

What's Really Under the Hood? Deconstructing the Near Future Vehicle through the Lens of Data Security and Privacy

Claudia Rast
Jennifer Dukarski

@RastLaw
@JDukarski

[*Rast@Butzel.com*](mailto:Rast@Butzel.com)
[*Dukarski@Butzel.com*](mailto:Dukarski@Butzel.com)

What are we Deconstructing?

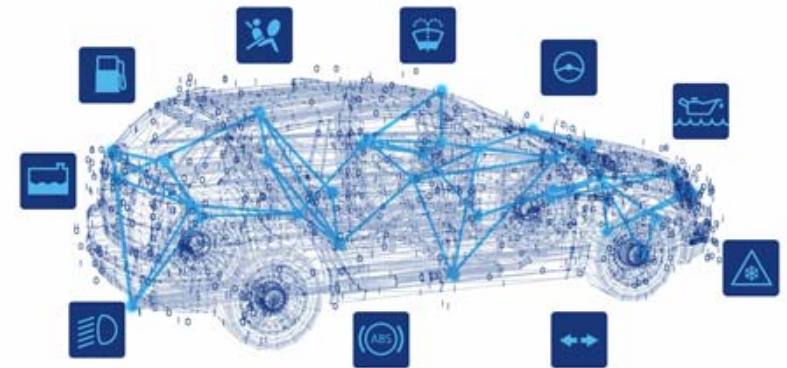
- We are Deconstructing:
 - The Technical
 - Industry Response
 - Existing Laws: Cybersecurity & Privacy
 - Regulations, Standards & Guidelines
 - Lawsuits & Claims: Product Liability, Recall, & Warranty

What's Really Under the Hood

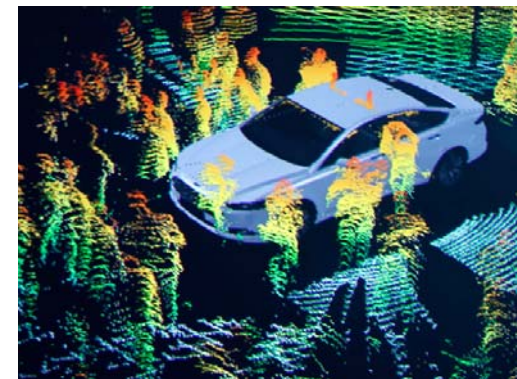
DECONSTRUCTING THE TECHNICAL

The Devices in our Vehicles

- Event data recorders
- Insurance dongles
- Diagnostic systems
- Navigation and entertainment systems
- Cellular connections and hot spots
- Autonomous vehicles may generate more than 300 TB of data per year!



Source: <http://360.here.com/wp-content/uploads/2013/08/Sensors.jpg>



Source: *IEEE Spectrum*

Understanding Data Flow Issues in Products

- What types of data exist?
 - Geo-location
 - Vehicle behavioral data
 - Event Data Recorder (“EDR”)
- How is it generated?
 - Automatically (EDR)
 - Opt In (Apple Play)
- Where is it kept?
 - Locally (the vehicle)
 - The “Cloud”
 - Data Centers (foreign and domestic)



Traditional (and new) Data Collections

- Driver's eye movements
- Weight of front seat passengers
- Driver's hands on the steering wheel
- Vehicle behavior data (speed, torque)
- Geolocation data
- Autonomous sensing data (radar, LIDAR, camera, ultrasonic, GNSS, IMU)

