WILMERHALE WEBINAR

State Privacy Laws Concerning Connected Cars

April 23, 2020

Speakers: D. Reed Freeman and Ali Jessani

Attorney Advertising

WILMERHALE®

WILMER CUTLER PICKERING HALE AND DORR LLP ®

Webinar Guidelines

- Participants are in listen-only mode
- Submit questions via the Q&A feature
- Questions will be answered as time permits
- Offering 1 CLE credit in California and New York*; applying for similar credit in Virginia
- The webcast is being streamed through your computer, so there is no dial-in number. For the best quality, please make sure your volume is up and other applications are closed. If you experience a delay or get disconnected, press F5 to refresh your screen at any time
- For additional help with common technical issues, click on the question mark icon at the bottom of your screen

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 those who watch on-demand webinar recordings.

WEBINAR

Speakers

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

Ali Jessani
Associate
WilmerHale
Ali.Jessani@wilmerhale.com

Agenda

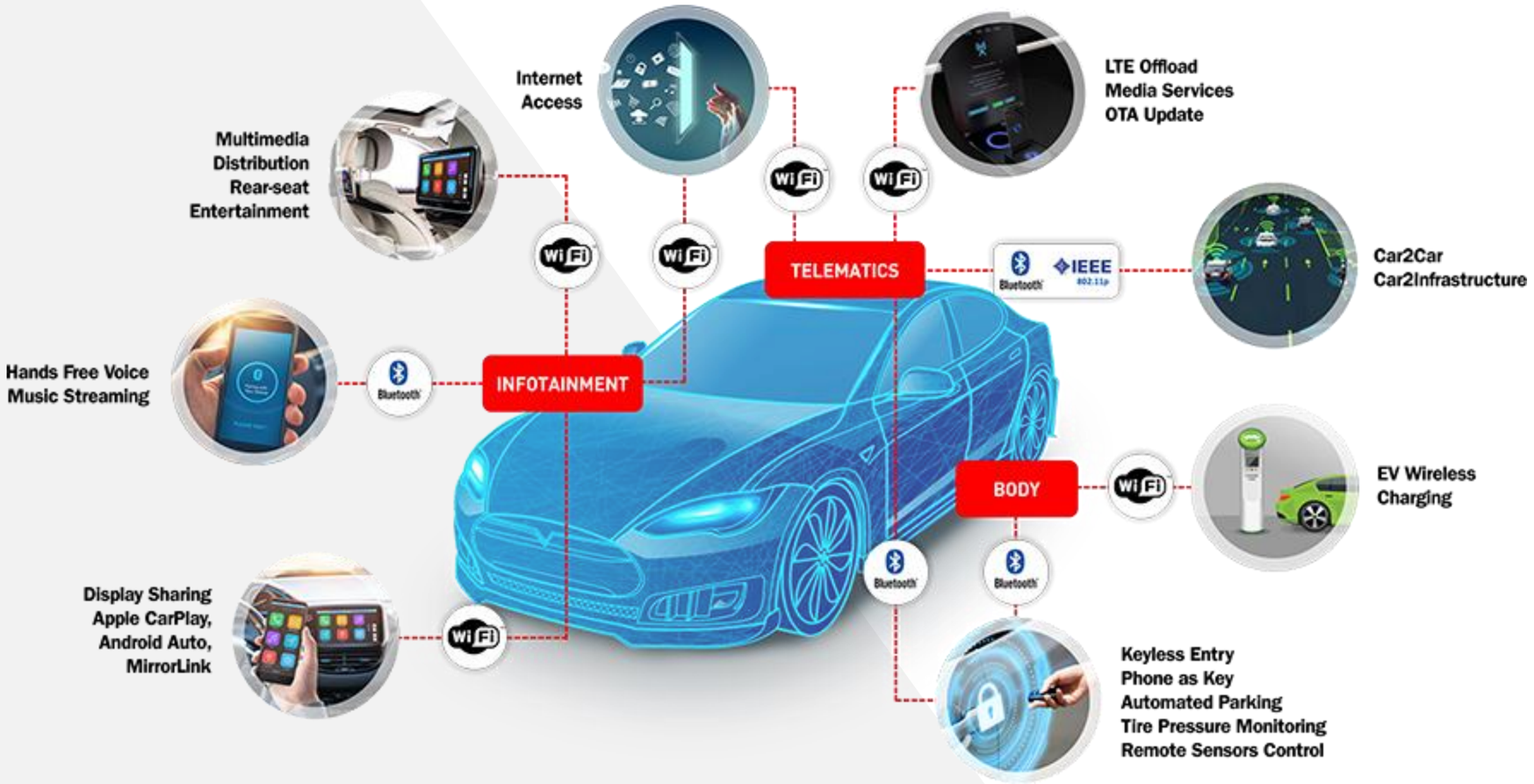
1. Introduction to autonomous and connected cars
2. Overview of the types of information they collect, store and disseminate
3. State regulations affecting privacy and cybersecurity concerns for connected cars
4. Summary of federal and international laws governing privacy and cybersecurity for connected cars
5. Steps to mitigate regulatory and litigation risk for the connected car atmosphere

What are Connected Cars and Autonomous Vehicles?

What are connected cars?

- Simply put, connected cars are Internet of Things (IoT) devices
- IoT connects multitude of devices through the Internet to collect and exchange data
  - E.g., “Smart” devices such as TVs and phones
- 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 are connected cars?



