A Policymaker's Guide to Connected Cars

BY ALAN MCQUINN AND DANIEL CASTRO | JANUARY 2018

Absent proactive public policies, the continued development and adoption of connected vehicles will slow.

In 2011, Akio Toyoda, the president of Toyota, unveiled a car concept he described as a "smartphone on wheels."[1] This metaphor is apt. Over the last decade, car manufacturers, technology companies, and broadband providers have connected vehicles to networks, automated many of their functions, and brought a wealth of innovative applications to consumers. Policymakers should take steps to spur the continued deployment of connected cars, especially by ensuring that connected cars can "talk" to connected infrastructure.

In the past, cars were primarily mechanical devices that used some electricity to power certain components, such as lights, radios, and spark plugs. Over the last two decades, cars have incorporated both mechanical and digital capabilities. Just as computers became increasingly connected to the Internet in the 1990s, cars are now becoming increasingly connected to networks and devices. Not only does this include connectivity to the Internet, it also includes connections to digital services provided by automakers, to the driver's smartphone, and to devices outside the vehicle, such as traffic lights, parking meters, other vehicles, and smart home equipment. Connected cars are becoming more common, with one report estimating that 90 percent of all new cars will have connectivity by 2020.[2] Another report estimates that by 2020, there will be 61 million cars with data connectivity in use globally.[3] But their deployment and functionality could be limited without supportive public policies.

Like smartphones, vehicles are becoming digital platforms that enable and support a vast array of mobility-related digital innovations. These platforms allow innovators and entrepreneurs to build new applications for drivers. Like smartphone makers, car makers maintain proprietary software for the vehicle while offering drivers access to a multitude of

apps and developers a centralized place to access potential customers. They bring virtual assistants, navigation software, entertainment, business applications, smart home applications, and productivity tools to the car. Tech companies, such as Microsoft, Apple, and Google, were the first movers in developing connected car platforms, and as a result, many car manufacturers feature auto platforms, such as Apple's CarPlay, Microsoft Connected Vehicle Platform, and Google's Android Auto, in their new models.[4] Automakers have also started creating alternative app systems for their newer models.[5] For example, Ford and Toyota created SmartDeviceLink, Jeep and Chrysler developed Uconnect, and BMW developed the ConnectedDrive Portal.[6] These connected car platforms will underpin new apps and services for vehicles. And just as mobile app developers have used smartphones' gyroscopes and accelerometers to create innovative apps that do initially unanticipated tasks, such as gauge sleep patterns, so too will car app developers use in-car sensors to create new services in unpredictable and beneficial ways.[7]

With more connected vehicles on the road, policymakers will encounter policy debates and challenges previously seen in other industries that have progressed along the technology adoption lifecycle.[8] Chief among these are concerns about public safety, data protection, liability, intellectual property, data standards, interoperability, and access to wireless spectrum. Policymakers will need to be proactive to address these issues in ways that support safety but also innovation. At the same time, governments will have to do their part by modernizing infrastructure to enable connected vehicles to connect to something more than the user's smartphone.

To address these challenges and fully enable connected car innovation, this report offers eight policy principles that should guide policymakers as they address connected vehicle policy issues:

- Support vehicle-to-everything (V2X) infrastructure.
- Promote national cooperation and interoperability for V2X.
- Incentivize companies to protect consumers.
- Ensure regulations are technology neutral.
- Rely on transparent industry-led standards for data protection.
- Restrict scope creep for regulators overseeing connected vehicle privacy.
- Allow vehicle owners to access and use their own data.
- Permit after-market modifications and repairs while protecting copyright holders' rights.

WHAT IS A CONNECTED CAR?

Connected cars are one of the technologies that makes up the Internet of Things (IoT), a term used to describe the set of physical objects embedded with sensors or actuators and connected to a network.[9] Automakers are embedding intelligence and sensing capabilities into vehicles using several different technologies, such as low-cost sensors, low-power, high-capacity processors, cloud computing, and wired and wireless connectivity.[10] As a result, vehicles have more data, connectivity, and interactivity.

More Vehicle Data

Automakers are increasingly embedding sensors into various parts of the vehicle: inside the engine, on the chassis, and within the vehicle itself. These sensors have enabled automakers to generate significant amounts of vehicle-related data. For example, on-board diagnostics (OBD) systems collect diagnostics data on many aspects of the engine, such as information on fuel levels, the ignition system, the transmission, and emission controls.[11] In addition, automakers and aftermarket parts manufacturers are adding sensors in other parts of the vehicle that are not traditionally tracked through the OBD system, from windshield wipers to headlights. For example, tire-pressure monitoring systems use sensors to continuously check the pressure in each of a vehicle's tires to warn a driver if the tire pressure drops below a certain threshold.[12] Other sensors gather geolocation information, data describing the real-world geographic location of a vehicle. A variety of technologies collect geolocation data, such as in-car telematics systems and transponders. Some advanced forms of geolocation tracking collect more detailed information about the use of a vehicle, such as driving behavior and a precise history of its locations.[13]

Different businesses may have access to this data. Broadband network operators, such as AT&T and Verizon, may have access to cell tower location data; automakers, such as Ford or Toyota, may have access to diagnostic and telematics data from the vehicle; operating system providers, such as Apple and Google, may have access to data from their connected car platforms; and intermediaries, including data resellers and data aggregators, such as Inrix, may purchase and resell third-party data. Moreover, cloud service providers, such as Cisco, help retain vehicle data for automakers to run analytics, update software, and more.[14] Importantly, not all of these businesses may use this data or develop business models around its use.

More Connectivity

Automakers and mobile network operators are also incorporating a variety of technologies into vehicles to connect them to multiple types of networks.

First, some connected car services—such as navigation systems and entertainment apps—use cellular networks for connectivity. Mobile networks also provide Internet connectivity to drivers and passengers. For example, automakers, such as GM, equip connected cars with 4G LTE to allow drivers to connect their personal devices to WiFi in the car to browse the Internet or access apps.[15] Broadband providers are taking the lead in managing data services for many manufacturers and consumers. For example, AT&T provides LTE connectivity to 25 car and truck manufacturers.[16] Likewise, Verizon offers LTE service plans for consumers with Toyota and Lexus connected vehicles.[17]

Second, many connected vehicles offer Bluetooth to link wirelessly to other devices, such as smartphones, within short distances of the vehicle. Bluetooth enables hands-free calling, in-car entertainment through the user's smartphone, locking and unlocking mechanisms, and more. For example, drivers can use Bluetooth to play music from apps on their smartphones through the cars' speakers.

Third, many automakers, broadband providers, and other companies are using several network technologies to enable communications between vehicles and infrastructure. The most widely used of these technologies is dedicated short-range communications (DSRC)—a two-way wireless communications protocol that allows connected vehicles to communicate to each other and to provide the driver with information regarding tolls, traffic signals, and school zones.[18] In addition to WiFi-like functionalities, DSRC can provide critical safety communications between cars, but its large spectrum allocation comes with a significant opportunity cost: the spectrum allocated for DSRC could prove a valuable boost to unlicensed technologies next door, particularly WiFi.

Other next-generation cellular technologies, such as cellular V2X (C-V2X) technology, could offer an alternative or improvement over DSRC. C-V2X technology uses low-latency radio communications that allow vehicles to connect with other systems directly, such as other vehicles, infrastructure, and cloud computing services.[19] While C-V2X uses cellular technologies, it does not rely on cellular networks to operate its V2V functions. In 2016, the standard development organization 3rd Generation Partnership Project created initial C-V2X standards, and the technology is already undergoing tests in San Diego, California.[20] Importantly, the safety-related V2V communications (either DSRC or C-V2X) require a relatively small amount of bandwidth, but specialized connections to maintain low-latency at highway speeds, for example.

DSRC and C-V2X communications are two technologies that could enable communications between vehicles and infrastructure.

Automakers are experimenting with a variety of models for charging customers for connected car services and connectivity costs, such as one-time payments and yearly contracts, as well as models for splitting costs between drivers and third-parties who may benefit from the data.[21]

More Interactivity

Drivers, passengers, other vehicles, and even infrastructure can interact with connected vehicles. Advances in machine-to-machine (M2M) communication allow networked devices to exchange information. Growth in M2M communication is largely driven by new transportation applications, with automotive systems—such as infotainment and telematics—predicted to make up as much as 98 percent of all M2M traffic by 2021.[22]

The increasing number of interfaces is also in part due to the growing prevalence of consumer IoT that has had secondary effects for connected vehicles, allowing vehicles to connect to devices in a driver's pocket, home, or office. The smart-home app HomeLink, for example, allows drivers to use their car's overhead console to open a garage door, turn on their house lights, unlock the door, or adjust their homes' heating and cooling.[23] Cars are also integrating with smartphones, enabling new services that utilize both platforms. Indeed, smartphones are a related platform that—due to having connectivity, certain sensors, and access to related apps—offers some of but not all the functions that connected vehicles offer.

Advances in communications technology for vehicles, referred to as vehicle-to-everything (V2X) communications, are also adding new interfaces for connected vehicles by making

their environment more interconnected.[24] There are several major V2X communications. First, vehicle-to-vehicle (V2V) communications involve communication between vehicles. For example, vehicles could exchange information on braking, direction of travel, speed, location, loss of stability, or upcoming accidents or road hazards. Second, vehicle-to-infrastructure (V2I) communications involve communications between vehicles and the roadway. For example, a vehicle involved in an accident might send an alert to nearby roadway signs, or a roadside unit on a curving highway might communicate to approaching vehicles that there is stopped traffic ahead. Third, vehicle-to-pedestrian (V2P) communications is a catch-all term for systems that avoid collisions by sensing nearby people and objects even when they are not visible to drivers. These systems can warn drivers, pedestrians, and bicyclists before an accident occurs.

CONNECTED CAR APPLICATIONS

Connected vehicle applications come in four primary categories based on how they connect with the vehicle, the user, a service, or other vehicle and infrastructure systems (Table 1). The following section will discuss each of these categories and offer examples of each. Importantly, some of these applications fit into multiple categories, but each is primarily associated with one. For example, navigation applications can use in-vehicle connectivity linking a transponder to the vehicle's on-board display, but this functionality is secondary to its interaction with the end user. Therefore, we classify navigation applications in the "Drivers and Passengers" category.

Table 1: Typology of connected car applications based on type of interaction.

Category	Description	Examples
In-Vehicle	Applications that involve interactions between different components within the vehicle.	Diagnostics, predictive maintenance, and safety applications.
Drivers and Passengers	Applications that involve interactions with a user within the vehicle.	Entertainment, navigation, personal device integration, and remote control.
Third-party Services	Applications that facilitate transactions with third parties using the vehicle.	In-car payment services, roadside assistance, insurance, and more.
Infrastructure and Other Vehicles	Applications that primarily operate through interactions with other vehicles and connected infrastructure.	Crash response, adaptive traffic lights, and emergency vehicle warnings.

In-Vehicle

In-vehicle connectivity applications involve communications that primarily occur within the vehicle between its various parts, but can also involve the driver. Applications in this category are oriented towards safety or maintenance. For example, in-vehicle connectivity applications include a wide array of advanced driver-assistance systems (ADAS), which are designed to help drivers in the driving process by providing them with essential information and automating difficult or repetitive tasks (e.g., braking, steering, keeping the vehicle in lane, parallel parking, backing up, etc.).[25] However, this report will not focus on applications that automate tasks without substantially interacting with the driver, such as automatic braking, electronic stability control, and automatic seat belt tensioners. Instead, this report will focus on applications that directly interact with the driver in some capacity.

Applications in the category also generate secondary data streams. For example, preventative maintenance systems send data back to the automaker for analytics purposes. Similarly, diagnostics systems share information with aftermarket devices and smartphone apps that analyze information from the vehicle.

Diagnostics Systems

Vehicle diagnostics applications—especially aftermarket devices and apps—allow drivers to use data gathering in the vehicle to diagnose engine problems, improve the maintenance of a vehicle, boost fuel efficiency and reduce costs. These systems track vehicle conditions and alert drivers to problems through on-board diagnostics (OBD) system.