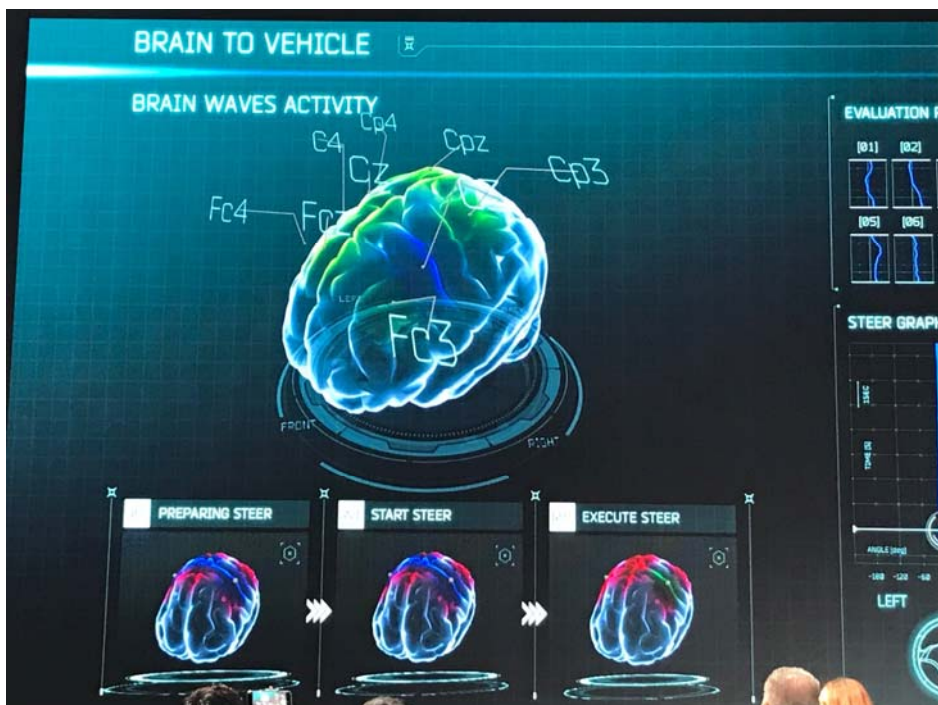


Emerging Biometrics Application to Improve Driver Safety

- Monitoring drivers' attention to prevent or alert in drowsy driving situations
- Assessing stressors in the driving function to mitigate escalating anger
- Predictive analytics to mitigate or respond to emergency situations disabling the driving function
- Providing autonomous mobility to those unable to perform driving tasks



Biometrics as an Automotive Feature



- **Nissan:** brain to vehicle applications to optimize steering and other features
- **Hyundai Genesis:** fingerprints and facial recognition for vehicle entry
- **Continental CAR Demo:** biometric ignition switch concept - facial recognition, fingerprint and voiceprint used to start the vehicle
- **Mitsubishi Electric:** EMIRAI concept that recognizes a driver's face then takes the temperature of the driver face while measuring the heart rate in the seat

What's Really Under the Hood

DECONSTRUCTING INDUSTRY RESPONSE

Consumer Privacy Protection Principles – Nov 2014

Alliance of Automobile Manufacturers & Association of Global Automakers

- Published “ *Consumer Privacy Protection Principles*,” sent to the FTC
- Offers baseline privacy commitments for automakers
- Based on the Fair Information Practice Principles, which have served as the basis for privacy frameworks in the US and around the world for over 40 years

Seven Principles:

- Transparency
- Choice
- Respect for Context
- Data Minimization, De-Identification & Retention
- Data Security
- Integrity & Access
- Accountability

What's Really Under the Hood

DECONSTRUCTING EXISTING LAWS: CYBERSECURITY & PRIVACY

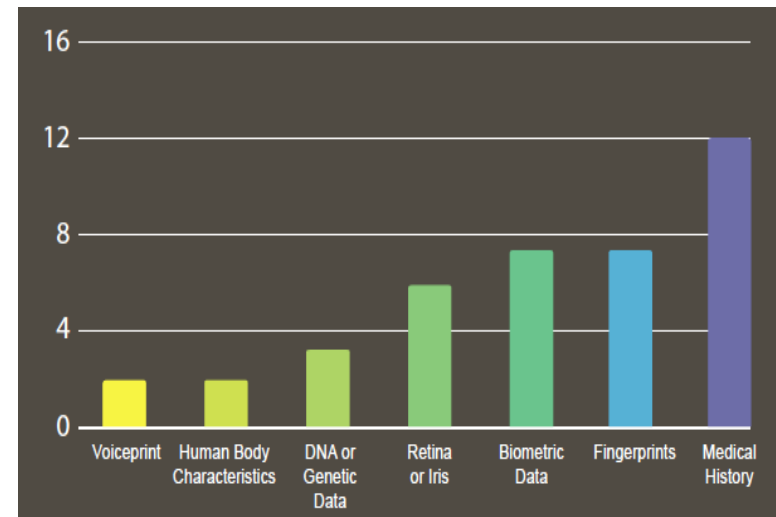
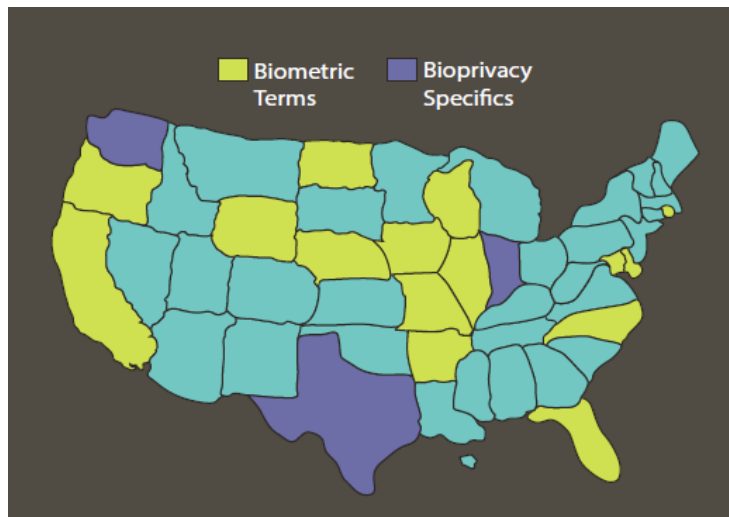
Privacy and Cyber Laws