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

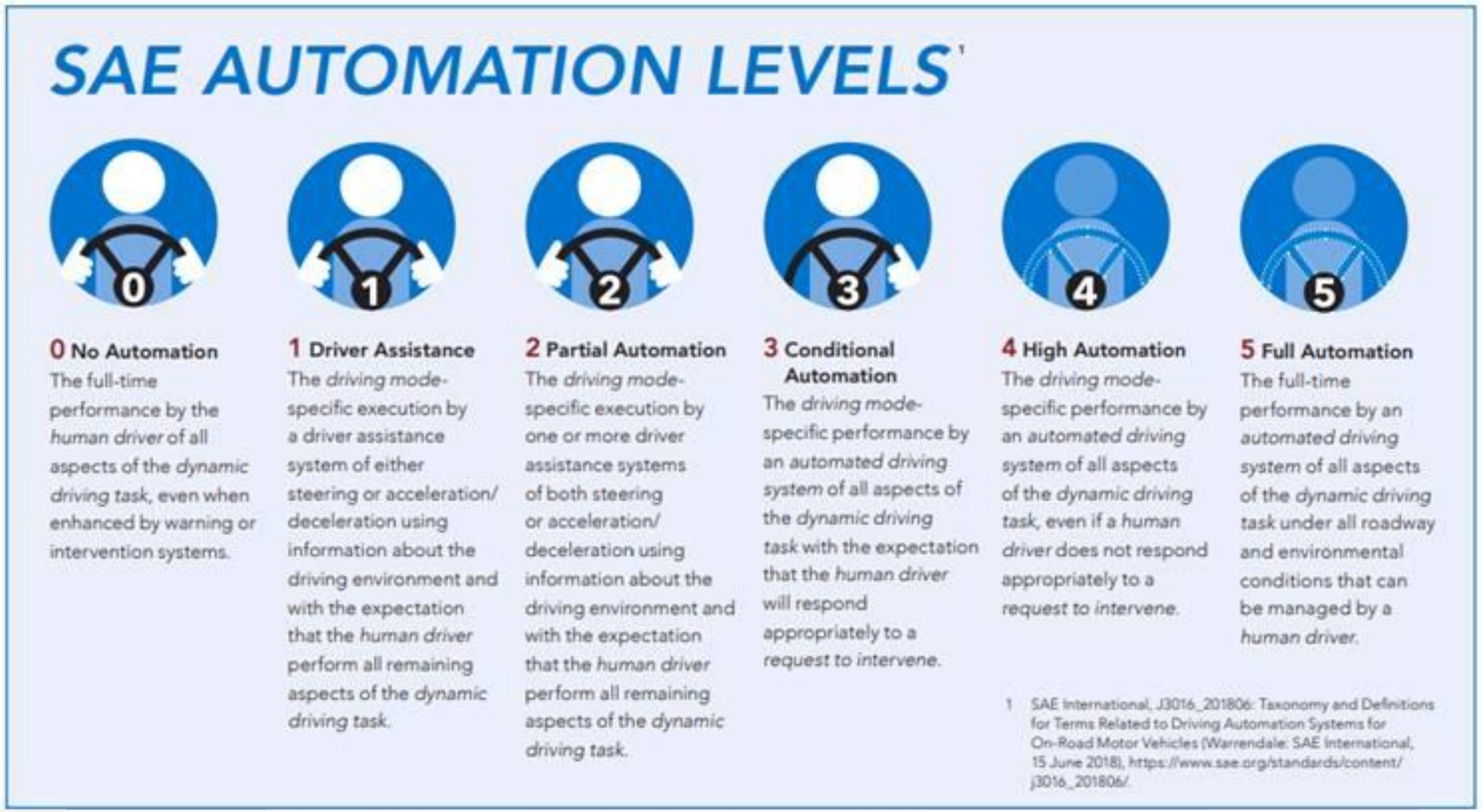
GCN The Technology that Drives Government IT
AI & Automation COVID-19 Cybersecurity Cloud Data & Analytics IoT Emerging Tech Public Safety State & Local

Autonomous vehicles deliver COVID-19 tests to lab

BY GCN STAFF | APR 08, 2020

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

May 22, 2019

Data collected by connected cars ends up with carmakers, not consumers

As connected cars collect data, they send it back to carmakers instead of consumers.