Since 1996, cars have been legally required to have in-car OBD systems, which gather information on a vehicle's power, computer, chassis, and body.[26] Until the last decade, however, beyond knowing whether the check-engine light was on, drivers could not easily access or use this information effectively.[27] Aftermarket devices and smartphone apps have changed this, allowing users to tap into this data to receive diagnostic information, track vehicle stats, and better maintain their vehicles.[28] Several smartphone apps combine this data with information from the phone's sensors (e.g., accelerometer and GPS data) to give an overall view of the vehicle's performance. For example, the smartphone app Dash uses an OBD adapter to analyze real-time data about a car's engine, send maintenance warnings, maintain a driver's trip history, and improve a vehicle's fuel efficiency.[29]

Predictive Maintenance

Data from OBD systems enables predictive maintenance analytics applications, which attempt to identify and fix potential problems before they arise. Predictive maintenance services pull data from a variety of sources (e.g., OBD systems, vehicle sensors, and warranty repairs) across thousands of vehicles, such as every make and model of every vehicle released over a year.[30] These systems then use predictive analytics to find performance anomalies that are difficult for humans to identify, allowing automakers, service providers, or fleet managers to fix problems before they occur. These applications provide significant utility for fleet management, enabling managers to monitor real-time and historic GPS-based information and engine performance data to track their fleet, monitor drivers, control fuel costs, schedule service, and inspect vehicles' behavior and state

of repair. For example, Zubie—a connected car platform—offers an automated maintenance solution that sends phone reminders to business fleet owners for proactive vehicle care.[31]

Blind Spot Detection Systems

Blind-spot detection systems are safety applications that provide warnings to drivers if another vehicle enters their blind spot while they are changing lanes. Blind spots are areas outside of a vehicle that the driver is unable to see because their line of sight is blocked. While mirrors can remove blind spots directly behind a driver, they often leave blind spot areas to either side of a vehicle. Blind spot detection systems use sensors to detect objects in a vehicle's blind spots and relay that information to the driver through alerts.[32] For example, Volvo and Ford offer blind-spot detection systems that use sensors to warn drivers if a vehicle enters their blind spot while they are changing lanes.[33] Some blind-spot detection systems use cameras to show useful information when backing up or directly display when an object is in one of a driver's blind spots.[34] Other safety related applications involve front-end collision avoidance, lane departure sensing, and parking assist systems.

Drivers and Passengers

User connection applications involve interactions between third-party service providers and users inside the vehicle, facilitated by the connected vehicle. Drivers use applications in this category for navigation, entertainment, or remote control of the vehicle. These applications can also connect a driver or passenger directly to personal devices, enabling services within the vehicle. For example, some connected car platforms allow users to link their vehicle with their connected home devices, such as the Nest Thermostat, to use voice commands to control the temperature of their home from the comfort of their vehicle.[35]

Navigation Systems

Integrated navigation systems combine geospatial data with real-time traffic information to guide a vehicle to its destination. These systems can automatically reroute a car around traffic jams and provide the user with information about weather, parking, and general points of interest on the road.

Navigation systems primarily use global positioning systems (GPS) receivers, which receive signals from multiple satellites to calculate a vehicle's position to within 10 meters of its actual location.[36] However, several researchers are working on improving positioning systems, such as highly precise GPS tracking and systems that exploit existing signals, such as cellular and Wi-Fi, that are significantly more accurate and will eventually be instrumental in autonomous driving applications.[37]

BOX 1: CONNECTED CAR NAVIGATION SYSTEMS

There are several integrated navigation systems currently offered for connected vehicles.

- **Proprietary in-car navigation systems**: Automaker-owned systems that come in a vehicle's on-board unit. For example, GM offers a factory integrated navigation system in certain models.[38]
- **Partnerships**: On-board unit systems that use services that result from partnerships with GPS-navigation companies. For example, Honda equips its 2016 models with Garmin-based navigation systems.[39]
- **Open-sourced mapping and navigation systems**: Some automakers are using data from public or private sources to create mapping and navigation apps. For example, Tesla updated its map systems using data from MapBox (an open-source mapping platform that consolidates several map sources) and Valhalla (an open source routing engine for navigation).[40]
- **Third-Party Navigation Apps:** Some connected car platforms feature third-party navigation apps or allow drivers to download these apps at their discretion. For example, Toyota's SmartDeviceLink lets users download mobile navigation apps from iOS and Android app marketplaces.[41]
- **Aftermarket Devices**: Drivers can use stand-alone devices that attach to a car's dashboard to help navigate their surroundings. For example, TomTom units are aftermarket devices that offer GPS navigation.[42]
- **Smartphones:** Drivers use smartphone applications, such as Google Maps, Waze, or HERE Maps, that when combined with a car mount turn a smartphone into an on-board navigation system.[43]

Parking and Gas

In addition to general navigation systems, there are several smartphone or smart car apps that are designed to help the driver locate specific nearby points of interest, such as parking, gas stations, ATMs, or bathrooms. While many of these apps are currently available for smartphones, connected vehicle drivers eventually should be able to access these applications using the display on the vehicle via connected car platforms (e.g., Android Auto, CarPlay, etc.).

First, parking apps help drivers find and compare parking spaces. For example, BestParking is an app that allows users to compare parking garages in major North American cities by price and location.[44] Similarly, the app Parker uses data from street sensors and government sources to find open parking spots in real time and guide drivers to them.[45] Other parking apps help users return to their parked cars. For example, Automatic Track uses real-time location data to help users find their cars quickly in a crowded parking lot.[46]

Second, there are several applications that track gas pricing and can navigate drivers directly to refueling stations. For example, crowdsourcing apps, like GasBuddy and Waze, asks users in the area to enter the prices they pay at the pump, directing users to the cheapest gas station.[47] Similarly, the app Gas Guru uses gas price information pulled from the Oil Price Information Service to direct users to cheap gas stations.[48]

In-Car Entertainment

Drivers and passengers have access to more in-car entertainment than ever before directly from their dashboards. One 2017 report estimates that due to greater availability of in-car connectivity and connected car platforms—such as CarPlay, Android Auto, and SmartDeviceLink—the in-car entertainment hardware market will reach $36 billion by 2021.[49] These platforms allow drivers and passengers to browse the Internet, connect to social media, send SMS messages, and access various forms of entertainment, such as music, news, radio and podcasts.

As the Internet of Things grows, connected vehicles will be able to interface with other devices beyond the driver's smartphone, connected home, or office.

These applications elicit some safety concerns, primarily due to distracted driving. In 2015, NHTSA reported that distracted driving was responsible for roughly 3,500 deaths.[50] To combat this epidemic and get drivers' attention back on the road, many app makers are working to cut down on drivers' desire to look at their phones or focus too long on in-car displays. For example, many platforms, such as Apple CarPlay and Nuance, allow drivers to control their connected car applications through voice recognition technology.[51] When the driver receives a notification, the system will read it aloud through natural speech, reducing the driver's need to look at a device. In addition, platforms such as Google's Android Auto, have another safety feature that connects users' smartphones to their dashboards, rendering them otherwise useless while driving.[52] As a result, drivers are less likely to get distracted by their phones.

Connected Home or Office

Drivers can use connected car platforms to link their vehicle directly with their smart home or office devices, controlling home or work appliances from the road. For example, HomeLink allows drivers to use their car's overhead console to open garage doors, lock or unlock front doors, turn on house lights, or adjust their home's air-conditioning.[53] Similarly, the Microsoft Connected Vehicle Platform allows drivers to access business applications, such as virtual assistants, to complete work tasks such as coordinating their calendar.[54]

Remote Control

Remote control applications allow drivers to remotely access and precondition their vehicles. Drivers can use these tools to remotely start a car, lock or unlock its doors, honk the horn, adjust air-conditioning, or limit where it can travel. For example, remote starters can warm up a cold car, protecting the passenger from cold winter mornings, while ensuring oxygen sensors and emission controls are working at peak efficiency before the driver operates the vehicle.[55] Similarly, remote monitoring applications, such as BMW's Connect+ app, allow a user to use a car's cameras to view its surroundings remotely from a smartphone.[56]

Other remote applications allow a user to control the car's behavior, including how fast it can travel and where it can go. Toyota's connected car platform Entune can set speed limits and map predetermined geographic boundaries using geo-fencing—creating a virtual geographic boundary with GPS.[57] Drivers can use this application to avoid toll roads or as a parental control for the vehicle, limiting how fast it can go, monitoring activity, or automatically sending an alert to parents if a teen driver leaves the predetermined area.[58]

Third-party Services

These applications allow users to make transactions with third parties using the vehicle. This category includes a range of both private-sector services—such as in-car payment services, vehicle recovery systems, roadside assistance apps, and insurance—as well as public-sector services—such as vehicle miles traveled, (VMT) taxes, street bump, and smart parking. Drivers can use these applications to request services or pay for taxes, tolls, gas, and parking. By using the connected vehicle to make transactions, companies can make services more convenient and cheaper. Moreover, both public and private entities can experiment with new business models. For example, insurers can use diagnostic and geolocation information gathered from the vehicle to offer insurance plans based on usage.[59]

In-Car Payment Services

Many car manufacturers, financial technology companies, and others are developing in-car payment services, whereby a driver can automatically pay for goods, parking, or gas using their vehicle. These services allow vehicles to function as mobile wallets, adding another layer of convenience and security for drivers. Furthermore, some of these systems can protect users from fraud or identity theft, such as by avoiding scams that steal credit card information directly from card readers at gas station pumps.[60]

Some of these systems are proprietary. For example, Audi's Audi Connect wireless parking-payment system connects cars and parking lots and gas stations, allowing users to automatically pay to park or fuel up.[61] Similarly, GM developed an app for its 2017 and 2018 models' infotainment systems called "Marketplace" that allows users to place orders and pay for goods, such as food from certain restaurants (e.g., Starbucks, Applebee's, and Dunkin' Donuts), as well as gas from select gas stations (e.g., Shell).[62] Other payment systems are powered by traditional payment companies. For example, Visa is teaming up with car manufactures, such as Honda, to turn cars into "wallets" and offer car-based commerce.[63] Visa's in-car app allows drivers to pay for gas or parking, or order take-out food from the comfort of their vehicles.[64]

Roadside Assistance

Roadside assistance applications quickly connect drivers to the nearest available tow truck. Until recently, many drivers relied upon the American Automobile Association (AAA), a membership-based roadside assistance company, as a precaution in the event that they found themselves stranded. While AAA does offer its own smartphone app for its members, new services are offering on-demand roadside assistance that connect drivers to the nearest

available tow truck, cutting costs and wait times by using GPS in a driver's phone or connected vehicle to guide the tow truck to them.

There are several apps available for connected cars that offer new forms of roadside assistance. For example, Urgent.ly offers on-demand roadside assistance services, where prices are determined by distance.[65] While the app was initially only offered on smartphones, some connected vehicle platforms, such as AT&T's Drive, now offer Urgent.ly.[66] In addition, Honk also offers on-demand roadside assistance, with the goal of expediting help. To speed up response time, Honk uses a proximity-based system that locates the nearest facility and asks drivers for additional time-saving information, such as whether they have a spare tire.[67] Honk is currently only offered for smartphones, and may soon be available on connected car platforms.

Vehicle Recovery Systems

The Federal Bureau of Investigation estimates that over 760,000 vehicles were stolen in the United States in 2016.[68] To combat this, vehicle recovery systems use a variety of technologies to track the position of a vehicle in real time or construct a history of where a vehicle has been to recover the vehicle if it is stolen. Vehicle manufacturers offer a range of vehicle recovery systems, such as GM's OnStar, BMW Assist, and Toyota Safety Connect.[69] In addition, some companies offer aftermarket options, such as LoJack, Smart Tracker, and Zoombak.[70] Most current vehicle recovery systems use a GPS transmitter and cellular transmitter to locate a vehicle's position. There are some limitations to this approach, such as "dead spots" when cellular service is not working or interference if the vehicle is parked in a structure. Conversely, LoJack uses a radio transmitter and a series of radio receivers to track and recover a vehicle. When the vehicle is stolen, police can use a remote command to turn on the transmitter, which broadcasts the vehicle's location to within 5 miles at a set frequency.[71]

As in-vehicle technology improves and cars become more interconnected, new anti-theft measures are becoming viable. Preventative measures like engine ignition cutoff, remote control, and remote locking, when combined with geolocation information, offer automakers new tools to stop thefts and locate stolen vehicles. For example, in 2016, responding to a police report of a stolen vehicle, BMW located and disabled the car through its ConnectedDrive platform, trapping the thief inside until police arrived.[72] As connected vehicles grow in prevalence, it will become increasingly difficult for thieves to steal cars.

