



Morgan Lewis

TECHNOLOGY MAY-RATHON

DRIVERS, START YOUR FIREWALLS: AUTOMOTIVE CYBERSECURITY

Ronald W. Del Sesto, Jr.
Mark Krotoski
Daniel Savrin
Robert Brundage
May 23, 2017

© 2017 Morgan, Lewis & Bockius LLP

AUTOMOTIVE CYBERSECURITY

PRESENTERS

DANIEL S. SAVRIN



PARTNER

Office: Boston

Email: daniel.savrin@morganlewis.com

Phone: +1.617.951.8674

- A leader of the Morgan Lewis Automotive Sector Initiative
- A leader of the Morgan Lewis Consumer Protection Defense Initiative.
- 25+ years experience representing automotive companies in antitrust, consumer protection, class action and other complex litigation, in responding to and defending government investigations and enforcement actions and in counseling on, among other topics, consumer protection, antitrust and dealer relations matters.
- Represents automotive companies before the Department of Justice, FTC, state attorneys general, state motor vehicle agencies and in federal and state courts.
- Co-Editor, *Consumer Protection Law Developments* (Second Edition) (2016)

Morgan Lewis

RONALD W. DEL SESTO, JR.



PARTNER

Office: Boston

Email: ronald.delsesto@morganlewis.com

Phone: +1.202.739.6023

- A leader of Morgan Lewis' Privacy and Cybersecurity initiative, represents technology companies on a broad range of issues including corporate, financial, regulatory, and cybersecurity.
- Advises automotive companies, financial institutions, private equity firms and venture capital funds with respect to telecommunications, media, and technology (TMT) sectors.
- Counsels automotive companies, software, technology, and communications clients on e-commerce, cloud computing, cybersecurity, privacy, surveillance obligations, and the provision of emergency services.
- Clients include domestic and international providers of all forms of communications services, wireless, and enhanced services; service providers using emerging technologies; large end-users of telecommunications services; electronic commerce providers; Internet service providers (ISPs); trade associations; Internet portals; and providers of Internet-protocol-enabled applications and services.

Morgan Lewis

Mark L. Krotoski



PARTNER

Office: Silicon Valley

Email: mark.krotoski@morganlewis.com

Phone: +1.650.843.7212

- Litigation partner in the Privacy and Cybersecurity and Antitrust practices.
- More than 20 years' experience handling cybersecurity cases and issues, he advises clients on mitigating and addressing cyber risks, developing cybersecurity protection plans, responding to a data breach or misappropriation of trade secrets, conducting confidential cybersecurity investigations, and coordinating with law enforcement on cybercrime issues where appropriate.
- Handles a variety of complex and novel investigations and high-profile cases and has led prosecutions and investigations of nearly every type of international and domestic computer intrusion, cybercrime, economic espionage, and criminal intellectual property cases.
- Served as the national coordinator for the Computer Hacking and Intellectual Property (CHIP) Program in the DOJ's Criminal Division, in addition to other DOJ leadership positions.

Morgan Lewis

ROBERT A. BRUNDAGE



OF COUNSEL

Office: San Francisco

Email: robert.brundage@morganlewis.com

Phone: +1.405.442.1243

- Handles civil appeals and assists trial counsel with difficult legal issues, complex motions, and jury instructions.
- More than 20 years experience representing automotive manufacturers in product-liability cases and class actions, in addition to a wide variety of other business disputes, ranging from federal preemption, telecommunications, and bankruptcy to employment and arbitration.
- Has handled cases in the U.S. Supreme Court, over half the federal courts of appeals, the California Supreme Court, every district of the California Court of Appeal, and many other federal and state trial and appellate courts.
- Certified as a specialist in appellate law by the State Bar of California Board of Legal Specialization and serves as Chair of the Appellate Practice Committee at the International Association of Defense Counsel.

Morgan Lewis

Overview

- Connected Cars and the Data They Use and Collect
- Cybersecurity Risks and Vulnerabilities
- Developing FTC Perspective
- Automotive Privacy Principles
- NHTSA Perspective
- Litigation Developments in Motor Vehicle Cybersecurity and Privacy
- Areas to Watch

AUTOMOTIVE CYBERSECURITY

**CONNECTED CARS AND THE
DATA THEY USE AND
COLLECT**

Advent of the Connected Cars

What are “Connected Cars”?

- 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, diagnostic, or other information as well as to interface with other cars, homes, offices or infrastructure.
- Part of the “Internet of Things.”
- The data generated and collected is part of “Big Data.”
- OnStar introduced in 1996 is considered the starting point of connected cars.

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

Morgan Lewis

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)

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.
 - At the end of 2016, another 6 states were considering legislation governing the disclosure of such information.

