WILMERHALE WEBINAR

Proceed With Caution: Privacy and Cybersecurity Issues Related to Autonomous Vehicles

November 6, 2019

Speakers: D. Reed Freeman and Ali Jessani

Attorney Advertising

Webinar Guidelines

- Participants are in listen-only mode
- Submit questions via the Q&A feature
- Questions will be answered as time permits
- Offering 1.0 CLE credit in California and New York*

WilmerHale has been accredited by the New York State and California State Continuing Legal Education Boards as a provider of continuing legal education. This program is being planned with the intention to offer CLE credit in California and non-transitional CLE credit in New York. This program, therefore, is being planned with the intention to offer CLE credit for experienced New York attorneys only. Attendees of this program may be able to claim England & Wales CPD for this program. WilmerHale is not an accredited provider of Virginia CLE, but we will apply for Virginia CLE credit if requested. The type and amount of credit awarded will be determined solely by the Virginia CLE Board. Attendees requesting CLE credit must attend the entire live program. CLE credit is not available for on-demand webinar recordings.

WEBINAR

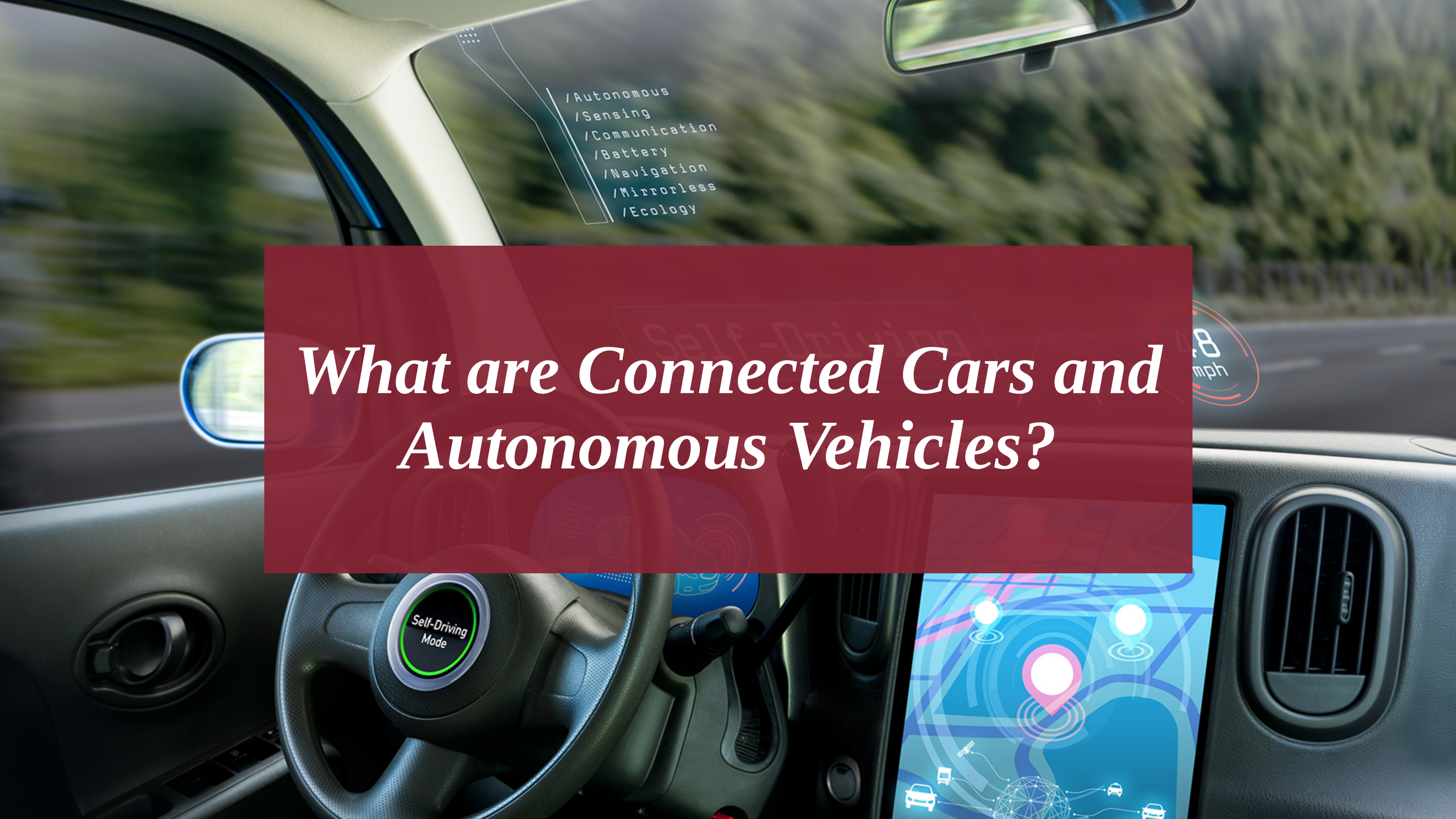
Speakers

D. Reed Freeman
Partner
WilmerHale
Reed.Freeman@wilmerhale.com

Ali Jessani
Associate
WilmerHale
Ali.Jessani@wilmerhale.com

Agenda

1. Introduction to autonomous and Internet-connected cars
2. Overview of the types of information they collect, store, and disseminate
3. Current regulatory landscape for AVs
4. Future privacy and cybersecurity laws and their effect on AVs
5. Litigation and regulatory risks for AV manufacturers regarding privacy and cybersecurity



What are Connected Cars and Autonomous Vehicles?