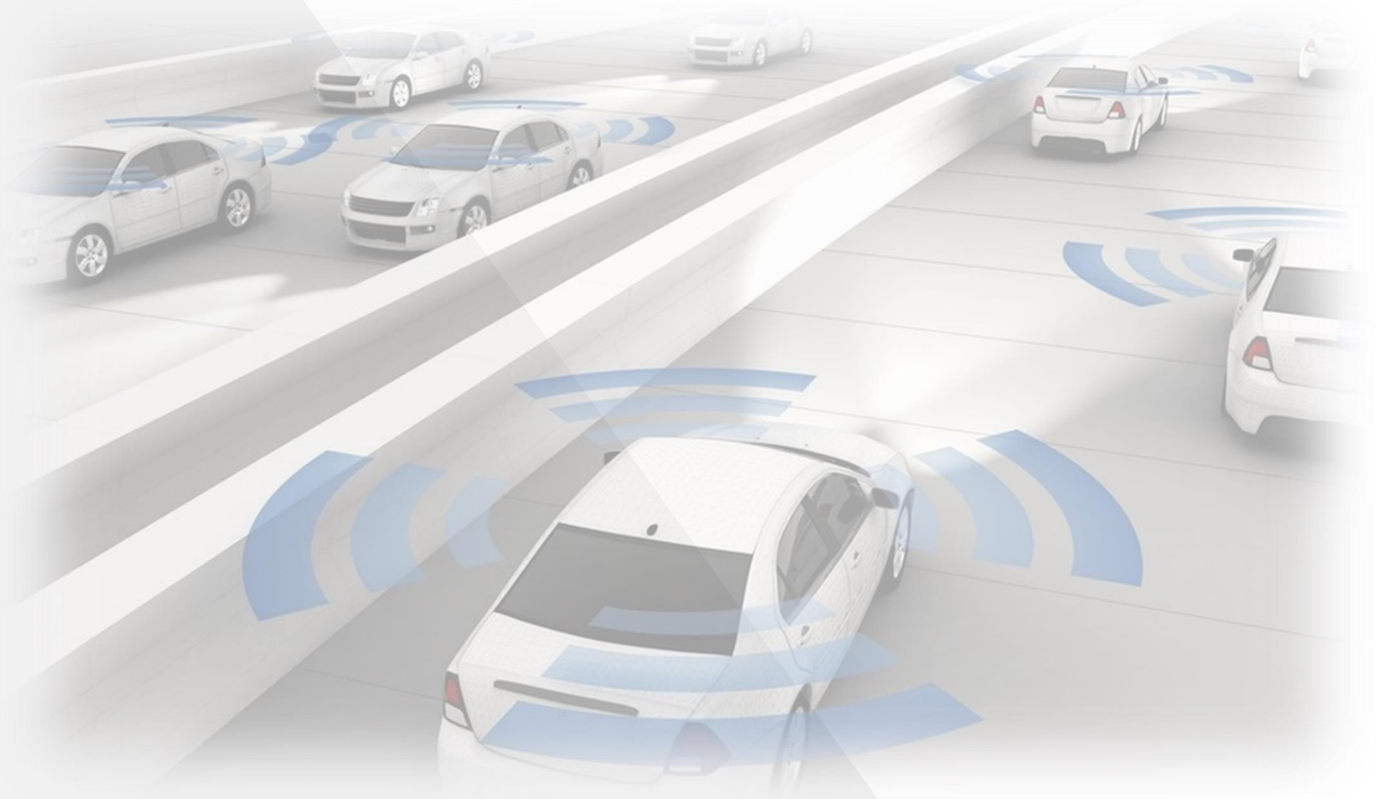
Potential for Technological Innovations from Level 2 to Levels 3 - 5

- Technology companies bringing new technology to automotive industry

WiFi

Cellular

Connectivity



Sensors

Voice recognition

GPS

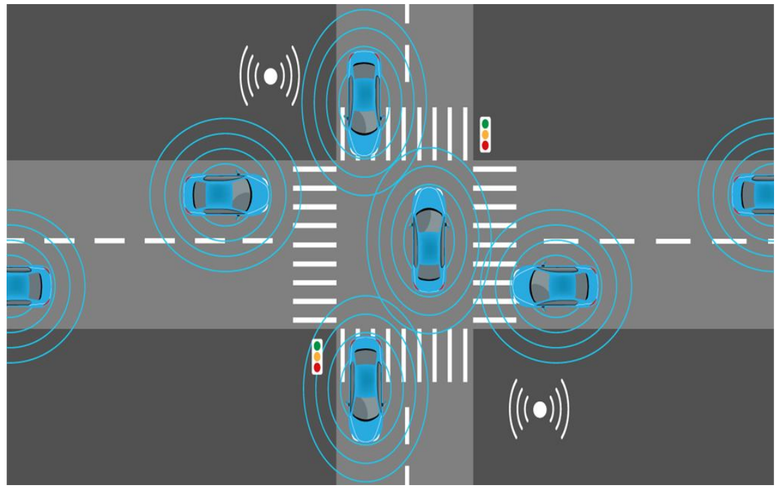
Slide derived from WilmerHale's presentation on November 16, 2019 titled "Proceed with Caution: Privacy and Cybersecurity Issues Related to Autonomous Vehicles"

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

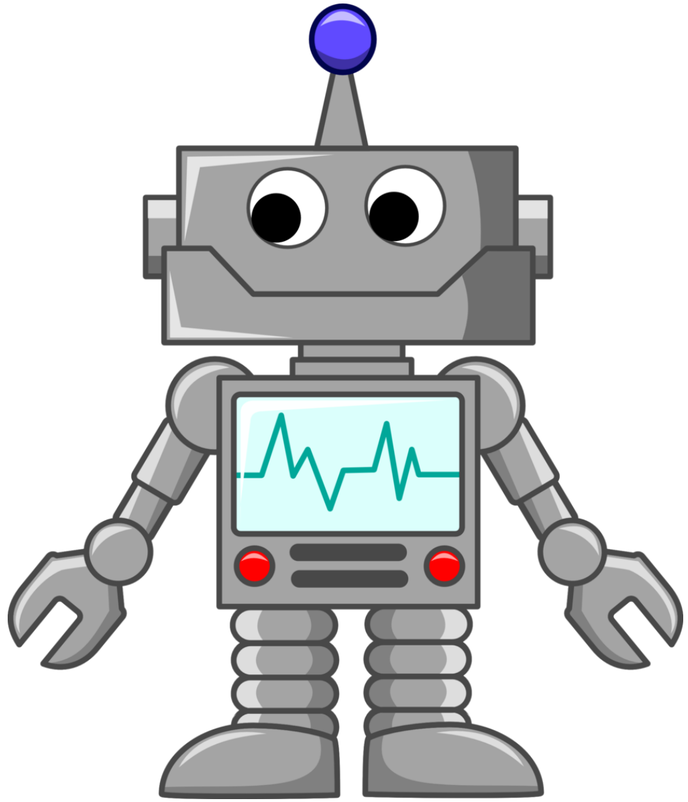
What information will autonomous vehicles collect?