AUTOMOTIVE CYBERSECURITY

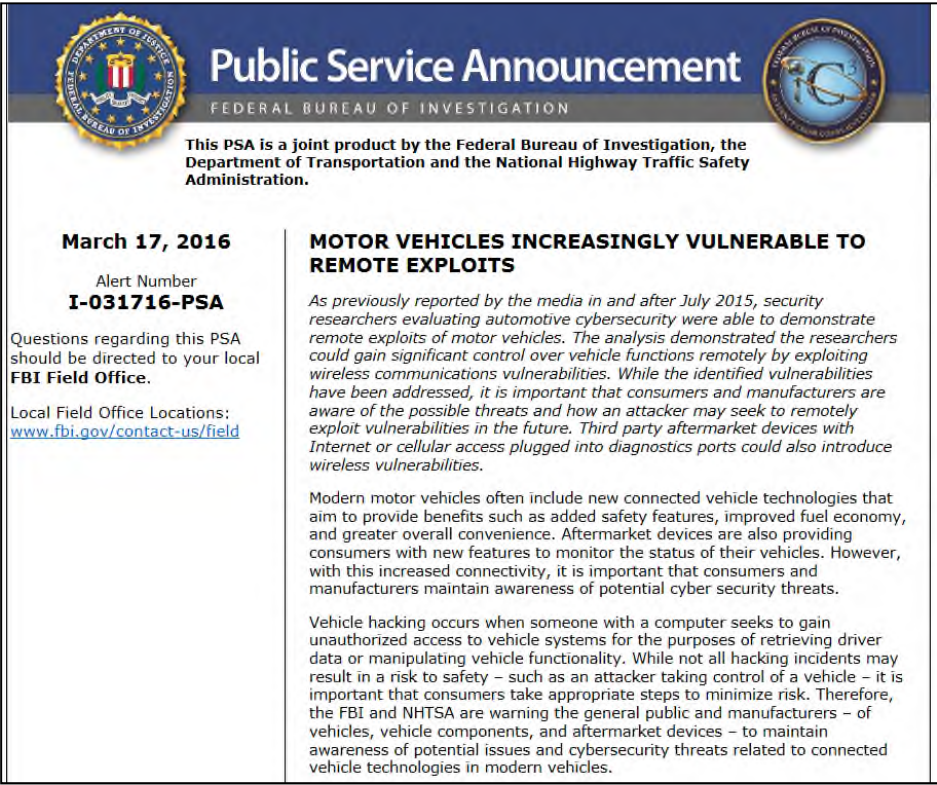
CYBERSECURITY RISKS AND VULNERABILITIES

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.

AUTOMOTIVE CYBERSECURITY

**DEVELOPING FTC
PERSPECTIVE**

Federal Trade Commission

- Federal Trade Commission – 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 – other than computers, smartphones, or tablets – that connect, communicate or transmit information with or between each other through the Internet.” Internet of Things, FTC Staff Report, January, 2015
- For purposes of FTC 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

Federal Trade Commission (cont'd)

- **January 25, 2017**: President Trump Appointed Ohlhausen as Acting Chair
 - Appointed Commissioner on April 4, 2012 to a term that expires in Sept. 2018
 - Joined by Commissioner Terrell McSweeney (appointed on April 28, 2014 to a term that expires in Sept. 2017)
- Ohlhausen has repeatedly expressed desire that the FTC approach “intervention decisions with a philosophy of regulatory humility . . . [such that] government actors must heed the limits of their knowledge, consider the repercussions of their actions, and be mindful of the private and social costs that government actions inflict.”

Acting Chair Ohlhausen's Views on Privacy

- **January 2015:** FTC Releases Staff Report on IoT
 - Commissioner Ohlhausen issues a separate statement
 - **Concurs** with much of the report:
 1. Agrees that IoT-specific legislation is not needed;
 2. Supports focus on consumer-oriented devices that collect sensitive information;
 3. Pointing to consumer harm resulting from data security failures, notes bipartisan FTC support for data security legislation;
 4. Agrees with the report's findings with respect to a myriad of methods to provide notice and choice while acknowledging the limits of these practices in the IoT space; and
 5. Highlights that a use-based approach may be the best way to address consumer privacy concerns

Acting Chair Ohlhausen's Views on Privacy (cont'd)

- **Dissents** on a few points
 1. Does not support report's recommendation for baseline privacy legislation
 2. Disputes recommendation for data minimization

Acting Chair Ohlhausen's Views on Privacy (cont'd)

- **January 2016:** FTC Releases Staff Report on Big Data
 - Commissioner Ohlhausen issues a separate statement
 1. Acknowledges the concerns of some that big data can deny opportunities and disadvantage some segments of the population;
 2. Highlights that businesses have strong incentives to compile accurate information about consumers and market forces act to correct inaccuracies;
 3. "To understand the benefits and risks of tools like big data analytics, we must also consider the powerful forces of economics and free-market competition."
 4. Hypothetical harms must be tested by economic reasoning and empirical evidence.

Acting Chair Ohlhausen's Views on Privacy (cont'd)

- **FTC Approach to Privacy:**

Opt-in consent: For unexpected collection or use of consumers' sensitive data such as Social Security numbers, financial information, certain geolocation data and information about children.

Opt-in vs. Opt-out: Regulations should maximize benefits while minimizing the costs. Opt-in or opt-out defaults should match typical consumer preferences such that costs (in the form of time and decision making) should only be imposed on consumers when it really matters. For sensitive information, this means opt-in; for non-sensitive information, opt-out.