Insurance

Insurers are using data collected by connected cars to offer smarter and cheaper insurance to drivers. Using data from the vehicle—such as diagnostic and geolocation information—insurers can create more precise rating variables that allow usage-based car insurance (UBI), also known as pay-as-you-drive (PAYD) insurance, whereby insurers base pricing on where, when, and how drivers operate their cars, offering competitive quotes for safer drivers.[73] UBI represents a significant departure from traditional insurance underwriting, changing how risk is assessed from a model based on group behavior (e.g., demographics) and proxy

variables (e.g., credit scores) to one based on data and sophisticated analytics.[74] UBI allows insurers to more accurately price insurance premiums and offer discounts for safer driving patterns and behavior. For example, the company Octo Telematics offers telematics analytics services to insurers that improves insurers' risk assessment and claims management, while reducing costs for drivers.[75] These systems are also good for the environment as they provide a market signal for driving less, since doing so results in lower premiums.

Auto Financing

Geolocation data and connected car technologies are changing the auto finance industry. Car dealers and finance companies now offer sub-prime car loans with the condition that applicants install starter interrupt devices in their vehicles. These GPS-equipped devices function as kill-switches for the ignition system of the borrower's car if the consumer does not make payments in a timely manner or make other arrangements with the dealer.[76] Vehicles in motion are not disabled. These devices send reminders to customers to assist in keeping track of their payment schedule and, according to industry, results in fewer delinquencies.[77] If buyers fail to make their payments, while they will be inconvenienced with a car that will not start, creditors will not immediately repossess the car—saving the owner repossession and storage costs.

Data from connected vehicles is also enabling innovation in other industries, such as the financial services sector, allowing for new products and services.

Vehicle Miles Traveled Taxes

Connected cars can also enable new ways to finance roads. Currently, roads are financed by a combination of gas taxes and general fund revenues. But virtually all transportation economists recognize that this is an inefficient way to fund roads, in part because users do not pay the full price of their use of the system.[78] For example, traveling on a crowded urban freeway imposes costs that are often an order of magnitude higher than traveling on a lightly-used rural road. Likewise, heavy-duty trucks impose more costs on the system than they pay, primarily due to pavement damage because of their weight.[79]

Vehicle miles traveled (VMT) systems address these problems by tying the price to the actual cost of driving. A VMT system works by recording on the vehicle's onboard computer system where and when it travels and the cost-per-mile segment of that travel. It then would automatically calculate and remit payments to road service providers (e.g. cities, counties, states, federal government and private toll road operators). Such a system can and should be designed so the only information passed on to providers is the amount of money paid, and never any trip information (e.g., the time of day or location of the trip). VMT can also be designed to promote more efficient use of highways, for example, by charging higher fees when roads are most congested to create incentives for drivers to shift modes or times of travel.[80]

Potholes

Potholes result in thousands of deaths and billions of dollars of vehicle damage each year.[81] However, due to the unpredictable nature of potholes and other poor road conditions, localities primarily rely on citizen reports to find and fix them. To address this problem, in 2011, Boston developed Street Bump, a smartphone application that crowdsources this

information by identifying potholes from cars' experiences driving over them and automatically relaying potholes' locations to the city transportation department.[82] The app uses the device's accelerometer to detect "bumps" on the road (e.g., potholes, manhole covers, drains, speed bumps, etc.) while the vehicle is in motion.[83] However, smartphone accelerometers can be inconsistent and using this app quickly drained smartphone batteries.[84]

Connected vehicles will improve this system. For example, Google is developing a system that uses in-car sensors and GPS to detect and avoid potholes.[85] When widely implemented on vehicles in a city, this system allows the company to gather information on bumpy roads, allowing it to direct drivers to navigate around them. While this technology is currently for Google's use in its navigation services, future iterations could allow drivers to opt-in to providing municipalities with this information to improve local roads.

Smart Parking

Some smart city applications, such as parking meters, when coupled with connected cars, can improve the efficiency of infrastructure and drivers, reduce traffic, and benefit the environment. Smart parking applications—municipal programs that use wireless sensors to detect metered parking space occupancy—allow cities to determine the right price to charge for parking, creating incentives for drivers to park in less-congested areas. For example, San Francisco launched the app SFpark in 2011 that showed drivers available parking in the city. The program reduced traffic volume, improved drivers' efficiency in finding parking, increased city revenues, and reduced weekday greenhouse gas emissions.[86] In the future, connected vehicle drivers may be able to access these services through the connected car platform on their vehicles' displays.

Infrastructure and Other Vehicles

Vehicle-to-everything (V2X) systems, including vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communications, allow connected vehicles to communicate with moving parts of the traffic system around them. They enable a large number of current and future applications for both public and private-sector entities. In connected vehicles, V2X systems can convey important information to the driver about road conditions, such as accidents or oncoming emergency vehicles. And for transportation authorities, V2X communications have the potential to improve the safety and efficiency of vehicles on roadways.

V2X communications applications are still relatively new, with automakers primarily leading these efforts. Indeed, while many automakers are starting to make it possible for vehicles to talk to other systems—the first V2V-enabled vehicle, the Cadillac CTS, became available in 2017—most traffic systems will not have the ability to talk back.[87] Some cities and states have launched pilot studies to create connected infrastructure. For example, the U.S. Department of Transportation granted $42 million in funding for three V2X pilot tests in New York City, Tampa, Florida, and the state of Wyoming.[88]

Eventually, the mass deployment of connected vehicles with V2X communications will become the backbone of future transportation systems. By gathering data from all the connected cars on the road (e.g., weather data, surface conditions, traffic conditions), transportation authorities will be able to analyze and share information about road conditions with connected vehicles, creating more efficient traffic flows, reducing congestion and emissions, and preventing accidents.

Crash Response

In 2016, there were an estimated 4.6 million motor-vehicle related injuries resulting in over 40,000 motor-vehicle related deaths in the United States, according to the National Safety Council.[89] To improve safety, automakers and government officials are working to improve and create new car features to enhance drivers' safety by responding to crashes. The traditional crash response system GM's OnStar, for example, has built-in sensors that, in the event of an accident, can predict the severity of injuries from the crash and route emergency services.[90] Newer services, such as the smartphone apps SOSmart and CamOnRoad, use smartphone sensors and past crash data to detect when a car is in an accident, find nearby hospitals, and notify authorities.[91] Furthermore, many automakers are including electronic data recorders (EDR)—also known as "black boxes"—that record information about the vehicle and driver behavior that can be used in the event of an accident. This information could include the car's speed, whether braking occurred, and whether people in the car were wearing seatbelts.[92]

Some information from each of these technologies will eventually help with V2X communication applications that warn drivers of approaching accidents, potential collisions, upcoming traffic, dangerous road conditions, and other dangers. These applications could then automatically call emergency services in the event of an accident. The U.S. Department of Transportation, states, and various automakers are undergoing pilot programs to fund and test the readiness of V2X safety technologies.[93]

Emergency Crash Notification

While the European Union has not mandated V2X communications, it has required new vehicles to come equipped with emergency communications capabilities. In June 2013, the European Commission proposed new regulations for an automated emergency crash notification system (eCall), which automatically dials Europe's emergency number in the event of a serious accident.[94] This system stays dormant until a crash occurs, at which point the vehicle communicates its location to emergency services, the time of the incident, and other information pertinent to safety-response personnel.[95] The eCall system works even if a driver is unconscious or is unable to use a phone. It can also be triggered manually by pushing a button in the vehicle. Once an emergency signal is initiated, mobile network operators identify it and route the call to public safety authorities.[96] eCall will be mandatory in all new vehicles in Europe starting in April 2018.[97] To date, the United States has no similar mandate for an automated emergency crash notification system.

Adaptive Traffic Lights.

Anyone who has driven a car has experienced the frustration of sitting at a red light with no vehicles going through the green light. This represents wasted time and wasted fuel. Local traffic planners try to program traffic lights based on expectations of traffic, but regardless of how good their efforts are, planned traffic signals are less efficient than dynamic ones. Some cities have attempted to build in some adaptivity to lights, but these technologies—usually road sensing loops—are expensive and only account for traffic that is stopped, not traffic following through the cross street. Connected vehicles interacting with connected traffic lights can change this through V2I communication, allowing traffic lights to respond to real-time traffic demands.[98] For example, if there are few cars going through a green signal but more cars stopped at a red signal, the light would automatically switch to allow the backed-up cars to proceed. Studies have suggested that giving connected vehicles the ability to communicate with traffic signals can significantly enhance traffic flows and reduce congestion.[99] Moreover, these V2I systems are significantly less expensive than traditional adaptive traffic-light-control technology, such as sensing loops, radar or video, not to mention they add new road capacity.[100]

This technology is currently in the test phase. For example, Tampa, Florida, is launching a project in 2018 to connect 10 area buses to traffic signals, which will prioritize their movements and the signals' response to traffic.[101] This project is one of three connected vehicle pilots funded by grants from the U.S. Department of Transportation. Similarly, Audi worked with Las Vegas, Nevada, to launch a V2I project in 2016 that allows its connected vehicles to receive real-time signal information from the city's traffic management system to make intelligent predictions about traffic conditions.[102]

Emergency Vehicle Warnings

Municipal governments will likely gain significant utility from connected vehicles for safety and emergency response services. It can often be difficult for drivers to move out of the way of emergency vehicles, especially when these cars must risk going through intersections where oncoming traffic does not have knowledge of the emergency vehicle. To solve this problem, several cities—including Grand Rapids and Palo Alto—are working with the company HAAS Alert to notify drivers in real time of upcoming ambulances, police cars, and fire trucks through V2V communications.[103] Ideally these systems would send automatic warnings to cars, letting the driver know that an emergency vehicle is behind them and that they should move over.

POLICY ISSUES

The United States has a complex regulatory environment for vehicles and infrastructure, with local, state, and federal government agencies creating rules for various aspects of vehicle travel. Traditionally, the U.S. Department of Transportation has focused on regulating how vehicles are built (e.g., setting airbag standards), while the states focus on regulating the operation of the vehicle (e.g., insurance, licensing, registration, traffic laws). Recently, however, these lines have started to blur as various states, including California, Nevada, and Michigan, have passed laws concerning the technology used in cars.[104] On the

other hand, Congress is considering the SELF DRIVE Act, which would establish a federal framework for the regulation of self-driving and connected cars.[105]

This complex regulatory environment is relevant to several policy issues for connected vehicles, including public safety, data protection, liability, market modifications, data standards, and spectrum availability. Moreover, slow action by federal and state governments has delayed the adoption of connected infrastructure. If the government does not tackle these issues properly, it will limit the development and deployment of connected vehicles.

Public Safety

The federal government has played an active role in vehicle safety since the National Traffic and Motor Vehicle Safety Act was passed in 1966, carving out this regulatory responsibility for the National Highway Traffic Safety Administration (NHTSA).[106] NHTSA is part of the Department of Transportation. It focuses primarily on regulating safety, ensuring that automobile manufacturers build safe vehicles and that policies are in place to prevent accidents. Over the past few years, NHTSA has released guidance in several areas related to connected vehicles, including for device makers, V2V applications, cybersecurity, and automation (these initiatives are discussed in further detail below).[107] Outside of the federal government, states have also considered or passed laws to address driver operation of vehicles. For example, states set traffic laws to reduce inappropriate behavior (e.g., driving under the influence, reckless driving, etc.) and rules for safe operation of equipment (e.g., headlight usage, child safety seats, etc.).

When it comes to mission-critical safety technologies, NHTSA regulatory guidance is critical to preventing accidents and saving lives.