- Criminal Code—Title 18
 - Computer Fraud & Abuse Act, 18 U.S.C. § 1030
 - Wiretap Act, 18 U.S.C. § 2511
 - Stored Communications Act (unlawful access), 18 U.S.C. § 2701
 - Identity Theft, 18 U.S.C. § 1028(a)(7) & § 1028A
 - Electronic Communications Privacy Act, 18 U.S.C. §§ 2510-2522
 - Economic Espionage Act, 18 U.S.C. §§ 1831-1839
- HIPAA/HITECH & GINA (Healthcare)
- FTC Act (Online Commerce)
- GLB & OCC (Financial),
- Federal Privacy Act (Gov't)

Privacy and Cyber Laws (Continued)

- FIPS 199 & 200
- Fair Credit Reporting Act
- State Data Privacy and Data Breach Laws
- General Data Privacy Regulation (GDPR)
- Data Protection Act 2018 (UK)
- California's "GDPR-lite" – California Consumer Privacy Act
- Nevada's "Act Related to Internet Privacy" – Senate Bill 220

State Biometric Privacy Laws



Illinois Biometric Information Privacy Act (BIPA), Texas Capture or Use of Biometric Identifier (CUBI), and Washington's Bioprivacy law establish state-specific biometric requirements. Additionally, over sixteen states have general data privacy laws that protect certain classes of biometric data.

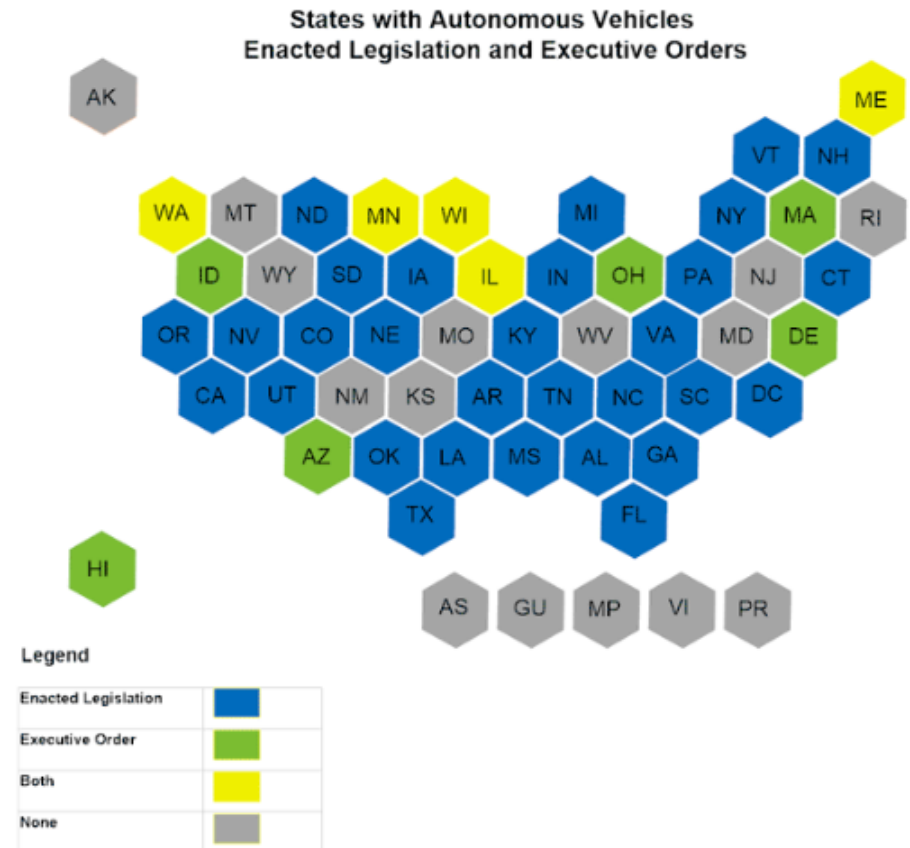
Thus, the Patchwork: Example – Cyber and Privacy

- Each state has a unique approach to managing cyber and privacy
- Some states have prescriptive areas (e.g., NYDFS) and others have the bare minimum requirements even in the event of data breaches (e.g., Michigan)



AV Regulations: Another 50 State Patchwork Example

- Similarly, autonomous vehicle regulations vary from state to state addressing:
 - Requirements for testing
 - Licensing requirements
 - Additional support and pilot programs
- States appear to be in a “Hunger Games” styled competition to be “THE” AV state