Do No Harm: "If a regulation imposes defaults that do not match consumer preferences, it imposes costs on consumers without improving consumer outcomes. The burdens imposed by a broad opt-in requirement may also have negative effects on innovation and growth."

AUTOMOTIVE CYBERSECURITY

AUTOMOTIVE PRIVACY PRINCIPLES

Automotive Privacy Principles

- Issued by the Alliance of Automobile Manufacturers and Global Automakers.
- “Hallmarks” of the Principles:
- First, consumers can expect transparency. Automakers will employ a variety of methods to provide consumers with clear notices of their privacy practices, including through owner’s manuals and company websites.
- Second, the most sensitive types of consumer information receive heightened protections. For many, information about where and how they drive is private. Under the Automotive Privacy Principles, automakers pledge to provide protections for sensitive information that goes beyond similar principles in other industry sectors.
- Third, automakers clearly state the limited circumstances where they may share information with government authorities.

Automotive Privacy Principles (cont'd)

Key Principles:

Transparency: Participating Members commit to providing Owners and Registered Users with ready access to clear, meaningful notices about the Participating Member's collection, use, and sharing of Covered Information.

Choice: Participating Members commit to offering Owners and Registered Users with certain choices regarding the collection, use, and sharing of Covered Information.

Respect for Context: Participating Members commit to using and sharing Covered Information in ways that are consistent with the context in which the Covered Information was collected, taking account of the likely impact on Owners and Registered Users.

Automotive Privacy Principles (cont'd)

Key Principles:

Data Minimization, De-Identification & Retention: Participating Members commit to collecting Covered Information only as needed for legitimate business purposes. Participating Members commit to retaining Covered Information no longer than they determine necessary for legitimate business purposes.

Data Security: Participating Members commit to implementing reasonable measures to protect Covered Information against loss and unauthorized access or use.

Integrity & Access: Participating Members commit to implementing reasonable measures to maintain the accuracy of Covered Information and commit to giving Owners and Registered Users reasonable means to review and correct Personal Subscription Information.

Morgan Lewis

Automotive Privacy Principles (cont'd)

Key Principles:

Accountability: Participating Members commit to taking reasonable steps to ensure that they and other entities that receive Covered Information adhere to the Principles.

Full Principles Document Available at : https://autoalliance.org/wp-content/uploads/2017/01/Consumer_Privacy_Principlesfor_VehicleTechnologies_Services.pdf

AUTOMOTIVE CYBERSECURITY

NHTSA PERSPECTIVE

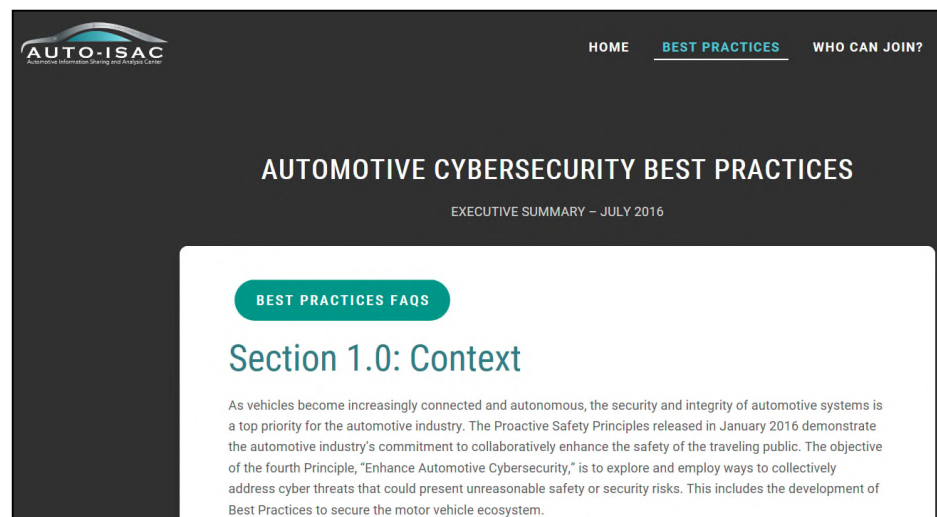
Emerging Regulatory Issues

- Preliminary Questions
 - Industry role
 - Which enforcers?
 - Concurrent jurisdiction
 - Level of regulation
 - Congressional role



Auto-ISAC

- Key Cybersecurity Functions
 - Security by design
 - Risk assessment and management
 - Threat detection and protection
 - Incident response
 - Collaboration and engagement with appropriate third parties
 - Governance
 - Awareness and training



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. The main content area features a news article titled "U.S. DOT issues Federal guidance to the automotive industry for improving motor vehicle cybersecurity" with a "← NEWS" link. Below the title are social media sharing icons for Facebook, Twitter, LinkedIn, and Email. The article date is "October 24, 2016 | Washington, DC" and the text begins with "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](#) [twitter](#) [in](#) [envelope](#)