One major focus of safety regulation for connected vehicles in both states and the federal government is on reducing distracted driving, which ranks as one of the leading causes of accidents. This problem has been exacerbated by the high adoption and use of portable devices, such as mobile phones, which present visual, manual and cognitive distractions to drivers.[108] In 2010, the National Transportation Safety Board (NTSB), an independent federal agency, issued recommendations that all states ban nonemergency use of portable electronic devices by drivers.[109] Most states have since adopted these policies. According to the Governors Highway Safety Association, as of October 2017, 15 states plus the District of Columbia, Puerto Rico, Guam and the U.S. Virgin Islands had passed legislation banning the handheld use of cell phones while driving.[110] In addition, 47 states plus the District of Columbia, Puerto Rico, Guam and the U.S. Virgin Islands had passed legislation prohibiting drivers from texting while driving.[111] In November 2016, NHTSA proposed draft guidance on driver distraction caused by mobile devices and other electronic devices in vehicles.[112] As of January 2018, NHTSA has not finalized this guidance. Besides portable devices, NHTSA has also focused on reducing distractions presented to drivers from in-vehicle electronics. In 2012, NHTSA released a set of voluntary guidelines for in-vehicle electronics provided by the manufacturer to help reduce distractions.[113]

Of course, not all safety-based rules for IT in vehicles have been developed by the government. Twenty-six organizations and companies have conducted consumer education

and outreach activities to dissuade people from driving while intoxicated.[114] Similarly, the Alliance of Automobile Manufacturers, an industry association, has adopted its own standards for in-vehicle electronics designed to protect public safety.[115]

On the other hand, public safety interests could also motivate greater use of connectivity in vehicles. For example, next-generation 9-1-1 will integrate V2X communications to allow emergency medical technicians to access more information about an accident before they arrive—such as the exact location of the vehicles and if the air bags deployed—so they can get to the accident faster, know who is injured, and have a good idea about the extent of their injuries.[116] This information can also be sent ahead to the emergency room, so doctors at the hospital can prepare to receive victims. Similarly, the primary motivation of the DOT's Connected Vehicle Safety Pilot Program in Ann Arbor, Michigan, is to study the effectiveness of using IT in vehicles and roadways to reduce accidents.[117] But legislation is required to permit the use of some of this technology, especially the autonomous component. For example, California, Nevada, and Florida have passed laws allowing the use of autonomous vehicles, albeit with certain restrictions to ensure public safety.[118] Furthermore, governors in states such as Arizona, Delaware, Massachusetts, Washington, and Wisconsin have issued executive orders that regulate the use of autonomous vehicles.[119]

Privacy and Security

Public and private-sector entities collect and store information about the location, speed, and occupancy of vehicles through many different connected vehicle technologies. Over the last few years, several high-profile media stories have drawn the attention of automakers, tech companies, and regulators alike to cybersecurity and privacy issues related to connected vehicles. For example, in 2015, a group of security researchers demonstrated that they could remotely access and hijack vehicles through their connected applications.[120] Indeed, because of security researchers' findings in 2015, Fiat Chrysler recalled 1.4 million vehicles due to security vulnerabilities, and Tesla quickly patched a security flaw in its cars' software.[121] Since that time, policymakers, automakers, businesses offering connected car services, and other interested third parties have paid more attention to the security and privacy of connected car products.

Different rules govern the privacy and security of this information in the United States depending on who collects it and for what purpose. This information is valuable for transportation planners, drivers, and businesses, but questions regarding data privacy and cybersecurity will likely shape how different entities can use the data.

Government Access to Data

In the public sector, multiple federal laws govern the use of personally identifiable information (PII). The three laws that set most requirements for how federal agencies handle this information are the Privacy Act of 1974, the Paperwork Reduction Act of 1980, and the E-Government Act of 2002.[122] The Privacy Act limits the PII that federal agencies can collect and distribute by forcing them to specify the purpose of collecting information, limiting collection to those purposes, and allowing individuals to review

information in their own records and request corrections if it is inaccurate. The Paperwork Reduction Act requires agencies to seek comment on proposed information collection activities and have an independent review process in place for information collection requests.[123] The E-Government Act requires federal agencies to conduct Privacy Impact Assessments to analyze what PII is stored in government systems, requiring security controls to protect this information. In addition to setting standards for federal agencies, federal legislation limits how states can use drivers' data. The Driver's Privacy Protection Act (DPPA) of 1994 sets standards and governs privacy and disclosure of PII gathered by state departments of motor vehicles (DMVs).[124]

Law enforcement relies upon location information and other data collected from connected vehicle applications to solve crimes and prosecute criminals. Some activists have voiced concern about law enforcement access to data from connected vehicles, but as with data gathered from other technologies, the government is constrained as to how and what it can collect.[125] Government access to private data is restricted by the Fourth Amendment, which protects against unreasonable search and seizure.[126] In 2011, the U.S. Supreme Court ruled unanimously in United States v. Jones that police need a warrant to use GPS to track vehicles.[127] In addition, other laws—such as the Electronic Communications Privacy Act and the USA PATRIOT Act—regulate law enforcement access to PII stored by the private sector. Moreover, the Supreme Court is currently reviewing whether law enforcement officials require a warrant to obtain cellphone location information from wireless carriers.[128]

State and local governments also use private data collected from connected vehicle applications to improve incident response and congestion on roads. For example, Waze's Connected Citizen program gives private data to local governments to improve traffic monitoring.[129] While all state governments have security measures to protect the data they gather, only 19 states have a specific statute requiring policies to ensure the privacy and security of data they retain.[130] Of these, 14 states require state government entities to develop retention policies to destroy or dispose of personal information when it is no longer of use.[131]

Private Sector Data Protections Rules

There are several federal laws that specifically address privacy and security of private-sector use of drivers' data. In 2015, Congress passed the Driver Privacy Act to limit the use of data gathered from electronic data recorders (EDR)—devices known as black boxes that record data in the event of a car accident.[132] The Driver Privacy Act specifies that the data from an EDR is the property of the vehicle owner, regardless of where it was manufactured. More generally, the Computer Fraud and Abuse Act (CFAA) prohibits individuals from obtaining information, accessing, or damaging a computer (i.e., a connected vehicle) without authorization.[133]

In general, there are two primary regulators that could intervene on data-protection issues for connected vehicles: NHTSA and the Federal Trade Commission (FTC). First, NHTSA has asserted its authority over data protection rules for connected vehicles, in both the

cybersecurity and privacy contexts. Regarding cybersecurity, NHTSA initiated an Advance Notice of Proposed Rulemaking and a Request for Information in 2014.[134] NHTSA's current privacy framework for connected cars is based on the National Institute of Standards and Technology's (NIST) fair information practice principles, and the 2007 Vehicle Infrastructure Integration Consortium Privacy Policies Framework.[135] NHTSA also considers privacy effects and implications in its regulation of connected vehicles. For example, in 1997 NHTSA issued recommendations for EDRs, and since that time has issued guidance on the use and protections of EDR data.[136] NHTSA has also taken privacy implications into account for other rules.[137] However, as the Government Accountability Office (GAO) has noted, NHTSA does not have a clearly defined role and responsibility as it relates to privacy issues of connected vehicles.[138]

Second, U.S. consumer protection law designates the FTC as the primary regulator for general data-protection enforcement, including for connected vehicles. The FTC enforces related laws on the Internet, such as the Children's Online Privacy Protection Act (COPPA), which regulates advertising targeted at children. The regulator also has the power to enforce against unfair or deceptive acts or practices, which it uses to bring enforcement actions against a wide range of entities who have not kept their promises to consumers in stated company privacy or security policies.[139] When a company acts unfairly or deceptively, such as by not following their stated principles, the FTC can bring enforcement actions against that company.[140] The FTC also has authority to ensure that developers of in-vehicle apps adhere to their stated terms of service, especially if some apps run on platforms outside of the vehicle, such as a mobile device. In June 2017, the FTC and NHTSA held a joint workshop on the privacy and data-security issues related to connected vehicles, bringing together a host of stakeholders from industry, the government, and civil society to analyze these issues.[141]

Besides regulators, other federal agencies have started efforts to understand and support the development of connected vehicles. For example, the National Telecommunications and Information Administration (NTIA) in the Department of Commerce released a request for comment and a subsequent report on the benefits, challenges, and role for government in fostering the Internet of Things, which included a discussion of privacy, security, and connected vehicles.[142] Similarly, NTIA has convened a multi-stakeholder process on security upgradability and patching for IoT devices to ensure a secure lifecycle for these devices.[143]

Congress has also considered draft legislation that could affect privacy and security for connected vehicles. For example, Senators Edward Markey (D-MA) and Richard Blumenthal (D-CT) released legislation in 2015 to require federal standards on anti-hacking, data security, privacy, and threat detection for future motor vehicles.[144] Other legislation that could affect connected vehicles, sponsored by Senators Mark Warner (D-VA) and Ron Wyden (D-OR), is aimed at security and management of the Internet of Things generally, such as requiring federal standards around how companies can update these devices.[145] In addition, Congress has proposed privacy legislation targeted at

geolocation information, such as the Geolocation Privacy and Surveillance Act [originally proposed in 2015 by Sen. Ron Wyden (D-OR) and Reps. Jason Chaffetz (R-UT) and John Conyers (D-MI), and reintroduced in 2017 by Rep. Blake Farenthold (R-TX)]; the Online Communications and Geolocation Protection Act [proposed in 2015 by Rep. Zoe Lofgren (D-CA), Ted Poe (R-TX), and Suzan Delbene (D-WA)]; and the Location Privacy Protection Act [proposed in 2015 by Sen. Al Franken (D-MN)].[146]

Finally, state legislatures have created data protection laws that affect connected vehicles. For example, most states have implemented data breach notification laws that require businesses and government agencies to notify individuals if PII has been lost or stolen.[147] Similarly, 17 states have specific laws that regulate data from EDRs.[148] In addition, several states, including California, are reviewing draft legislation for all aspects of autonomous vehicles, including privacy and cybersecurity.[149] In the future, states may craft their own legislative requirements or guidelines for in-vehicle advertising, as they have for mobile online advertising.

Transparent industry-led standards help avoid conflicts of interest, jurisdictional conflicts, and legal limitations.

Self-Regulatory Efforts

The private sector has also initiated several self-regulatory measures for both privacy and security for connected vehicles. When made public, the FTC backs up these efforts to ensure that companies keep their promises.

First, automakers and other entities have created self-regulatory frameworks with regard to privacy. In 2014, automakers unveiled a series of commitments, called the Consumer Privacy Protection Principles for Vehicle Technologies and Services, that follow strict privacy standards for data collected from connected vehicles.[150] These include commitments to higher protections for PII, transparency, consumer choice, retention and de-identification. More generally, various industry and non-profit associations, including the Direct Marketing Association, the Digital Advertising Alliance, and the Better Business Bureau have developed a voluntary self-regulatory program for online advertising, including for mobile advertisements.[151] In the future, automotive industry associations, or their advertisers, could also develop their own industry codes of conduct for in-vehicle advertising (e.g., not advertising alcohol to drivers).

Second, the private sector has developed self-regulatory frameworks around cybersecurity and connected vehicles. In 2015, the Alliance of Automobile manufacturers and the Association of Global Automakers established an Information Sharing and Analysis Center (ISAC) for the industry to respond to cybersecurity threats.[152] The auto ISAC is introducing a series of best practices on various aspects of vehicle cybersecurity, including governance, risk management, threat detection, training, and collaboration with appropriate third parties. Since the auto ISAC was created, membership in the organization has expanded to heavy trucking manufacturers, vehicle suppliers, and commercial vehicle companies.[153] As of November 2017, the ISAC has only made best practices available to members, not the public.

Liability

Liability is also an important policy issue that affects the development and deployment of connected vehicles. Traditionally, car owners have been liable for losses arising from accidents caused by their vehicles (and are thus required to have third-party liability insurance), while manufacturers have been liable if a fault or defect in their product resulted in the accident. Many companies that offer connected vehicle services, including mobile network operators, computer hardware manufacturers, app developers, and automakers, all face legal claims that they are liable for accidents caused while using their products.[154] Because automakers are generally responsible for physical defects in their vehicles if they result in operational failures, this also holds true for errors in computer code. But as the amount of code that is running on vehicles grows, the defects in vehicles are more likely to be in software than in the physical components. These new demands will spread liability across dozens of entities, such as app developers, automakers, network operators, device suppliers, and others.

The changing state of liability for connected cars will affect how they are insured, especially as connected cars evolve into autonomous vehicles. For example, car owners may be liable for the actions of a vehicle they are not driving, and companies providing apps, such as navigation or diagnostics, may be responsible for incorrect information. Insurance may also change to cover new risks, such as the malicious interference of a connected vehicle or the breach of personal data connected with a vehicle. Moreover, federal, state, and local governments may also face liability for accidents caused by failures in V2X communications or failure to deploy these technologies on known dangerous roads.