Defining Autonomous Vehicles

Cars connected to the Internet **sense their surroundings** and move **without human input**

Advantages

- Reduced cost of accidents
- Increased safety
- Reduction in traffic collisions and injuries
- Increased traffic flow
- Environmentally friendly
- Increased human welfare
- Lower operational costs

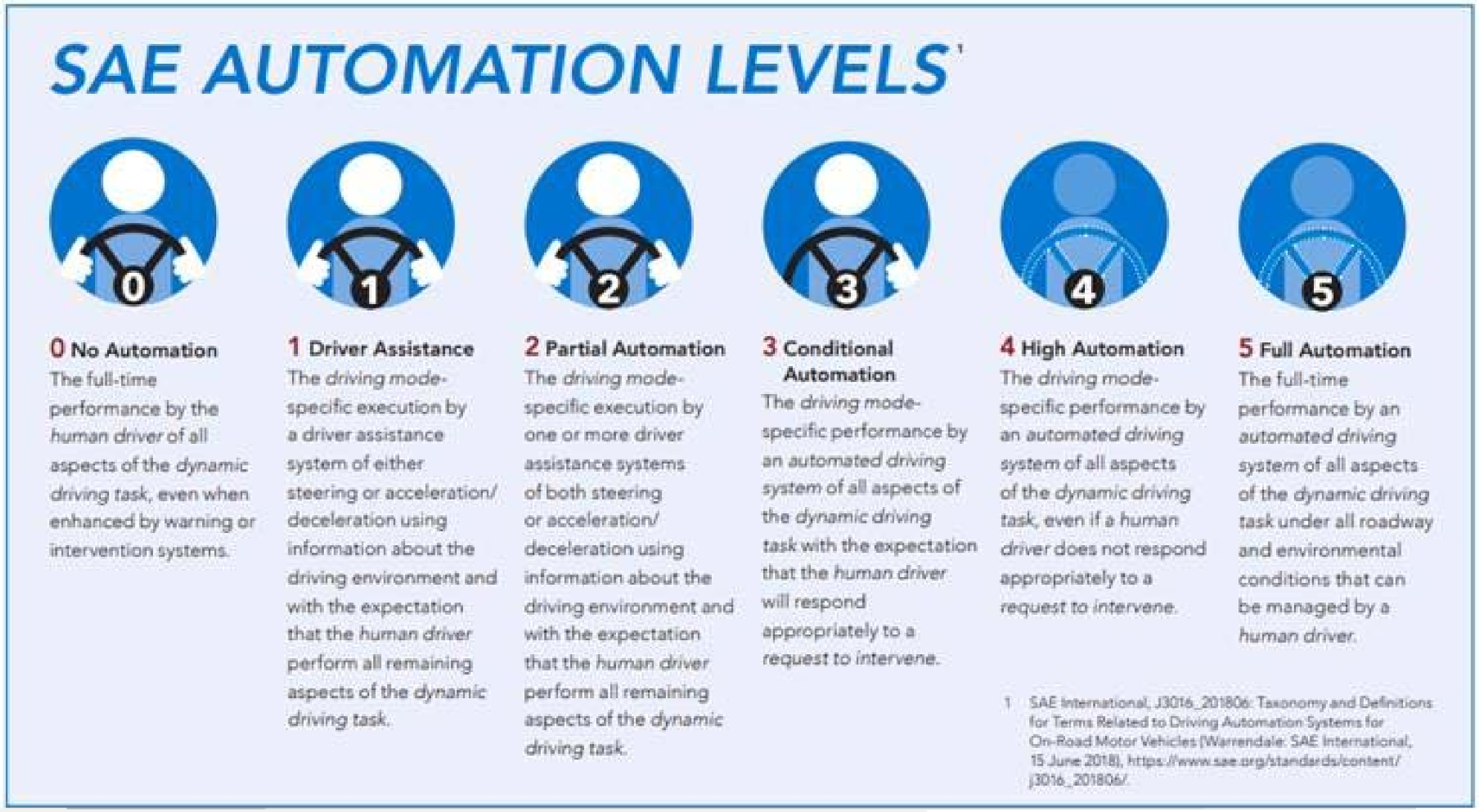
“There will be 21 million autonomous vehicles on the world’s roads by 2035”

Disadvantages

- Legal framework and government regulations
- Loss of privacy; security concerns
- Potential for loss of driving jobs in road transport
- Increased suburbanization
- Potential worsening of urban congestion

What Do We Mean by "Autonomous Driving"?

Autonomous Driving Levels 0 to 5



Level 2 (and lower) vehicles already collect tons of valuable information

- Who You Are
  - Contacts, text messages, music preferences
- Where You Go
  - GPS information, i.e., where you like to shop, what restaurants do you eat at, etc.
- Your Driving Habits
  - Do you wear a seatbelt, do you speed etc.
  - Event Data Recorders collect much of this information already

The New York Times

Your Car Knows When You Gain Weight

Vehicles collect a lot of unusual data. But who owns it?

By Bill Hanvey

Mr. Hanvey is president and chief executive officer of the Auto Care Association.