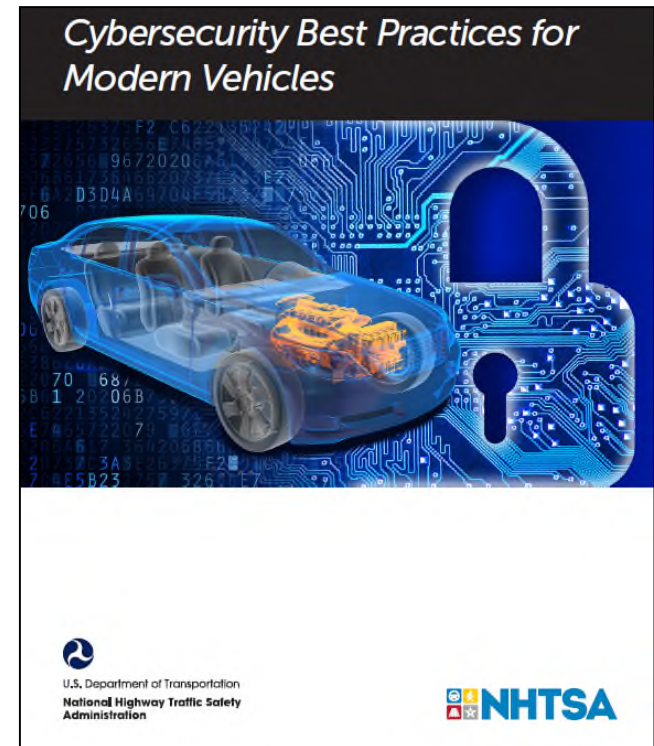
October 24, 2016 | Washington, DC

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

Morgan Lewis

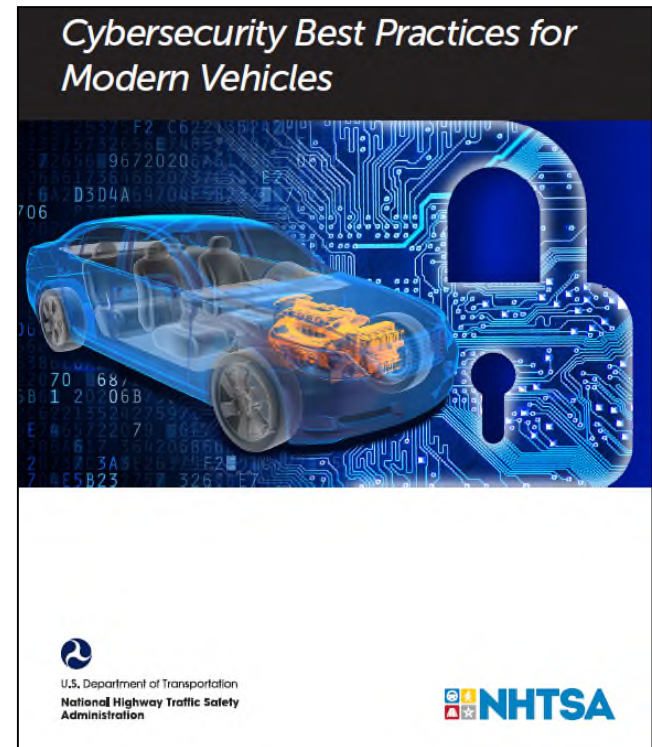
NHTSA Cybersecurity Guidance (cont'd)

- Non-Binding
- Layered approach
 - Risk-based prioritized identification and protection
 - Timely detection and rapid response to incidents
 - Methods and measures for rapid recovery from incidents
 - Lessons learned through information sharing



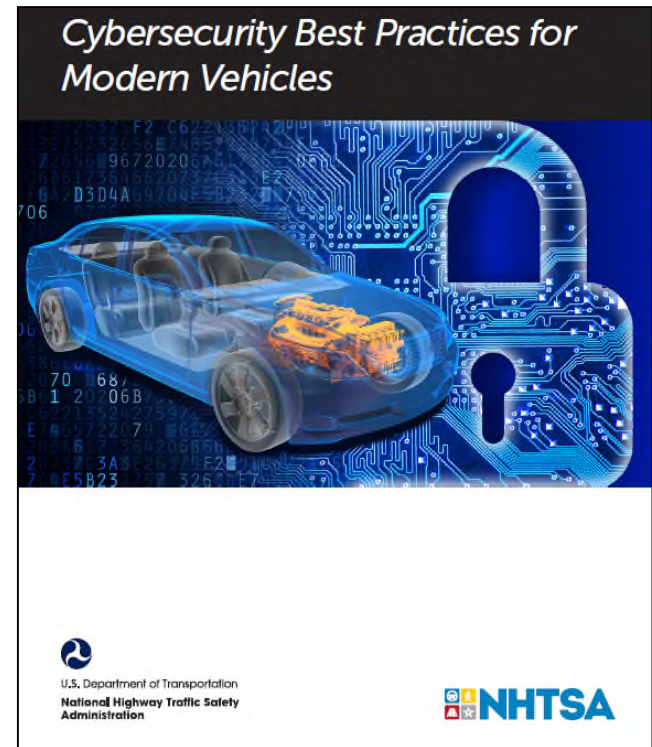
NHTSA Cybersecurity Guidance (cont'd)

- Promote “cybersecurity oriented leadership within the organization” throughout the entire product development cycle
- Incorporate “an ongoing risk management framework” to assess vulnerabilities at each stage in the process: including in “the entire supply-chain of operations; and in “ the organization” over the product development cycle



