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

Claudia Rast @RastLaw
Jennifer Dukarski @J Dukarski
Rast@Butzel.com
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!
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
DECONSTRUCTING EXISTING LAWS: CYBERSECURITY & PRIVACY

What's Really Under the Hood
Privacy and Cyber Laws

• Criminal Code—Title 18
  – Computer Fraud & Abuse Act, 18 U.S.C. § 1030
  – 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

• 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
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

<table>
<thead>
<tr>
<th>State</th>
<th>Statute</th>
<th>Requires disclosure of event data recorders (“sensing diagnostic modules”) in vehicles</th>
<th>Prohibits download of data, except under stated conditions:</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>Arkansas</td>
<td>Ark. Code § 23-112-107</td>
<td>In a written notice at time of new vehicle purchase from dealership. Also requires disclosure in agreements with subscription services.</td>
<td>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.</td>
<td>Permission cannot be a condition of payment/settlement of an insurance claim, or of a lease or insurance agreement.</td>
</tr>
<tr>
<td>California</td>
<td>Calif. Veh. Code § 9901</td>
<td>In the owner’s manual of new cars. Also requires disclosure in agreements with subscription services.</td>
<td>1) with owner’s consent; 2) court order; 3) vehicle safety research; 4) diagnosing, servicing, or repairing the vehicle.</td>
<td></td>
</tr>
<tr>
<td>Colorado</td>
<td>CRS §§ 42-4-2401 to -2403</td>
<td>In or along with the owner’s manual of vehicles manufactured after May 2017 and sold or leased in Colorado. Also requires disclosure in agreements with subscription services.</td>
<td>1) with owner’s written consent within 30 days of renewal; 2) court order; 3) vehicle safety research; 4) diagnosing, servicing, or repairing the vehicle; 5) in legal discovery.</td>
<td></td>
</tr>
</tbody>
</table>
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

  - 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.
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 2.0 (AV 2.0) 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 2.0 builds upon—but does not rewire—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 2.0, U.S. DOT’s surface transportation operating administrators 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. 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.

AV 2.0 includes six principles that guide U.S. DOT’s programs and policies on automation and five implementation strategies for how the Department can facilitate these principles into action (see facing page).

AV 2.0 Provides New Multimodal Safety Guidance

In accordance with the Department’s AV 2.0 implementation principle, AV 2.0 outlines how automation will be safely integrated across passenger vehicles, commercial vehicles, on-road transit, and the roadways on which they operate. Specifically, AV 2.0:

- Affirms the approach outlined in A Vision for Safety 2.0 and encourages automated driving system developers to make their systems as safe as possible to the best of their ability, recognizing that different vehicle types have different capabilities.
- Requires the Department to ensure that the integration of automation technologies into the transportation system is done in a manner that maximizes benefits and minimizes risks.
- Requires the Department to ensure that the integration of automation technologies into the transportation system is done in a manner that maximizes benefits and minimizes risks.

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 efficient testing and operation of automated vehicles.

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

The Department will continue its cooperative, non-regulatory approach to supporting development of non-regulatory voluntary technical standards and other documents across internal model partners. The Department will continue to share information with the public and stakeholders as it advances the development of new technical standards.

1. Gather information from relevant industry partners and stakeholders on the benefits and challenges of developing and implementing new technical standards.
2. Identify and disseminate new technical standards that could provide benefits to the transportation industry and the general public.
3. Work to ensure implementation of new technical standards by supporting the development of new technical standards and other documents across internal model partners.

The Department will continue its cooperative, non-regulatory approach to supporting development of non-regulatory voluntary technical standards and other documents across internal model partners. The Department will continue to share information with the public and stakeholders as it advances the development of new technical standards.

The Department will continue its cooperative, non-regulatory approach to supporting development of non-regulatory voluntary technical standards and other documents across internal model partners. The Department will continue to share information with the public and stakeholders as it advances the development of new technical standards.

This document is a living document and will be updated as new information becomes available.
At the End of the Day: Reliance on Standards

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

ISO/SAE 21434 – High-level Timeline

- Kickoff meeting
  October 17th, 2016

- ISO WD/SAE Internal Committee Ballot
  April 2018

- ISO CD/SAE Wider Committee Ballot
  Sept 2018

- ISO DIS/SAE MVC Ballot
  April 2019

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.

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\text{ }product...\text{is }\text{defective in design} \text{ when the }\text{foreseeable risks} \text{ of harm posed by the product }\text{could have been reduced or avoided} \text{ by the adoption of a }\text{reasonable alternative design} \text{ 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
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

- 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?
Thank you!

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