- 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

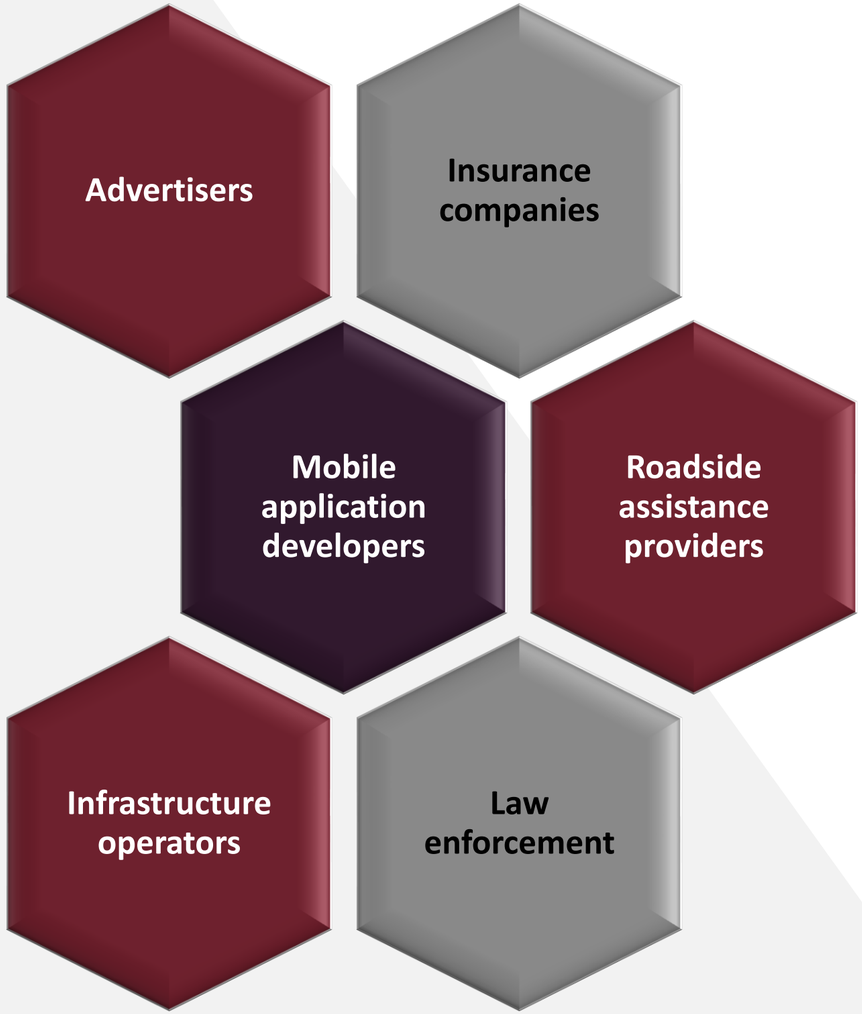


What information will autonomous vehicles collect?

- Information to improve algorithms and machine learning
  - Autonomous vehicles rely on algorithms and machine learning to advance their driving capability
  - Some of this information may be regulated, either directly or because it qualifies as “personal information” under state privacy laws

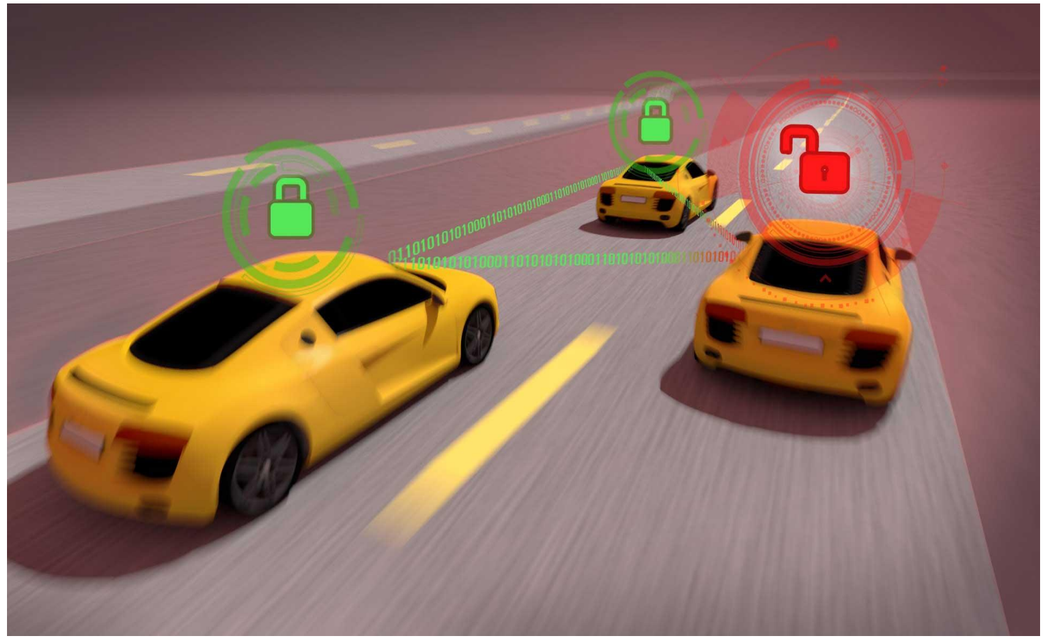


Who is this information valuable to?