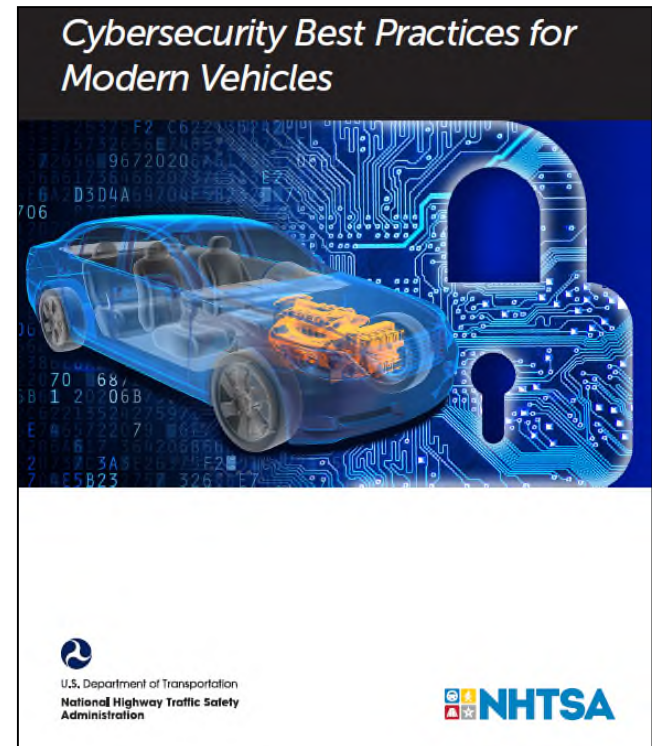
NHTSA Cybersecurity Guidance (cont'd)

- In “an ongoing risk management framework” assess vulnerabilities at each stage in the process, including “the entire supply-chain of operations”
- Implement “a documented process for responding to incidents, vulnerabilities, and exploits” that clearly delineates roles and responsibilities for each responsible group within the organization



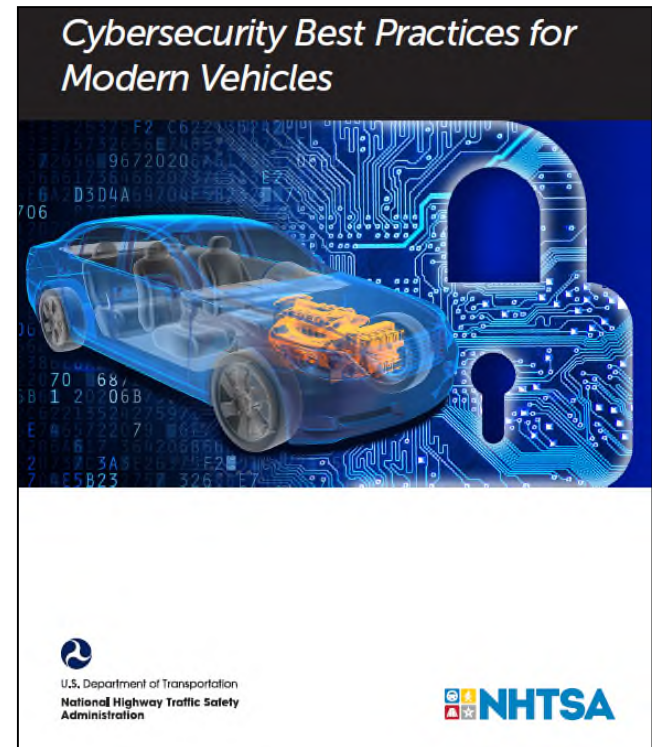
NHTSA Cybersecurity Guidance (cont'd)

- Conduct cybersecurity testing, including penetration testing, by “qualified testers who have not been part of the development team, and who are highly incentivized to identify vulnerabilities”
- Adopt self-auditing programs that include periodic risk assessments and review of organizational decisions
- Encourage information sharing about cybersecurity risks and incidents including through the Auto Automotive Information Sharing and Analysis Center (ISAC)



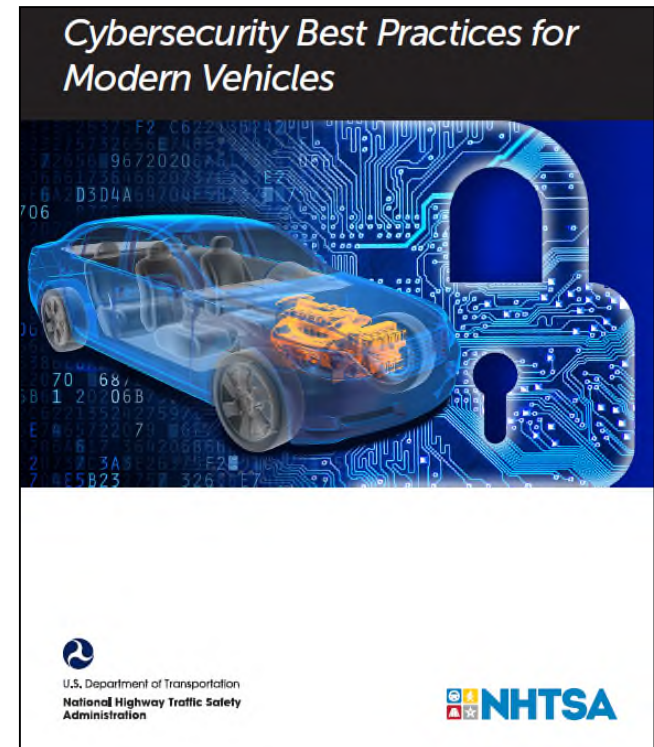
NHTSA Cybersecurity Guidance (cont'd)