May 20, 2019

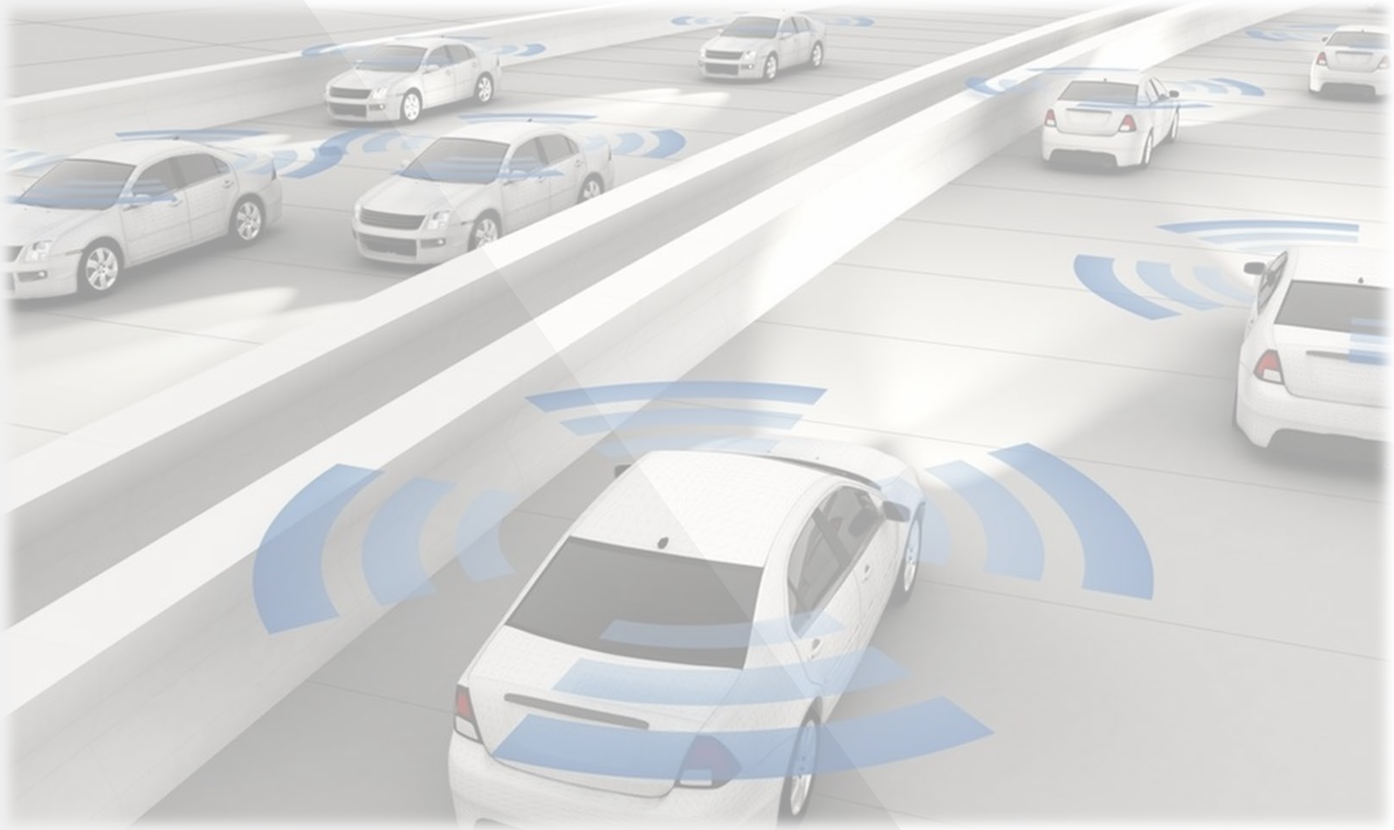
Potential for Technological Innovations from Level 2 to Levels 3 - 5

- Technology companies bringing new technology to automotive industry

WiFi

Cellular

Connectivity



Sensors

Voice recognition

GPS

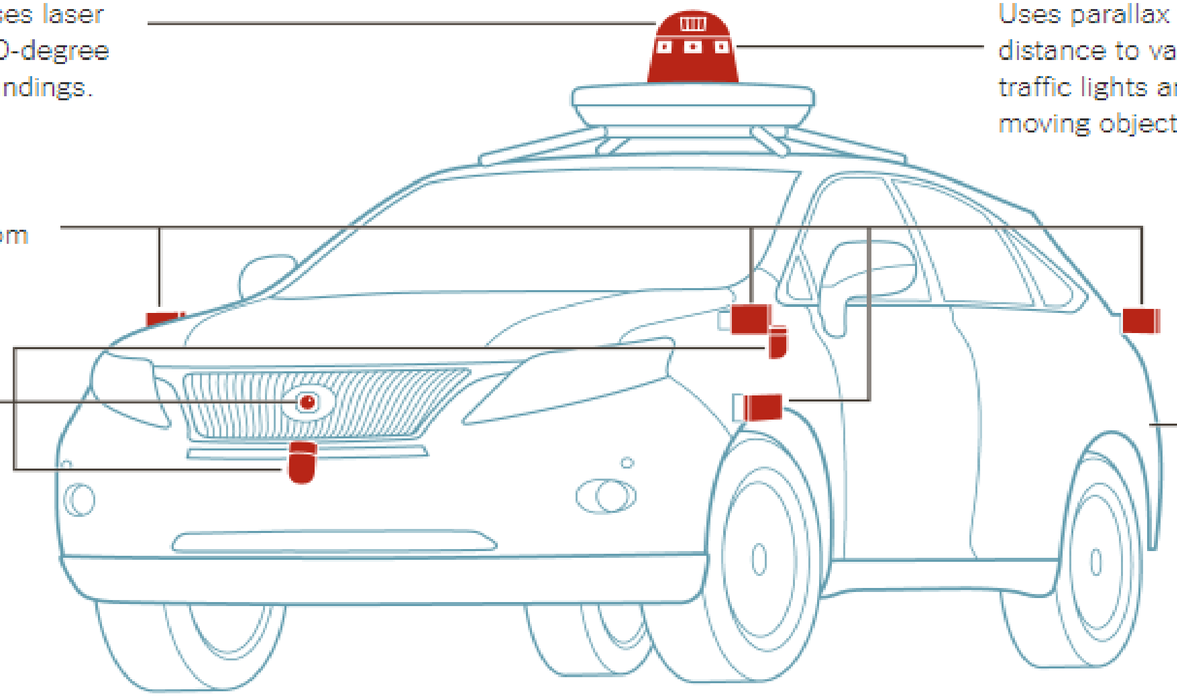
The New York Times

How Driverless Cars See the World Around Them

LIDAR UNIT
Constantly spinning, it uses laser beams to generate a 360-degree image of the car's surroundings.