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



MOTHERBOARD
TECH BY VICE

Hacker Finds He Can Remotely Kill Car Engines After Breaking Into GPS Tracking Apps

"I can absolutely make a big traffic problem all over the world," the hacker said.

By Lorenzo Franceschi-Bicchierai

Apr 24 2019, 12:07pm Share Tweet Snap

How States Can Regulate Connected Cars

Overview of State Regulation in the Connected Car Context

- States can regulate privacy and cybersecurity in connected and autonomous cars directly
  - Few states so far have enacted such laws yet, though several more bills are pending in legislatures across the country
- States can pass comprehensive privacy bills that also apply to the connected car atmosphere
  - The California Consumer Privacy Act is a prime example
- States can regulate specific aspects of privacy and cybersecurity that affect autonomous and connected cars because of the vast amount of information they collect
  - Breach notification laws
  - Biometric laws
  - IoT
  - Other (geolocation, AI, unfair trade practices, etc.)

States Directly Regulating AVs and Connected Cars

- 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 most of them do not address privacy and cybersecurity
- California and Maine have passed regulations regulating privacy concerns in AVs
- A few other states have considered such legislation in 2019 and 2020

States Directly Regulating AVs and Connected Cars

- **California:**
  - California requires 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

- **Maine:**
  - In January of 2020 (and effective as of April 2020), Maine enacted regulations requiring AV developers participating in the state's AV Pilot Project to provide to its Commission on Autonomous Vehicles information on the AV's data collection practices, including information on what data will be collected, how it will be used, how privacy will be protected and how security will be maintained, including customer feedback in the conduct of the Pilot Project and crash data

AV Data Privacy and Security Proposed State Legislation in 2019-2020

- Michigan HB 4389: Would require AV manufacturers to make available a privacy statement to pilot program participants disclosing its data handling practices in connection with the applicable AV.

- Massachusetts HB 3013: Would require the Department of Transportation to consider privacy considerations when implementing AV regulations

- Minnesota HR 242: Would require all data collected as part of the AV pilot program to be subject to the Minnesota Government Data Practices Act

States Regulating Connected Cars Through Comprehensive Privacy Laws

- What is a “comprehensive” data privacy law?
  - Instead of regulating privacy in specific contexts (such as HIPAA for healthcare and the GLBA for financial institutions), comprehensive data privacy laws regulate all data that businesses collect from consumers in all contexts
  - Create individual rights for consumers
  - Examples include General Data Protection Regulation in the EU and the California Consumer Privacy Act in California

California Consumer Privacy Act (CCPA)

- Went into effect January 1, 2020; scheduled to be enforceable by the California AG on July 1, 2020 (though enforcement may be delayed by COVID-19)
- 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

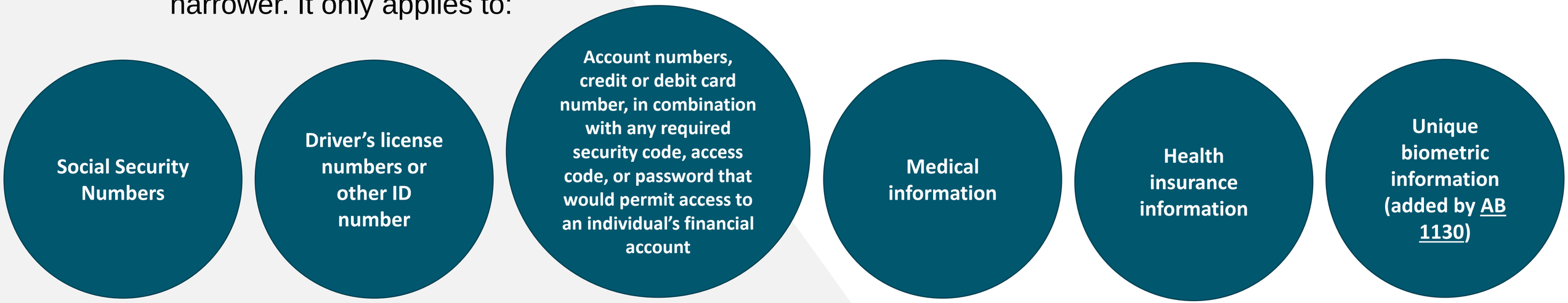
Categories of personal information AVs could collect include:

- Geolocation Information
- Biometrics
- Unique identifiers
- Internet or other network activity
- Inferences