- Consider the role of aftermarket devices (such as cell phones and insurance dongles [devices that monitor driving habits])
- Remove unnecessary network services to control the proliferation of network ports and limit attack vectors
- Limit software developer access to ECUs where “no foreseeable operational reason” exists
- Maintain sufficient log records to identify how the cyber attacks occurred or detect trends



NHTSA Cybersecurity Guidance (cont'd)

- Implement employee training to educate the entire automotive workforce on new cybersecurity practices, and share lessons learned
- Address serviceability issues by providing “strong vehicle cybersecurity protections that do not unduly restrict access by authorized alternative third-party repair services.”



Congress

- NHTSA conduct study to determine and recommend standards for the regulation of the cybersecurity of motor vehicles:
 - measures necessary to separate critical software systems that can affect the driver's control of the movement of the vehicle from other software systems;
 - measures necessary to detect and prevent or minimize anomalous codes, in vehicle software systems, associated with malicious behavior;
 - techniques necessary to detect and prevent, discourage, or mitigate intrusions into vehicle software systems;
 - best practices to secure driving data about a vehicle's status or about the owner, lessee, driver, or passenger of a vehicle that is collected; and
 - a timeline for implementing systems and software that reflect such measures, techniques, and best practices.

Morgan Lewis

115TH CONGRESS 1ST SESSION	H. R. 701
To direct the Administrator of the National Highway Traffic Safety Administration to conduct a study to determine appropriate cybersecurity standards for motor vehicles, and for other purposes.	
IN THE HOUSE OF REPRESENTATIVES	
JANUARY 24, 2017	
Mr. WILSON of South Carolina (for himself and Mr. TED LIEU of California) introduced the following bill; which was referred to the Committee on Energy and Commerce	
A BILL	
To direct the Administrator of the National Highway Traffic Safety Administration to conduct a study to determine appropriate cybersecurity standards for motor vehicles, and for other purposes.	
1 <i>Be it enacted by the Senate and House of Representa-</i>	
2 <i>tives of the United States of America in Congress assembled,</i>	
3 SECTION 1. SHORT TITLE.	
4 This Act may be cited as the "Security and Privacy	
5 in Your Car Study Act of 2017" or the "SPY Car Study	
6 Act of 2017".	

AUTOMOTIVE CYBERSECURITY

**LITIGATION DEVELOPMENTS
IN MOTOR VEHICLE
CYBERSECURITY AND
PRIVACY**

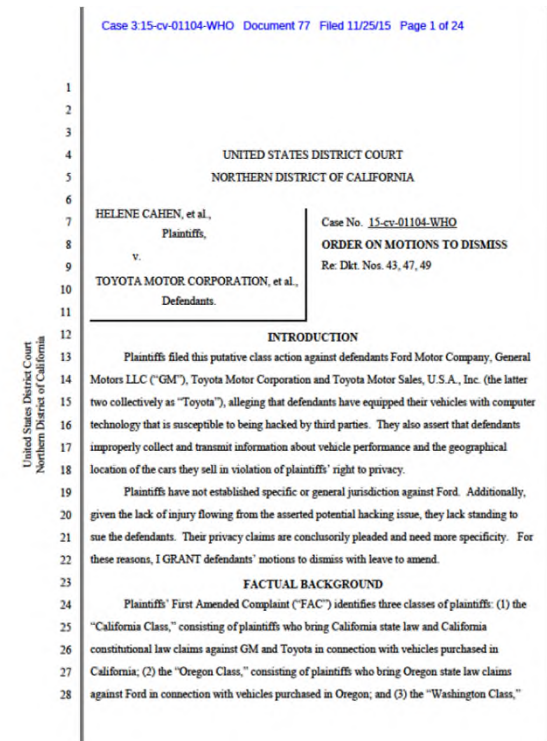
Cybersecurity and Privacy Putative Class Actions

- *Cahen v. Toyota Motor Corporation, et al.* U.S. District Court for the Northern District of California and now U.S. Court of Appeals for the Ninth Circuit.
- Plaintiffs sued Toyota, Ford and GM, alleging:
 - That defendants equipped their vehicles with computer technology that is susceptible to being hacked by third parties.
 - That defendants improperly collected and transmitted information about vehicle performance and the geographical location of the cars they sell.
- Multiple legal theories
 - Unfair Competition
 - California Consumers' Legal Remedies Act
 - False Advertising
 - Breach of implied warranty of merchantability
 - Breach of warranty or contract (failing to repair or replace vehicles)
 - Misrepresentation
 - Invasion of privacy under California Constitution's right of privacy

Cybersecurity and Privacy Putative Class Actions (cont'd)