RADAR SENSORS
Measure the distance from the car to obstacles.

ADDITIONAL LIDAR UNITS



CAMERAS
Uses parallax from multiple images to find the distance to various objects. Cameras also detect traffic lights and signs, and help recognize moving objects like pedestrians and bicyclists.

MAIN COMPUTER (LOCATED IN TRUNK)
Analyzes data from the sensors, and compares its stored maps to assess current conditions.

By Guilbert Gates | Source: Google | Note: Car is a Lexus model modified by Google.

Connected Cars as IoT Devices

- Simply put, IoT devices are physical devices that connect to the Internet
  - E.g., “Smart” devices such as TVs and phones
- IoT connects multitude of devices through the Internet to collect and exchange data
- Connected cars will need to communicate with each other and with infrastructure, such as traffic lights, and the Internet and cellular connectivity allow for this communication
- Technology enables communication between vehicles regarding speed, trajectory, malfunction and may reduce potential for collisions
  - Also allows for more points of data collection and more points of access for hackers

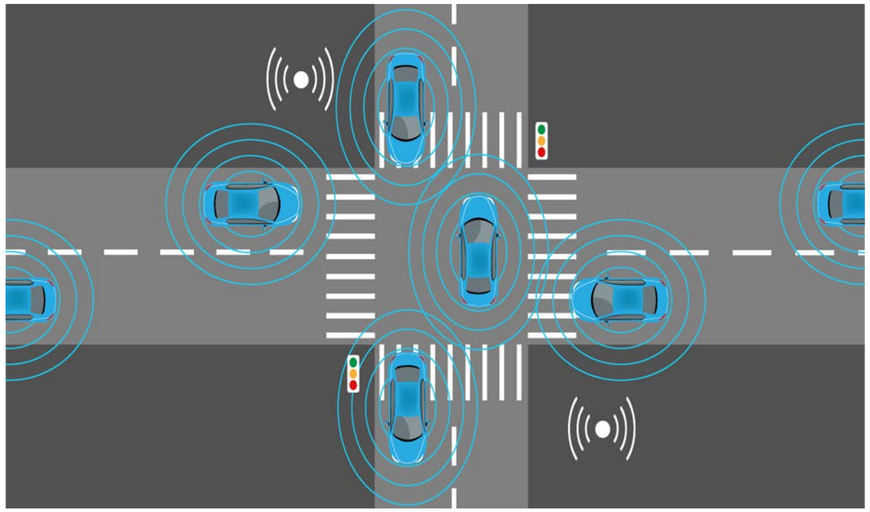
What information will autonomous vehicles collect?

- Biometrics and driver behavior analytics
  - Biometric information includes face scans, fingerprints, voiceprints, iris scans
  - Level 3 (conditional automation) and higher vehicles may use this information to, for example, see if your eyes are still on the road so that you can take control of the vehicle if need be
  - The fact that autonomous vehicles need cameras on the outside of the car means that they will have the ability to collect information on pedestrians

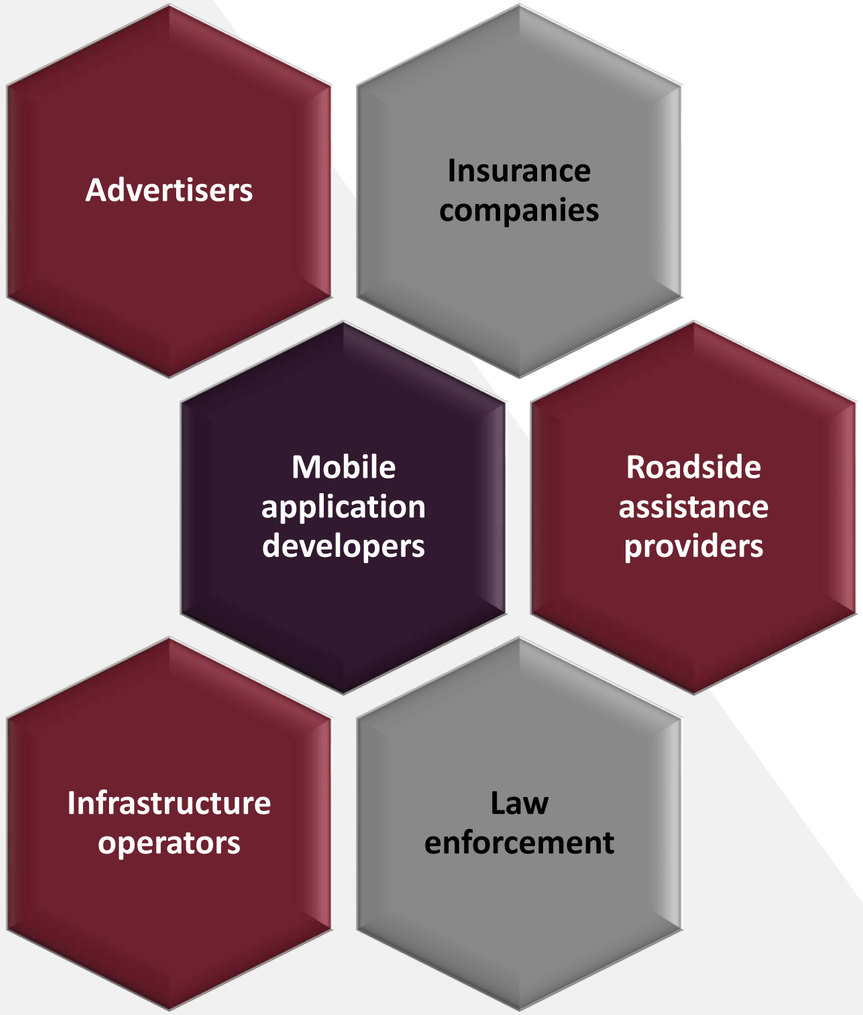
What information will autonomous vehicles collect?