State Laws & Automotive Data Ownership

- These laws often address
 - Whether disclosure is allowed in the owner’s manual or in the purchase agreement
 - The conditions under which data may be downloaded (consent, emergency, court order, etc.)
 - Ownership of the data

State	Statute	Requires disclosure of event data recorders ("sensing diagnostic modules") in vehicles	Prohibits download of data, except under stated conditions:	Other
Arkansas	Ark. Code § 23-112-107	In a written notice at time of new vehicle purchase from dealership. Also requires disclosure in agreements with subscription services.	1) with owner’s written consent; 2) court order; 3) emergency investigation; 4) emergency medical care; 5) medical and vehicle safety research; or 6) to diagnose, service, or repair the vehicle; 7) probable cause of an offense.	Permission cannot be a condition of payment/ settlement of an insurance claim, or of a lease or insurance agreement.
California	Calif. Veh. Code § 9951	In the owner’s manual of new cars. Also requires disclosure in agreements with subscription services.	1) with owner’s consent; 2) court order; 3) vehicle safety research; 4) diagnosing, servicing, or repairing the vehicle.	
Colorado	CRS §§ 42-4-2401 to -2403	In or along with the owner’s manual of vehicles manufactured after May 2007 and sold or leased in Colorado. Also requires disclosure in agreements with subscription services.	1) with owner’s written consent within 30 days of retrieval; 2) court order; 3) vehicle safety research; 4) diagnosing, servicing, or repairing the vehicle; 5) in legal discovery.	

Presidential Action: Executive Order 13691

Promoting Private Sector Cybersecurity Information Sharing strongly encourages the development and formation of industry-specific Information Sharing and Analysis Organizations and calls on private companies, nonprofit organizations, executive departments, agencies, and other entities to “share information related to cybersecurity risks and incidents and collaborate in as close to real time as possible



What's Really Under the Hood

DECONSTRUCTING THE REGULATIONS, STANDARDS & GUIDELINES

The Historical Regulatory Power of NHTSA

- The Motor Vehicle Safety Act (1966):
 - compel industry to pursue innovations,
 - make rules to ensure citizens are safe in their vehicles, and
 - oversee the recall of defective vehicles
- In its first decade, NHTSA lost 6 of 10 rulemaking cases
- But, the recall mandate led to the “Ice Age of Rulemaking” (1987-2002)



Jerry Mashaw and David Harfst. *From Command and Control to Collaboration and Deference: The Transformation of Auto Safety Regulation*. 34 YALE J. ON REG. 167 (2018)

NHTSA & Cybersecurity

- In 2012, NHTSA established a new division, **Electronic Systems Safety Research**, to conduct research on the safety, security, and reliability of complex, interconnected, electronic vehicle systems.
- NHTSA expanded its research and testing capabilities in vehicle electronics at the **Vehicle Research and Test Center in East Liberty, Ohio**.
- NHTSA established an internal agency working group, the **Electronics Council** responsible for collaborating on issues related to vehicle electronics, including cybersecurity.

NHTSA & Cybersecurity

- In 2016, NHTSA released *Cybersecurity Best Practices for Modern Vehicles* which encourages the industry to:
 - Perform cybersecurity gap assessments
 - Execute cybersecurity plans
 - Integrate controls into vehicle systems and business operations
 - Report and monitor progress through iterative cycles



The Role of the FTC in Privacy & Automobiles

- Examples of Automotive Related Rules:
 - Financial Privacy Rule
 - Used Car Rule
 - Interpretation of the Magnuson-Moss Warranty Act
 - Deceptive Pricing and Advertising
- Privacy
 - Section 5 of the FTC Act (bars unfair and deceptive acts)
 - Enforcement of consumer privacy and security laws



The FTC & Consent: The Lessons of Vizio



- Starting in 2014, Vizio televisions tracked what consumers were watching and transmitted the data to remote servers

- The data included IP addresses, wired and wireless MAC addresses, WiFi signal strength, and nearby WiFi access points that were sent to data aggregators who matched the data to individual consumers

Vizio – The Fallout

- The FTC and the New Jersey AG filed a complaint resulting in a \$2.2 million settlement
- What did Vizio get wrong?
 - Collected data using an automated content recognition software without user consent or knowledge
 - Stored 100 billion data points collected daily on 10 million viewers for an indefinite period of time
 - Sold viewing history to third parties

How the Regulators Have Responded

EXECUTIVE SUMMARY

Preparing for the Future of Transportation: Automated Vehicles 3.0 (AV 3.0) advances U.S. DOT's commitment to supporting the safe, reliable, efficient, and cost-effective integration of automation into the broader multimodal surface transportation system. AV 3.0 builds upon—but does not replace—voluntary guidance provided in *Automated Driving Systems 2.0: A Vision for Safety*.