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

CCPA Class Action Risk

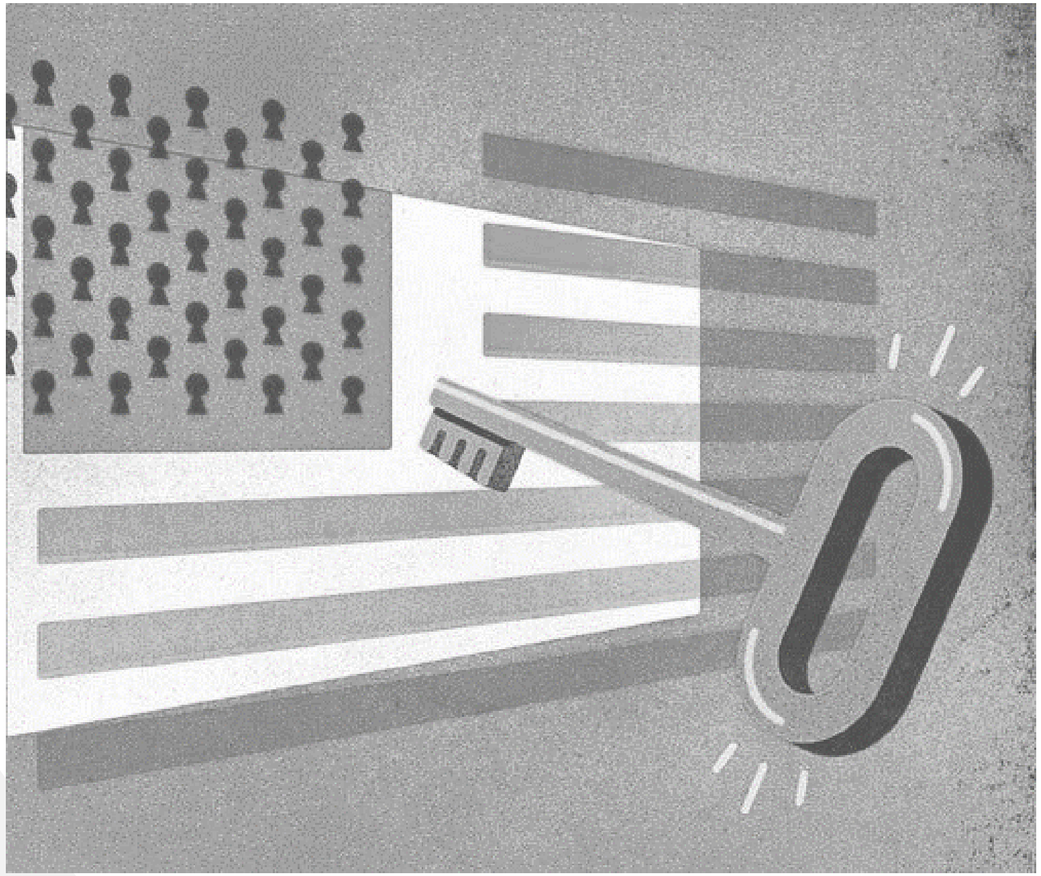
- CCPA creates private right of action for any "consumer whose nonencrypted or nonredacted personal information…is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain *reasonable* security procedures and 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:



- First class action lawsuit under the CCPA was filed on February 3

Copycat CCPA Legislation

- At least 11 states proposed comprehensive data privacy laws similar to the CCPA during the 2020 legislative session; other states continued to debate comprehensive privacy laws introduced in 2019
  - WA, HI and NH a few examples
  - None were signed into law, though the Washington bill did pass the state senate for the second year in a row
- A number of other states have proposed and implemented more limited privacy legislation
  - Nevada enacted a right to opt-out of sale law in 2019
- Patchwork of legislation could eventually inspire a comprehensive national data privacy law



States Regulating Other Aspects of Privacy and Cybersecurity that Affect Connected Cars

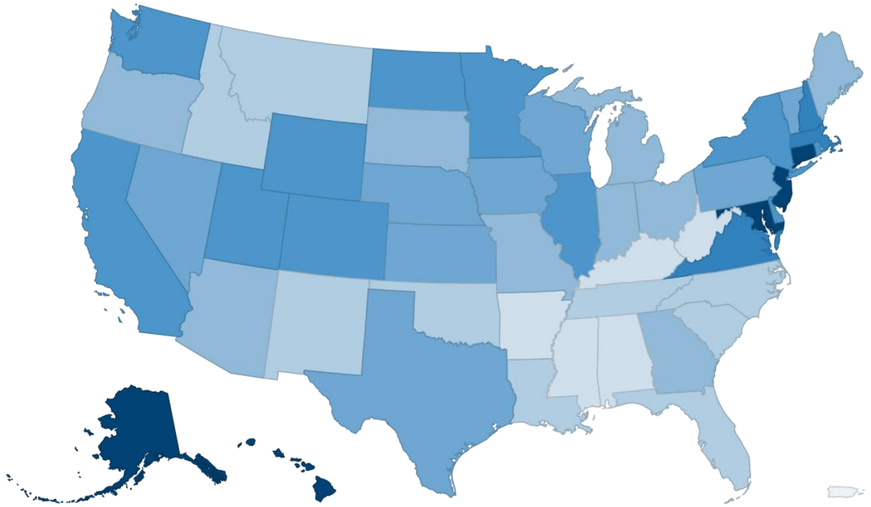
Breach notification laws

Biometrics

IoT

Other

Breach Notification Laws



- All 50 states have a data breach notification law
  - The definition of “personal information” in these laws varies
- State breach notification laws are evolving to include more information that AVs may collect
  - For example, NY’s SHIELD Act (passed in 2019) expanded the definition of covered “private information” information to include biometrics. California also added biometrics to its definition of “personal information” last year.
  - 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

Went into effect March 2020

State Biometric Laws

- Texas, Washington and Illinois have special requirements regarding the collection, storage and sharing of biometric information
- 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.