— Geolocation Information and Telematics

- GPS antennae mean that autonomous vehicles will know exactly where they (and you) are at all times
- Connected cars need to know where other vehicles, as well as people and pedestrians are, in order to function properly
- Level 4 (high automation) and Level 5 (full automation) vehicles will allow you to input destinations, as well as allow you to be picked up wherever you are

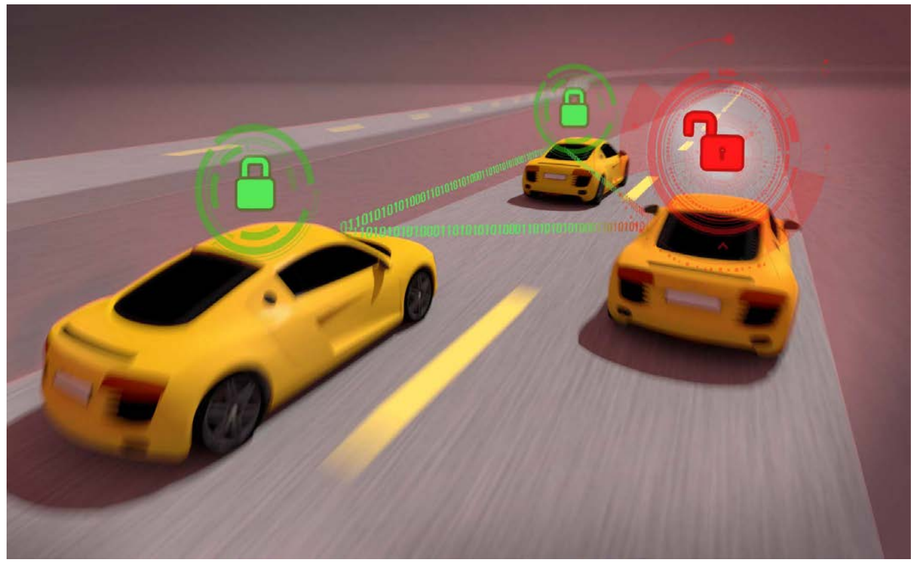


Who is this information valuable to?



Autonomous vehicles pose increased risks of cyber attacks

- Almost all aspects of driverless cars will be connected to the Internet, which means more access points for potential hackers
- In 2016, the FBI released a public service announcement stating that motor vehicles are increasingly vulnerable to remote exploits
- There have been more than 260 cyberattacks on connected cars since 2010, according to UpStream Security



The Current Regulatory Framework

Federal Laws and Regulations

- No federal law specifically for AVs, though legislation has been proposed
  - SELF DRIVE Act passed the House of Representatives in 2017
    - Would require manufacturers to have privacy and cybersecurity plans before selling AVs
  - Senate version of the bill, AV START Act, stalled. House and Senate committees are working on a drafting a new bill
- Driver's Privacy Protection Act offers some protection for personal information collected by state DMVs
- Motor vehicles in general are regulated by the DOT and NHTSA
- NHTSA first released AV guidance in 2016 and then again in 2017
- Latest NHTSA guidance, AV 3.0, was released in September 2018
  - Limited privacy and cybersecurity guidance
  - NHTSA said that it would work with other federal agencies, such as the FTC and DHS, on addressing these issues

FTC Enforcement

- The Federal Trade Commission enforces privacy and cybersecurity violations through its authority under Section 5 of the FTC Act

Case in point: The FTC's recent settlement with DealerBuilt

DealerBuilt is a software company collects large quantities of personal information on auto dealership customers and employees.

A company employee allegedly connected a storage device to the company's backup network that was not securely configured and that remained insecure for 18 months. DealerBuilt allegedly did not perform any testing to detect the vulnerability, and the FTC alleges that this failure led to a data breach in 2016, resulting in 12.5 million consumers having their personal information compromised.

As part of the consent order, DealerBuilt is required to, among other things:

- *Implement and maintain a comprehensive information security plan;*
- *Annually certify compliance with the plan to the FTC; and*
- *Provide annual cybersecurity training to its employees and reporting to its board*

FTC Enforcement

– The FTC held a connected car workshop in 2017 and issued a staff perspective in 2018

Key Takeaways

1. Connected cars will collect information from consumers in ways that will be beneficial
2. The type of data collected can range from aggregated data to sensitive personal information
3. Consumers may be concerned about unexpected uses of their data
4. Connected cars will create potential cybersecurity risks

Recommendations

1. Manufacturers should share information with groups like the Society of Automotive Engineers
2. Connected car networks should include network design solutions, such as separating safety-critical functions
3. Risk assessment and mitigation should be incorporated throughout the development and sale process
4. Industry self-regulation should set appropriate standards