Automation technologies are new and rapidly evolving. The right approach to achieving safety improvements begins with a focus on removing unnecessary barriers and issuing voluntary guidance, rather than regulations that could stifle innovation.

In AV 3.0, U.S. DOT's surface transportation operating administrations come together for the first time to publish a Departmental policy statement on automation. This document incorporates feedback from manufacturers and technology developers, infrastructure owners and operators, commercial motor carriers, the bus transit industry, and State and local governments.² This document considers

automation broadly, addressing all levels of automation (SAE automation Levels 1 to 5), and recognizes multimodal interests in the full range of capabilities this technology can offer.³

AV 3.0 includes six principles that guide U.S. DOT programs and policies on automation and five implementation strategies for how the Department translates these principles into action (see facing page).

AV 3.0 Provides New Multimodal Safety Guidance

In accordance with the Department's first automation principle, AV 3.0 outlines how automation will be safely integrated across passenger vehicles, commercial vehicles, on-road transit, and the roadways on which they operate. Specifically, AV 3.0:

- Affirms the approach outlined in *A Vision for Safety 2.0* and encourages automated driving system developers to make their

Voluntary Safety Self-Assessments public to increase transparency and confidence in the technology.

- Provides considerations and best practices for State and local governments to support the safe and effective testing and operation of automation technologies.
- Supports the development of voluntary technical standards and approaches as an effective non-regulatory means to advance the integration of automation technologies into the transportation system.
- Describes an illustrative framework of safety risk management stages along the path to full commercial integration of automated vehicles. This framework promotes the benefits of safe deployment while managing risk and provides clarity to the public regarding the distinctions between various stages of testing and full deployment.
- Affirms the Department is continuing its work to preserve the ability for transportation safety applications to function in the 5.9 GHz spectrum.

³ SAE International, J3016_201806: Taxonomy and Definitions for Terms Related to Driving Automation Systems for On-Road Motor Vehicles (Warrendale: SAE International, 15 June 2018), https://www.sae.org/standards/content/j3016_201806/.

² See Appendix B for a summary of public input received.

- Supports the development of voluntary technical standards and approaches as an effective non-regulatory means to advance the integration of automation technologies into the transportation system.

APPENDIX C

VOLUNTARY TECHNICAL STANDARDS FOR AUTOMATION

Standardization-related needs associated with surface vehicle automation are in various stages of identification, development, definition, and adoption. Standardization-related documents can include voluntary technical standards published by standards developing organizations (SDOs) as well as specifications, best practices descriptions and other types of documents. These include ISO 26262 Road Vehicles Functional Safety and SAE's J3016_201806 Taxonomy and Definitions for Terms Related to On-Road Motor Vehicle Automated Driving Systems. There are many existing standards, but they may not fully address automated vehicle needs. Some standards specific to automated vehicles and many standards in other automation-relevant domains have been developed, but gaps remain where activity is underway or anticipated.

In addition to those standards that support interoperable integration, many standards development efforts are focused on describing common terminology, required performance capabilities, and interfaces between subsystems inside automated systems. These efforts include both automation-specific standards and domain-specific standards—for example, Information and Communications Technology (ICT) standards—applicable to subsystems and technologies that are then integrated into the overall automation system or surface transportation system. There are also sets of published best practices and frameworks that complement and are used in conjunction with voluntary technical standards. For example, the NIST cybersecurity framework describes a holistic approach to mitigating cyber threats across complex systems.

The Department will continue our cooperative, coordinated approach to supporting development of stakeholder-driven voluntary technical standards and similar documents across internal modal partners. The Department will follow a similar process to the approach for modernizing regulation, including:

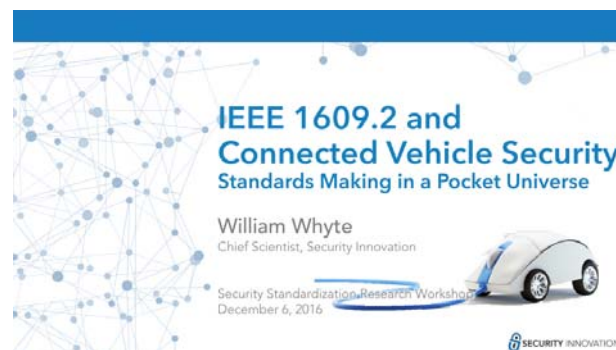
1. **Gather information** through research, internal analysis, and stakeholder engagement on voluntary technical standardization needs.
2. **Explore and execute new approaches** to meet technical challenges in a way acceptable to the broad, diverse stakeholder community.
3. **Work to ease implementation** of automated vehicle products by supporting development of voluntary technical standards, system architecture options and user services for the interface between vehicles and infrastructure, along with companion software toolsets and implementation support programs.

