Road Traffic Act
- Ethical Guidelines released in 2017
 - Self-driving cars must do the least amount of harm if put into a situation where hitting a human is unavoidable, and cannot discriminate based on age, gender, race, disability, or any other observable factors.



Germany: Recent Amendments to the German Road Traffic Act

- In June 2017, Germany adopted a law amending the German Road Traffic Act that sets out the legal framework for automated driving. The main provisions include:
 - A definition for highly and fully automated vehicles. The definition does not include "autonomous vehicles" that do not require a driver (*i.e.*, Level 5 vehicles).
 - The use of automated vehicles is allowed within the limits of the intended use. The system must inform the driver if a given use is not within the limits of the intended use.
 - The driver is allowed to avert his/her attention from the traffic. However, the driver must remain aware and perceptive in order to take control of the vehicle either when prompted or when the conditions for the automated driving are no longer available
 - The recorded data must be kept for 6 months, and in case of an accident for 3 years. The data must be deleted after.
 - Cars with automated driving systems must be equipped with a black box.

France

- Post and Communications Code, and other telecommunications regulations. France also follows EU spectrum rules
- French Highway Code
- GDPR
- French Data Protection Act
- CNIL's Compliance Pack Guidance



France: CNIL Compliance Pack

- CNIL, the French data protection authority, released a “compliance pack” with guidance for connected vehicles, (*i.e.*, vehicles that communicate with the outside world (mobile applications, other vehicles, infrastructure, etc.) for the processing of personal data.
- Takes into account current French data protection regulations as well as the GDPR
- The document identifies three scenarios for processing personal data:
 - **Scenario No. 1 “IN => IN”**: the data collected in the vehicle remains in the vehicle without transmission to the service provider
 - Example: an electric vehicle that processes data directly in the vehicle for display with tips in real time on the on-board computer
 - Envisaged purposes: improving driving or on-board experience (infotainment); improving driving behavior for security purpose and maintenance; automated driving assistance; unlocking; activation of certain vehicle controls with the driver’s biometric data.
 - **Scenario No. 2 “IN => OUT”**: the data collected in the vehicle is transmitted outside to provide a service to the data subject
 - Example: “Pay as you drive” contract with an insurance company
 - Envisaged purposes: improving products and services; providing commercial services to the user; combatting theft, accident studies; eCall
 - **Scenario No. 3 “IN => OUT => IN”**: the data collected in the vehicle is transmitted outside to trigger an automatic action in the vehicle
 - Example: dynamic “Information on traffic” with calculation of a new route following an incident on the road
 - Envisaged purposes: remote maintenance; improving the driving experience.

Japan

- Road Transport Vehicle Act (Act No. 185 of 1951)
- Telecommunication Business Act, Radio Act, and other telecommunications regulations
 - 5770-5850 MHz is allocated for electronic toll as well as for vehicle-to-vehicle communication systems. However, due to spectrum congestion in that band in some parts of Japan, the Japanese Government allocated the 755.5-764.5 MHz (760 MHz band) to ITS applications.
 - A new standard (ARIB STD-T109) was developed for this Japan-proprietary "Driving Safety Support Systems".
 - Vehicle radar rules also in the 79 GHz band
- Act on the Protection of Personal Information



Japan

- Continental, Ericsson, Nissan, NTT DOCOMO, INC., OKI and Qualcomm Technologies, Inc. will carry out Cellular Vehicle-to-Everything (C-V2X) trials in Japan to show the enhanced range reliability and latency benefits of C-V2X direct communications operated in the 5 GHz band.
 - The trial results will help develop the new equipment ecosystem as we prepare for the connected car of the future and the industry's evolutionary transition towards 5G.
- Japan has established a roadmap for the introduction of automated driving in Japan.
 - Government is contemplating the introduction of complete autonomous vehicles into the market in the late 2020's.
 - Less autonomous vehicles can be brought on public roads, provided there is a driver inside the vehicle who must handle the steering wheel, brakes and other equipment.
 - No special government approval for conducting road experiments if the vehicle satisfies applicable safety standards and has a driver.
 - National Police Agency has issued guidelines for tests.

Australia

- Road Transport Legislation - Australian Road Rules
 - The Australian National Transport Commission (NTC) released a discussion paper on changing driving laws to support automated vehicles in October 2017 with request for comment. Additional legislative action is expected in the coming months.
- Telecommunications Act 1997, Radiocommunications Act 1992, and other telecommunications regulations
- Federal Privacy Act 1988 (Cth) (Privacy Act) and its Australian Privacy Principles (APPs), in addition to State/Territory legislation



Australia

- The Australian Communications and Media Authority (ACMA) allows the country's road traffic authorities to roll out ITS which enable vehicle-to-vehicle, vehicle-to-person or vehicle-to-infrastructure communications.
 - Radiocommunications (Intelligent Transport Systems) Class License 2017
- The regulations allow the 5.9 GHz band to be used for ITS in Australia.
- Australia has also allocated the 79 GHz band for vehicle radars on an unlicensed basis, provided that the use of these devices are not to be used within the nominated distance of a specified Australian radio-astronomy site and that the device complies with relevant industry standards.

Singapore

- IMDA opened up the 5.9 GHz band for ITS applications under mobile service allocation in 2017.
- The Road Traffic (Amendment) Act 2017, which specifically regulates autonomous car trials.
 - The rules require authorization from the Singapore Land Transport Authority ("LTA") for trial of an autonomous vehicle or automated vehicle technology, or use of an autonomous vehicle, on any public road
- Personal Data Protection Act (PDPA), which governs the collection, use, disclosure and care of personal data, and accompanying regulations
- Telecommunications Act and other telecommunications regulations



Cross-Border

- 29 European countries, members of the European Union and of the European Economic Area (Norway and Switzerland) signed a Letter of Intent last year to intensify cooperation on testing of automated road transport in cross-border test sites.
- Signatory countries designated digital cross-border corridors, where vehicles would physically move across borders and where the cross-border road safety, data access, data quality and liability, connectivity and digital technologies can be tested and demonstrated.
 - Goal is to use testing to update European policies in cybersecurity, privacy, 5G, IoT, etc.
 - First set of cross-border corridors (mostly in Northern Europe) agreed in September 2017.

THANK YOU

© 2018 Morgan, Lewis & Bockius LLP
© 2018 Morgan Lewis Stamford LLC
© 2018 Morgan, Lewis & Bockius UK LLP

Morgan, Lewis & Bockius UK LLP is a limited liability partnership registered in England and Wales under number OC378797 and is a law firm authorised and regulated by the Solicitors Regulation Authority. The SRA authorisation number is 615176.

*Our Beijing office operates as a representative office of Morgan, Lewis & Bockius LLP. In Shanghai, we operate as a branch of Morgan Lewis Consulting (Beijing) Company Limited, and an application to establish a representative office of the firm is pending before the Ministry of Justice. In Hong Kong, Morgan Lewis operates through Morgan, Lewis & Bockius, which is a separate Hong Kong general partnership registered with The Law Society of Hong Kong as a registered foreign law firm operating in Association with Luk & Partners. This material is provided for your convenience and does not constitute legal advice or create an attorney-client relationship. Prior results do not guarantee similar outcomes. Attorney Advertising.

Morgan Lewis