Cahen v. Toyota Motor Corporation, et al. (cont'd)

- Dismissed
 - Cybersecurity: No injury and no standing to sue in federal court
 - Plaintiffs “do not allege that anybody outside of a controlled environment has ever been hacked.”
 - Threat of future harm from hacking insufficient
 - No allegation of concrete harm from collection and tracking of personal data.
 - Privacy: Failure to state claim.
 - Driving history, performance and location are not sensitive and confidential information.
 - Plaintiffs’ fear that data will be disclosed and cause hacking is speculative.
 - Plaintiff appealed to U.S. Court of Appeals for Ninth Circuit – pending.
- Morgan Lewis**



Cybersecurity and Privacy Putative Class Actions (cont'd)

Flynn vs FCA U.S. LLC, et al.

- Plaintiffs allege that FCA vehicles equipped with Harman-manufactured infotainment systems suffer from defects that make them vulnerable to hacking and remote access
- Purported class action
- No privacy allegations
- Legal theories (Illinois and Missouri law)
 - Breach of implied warranty
 - Misrepresentation
 - Negligent design
 - Failure to warn about cyber-vulnerability
 - Unjust enrichment
 - Consumer-protection laws

Case 3:15-cv-00855-MJR-DGW Document 1 Filed 08/04/15 Page 1 of 42 Page ID #1

IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF ILLINOIS

BRIAN FLYNN; and GEORGE)
and KELLY BROWN on behalf)
of themselves and all others)
similarly situated,)
)
Plaintiffs,) Case No. 3:15-cv-855

v.)
)
FCA US LLC f/k/a)
CHRYSLER GROUP LLC and)
HARMON INTERNATIONAL)
INDUSTRIES, INC.)
Defendants.)

CLASS ACTION COMPLAINT

NOW COMES Plaintiffs Brian Flynn and George and Kelly Brown, on behalf of themselves and all others similarly situated, and for their Class Action Complaint pursuant to Rule 23 of the Federal Rules of Civil Procedure, allege as follows:

NATURE OF ACTION

1. Plaintiffs, and the Class members they propose to represent, purchased or leased defective vehicles manufactured by Defendant FCA US LLC. The defective vehicles come equipped with an infotainment system called "uConnect." Defendant Harmon International Industries, Inc. is the manufacturer and supplier of the uConnect systems.
2. These vehicles are defectively designed in that this uConnect system has the access and capability to communicate over vehicle networks that control critical powertrain and safety related functions. uConnect is vulnerable to malicious computer hacks and should thus be segregated from other critical vehicle systems.

Cybersecurity and Privacy Putative Class Actions (cont'd)

Flynn vs FCA U.S. LLC, et al. (cont'd)

- Court has dismissed some claims and some plaintiffs were sent to arbitration.
- Court has ruled:
 - Plaintiffs lack federal-court standing to pursue damages for risk of harm.
 - Plaintiffs can't seek court-ordered recall.
 - Some theories fail to state claims under state laws.
- Case continues

Case 3:15-cv-00855-MJR-DGW Document 1 Filed 08/04/15 Page 1 of 42 Page ID #1

IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF ILLINOIS

BRIAN FLYNN; and GEORGE)
and KELLY BROWN on behalf)
of themselves and all others)
similarly situated,)
)
Plaintiffs,) Case No. 3:15-cv-855
)
v.)
)
FCA US LLC f/k/a)
CHRYSLER GROUP LLC and)
HARMON INTERNATIONAL)
INDUSTRIES, INC.)
Defendants.)

CLASS ACTION COMPLAINT

NOW COMES Plaintiffs Brian Flynn and George and Kelly Brown, on behalf of themselves and all others similarly situated, and for their Class Action Complaint pursuant to Rule 23 of the Federal Rules of Civil Procedure, allege as follows:

NATURE OF ACTION

1. Plaintiffs, and the Class members they propose to represent, purchased or leased defective vehicles manufactured by Defendant FCA US LLC. The defective vehicles come equipped with an infotainment system called "uConnect." Defendant Harmon International Industries, Inc. is the manufacturer and supplier of the uConnect systems.

2. These vehicles are defectively designed in that this uConnect system has the access and capability to communicate over vehicle networks that control critical powertrain and safety related functions. uConnect is vulnerable to malicious computer hacks and should thus be segregated from other critical vehicle systems.

Future Litigation

- Privacy
 - If hackers obtain consumers' private information (from manufacturer's servers or by hacking vehicles), plaintiffs may attempt "traditional" data-breach suit
 - Class actions
 - Shareholder derivative suits
 - Analogy: Target, Home Depot litigation
 - Many of same legal issues as in other data-breach suits, including
 - Standing in federal court (*Spokeo*)
 - Questions re whether privacy laws provide private right of action
 - Whether plaintiffs were damaged and how to calculate damages
 - Timeliness of notice to affected consumers
 - Potential SEC enforcement if material to stock price and not appropriately disclosed
- Product liability
 - If hackers gain control of vehicle and cause a crash, risk of traditional product liability suit