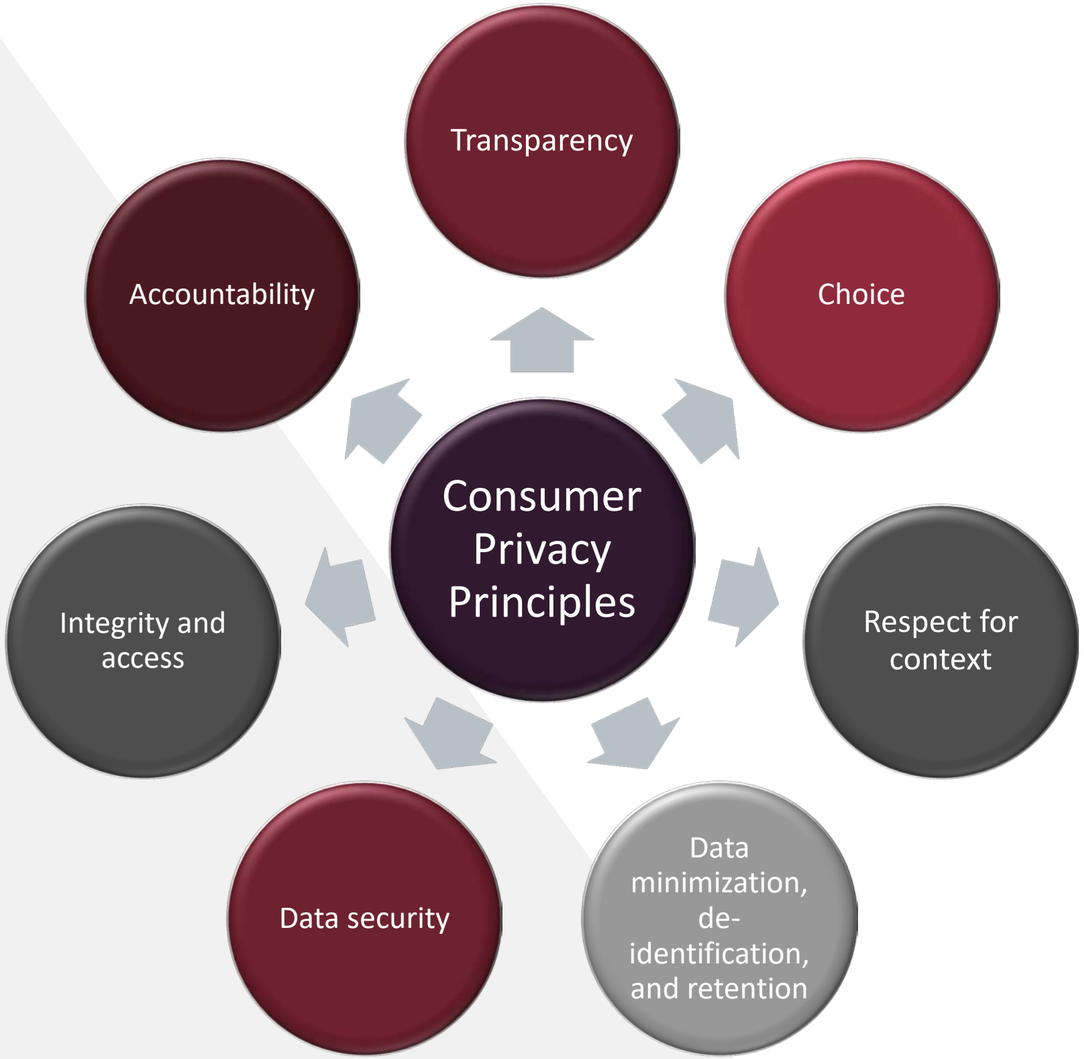
State Law

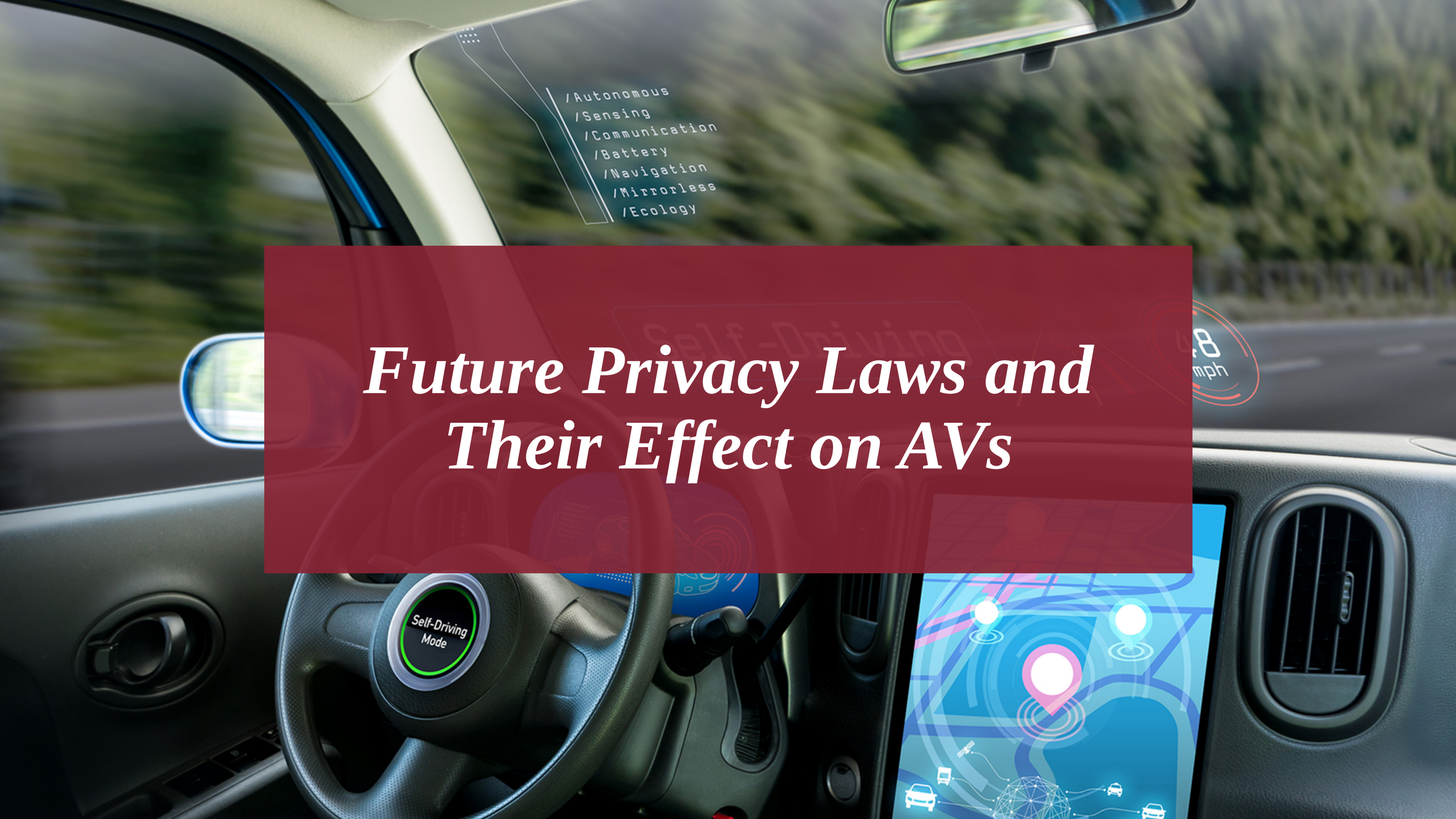
- 36 states and the District of Columbia have either passed legislation or issued an executive order pertaining to AV development and deployment regulations/standards
- These laws are mostly focused on issues relating to AV testing and development, as well as pedestrian safety, but not privacy or cybersecurity issues
- Some states have addressed privacy concerns
  - California, for example, will require AV manufacturers to either provide written disclosures to the passengers of a vehicle that describe the personal information collected by the AV that is not necessary for the safe operation of the AV or to anonymize that information. 13 CCR § 228.24
  - If a manufacturer collects non-anonymized information, it shall obtain written approval from the owner or lessee of the vehicle for any information that is not necessary for the safe operation of the vehicle