Rules for insurance and liability are set by the states, with each state having its own insurance commission that sets its own regulations for the insurance industry. This system has created a complex patchwork of regulations, where insurers (and drivers) must abide by 50 different standards depending on the location of an incident. This is especially problematic for automotive insurance covering liability for injury and property damage. In addition, some state privacy laws can prevent the use of more complex insurance schemes that are based on more granular tracking of driver behavior by in-vehicle IT systems or on discounts for automated vehicle safety features (e.g., front-end collision avoidance). For example, California specifies three risk factors that insurance companies can use in their rating systems, generally limiting how insurers can incorporate usage-based insurance (UBI) features into underwriting and pricing.[155] Conversely, Illinois allows insurers to use any risk factors they want if they have full transparency.[156] In either case, if individual states continue to create their own rules, this patchwork may prevent the adoption of broader UBI systems or discounts for automated safety features. Many of the unresolved liability questions will be solved through state legislation, and different stakeholders will seek different outcomes.

After-Market Modifications and Copyright Issues

The United States has a long history of allowing independent repair shops and individual vehicle owners to make repairs, tinker, and modify their vehicles. In 1975, the Magnuson-

Moss Warranty Act banned manufacturers from voiding a vehicle's warranty or denying coverage under a warranty to vehicle owners for using a repair shop other than the dealer.[157] Similarly, the 1990 Clean Air Act that required on-board diagnostics (OBD) systems in cars also required automakers to provide independent repair shops the same information as franchised car dealers to access those devices.[158] However, OBD devices are no longer the only component of cars that gather data. Over the last few decades, car manufacturers and after-market parts makers have started embedding software linked to sensors in different aspects of a vehicle, from steering wheels to tires and more.

Because businesses license this software, some manufacturers have argued that vehicle owners should not access or tamper with the proprietary code of their vehicles.[159] These manufacturers base these claims on intellectual property provisions in the Digital Millennium Copyright Act. In part, companies have pushed policymakers, such as at the U.S. Copyright Office, for anti-tampering rules to limit their exposure to monetary damages from software that does not perform as expected. (Indeed, questions of liability become more complicated if third-party software is running on a vehicle or if owners can modify the software that is pre-installed on their vehicle.)[160]

While this approach would help reduce the chances of an accident caused by individuals or errant mechanics tampering with a vehicle, there are also several drawbacks. First, this approach limits how owners can change or modify their vehicles. Without these restrictions, owners may be able to load aftermarket software on their vehicles to improve performance or gain access to additional features, just as computer owners today can "overclock" their PCs or "root" or "jailbreak" their smartphones. Second, this approach limits how car manufacturers and device makers share vehicle diagnostics data that is not accessible through an OBD port (e.g., data from tire pressure monitoring systems or services like OnStar) with independent auto maintenance services or individuals who wish to self-repair. Therefore, restricting the after-market repairs market could lead to fewer choices and higher costs for consumers. Finally, completely restricting access to vehicle software can impair independent researchers' ability to test the vehicles' features. For example, in 2015, the Environmental Protection Agency discovered that Volkswagen had equipped 11 million diesel-powered vehicles with software capable of evading emissions testing, which some observers argued would have been more easily detected if not for DMCA protections that limited researchers from accessing the technological protection measures inside vehicles' software.[161]

Policymakers have tried to tackle this challenge and get the balance right in a few ways. In 2015, the U.S. Copyright Office issued a ruling that gives vehicle owners and researchers limited access to embedded systems, while preventing the owner from transferring this authority to third parties, such as independent repair shops.[162] Conversely, 12 states have passed "Right to Repair" legislation that requires manufacturers to share information necessary to repair vehicles.[163] To address these issues and avoid a patchwork of state regulations, automakers and manufacturers announced a nation-wide memorandum of understanding in 2014 to use a standard, non-proprietary interface for mechanics to access

a car's diagnostic data starting with model year 2018; and they have promised to sell repair tools and service information at a fair price.[164] Information that manufacturers believe to be a trade secret or proprietary is exempt from the agreement.

Data Standards and Interoperability

Connected vehicles collect and send a variety of different information to communicate and interact with other vehicles and their surrounding environment, reducing costs, improving safety and making vehicle operations more efficient. However, for these systems to work, connected vehicles must be able to share information with a range of different external systems, such as local authorities, automotive manufacturers, and app developers. This means that these data flows require interoperability and harmonization. Indeed, it will be impossible to enable V2X communications if smart infrastructure does not use the same protocols for communications.

Currently, efforts to create connected vehicle standards are primarily led by the private sector through independent standards-development organizations. For example, the bloTope project has set up two open-source standards for internet of things (IoT) devices, including connected vehicles: The Open Group O-DF and O-MI standards.[165] O-DF is a way of encoding and describing information in IoT devices, like HTML for the Internet. O-MI is a format for exchanging information between IoT devices, like HTTP for the Internet.

Spectrum

The successful deployment of connected vehicle systems will require access to bandwidth, regionally harmonized spectrum standards, and continued innovation in wireless technology. Spectrum is necessary for V2X communications. Several different technologies are jockeying for use in communications between vehicles. In the context of standards, the most talked about of these technologies are dedicated short range communications (DSRC) and cellular V2X (C-V2X) technology[166] Two federal agencies will have significant impact on spectrum decisions for connected vehicles: the Federal Communications Commission (FCC), and the National Highway Traffic Safety Administration (NHTSA).

First, the FCC manages spectrum in the United States, affecting at least three applications: V2X communications; vehicular radar technologies communications; and transmission of traffic data to vehicles. For V2X communications, the FCC allocated 75 MHz in the 5.9 GHz band for DSRC in 1999.[167] In addition, for vehicle RADAR technologies that companies use for collision-avoidance, the FCC adopted rules that use of the 76-77 GHz band in 1995, and recently expanded the vehicular RADAR band to 76 to 81 GHz.[168] Finally, the FCC allocated spectrum and created licensing frameworks for transmitting traffic data to in-vehicle navigation systems. There are two principle methods for in-vehicle navigation systems: over mobile networks (e.g., 3G or 4G wireless networks), and FM radio using the Traffic Message Channel (TMC).

Second, NHTSA has also proposed rulemakings around what types of technologies connected vehicles can use for V2X communications. In 2014, NHTSA released an

advanced notice and an accompanying research report, called the "Readiness Report," to access the readiness of applications of V2V communications.[169] In the report and a subsequent notice for proposed rulemaking in 2016, NHTSA proposed a mandate for all V2V communications to use DSRC to "standardize the content, initialization time and transmission characteristics of the basic safety message regardless of the V2V communication technology potentially used."[170] NHTSA accepted an initial round of public comments on the rule and indicated it would be finalized in 2019 and would begin to take effect in 2021.[171] However, recent reports indicate that this proposed rule may take longer to implement than originally anticipated.[172]

Infrastructure

Intelligent transportation systems (ITS) have traditionally referred to technologies that allow infrastructure elements within a nation's transportation system (e.g., roads, bridges, traffic lights, toll booths, message signs, etc.) to become intelligent by embedding them with sensors and empowering them to communicate with each other.[173] However, as more vehicles become interconnected and gain the ability to communicate with infrastructure, ITS will rely on V2X communications systems to vastly improve safety, operational performance, convenience, and environmental benefits of the transportation grid.[174] Indeed, the Department of Transportation's Connected Vehicle Research Program envisions the deployment of technologies that, if widely available in vehicles, highways, and in roadside intersection equipment, would enable the core elements of the transportation system to communicate.[175] However, governments face barriers in building next generation ITS, including funding and local barriers to deployment.

Policymakers often focus ITS investments on expensive roadside installations, rather than how to treat connected cars as the cornerstone of future ITS systems for roads and highways.

Relative to its potential, federal and state governments invest little on ITS. From 1992 to 2012, the U.S. Department of Transportation (DOT) allocated approximately $4.5 billion for ITS research and deployment.[176] During that same period, the DOT allocated more than $962 billion for roads and transit.[177] This indicates that only 0.47 percent of surface transportation funding goes to ITS, much of which is focused on road sensors rather than V2X communications. The federal government has since improved upon this funding. In 2015, the President signed the Fixing America's Surface Transportation Act (FAST Act) into law, which authorized somewhat increased funding levels for ITS.[178]

The federal government has approved some funding for communications infrastructure for V2X communications. In the United States, the objective of the U.S. Department of Transportation's Connected Vehicle Research Program (formerly called IntelliDriveSM) has been to deploy and enable a communications infrastructure that supports V2X communications for a variety of vehicle safety applications and transportation operations.[179] The U.S. Department of Transportation also allocated $42 million in 2015 for three large-scale pilots of V2X communications technologies in the state of Wyoming, New York City, and Tampa, Florida.[180] Furthermore, in August 2017 the U.S. Department of Transportation started allowing state and local governments to apply for grant funding for V2X communications infrastructures through the Infrastructure for Rebuilding America (INFRA) discretionary grant program.[181] INFRA, which was

established by the FAST Act, makes approximately $1.5 billion available for infrastructure projects.[182]

One component of smart infrastructure will be the deployment of ubiquitous next-generation networks. Wireless carriers are attempting to roll out small cells—antennas as small as a lunch box that can be placed on lampposts, traffic lights, or buildings—to improve wireless infrastructure. However, many local governments and municipalities have slowed this deployment through zoning and permitting barriers based on concerns over aesthetics, noise, and rights-of-way issues. To push back on these barriers, in 2017, the FCC announced a proposed rulemaking considering whether to pre-empt local governments from creating unnecessary or unreasonable regulatory barriers to wireless infrastructure deployment in public rights of way.[183] In addition, at least 20 states are considering legislation that would ease small-cell vendors' access to local infrastructure for small-cell deployment.[184] For their part, local governments and municipalities are pushing back on efforts to restrict their authority over zoning and permitting.[185]

POLICY PRINCIPLES FOR CONNECTED CARS

Absent proactive public policies, the full benefits of connected cars will not come to fruition, and the continued development and adoption of connected vehicles will slow. The following are eight principles that policymakers should follow to spur the deployment of connected vehicles and maximize their societal benefit.

Support V2X Infrastructure

Connected vehicles work best if they can connect to infrastructure. But why buy a connected vehicle if there is no infrastructure for it to talk to? It is time for the federal government, with the help of state and local governments, to dramatically accelerate the deployment of connected infrastructure by focusing its intelligent transportation system (ITS) strategy on V2X communications.

In the past, most ITS implementations have tried to work without a connected car at the center. For example, Japan launched its Vehicle Information and Communication System (VICS) nationwide in 2003, which relied upon an expensive array of road-side probes to generate real-time traffic information.[186] Similarly, the focus of many state ITS projects in the early 2000s was on roadside installations, such as sensors that collected real-time traffic and weather information, as well as measured weight.[187] These systems, which were created before the iPhone was released, were costly and quickly fell out of date.

Instead of focusing ITS investments on expensive roadside installations, policymakers should treat connected cars as the cornerstone of future ITS systems for roads and highways. In other words, "ITS 2.0" should primarily focus on V2X communications. Other countries have already changed their ITS implementation to focus on V2X communications. For example, when VICS proved to be outdated, Japan developed a V2V-based cooperative vehicle-highway system, called Smartway. This system evolved from concept development in 2004, to a limited pilot stage in 2007, to initial national deployment in 2010.[188] This proved to be an extremely fast development timeline.

Furthermore, federal and state agencies should adopt ITS 2.0 strategies in areas they influence. Each agency should develop a strategy for how it can help speed the transition to ITS 2.0 infrastructure. For example, besides testing pilot studies of V2X communications, the U.S. Department of Transportation should develop a comprehensive innovation strategy that articulates how it can promote the rapid deployment and adoption of proven V2X technologies. The Department of Transportation has already started these efforts by grant funding for V2X communications infrastructures through the Infrastructure for the Rebuilding America (INFRA) discretionary grant program.[189]

Beyond focusing on the connected vehicle, this strategy should include identifying innovative ways of using related technologies to drive high impact in larger intelligent transportation systems, such as emergency vehicle warning systems, VMT, adaptive traffic signal lights, and connected parking meters. The Department of Transportation should then co-fund with states and cities transformative pilot projects for these technologies, working in conjunction with automakers. For example, DOT should launch a smart-traffic-signal pilot program whereby every traffic light in a city would be able to communicate with a connected vehicle.

For connected car technologies not related to safety, regulators should adopt the principle of permissionless innovation, allowing companies and users to create new products without being subject to unnecessary regulations.