Means include cooperation and funding support to SDOs, cooperation with industry and governmental partners, making Federal technical expertise available, and international coordination.
4. **Cooperate with stakeholders** to maximize interoperability throughout North America as well as to take advantage of common international interests and global expertise by leveraging work across multiple regions and markets.

Vehicle automation systems represent one element of a larger system-of-systems architecture within surface transportation. Vehicle manufacturers

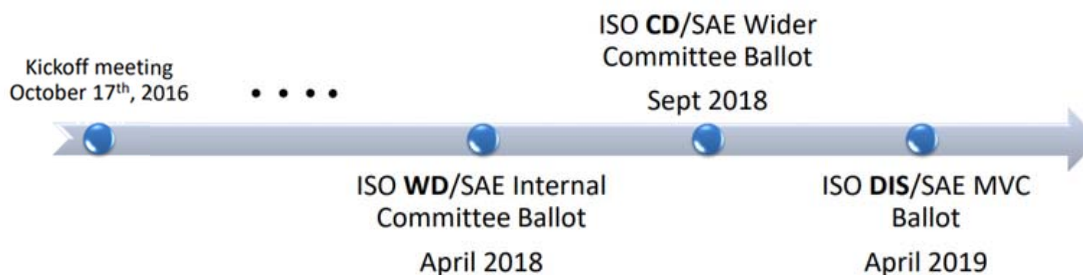
At the End of the Day: Reliance on Standards

- ISO 26262
- ISO/SAE 21434
- ISO/PAS 21448



1. Vocabulary		
2-3 Overall safety management	2-4 Safety management during the concept phase and the product development phases	2-7 Safety management during production, operation, service and decommissioning
3. Concept phase		
3-4 Item definition	4-3 Concept topics for the product development at the system level	4-9 Safety validation
3-6 Hazard analysis and risk assessment	4-4 Technical safety concept	4-8 System and item introduction and verification
3-7 Functional safety concept	4-7 System architectural design	
4. Product development at the system level		
5. Production, operation, service and decommissioning		
5-8 Planning for production, operation, service and decommissioning		
7-4 Production		
7-7 Operation, service and decommissioning		
6. Product development at the hardware level		
6. Product development at the software level		
6-4 Concept topics for the product development at the hardware level	6-4 Specific topics for the product development at the software level	
6-5 Specification of hardware safety requirements	6-5 Specification of software safety requirements	
6-7 Hardware design	6-7 Software architecture design	
6-8 Evaluation of the safety-critical hardware architectural metrics	6-8 Software unit design and implementation	
6-9 Evaluation of the safety-critical hardware architectural metrics	6-9 Software unit verification	
6-10 Hardware integration and verification	6-10 Software integration and verification	
6-11 Testing of the embedded software		
8. Supporting processes		
8-4 Interfaces within distributed developments	8-8 Verification	8-14 Proven in use argument
8-6 Specification and management of safety requirements	8-10 Documentation management	8-15 Interfacing a base vehicle or item in an application out of scope of ISO 26262
8-7 Configuration management	8-11 Confidence in the use of software tools	8-18 Integration of safety-related systems not developed according to ISO 26262
8-8 Change management	8-12 Qualification of software components	
	8-13 Evaluation of hardware elements	
9. ASIL-oriented and safety-oriented analyses		
9-4 Requirements decomposition with respect to ASIL tailoring	9-7 Analysis of dependent failures	
9-6 Criteria for coexistence of elements	9-8 Safety analyses	
10. Guideline on ISO 26262		

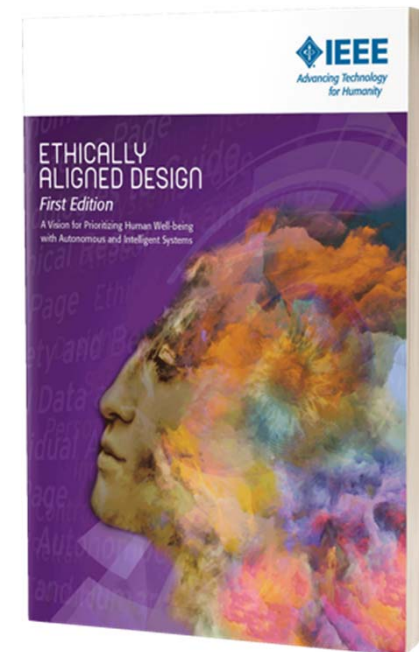
ISO/SAE 21434 – High-level Timeline



Expect a late 2019 or 2020 release

Data Privacy Ethics and Intelligent Systems

- **Data Agency**–A/IS creators shall empower individuals with the ability to access and securely share their data, to maintain people’s capacity to have control over their identity.
- **Transparency**–The basis of a particular A/IS decision should always be discoverable.
- **Accountability**–A/IS shall be created and operated to provide an unambiguous rationale for all decisions made.
- **Awareness of Misuse**–A/IS creators shall guard against all potential misuses and risks of A/IS in operation.