State Law

- All 50 states have a data breach notification law
  - The definition of personal information in these laws varies, but some include information that connected cars may collect (such as biometrics)
- Texas, Washington, and Illinois have special requirements regarding the collection, storage, and sharing of biometric information
- State tort law may provide potential causes of action for plaintiffs
- Private lawsuits
  - Mehlman v. General Motors, No. RG19013705 (Cal. Sup. Ct. Apr. 4, 2019).
  - Lawsuit brought against GM under California's Unfair Competition Law for allegedly monetizing consumer data through On-Star system without compensating consumers
  - Such lawsuits could become more prevalent with autonomous vehicles

Self-Regulatory Bodies: Alliance for Automobile Manufacturers





Future Privacy Laws and Their Effect on AVs

Overview: Why should AV and connected car companies worry about privacy laws?

- AVs and connected cars need information to operate, and the regulatory landscape is changing such that more and more of this information is becoming regulated
- Some laws, like the CCPA, will regulate almost all of the personal information that AVs collect, while others, like state biometric laws, will regulate smaller (but important) parts of personal information collected
- Tip: Being aware of regulatory trends (such as the expanding definition of personal information and the focus on individual data rights) can help AV and connected car companies incorporate "privacy by design" principles as they are developing necessary technology
- This will help with compliance and minimize the risk posed by regulatory enforcement and private lawsuits

California Consumer Privacy Act (CCPA)

- Comprehensive data privacy law, similar to the General Data Protection Regulation in EU
- In addition to other requirements, the CCPA requires "businesses" to provide California residents with individual data privacy rights including:
  - Right to Notice
  - Right to Access
  - Right to Delete
  - Right to Opt-Out of Sale
  - Right to Nondiscrimination

CCPA

- Personal information is defined broadly as information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household

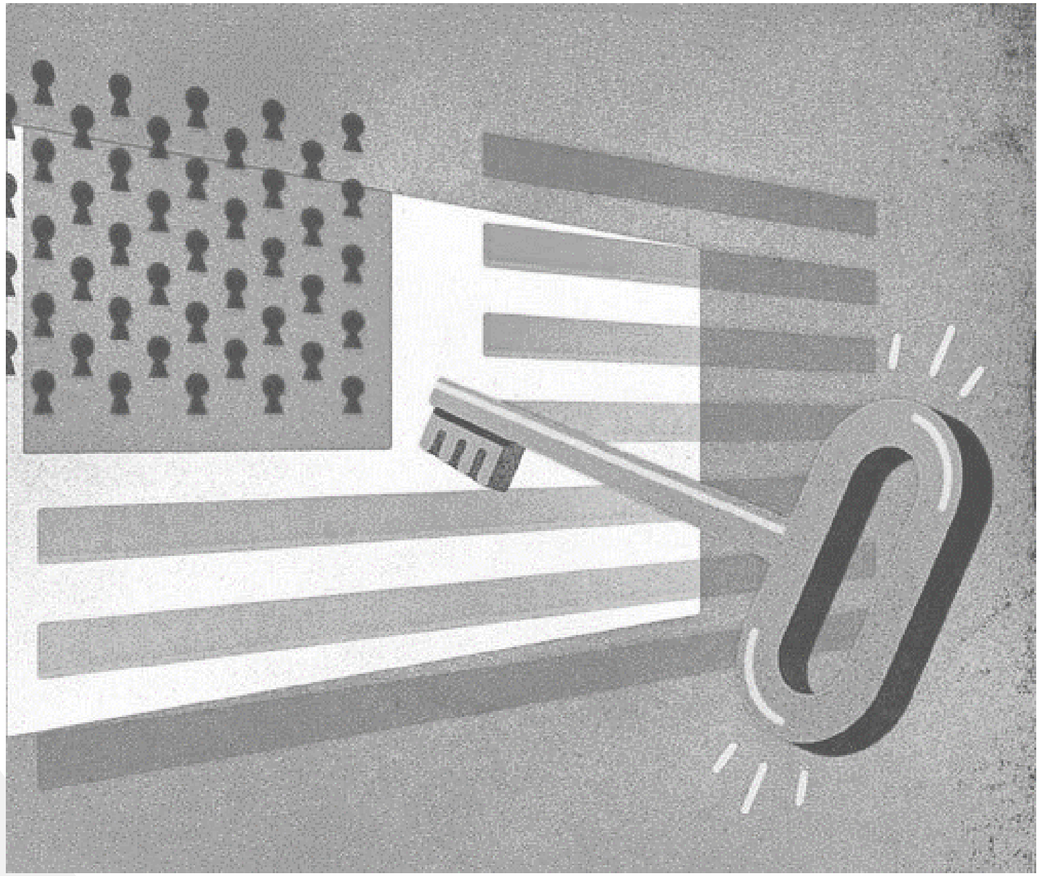
Categories of personal information AVs could collect include:

- Commercial information
- Biometrics
- Unique identifiers
- Internet or other network activity
- Geolocation data

- Aggregated and deidentified information are excluded
- Also excluded is personal information collected pursuant to the Driver's Privacy Protection Act

Copycat CCPA Legislation

- At least 10 states proposed comprehensive data privacy laws similar to the CCPA during the 2019 legislative session
  - MA, WA, and NY are a few examples
  - None were signed into law
- States also proposed other privacy laws that could impact the data collected by AVs
  - Illinois, for example, considered a bill that would regulate geolocation information
- Many more states are likely to take up similar data privacy bills in 2020
- Patchwork of legislation could eventually inspire a comprehensive national data privacy law



California and Oregon's IoT Security Bills

- California and Oregon's IoT security laws will require connected devices to be equipped with "reasonable security features"
- Both go into effect January 1, 2020
- California's law is enforceable by the California AG, city attorney, county counsel, or district attorney and Oregon's law is enforceable by the OR AG or a district attorney

Other Evolving State Laws

- Florida, New York, Arizona, and Massachusetts all considered biometric privacy laws in 2019
  - Trend will likely continue
- State breach notification laws are evolving to include more information that AVs may collect
  - For example, NY's SHIELD Act expanded the definition of covered "private information" information to include biometrics
  - The SHIELD Act also requires businesses that own or license computerized private information of NY residents to "develop, implement, and maintain reasonable safeguards to protect the security of, confidentiality and integrity" of personal information
    - Requires reasonable administrative, technical, and physical safeguards

Where is the risk?

Potential FTC Investigations

- The FTC has used its authority under Section 5 of the FTC Act to bring cases against companies for both privacy and cybersecurity violations
  - Examples include having inadequate data security practices in place that lead to a data breach or failing to comply with the practices listed in the company's privacy policy
- AVs have the potential to collect and store so much information; implementing adequate data privacy and data security practices will be critical to avoid FTC scrutiny

State Regulatory Enforcement Actions

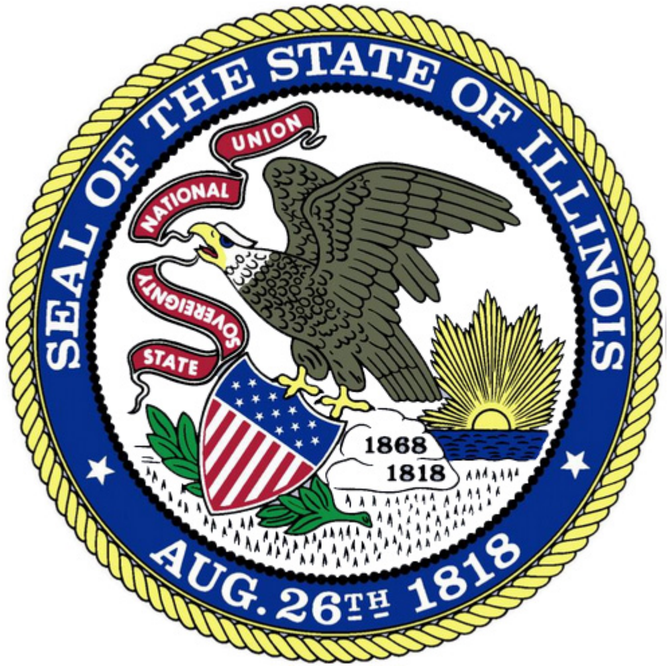
- AV manufacturers will likely collect many categories of personal information covered under the CCPA
  - Those that qualify as “businesses” and collect information from California residents will have to comply with the law
  - Unclear as to how aggressive California AG will be enforcing the CCPA
  - But fines could be extensive based on the sheer amount of information available to AVs and connected cars
    - Statutory damages for actions brought by the California AG can be as high as $7,500 per violation
- Other state regulations could also lead to enforcement actions
  - California’s IoT security law
  - Breach notification laws
  - Other state laws that regulate a particular type of information applicable to AVs

Class Action Risk

- CCPA creates private right of action for any "consumer whose nonencrypted or nonredacted personal information…is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain *reasonable* security procedures and practices…"
  - Reasonable is not defined in the statute or in the draft regulations
  - Damages can be as high as $750 per violation
- But note that the definition of "personal information" as it applies to the private right of action is much narrower. It only applies to:
  - Social Security Numbers
  - Driver's license numbers or other ID number
  - Account numbers, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account
  - Medical information
  - Health insurance information
  - Unique biometric information (added by AB 1130)
- Plaintiffs may try and use California's Unfair Competition Law for a broader private right of action

Class Action Risk

- Biometric Information Privacy Act (BIPA) in Illinois has a private right of action, attorneys' fees, and statutory damages
  - Lawsuits under BIPA have skyrocketed since a ruling by the Illinois Supreme Court in January stating actual injury is not needed to bring claims under the law
    - Rosenbach v. Six Flags Entertainment Corp., 2019 IL 123186



Class Action Risk

- State unfair competition laws could provide another basis for private litigants to sue manufacturers for their data collection and data security practices regarding AVs
  - Lawsuits such as the one brought against GM for its data collection through OnStar could become more prevalent
- State tort law can also lead to class action lawsuits
  - Cyber negligence claims
  - Privacy torts

Questions?

D. Reed Freeman
Partner
WilmerHale
Reed.Freeman@wilmerhale.com

Ali Jessani
Associate
WilmerHale
Ali.Jessani@wilmerhale.com