Promote National Cooperation and Interoperability for V2X Systems

V2X systems prove most effective when operated at scale—often at a national or international level—and must be adopted by the overall system and by individual users at the same time to be most successful.[190] For example, purchasing a cooperative connected vehicle system does a vehicle owner little good if it works in one state but does not work in other states that the driver frequents. These systems work most optimally when operated at scale. For example, it makes little sense for states to independently develop technical standards for vehicle miles traveled (VMT) usage-fee systems.[191] Effective VMT systems require an on-board unit, a back-end payment system, and a system to assign prices to road segments. If widely implemented, it would be inefficient and unnecessary to force auto manufacturers to make or install up to 50 different on-board devices to accommodate states' potentially differing implementations of a VMT system.

Instead, policymakers should promote coordination and interoperability—the ability of different IT systems to communicate, exchange data, and cooperatively use that data—between different state and local implementations of V2X technologies.[192] There are many steps that the federal government can take to ensure these technologies are interoperable and can function nationally, including by harmonizing standards, encouraging collaboration between governments, and developing industry certifications. The Department of Transportation, through its ITS strategic plan, is already creating a roadmap for international interoperability.[193] This strategy should include efforts to support collaboration between states and localities, such as by creating an organization that facilitates an inter-state dialogue on ITS technologies, including vehicle-miles traveled systems, to push state regulators to create interoperable systems that do not inhibit cross-border travel.[194] Similarly, the Department of Transportation should certify technologies and create buyers' guides for state and municipal governments to allow subnational

governments to make competitive choices in purchases of connected infrastructure technologies, while ensuring interoperability.

Incentivize Companies to Protect Consumers from Harm

In the United States, regulators such as the NHTSA, FTC, FCC and states closely scrutinize connected vehicle applications to protect consumers. This regulatory oversight ensures that companies focus adequately on safety, promotes fair competition, and upholds consumer protections. When it comes to mission-critical safety technologies, regulators should continue to scrutinize and regulate to prevent accidents and save lives. However, for connected car technologies that do not affect safety, regulators should adopt the principle of permissionless innovation, allowing companies and users to experiment and create new products without being subject to unnecessary regulations.[195] Companies creating apps for a connected car platform should not need to get permission from the government, just as web developers did not need to get permission to launch a website in 1999; nor did app developers need to get permission to create an app for the iPhone in 2009.

When regulatory action is necessary, to maximize its effectiveness and minimize any negative effects, any agency action should create a system of incentives that promotes desirable behavior and discourages undesirable behavior in a marketplace, doing so in a way that limits compliance costs. However, as the economy has become more innovation-based, some regulators have put considerably less focus on how regulatory agencies can both protect consumers and avoid undermining incentives for innovation. Regulators can also go too far and regulate against companies acting in good faith to bring innovations to market. This approach would limit innovation, especially in connected vehicle app makers, because if innovators fear they will be punished for every mistake, they will be much less assertive in trying to develop the next connected car app and will spend more time and effort on compliance, rather than innovation.

Regulators should also distinguish between a company's actions that intentionally violate regulations and cause harm to consumers and inadvertent mistakes that cause little to no harm, because blanket penalties and remedies regardless of circumstance will result in less innovation. Regulators should evaluate enforcement actions based on two dimensions: whether the company acted intentionally or negligently, and whether a company's action resulted in real consumer harm.[196] Regulators should then use a sliding scale to determine penalties, where unintentional, harmless actions receive no penalty, and intentional, harmful actions receive large penalties. As they evaluate enforcement actions, regulators should treat negligence as intentional. This strategy will not punish companies for innovating and will send clear signals to companies about what behavior is off-limits to better protect consumers.

Ensure Regulations Are Technology Neutral

Policymakers should adopt technology-neutral rules that neither favor nor disadvantage any connected-vehicle technology, to create a level playing field for innovation. For example, Internet privacy laws should not distinguish whether a user is accessing content from a

connected car or a smartphone. Regulators should treat similar products and services with similar rules. For example, navigation apps that collect geospatial data to route drivers to a destination are similar to parental control apps that use geospatial data to geofence a vehicle. Of course, as this report has detailed, not all connected vehicle applications or their associated concerns are the same. Where there are differences in technologies, and where rules are appropriate, policymakers should establish rules that recognize the risks distinct to (or irrelevant to) connected vehicle applications.

Rely on Transparent Industry-Led Standards for Data Protection

The growing availability of vehicle data has allowed companies to create the connected vehicle applications discussed in this report and will continue to enable applications that we cannot imagine today. However, unnecessarily restricting how companies collect or use vehicle data could limit this innovation. Policymakers should focus on voluntary self-regulatory principles for the auto industry to protect the cybersecurity and privacy of vehicle owners. Self-regulation is a vital part of the digital economy, allowing a host of diverse industries to govern industry practices on a range of issues.[197] Businesses use self-regulation to decrease risks to consumers, increase public trust, and combat negative public perceptions. Where standard regulations may be rigid, self-regulation benefits the economy by creating a more flexible regulatory environment than is typically found with government regulation. Industry experts review current activities, identify best practices, and develop these into industry guidelines. These processes can also avoid conflicts of interest, jurisdictional conflicts, and legal limitations.[198] Ideally self-regulation should include all stakeholders, produce clear and transparent rules, and be overseen by an independent organization to assess its effectiveness.

If not unnecessarily restricted, the availability and use of vehicle data will enable continued innovation in connected vehicle applications.

Of course, self-regulatory efforts are not without government oversight. Through its "unfair or deceptive acts" enforcement, the Federal Trade Commission (FTC) can bring enforcement actions against any entity that has not kept its promises to consumers in a stated company privacy or cybersecurity policy. These enforcement actions can result in a consent decree, whereby the company faces penalties for future misconduct. During the span of a consent decree—which can last up to 20 years—the company can be subject to an audit by the FTC and violations can result in steep fines. While this type of enforcement is imperfect and can be a backdoor to de-facto regulations, it allows for regulators to police voluntary self-regulatory principles.[199] As previously discussed, automakers released voluntary privacy principles in 2014.[200] Policymakers should look to these flexible, voluntary principles and avoid imposing one-size-fits-all rules on all businesses and individuals involved in connected vehicles. Doing so can help prevent harmful limits on useful data collection, and allow automakers to stay ahead of threats and adjust privacy controls to respect individual choice.[201]

Beyond best practices and self-regulatory principles, policymakers should ensure automakers, aftermarket parts manufactures, app developers, and other third parties are transparent in their cybersecurity practices for connected vehicles. Consumers already enjoy this level of transparency for vehicle safety. When consumers purchase vehicles, tires, or

even car seats, they can review safety ratings to inform their choices. For example, NHTSA's 5 Star Safety Ratings test the safety performance of individual vehicles across several crash metrics.[202] However, no similar rating system, or the information to support such ratings, exists to help consumers understand the cybersecurity practices of automakers. This absence of transparency in cybersecurity policies has created the type of information asymmetry that leads to inefficient markets. As a result, consumers (or tech-savvy reporters or consumer advocacy groups) cannot easily differentiate between secure and insecure products. Policymakers should require automakers to publish their cybersecurity practices in the same way they publish privacy policies. By creating transparent policies for cybersecurity, policymakers can allow companies the freedom to manage risks while ensuring accountability and oversight. For example, NHTSA could create testing mechanisms around the cybersecurity claims of automakers, and the FTC can bring enforcement actions against companies that break their promises.

Restrict Scope Creep for Regulators Overseeing Connected Vehicle Privacy

In recent years, regulators that were not traditionally tasked with protecting privacy have expanded their scope due to the increased digitization of goods. NHTSA, for example, which has traditionally focused on protecting the safety of vehicles, has proposed several rules in recent years regarding consumer privacy related to its rulemakings. Policymakers should ensure that NHTSA, and the Department of Transportation as a whole, do not continue to expand their authority over consumer privacy.[203] Instead, this oversight should come from existing regulators, such as the FTC, which already has purview over consumer privacy issues.

While adding new privacy regulators can seem like a noteworthy goal, it often results in unintended consequences. NHTSA's intent is likely to demonstrate that it is aware that consumer data is a necessary ingredient in the development, testing, and improvement of connected vehicles. However, developing independent recommendations for data privacy creates redundant and potentially conflicting regulatory barriers that automakers and other businesses that offer services to connected vehicles must overcome, and does little to protect consumers. Indeed, as the Government Accountability Office (GAO) has noted, NHTSA lacks a clearly-defined role as it relates to privacy issues.[204] Without a defined role, NHTSA's privacy efforts could lead to consumer and business confusion. For example, consumer data transmitted through a connected car application should not have different levels of privacy protection than the same information transmitted through a smart phone or smart home device. Otherwise, consumers, app developers and other businesses would find it difficult to make sense of unnecessary differences.

Allow Vehicle Owners to Access and Use Their Own Data

Connected vehicles generate a variety of data, such as geolocation information, diagnostic reports, purchasing records, browsing histories, and entertainment preferences. This data will be most beneficial if car owners have access to it directly and can authorize third parties to access it on their behalf to enable innovative services, such as UBI insurance. Policymakers should encourage automakers to share vehicle data via application

programming interfaces (API)—software functions that allow developers to access data stored in computer systems in a pre-specified, machine-readable format. Ideally, the auto industry will standardize both the data generated by vehicles as well as the APIs to make it easier for developers to access and use this information in third-party applications and services.

Permit After-Market Modifications and Repairs While Protecting Copyright Holders' Rights

Just as the Magnuson-Moss Warranty Act of 1975 ensured vehicle owners can physically modify their vehicles without voiding warranties, so to should policymakers ensure this principle extends to the digital era. Policymakers should focus on striking the right balance between protecting vehicle software copyright holders' rights and allowing car owners and third-party providers the ability to examine the software in their vehicles to diagnose and repair problems or lawfully modify their vehicles. As policymakers evaluate these issues they should consider policies that both protect automakers' interests and allow vehicle owners to make lawful modifications to their vehicles.

First, policymakers should enable competition in the independent repairs market by ensuring automakers provide information and repair software to all third parties in the same manner. Automakers should not be allowed to discriminate between independent repair shops and franchised car dealers in the information they provide to help mechanics fix their products. Similarly, an automaker that licenses a tool designed to fix a software problem in its vehicles should make this available on similar terms to all third parties. This does not mean automakers should be required to reveal proprietary information, but rather that they treat all third parties fairly in how they license copyrighted information.

Second, policymakers should allow vehicle owners (or authorized users) to legally modify their vehicles, including by adding or modifying software. This includes adding third-party programming or custom software or devices to a vehicle. Of course, this does not mean automakers should be held liable when vehicle owners change software in a way that causes injury, just as modifying a vehicle's brakes in an unsafe way should not make the automaker liable or overclocking a computer chip does not make the chip maker responsible if the computer overheats. Moreover, vehicle owners or trusted third parties should not modify vehicle software in a way that circumvents built-in copyright protections, such as by bypassing digital-rights-management access controls. For example, vehicle owners should not be legally allowed use this ability to modify their vehicles to copy proprietary software from the car, nor should they download or illegally stream copyrighted content from their vehicles (e.g., satellite radio). Indeed, most vehicles will have built-in functions that a vehicle manufacturer may want to lock-down for safety reasons or because they are proprietary. In these circumstances, policymakers should ensure manufacturers are transparent about what software is protected.

Furthermore, policymakers should ensure that consumers' ability to modify their vehicles does not circumvent software-based business models. Some manufacturers use protected

code in a vehicle to offer a range of products to their customers. For example, Tesla sells its Model S with an electronically limited battery capacity of 60 kWh, offering drivers the option to upgrade this capacity to 75 kWh for a fee.[205] With this option, drivers can choose to save money at the cost of the vehicle's range, or can choose to unlock their cars' battery capacities later. This form of differential pricing helps automakers better align prices with what customers are willing to pay while keeping prices competitive to retain the business of price-sensitive customers.[206] Innovative business models that operate based on in-car software can lead to market expansion and better customer engagement, and policymaker should ensure they remain viable.

CONCLUSION

While fully automated cars are still a prospect of the future, connected vehicles are here today. The connected vehicle applications discussed in this report are just the start. As companies continue to experiment and these technologies scale, consumers will enjoy a wide array of products and services that we cannot imagine today. These innovations will improve safety, security, mobility, and convenience for consumers. But absent proactive public policies, progress will be slower and more limited than it need be.