- At least seven states proposed commercial biometric privacy laws similar to those in Texas, Illinois and Washington during the last two years, though none passed into law

Alabama, Arizona and South Carolina are a few examples

- Other states, such as Idaho and Louisiana, are looking to specifically regulate facial recognition technology

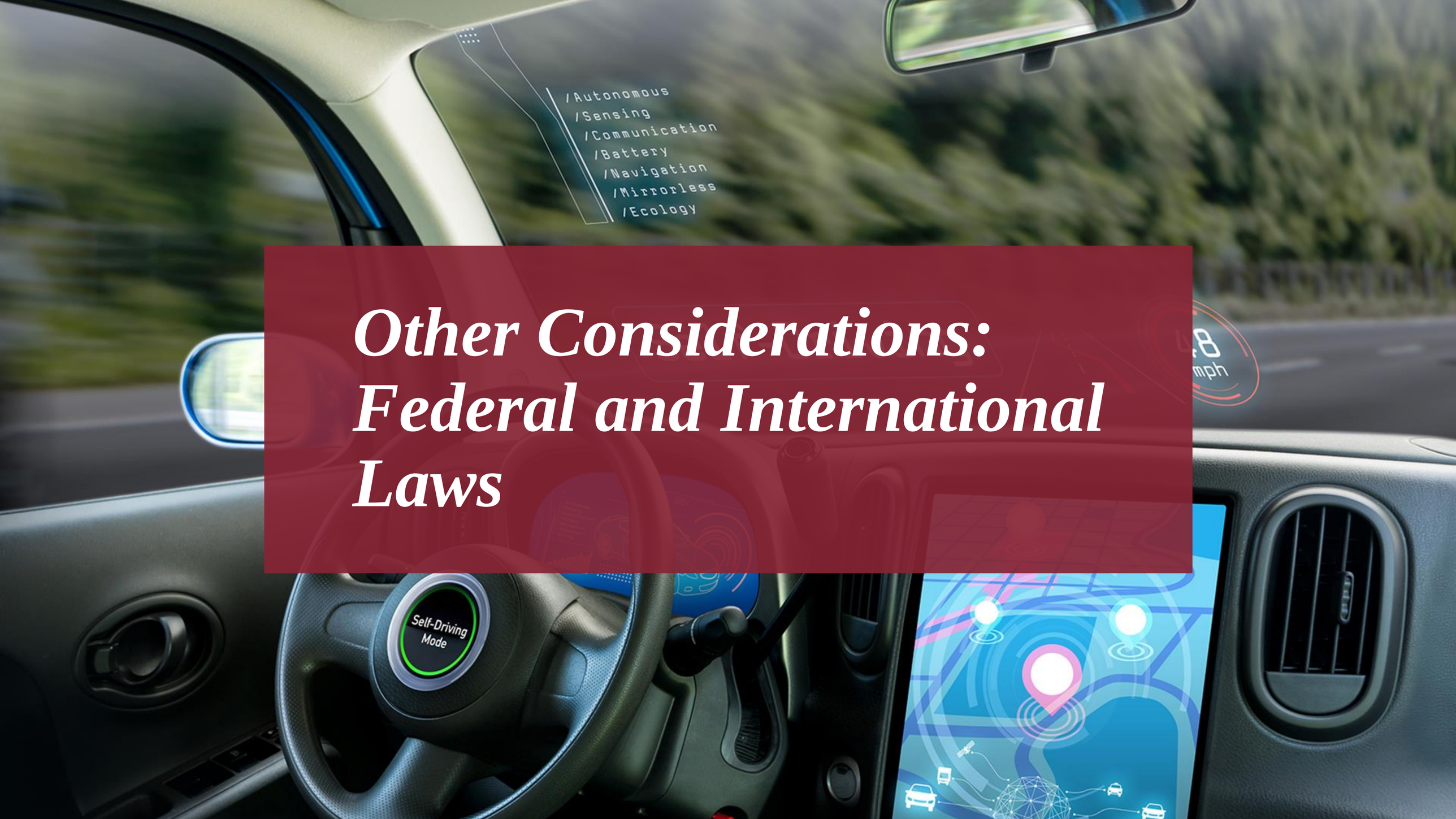
California and Oregon's IoT Security Bills

- California and Oregon's IoT security laws require connected devices to be equipped with "reasonable security features"
- Both went 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 State Laws Affecting Connected Cars

- During the last two legislative sessions, a number of states have considered regulating geolocation information
- States may further regulate how companies use AI
- State tort law may provide potential causes of action for plaintiffs
- **Private lawsuits under state unfair competition laws**

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)	*Cahen v. Toyota Motor Corp.*, 717 F. App'x 720, 723 (9th Cir. 2017) (plaintiffs alleged that Toyota and GM's car computers lacked proper security and that they shared information about plaintiffs with third parties without securing the transmission; district court dismissed the case on lack of proper standing and the 9th Circuit affirmed).