AUTOMOTIVE CYBERSECURITY

AREAS TO WATCH

State regulation of cyber and data security

- Besides NHTSA and FTC, at least one state has moved to regulate automotive cyber-security
 - California DMV's proposed autonomous-vehicle regulations require manufacturer to certify that the vehicle meets best practices for detecting and responding to cyberattacks.
 - Industry has questioned need for requirement since other laws already address cybersecurity and apply to autonomous cars. No formal decision yet.
 - Depending on outcome, could see other states following suit, particularly if there is a major automotive cybersecurity incident.
- More than half the states have data-disposal laws.
- Over a dozen states have laws addressing data security (e.g. require businesses maintaining personal information of resident of that state to follow reasonable security practices and protect against unauthorized access)

Data Breach Laws and Litigation

- 48 states + DC, Puerto Rico, Guam, Virgin Islands have data breach notification laws requiring notification to individuals and/or governmental entities when certain kinds of data breaches occur
 - Enforcement actions
 - Private rights of action
 - Class actions
- Will automakers be targeted?
- Valuable information maintained in vehicles or by automakers' or third-party servers:
 - Name/address/financial account information used to subscribe to services
 - Contact/phone/address book from synced phones
 - Location information
 - Users' biometric information (fingerprint, face) for vehicle's user recognition
 - Automated license plate recognition system information
 - Garage-door codes (useful for thieves)

Upcoming NHTSA/FTC Workshop – June 28

- Topics on the Agenda:
 - the types of data vehicles with wireless interfaces collect, store, transmit, and share;
 - potential benefits and challenges posed by such data collection;
 - the privacy and security practices of vehicle manufacturers;
 - the role of the FTC, NHTSA, and other government agencies regarding privacy and security issues related to connected vehicles; and
 - self-regulatory standards that might apply to privacy and security issues related to connected vehicles.

NHTSA/FTC workshop announcement available at: <https://www.ftc.gov/news-events/events-calendar/2017/06/connected-cars-privacy-security-issues-related-connected>

Morgan Lewis

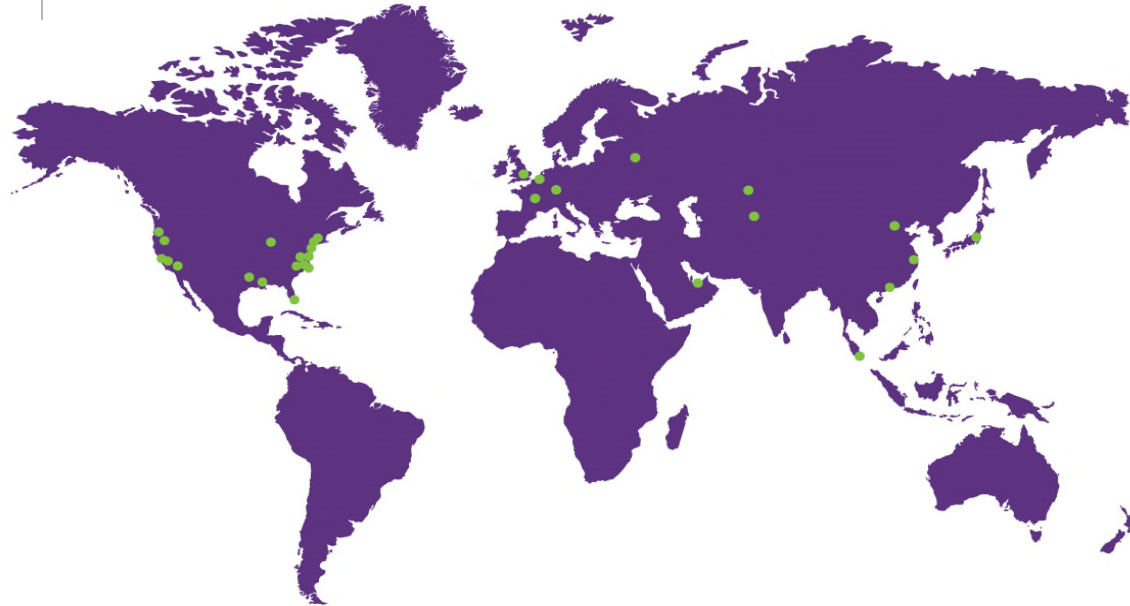
AUTOMOTIVE CYBERSECURITY
QUESTIONS?

Our Global Reach

Africa
Asia Pacific
Europe
Latin America
Middle East
North America

Our Locations

Almaty	Dallas	London	Paris	Shanghai*
Astana	Dubai	Los Angeles	Philadelphia	Silicon Valley
Beijing*	Frankfurt	Miami	Pittsburgh	Singapore
Boston	Hartford	Moscow	Princeton	Tokyo
Brussels	Hong Kong*	New York	San Francisco	Washington, DC
Chicago	Houston	Orange County	Santa Monica	Wilmington



Morgan Lewis

*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 has filed an application to become a registered foreign law firm and is seeking approval with The Law Society of Hong Kong to associate with Luk & Partners.

THANK YOU

© 2017 Morgan, Lewis & Bockius LLP
© 2017 Morgan Lewis Stamford LLC
© 2017 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 has filed an application to become a registered foreign law firm and is seeking approval with The Law Society of Hong Kong to associate 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