What's Really Under the Hood

DECONSTRUCTING LAWSUITS & CLAIMS: PRODUCT LIABILITY, RECALL, AND WARRANTY

Product Liability: Design Defect

- Did the manufacturer **properly weigh alternatives** and **evaluate trade-offs** and thereby develop a **reasonably safe product**?
- Some States: no continuing duty for a manufacturer to repair or recall a product to bring it up to the current **state of the art** for safety features.

“A product . . . is **defective in design** when the **foreseeable risks** of harm posed by the product **could have been reduced or avoided** by the adoption of a **reasonable alternative design** by the seller . . . and the omission of the alternative design renders the product not reasonably safe.”

Duty to Warn

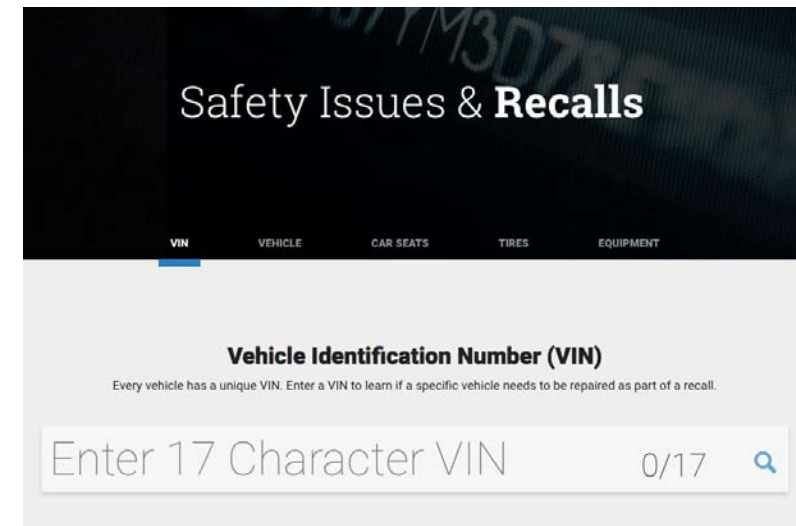
- A manufacturer has a **duty to give adequate warnings** about that product for injuries sustained that were **foreseeable**, not whether the use was intended.
- The **placement, content, adequacy** and **effectiveness** of **warnings** are issues that arise in connection with warnings claims.
- Some states have **relaxed the duty to warn** for simple products where the **danger is open and obvious** to all.

Misrepresentation

- A claim in a products liability suit may be based on **false or misleading information** that is conveyed by the manufacturer of a product. A person who relies on the information conveyed by the seller and who is harmed by such reliance may recover for **misrepresentation**.
- *“We’re spending less time in near-collision states,”* said Chris Urmson, the leader of Google’s autonomous-car program. *“Our car is driving more smoothly and more safely than our trained professional drivers.”*

Automotive Recalls: 573 Reporting

- Determination of a Safety-Related Defect
 - Promotes “the performance of motor vehicles or motor vehicle equipment in a way that protects the public against unreasonable risk of accidents occurring because of the design, construction or performance of a motor vehicle, and against unreasonable risk of death or injury in an accident, and includes non-operational safety of a vehicle.”
- Non-compliance with a Federal Motor Vehicle Safety Standard
 - No current cybersecurity FMVSS



The screenshot shows the 'Safety Issues & Recalls' section of the NHTSA website. It features a navigation bar with tabs for 'VIN', 'VEHICLE', 'CAR SEATS', 'TIRES', and 'EQUIPMENT'. The 'VIN' tab is selected. Below the navigation bar, the heading 'Vehicle Identification Number (VIN)' is displayed, followed by the text 'Every vehicle has a unique VIN. Enter a VIN to learn if a specific vehicle needs to be repaired as part of a recall.' A search input field contains the text 'Enter 17 Character VIN' and a character count '0/17'. A search icon is located to the right of the input field.

Recall: Radio Software Security Vulnerabilities

- ***NHTSA Campaign No. 15V-461:*** Exploitation of the software vulnerability may result in unauthorized remote modification and control of certain vehicle systems, increasing the risk of crash
- ***Defect:*** Some Chrysler 2013-2015 MY vehicles equipped with RA3 or RA4 model radios have certain software security vulnerabilities which could allow unauthorized third-party access to some networked vehicle control systems. Exploitation of the software security vulnerabilities required extensive technical knowledge, physical access to a subject vehicle and a long period of time to write applicable code.