ENDNOTES

1. Hans Greimel, "Toyota Unveils 'Smartphone on Wheels' Concept Car for Tokyo Show," *Autoweek*, November 27, 2011, http://www.autoweek.com/article/20111128/TOKYO/111129928, (accessed January 1, 2018).
2. Henry Bzeih, Greg Ross, Nicolas Nollet, "Connected Car Industry Report," (Telefónica, 2014), https://iot.telefonica.com/multimedia-resources/connected-car-industry-report-2014-english, (accessed January 1, 2018).
3. Gartner, "Gartner Says Connected Car Production to Grow Rapidly Over Next Five Years," news release, September 16, 2016, http://www.gartner.com/newsroom/id/3460018, (accessed January 1, 2018).
4. "Hit the Road with Android Auto," *Android Auto*, https://www.android.com/auto/, (accessed January 1, 2018). For example, 61 automobile brands enable Android Auto in at least one of their models.
5. Jacob Kastrenakes, "Why Carmakers Want to Keep Apple and Google at Arm's Length," *The Verge,* January 13, 2017, https://www.theverge.com/2017/1/13/14268252/apple-carplay-google-android-auto-vs-carmakers, (accessed January 1, 2018).
6. See, "About SDL," SmartDeviceLink Consortium, https://smartdevicelink.com/about/, (accessed January 6, 2018); "Connected Driving, Evolved," *Uconnect*, https://www.driveuconnect.com/, (accessed January 6, 2018); "My BMW ConnectedDrive," *BMW*, https://connecteddrive.bmwusa.com/cdp/release/internet/servlet/login?locale=en_US, (accessed January 6, 2018).
7. Josh Archer, "5 iPhone Apps that Use the Gyro/Accelerometer in an Interesting Way," *Medium*, November 27, 2015, https://medium.com/make-school/5-iphone-apps-that-use-the-gyro-accelerometer-in-an-interesting-way-33f5814ac84c, (accessed January 1, 2018).
8. Daniel Castro, "The Road Ahead: The Emerging Policy Debates for IT in Vehicles," (The Information Technology and Innovation Foundation, April 2013), http://www2.itif.org/2013-road-ahead.pdf, (accessed January 8, 2018).
9. Daniel Castro and Jordan Misra, "The Internet of Things," (The Center for Data Innovation, November 2013), http://www2.datainnovation.org/2013-internet-of-things.pdf, (accessed January 8, 2018).
10. Ibid.
11. "OnBoard Diagnostic II (OBD II) Help," *AA1Car.com*, http://www.aa1car.com/obd2help/, (accessed January 1, 2018).
12. Jeremy Laukkonen, "Monitoring Your Tire Pressure," *Lifewire,* October 19, 2016, https://www.lifewire.com/monitoring-tire-pressure-534815, (accessed January 1, 2018).
13. Jean-Pierre Hubaux, Srdjan Capkun and Jun Luo, "The Security and Privacy of Smart Vehicles," (IEEE Security & Privacy, May-June 2004), 49 – 55.
14. "Cisco Jasper Control Center for Connected Cars," *Cisco*, https://www.jasper.com/control-center-for-connected-cars, (accessed January 1, 2018).
15. Kirsten Korosec, "Why GM is Slashing the Price of its In-Car Wireless Data Plans," *Fortune*, June 30, 2016, http://fortune.com/2016/06/29/gm-cut-4g-price/, (accessed January 1, 2018).
16. "Connected Car News," *AT&T*, http://about.att.com/sites/internet-of-things/connected_car, (accessed January 1, 2018).
17. "Connected Car Wi-Fi FAQs," *Verizon Wireless*, https://www.verizonwireless.com/support/connected-car-faqs/, (accessed January 1, 2018).
18. "DSRC: The Future of Safer Driving," *U.S. Department of Transportation*, https://www.its.dot.gov/factsheets/dsrc_factsheet.htm, (accessed January 1, 2018). DSRC is a standard developed by the Federal Communications Commission and the International Standards Organization.

19. Qualcomm, "10 Facts You Need to Know About Cellular-V2X," *Light Reading*, December 7, 2017, http://www.lightreading.com/webinar.asp?webinar_id=1089, (accessed January 1, 2018).
20. Dino Flore, "Initial Cellular V2X standard completed," *3GPP*, September 26, 2016, http://www.3gpp.org/news-events/3gpp-news/1798-v2x_r14, (accessed January 5, 2018); Qualcomm, "Qualcomm Announces Groundbreaking Cellular-V2X Solution to Support Automotive Road Safety, Helping to Pave a Path for the Future of Autonomous Driving," news release, September 1, 2017, https://www.qualcomm.com/news/releases/2017/09/01/qualcomm-announces-groundbreaking-cellular-v2x-solution-support-automotive, (accessed January 5, 2018).
21. "Split Charging & Revenue Management Capabilities for Connected Car Services," *GSMA*, February 2013, https://www.gsma.com/iot/wp-content/uploads/2013/02/cl_ma_ChargingRevenue_02_13.pdf, (accessed January 5, 2018).
22. Patrick Nelson, "Vehicles to Make up 98% of M2M Traffic by 2021," *NetworkWorld*, August 8, 0216, https://www.networkworld.com/article/3105021/mobile-wireless/vehicles-to-make-up-98-of-m2m-traffic-by-2021.html, (accessed January 5, 2018).
23. "What is HomeLink," *HomeLink*, http://www.homelink.com/home/welcome, (accessed January 5, 2018).
24. "Vehicle-to-X (V2X) communication technology," *Siemens*, 2015, https://www.mobility.siemens.com/mobility/global/SiteCollectionDocuments/en/road-solutions/urban/trends/siemens-vehicle-to-x-communication-technology-infographic.pdf, (accessed January 5, 2018).
25. Seunghyuk Choi, Florian Thalmayr, Dominik Wee, and Florian Weig, "Advanced driver-assistance systems: Challenges and opportunities ahead," (McKinsey & Company, February 2016), http://www.mckinsey.com/industries/semiconductors/our-insights/advanced-driver-assistance-systems-challenges-and-opportunities-ahead, (accessed January 5, 2018).
26. "What is OBD-II," *OBDII Homepage*, http://www.obdii.com/background.html, (accessed January 5, 2018).
27. Phil Berg, "10 Diagnostic Apps and Devices to Make You a Better Driver," *Popular Mechanics,* February 21, 2012, http://www.popularmechanics.com/cars/how-to/g767/10-diagnostic-apps-and-devices-to-make-you-a-better-driver/, (accessed January 5, 2018).
28. Ibid.
29. "Dash," *Dash*, https://dash.by, (accessed January 5, 2018).
30. Dmytro Ternovyi, "5 Ways predictive Analytics is Shaping the Connected Car Industry," *Ignite,* https://igniteoutsourcing.com/publications/predictive-analytics-in-connected-car-industry, (accessed January 5, 2018).
31. "Zubie introduces new preventive vehicle maintenance app tools for small business fleets," *Zubie*, February 4, 2016, http://zubie.com/2016/02/04/zubie-introduces-new-preventive-vehicle-maintenance-app-tools-for-small-business-fleets/, (accessed January 5, 2018).
32. Jeremy Laukkonen, "Decoding Blind Spot Detection and Warning Systems," *Lifewire,* March 10, 2017, https://www.lifewire.com/decoding-blind-spot-detection-534803, (accessed January 5, 2018).
33. Ibid.
34. Jeremy Laukkonen, "Back Up Sensors and Rear View Cameras," *Lifewire, October 19*, 2016, https://www.lifewire.com/back-up-sensors-rear-view-camera-534802, (accessed January 5, 2018).
35. Nick Lavars, "Nest adds integration with Automatic connected car adapter," *New Atlas*, January 13, 2015, https://newatlas.com/nest-integration-automatic-connected-car-adapter/35596/, (accessed January 5, 2018).

36. "Super-Precise GPS Could Mean Advances for Self-Driving Cars, Wearable Tech," *GovTech*, February 17, 2016, http://www.govtech.com/fs/Super-Precise-GPS-Could-Mean-Advances-for-Self-Driving-Cars-Wearable-Tech.html, (accessed January 5, 2018).

37. Ibid; Sarah Nightingale, "Next-generation navigation system uses existing cellular signals, not GPS, will support autonomous vehicle development," *PHYS ORG*, October 13, 2016, https://phys.org/news/2016-10-next-generation-cellular-gps-autonomous-vehicle.html, (accessed January 5, 2018).

38. For example, see "MVI: Mobile Voice Integration," *General Motors*, https://www.gm-navigation.com/, (accessed January 7, 2018).

39. "Honda Navigation Updates," *Garmin*, https://honda.garmin.com/honda/, (accessed January 7, 2018).

40. Fred Lambert, "Tesla is updating its maps and navigation with open source mapping platforms," *Electrek*, July 3, 2017, https://electrek.co/2017/07/03/tesla-map-navigation-open-source-platforms/, (accessed January 7, 2018); Kevin Fitchard, "Google Maps Navigates its Way into Kia, Hyundai Connected Cars," *Gigaom*, January 2, 2013, https://gigaom.com/2013/01/02/google-maps-navigates-its-way-into-kia-hyundai-connected-cars/, (accessed January 7, 2018).

41. "Android Implementation," *SmartDeviceLink*, https://smartdevicelink.com/en/docs/android/master/, (accessed January 7, 2018).

42. "Navigation," *Garmin*, https://www.tomtom.com/en_us/, (accessed January 7, 2018).

43. See, *Google Maps*, https://www.google.com/maps;, (accessed January 7, 2018); "Update your navigation system map," *HERE Maps*, http://mapupdate.navigation.com/, (accessed January 7, 2018); "Get the best route, every day, with real–time help from other drivers," *Waze*, https://www.waze.com/, (accessed January 7, 2018).

44. *BestParking.com*, http://www.bestparking.com/, (accessed January 7, 2018).

45. "Parker," *Streetline*, https://www.streetline.com/our-solutions/, (accessed January 7, 2018).

46. "How It Works," *Automatic*, https://www.automatic.com/, (accessed January 7, 2018).

47. David Goldman, "5 Best Apps for Cheap Gas," *CNN*, December 29, 2014, http://money.cnn.com/2014/12/29/technology/mobile/gas-price-apps/index.html, (accessed January 7, 2018). GasBuddy incentivizes its users to post this information by offering a weekly drawing for a $100 gas card.

48. "Gas Guru: Cheap Gas Prices," *GooglePlay*, https://play.google.com/store/apps/details?id=com.yellowpages.android.gas, (accessed January 7, 2018).

49. "Car Poised to be CE's 'Fifth Screen'," *Future Source Consulting*, February 6, 2017, https://www.futuresource-consulting.com/Press-Connected-Car-in-Automotive-Market-0217.html, (accessed January 7, 2018).

50. "Distracted Driving," *U.S. National Highway Traffic Safety Administration*, https://www.nhtsa.gov/risky-driving/distracted-driving, (accessed January 7, 2018).

51. "Talk to Me: The Present & Future of In-Car Speech Recognition," *GlobalMe*, July 26, 2017, https://www.globalme.net/blog/the-present-and-future-of-in-car-speech-recognition, (accessed January 7, 2018).

52. Dan Seifert, "Android Auto review," *The Verge*, May 26, 2015, https://www.theverge.com/2015/5/26/8659671/android-auto-in-car-system-review-smartphone-hyundai-sonata, (accessed January 7, 2018).

53. "What is HomeLink," *HomeLink*.

54. "Helping Automakers Drive Innovation Through Connected Cars," *Microsoft*, January 4, 2017, https://blogs.microsoft.com/iot/2017/01/05/helping-automakers-drive-innovation-through-connected-cars, (accessed January 7, 2018).