Other Considerations: Federal and International Laws

Federal Laws Governing AVs and Connected Cars

- NHTSA within the Department of Transportation has authority over AVs
  - Released fourth version of AV Guidance in January of 2020
- The Federal Trade Commission enforces privacy and cybersecurity violations through its authority under Section 5 of the FTC Act
  - Held a connected car workshop in 2017 and released a staff perspective on connected cars in 2018
  - Also released AI guidance in April of 2020
- Congressional Action:
  - The House of Representatives passed the SELF DRIVE Act in 2017 that regulated AVs and included privacy and cybersecurity provisions; did not pass Senate and has not been taken up again seriously by Congress
  - Congress was also considering a number of comprehensive data privacy bills earlier in the year

Would require AV manufacturers to develop a written privacy plan, as well as a written cybersecurity policy

FTC Connected Car Workshop

– 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

FTC Guidance on AI

Ask questions before you use the algorithm

Be transparent

Explain your decisions to consumers

Ensure that your decisions are fair

Ensure that your data and models are robust and empirically sound

Hold yourself accountable for compliance, ethics, fairness and nondiscrimination

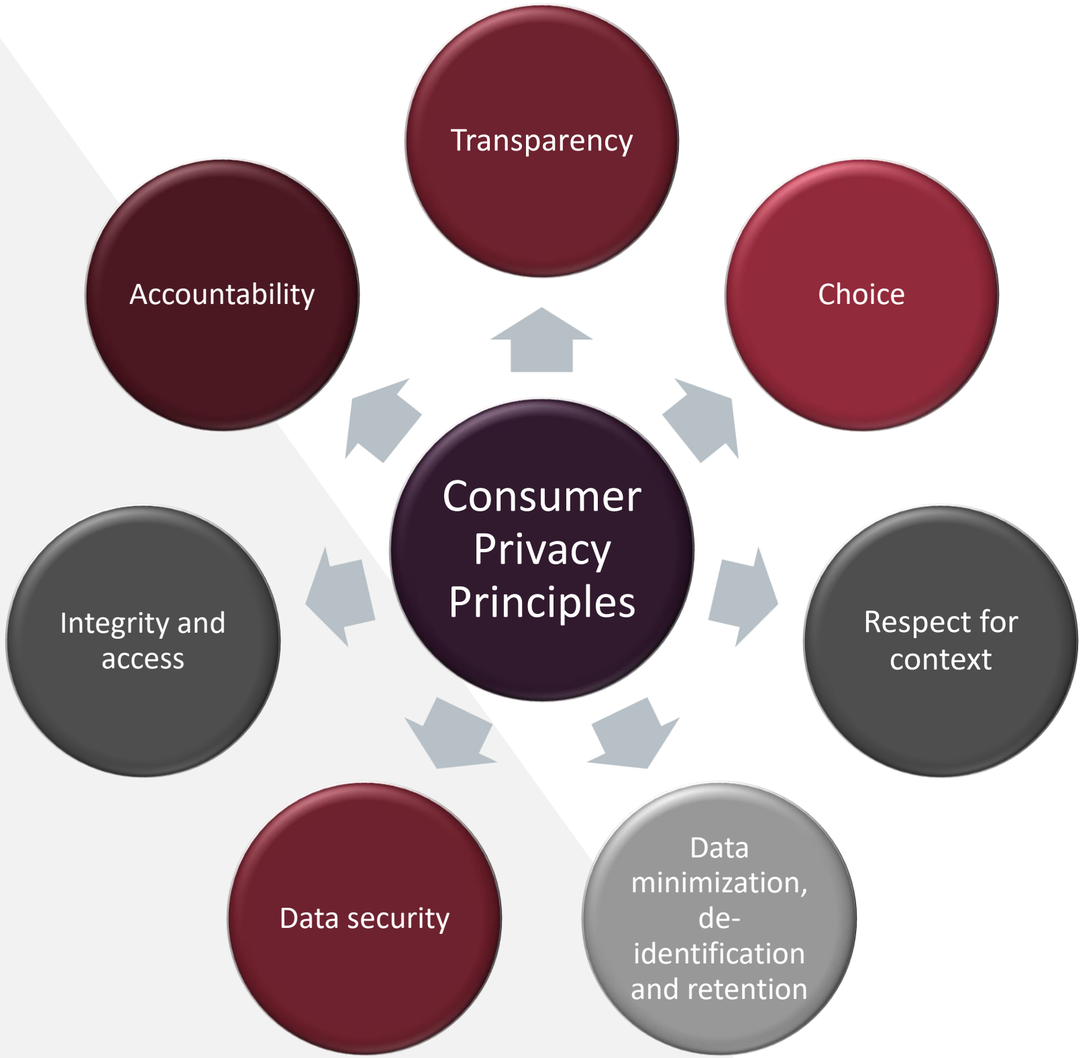
International Laws Governing AVs and Connected Cars

- The GDPR in the EU applies to the connected car atmosphere if businesses target or monitor EU residents
- The EU also released guidelines on personal data collected from connected vehicles in January of 2020
- Other comprehensive privacy laws, such as those in Brazil (effective August 2020) and South Korea, may also affect connected car manufacturers depending on the data they are collecting

EU Connected Car Recommendations

- Categories of information and purposes for collection
- Data minimization and relevance
- Data protection by design and default
- Rights of the data subject
- Data security and confidentiality
- Transfer of personal data to third parties and outside of EU

Self-Regulatory Bodies: Alliance for Automobile Manufacturers



What can be done to mitigate risk?

Steps to Mitigate Regulatory and Litigation Risk

1. Data map
   - Understand what information you collect, for what purposes, and with whom you share it with
2. Know your playing field
   - Understand what rules and regulations could potentially apply to you
3. Be transparent
   - Provide appropriate notices of data collection practices and obtain consent when required to do so
4. Incorporate "privacy by design" principles, including data minimization, purpose specification, onward disclosure and storage in in de-identified form, if possible
5. Implement and maintain reasonable security procedures, including a written information security policy compliant with laws in Massachusetts, New York and the FTC's Start with Security and Stick with Security guidance

Questions?

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

Ali Jessani
Associate
WilmerHale
Ali.Jessani@wilmerhale.com