Cahen v. Toyota

Cahen v. Toyota Motor Corp., 147 F. Supp. 3d 955 (N.D. Cal. 2015), *aff'd*, 717 F. App'x 720 (9th Cir. 2017)

- **Consumers sued Ford, GM, and Toyota** alleging that the vehicles were equipped with technology that was **susceptible to being hacked**. Cahen's claims included an **Invasion of Privacy claim** under Article I of the California Constitution
- The court found that there was **no proof that the harm** of a hack was "certainly impending" and only showed that it was **possible**

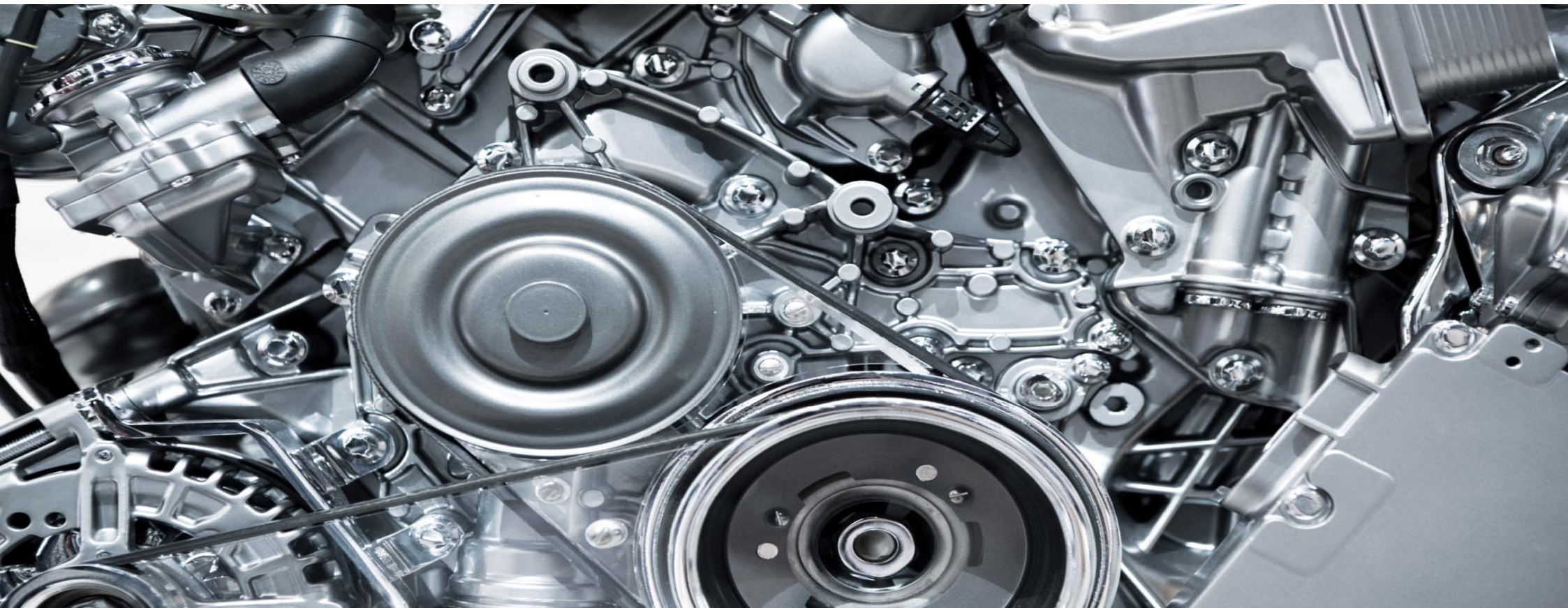
Flynn v. FCA (Chrysler) and Harman

FCA US LLC et al. v. Flynn et al., No. 18-398, *cert. denied*, 2019 WL 113533 (U.S. Jan. 7, 2019).

- Purchasers and lessees brought **class action** against vehicle manufacturer and component manufacturer, alleging that design **flaws** in vehicles' integrated phone, navigation, and entertainment control made vehicles **vulnerable to hackers**.
- Manufacturers moved for summary judgment
 - Magnuson-Moss Warranty Act
 - Illinois Consumer Fraud Act, Michigan Consumer Protection Act, Missouri Merchandising Practices Act
 - Unjust enrichment
- Purchasers and lessees moved for class certification
- **Litigation is Ongoing**: Currently in significant discovery disputes

Wrap Up & Take-Aways

- Collection of Data will Continue
- The Drive to Monetize
- Laws addressing Privacy & Security will Appear from all Directions
 - Foreign
 - Federal
 - State
- Private Rights of Action in State Laws
- Voluntary Guidelines → Mandates?



BUTZEL
LONG

Thank you!

Claudia Rast Rast@Butzel.com @RastLaw
Jennifer Dukarski Dukarski@Butzel.com @JDukarski