55. Jeremy Laukkonen, "How Remote Car Starters Work," *Lifewire*, December 17, 2017, https://www.lifewire.com/car-tech-key-concepts-534877, (accessed January 7, 2018).
56. Nico DeMattia, "BMW Connected+ to Change the Way You Connect With Your Car," *MBWBlog*, July 28, 2017, http://www.bmwblog.com/2017/07/28/bmw-connected-change-way-connect-car/, (accessed January 7, 2018).
57. "Toyota Entune Parental Controls," *Toyota Entune*, October 11, 2017, http://toyota-entune.com/toyota-entune-parental-controls/, (accessed January 7, 2018).
58. Mojio, "Mojio Launches New Mechanic and Car Alarm Connected Car Apps for Android," press release, June 2, 2015, https://www.moj.io/new-connected-car-apps-for-android/, (accessed January 7, 2018).
59. "Usage-based Insurance and Telematics," *National Association of Insurance Commissioners*, November 14, 2017, http://www.naic.org/cipr_topics/topic_usage_based_insurance.htm, (accessed January 7, 2018).
60. Susan Ladika, "Gas Pump and ATM Skimmers: How to Spot Them," *CreditCard.com*, December 22, 2017, https://www.creditcards.com/credit-card-news/gas-station-skimmer-fraud.php, (accessed January 7, 2018).
61. C.C. Weiss, "No More Quarters or Tickets: Audi Tests Wireless Parking Payments," *New Atlas*, June 11, 2013, https://newatlas.com/audi-wireless-parking-payments/27864/, (accessed January 7, 2018).
62. Andrew Krok, "GM Marketplace lets your car buy donuts and coffee," *Road Show*, December 5, 2017, https://www.cnet.com/roadshow/news/gm-marketplace-lets-your-car-buy-donuts-and-coffee/, (accessed January 7, 2018).
63. "Let Your Car Pick Up the Tab," *VISA*, https://usa.visa.com/visa-everywhere/innovation/let-your-car-pick-up-the-tab.html, (accessed January 7, 2018).
64. VISA, "The Connected Car Is Here," *YouTube*, video, March 4, 2015, https://www.youtube.com/watch?v=8HDy1ZIGg78, (accessed January 7, 2018).
65. "Service You Can Count On," *Urgent.ly*, https://www.geturgently.com/urgently-roadside-assistance-services, (accessed January 7, 2018).
66. Urgent.ly, "AT&T's Drive Connected Car Platform Adds Ugent.ly," news release, February 24, 2016, https://www.geturgently.com/blog/att-drive-connected-car-platform-adds-urgently, (accessed January 7, 2018).
67. "Roadside Assistance, Simplified," *Honk*, https://www.honkforhelp.com/, (accessed January 7, 2018).
68. "2016 Crime in the United States: Motor Theft," (Federal Bureau of Investigations, 2016), https://ucr.fbi.gov/crime-in-the-u.s/2016/crime-in-the-u.s.-2016/topic-pages/motor-vehicle-theft, (accessed January 7, 2018).
69. Jeremy Laukkonen, "What is Vehicle Tracking?" *Lifewire*, July 27, 2017, https://www.lifewire.com/what-is-vehicle-tracking-534827, (accessed January 7, 2018).
70. Ibid.
71. Jeremy Laukkonen, "What is LoJack, and How Does It Work?" *Lifewire*, July 19, 2017, https://www.lifewire.com/what-is-lojack-534878, (accessed January 7, 2018).
72. Hudson Hongo, "BMW Remotely Locks Stolen Car with Alleged Thief Still Inside," *Gizmodo*, December 05, 2016, https://gizmodo.com/bmw-remotely-locks-stolen-car-with-alleged-thief-still-1789674614, (accessed January 4, 2018).
73. "Usage-based Insurance and Telematics," *National Association of Insurance Commissioners*.
74. "The New Auto Insurance Ecosystem: Telematics, Mobility and the Connected Car," (Cognizant: August 2012), https://www.cognizant.com/InsightsWhitepapers/The-New-Auto-Insurance-Ecosystem-Telematics-Mobility-and-the-Connected-Car.pdf, (accessed January 7, 2018).
75. "About Octo," *Octo,* https://www.octotelematics.com/, (accessed January 7, 2018).

76. "What is a Starter Interrupt Device?" *Deal Pack Blog,* June 27, 2012, http://www.dealpack.com/what-is-a-starter-interrupt-device, (accessed January 7, 2018).

77. Ibid.

78. "The Economic Benefits of Vehicle Miles Traveled (VMT)-Reducing Placemaking: Synthesizing a New View," (National Center for Sustainable Transportation, November 2017), https://ncst.ucdavis.edu/wp-content/uploads/2016/10/NCST-TO-030-Boarnet-Economic-Benefits-of-Placemaking_FINAL-WP_Nov-2017.pdf, (accessed January 7, 2018).

79. Robert Atkinson, "A New Way to Pay for State Highways," *St. Louis Post-Dispatch,* December 7, 2017, http://www.stltoday.com/opinion/columnists/a-new-way-to-pay-for-state-highways/article_7071aaf0-5795-53d1-8df5-fd855fbf7fa0.html, (accessed January 7, 2018).

80. "Alternative Approaches to Funding Highways," *Congressional Budget Office,* March 2011, http://www.cbo.gov/publication/22059, (accessed January 7, 2018).

81. "The Pothole Facts," *Pothole.Info,* 2018, https://www.pothole.info/the-facts/, (accessed January 7, 2018); "Fact Sheet: Pothole Damage," *AAA*, 2016, http://publicaffairsresources.aaa.biz/wp-content/uploads/2016/02/Pothole-Fact-Sheet.pdf ,(accessed January 7, 2018). Of approximately 33,000 traffic fatalities each year, one-third involve poor road conditions.

82. "Street Bump," *City of Boston*, March 21, 2017, https://www.boston.gov/departments/new-urban-mechanics/street-bump, (accessed January 7, 2018).

83. Theodora Brisimi et al., "Sensing and Classifying Roadway Obstacles in Smart Cities: The Street Bump System," (IEEE, December 6, 2015), http://sites.bu.edu/paschalidis/files/2016/07/Streetbump-author-submitted-final.pdf, (accessed January 7, 2018).

84. John Sutter, "Street Bump app detects potholes, tells city officials," *CNN,* February 16, 2012, http://www.cnn.com/2012/02/16/tech/street-bump-app-detects-potholes-tells-city-officials/index.html, (accessed January 7, 2018).

85. Andrew Liszewski, "Google Wants To Use Your Car's GPS To Track Potholes," *Gizmodo,* October 15, 2015, https://gizmodo.com/google-wants-to-use-your-cars-gps-to-track-potholes-1726369626?utm_campaign=socialflow_gizmodo_twitter&utm_source=gizmodo_twitter&utm_medium=socialflow, (accessed January 7, 2018).

86. "Pilot Evaluation," *SF Park*, http://sfpark.org/about-the-project/pilot-evaluation/, (accessed January 7, 2018).

87. Cadillac, "V2V Safety Technology Now Standard on Cadillac CTS Sedans," press release, March 9, 2017, http://media.cadillac.com/media/us/en/cadillac/news.detail.html/content/Pages/news/us/en/2017/mar/0309-v2v.html, (accessed January 7, 2018).

88. U.S. Department of Transportation, "U.S. Department of Transportation Announces up to $42 Million in Next Generation Connected Vehicle Technologies," press release, September 14, 2015, https://www.its.dot.gov/press/2015/ngv_tech_announcement.htm, (accessed January 7, 2018).

89. "NSC Motor Vehicle Fatality Estimates," (National Safety Council, December 2016), http://www.nsc.org/NewsDocuments/2017/12-month-estimates.pdf, (accessed January 7, 2018).

90. "Technology That Can Send the Right Help," *OnStar*, https://www.experienceonstar.com/view/innovation-automatic-crash-response, (accessed January 7, 2018).

91. "Crash Detection App," *SOS Smart,* http://www.sosmartapp.com/, (accessed January 7, 2018); "Car Video Recorder and GPS Navigator in the Same Application," *CamOnRoad*, https://camonroad.com/, (accessed January 7, 2018).

92. Tara Baukus Mello, "Event Data Recorders: Coming to Your Car?" *Bankrate.com*, January 11, 2013, http://www.bankrate.com/finance/auto/event-data-recorders-coming-to-your-car.aspx, (accessed January 5, 2018).

93. U.S. Department of Transportation, "U.S. Department of Transportation Announces up to $42 Million in Next Generation Connected Vehicle Technologies," news release, September 14, 2015, https://www.transportation.gov/briefing-room/us-department-transportation-announces-42-million-next-generation-connected-vehicle; https://wydotcvp.wyoroad.info/, (accessed January 8, 2018).

94. European Commission, "eCall: automated emergency call for road accidents mandatory in cars from 2015," news release, June 13, 2013, http://europa.eu/rapid/press-release_IP-13-534_en.htm, (accessed January 8, 2018).

95. "eCall in all new cars from April 2018," *European Commission*, April 28, 2015, https://ec.europa.eu/digital-single-market/en/news/ecall-all-new-cars-april-2018, (accessed January 8, 2018).

96. "The eCall Program: Overview and Design Considerations," (Sierra Wireless, 2014), available on Scribd, https://www.scribd.com/document/101015129/The-eCall-Program-Overview-and-Design-Considerations, (accessed January 8, 2018).

97. "eCall in all new cars from April 2018," *European Commission.*

98. Eddie Curtis, "Adaptive Signal Control Technology," *U.S. Federal Highway Administration,* U.S. Department of Transportation, September 8, 2017, https://www.fhwa.dot.gov/innovation/everydaycounts/edc-1/asct.cfm, (accessed January 8, 2018).

99. Peng Jing, Hai Huang, and Long Chen, "An Adaptive Traffic Signal Control in a Connected Vehicle Environment: A Systematic Review," (Information, 2017) 8(3), 101, August 22, 2017, http://www.mdpi.com/2078-2489/8/3/101, (accessed January 8, 2018).

100. Ibid.

101. Sarah Perez, "Tampa Offers First Demo of its Connected Vehicle Technology Project, Launching with 1,600 Cars in 2018," *TechCrunch*, November 13, 2017, https://techcrunch.com/2017/11/13/tampa-offers-first-demo-of-its-connected-vehicle-technology-project-launching-with-1600-cars-in-2018/, (accessed January 7, 2018).

102. Audi, "Audi Launches First Vehicle-to-Infrastructure (V2I) Technology in the U.S. Starting in Las Vegas," press release, December 6, 2016, https://www.audiusa.com/newsroom/news/press-releases/2016/12/audi-launches-vehicle-to-infrastructure-tech-in-vegas, (accessed January 7, 2018).

103. Ryan McCauley, "Connected Vehicle Tech Could Ease Routes for First Responders," *GovTech,* November 23, 2016, http://www.govtech.com/fs/Connected-Vehicle-Tech-Could-Ease-Routes-for-First-Responders.html, (accessed January 7, 2018).

104. Aarian Marshall, "Congress Finally Gets Serious About Regulating Self-Driving Cars," *Wired*, July 19, 2017, https://www.wired.com/story/congress-autonomous-self-driving-car-regulations/, (accessed January 7, 2018).

105. SELF DRIVE Act, H.R.3388 (2017), 115th Cong. (2017).

106. Jerry L. Mashaw, "Regulation and Legal Culture: The Case of Motor Vehicle Safety," *Faculty Scholarship Series*, Paper 1147, 1987, http://digitalcommons.law.yale.edu/fss_papers/1147, (accessed January 7, 2018).

107. *U.S. National Highway Traffic Safety Administration,* "U.S. DOT advances deployment of Connected Vehicle Technology to prevent hundreds of thousands of crashes," *press release*, December 13, 2016, https://www.nhtsa.gov/press-releases/us-dot-advances-deployment-connected-vehicle-technology-prevent-hundreds-thousands, (accessed January 7, 2018); "Cybersecurity Practices for Modern Vehicles," *U.S. National Highway Traffic Safety Administration*, (Report No. DOT HS 812 333), October 2016, https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/documents/812333_cybersecurityformodernvehicles.pdf,

(accessed January 7, 2018); "Automated Driving Systems: A Vision For Safety," *U.S. National Highway Traffic Safety Administration,* (Report No. DOT HS 812 – 442), September 2016, https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/documents/13069a-ads2.0_090617_v9a_tag.pdf, (accessed January 7, 2018).

108. "Understanding the distracted brain," *National Safety Council*, March 2012, http://distracteddriving.nsc.org, (accessed August 8, 2018).

109 "Highway Accident Report: Multivehicle Collision Interstate 44 Eastbound Gray Summit, Missouri," *National Transportation Safety Board*, August 5, 2010, http://www.ntsb.gov/doclib/reports/2011/HAR1103.pdf, (accessed January 7, 2018). The NTSB issued these recommendations in response to finding a pattern of serious vehicle accidents resulting from the use of portable electronic devices in its crash investigations.

110. "Distracted Drivers," *Governors Highway Safety Association*, http://www.ghsa.org/state-laws/issues/Distracted-Driving, (accessed January 7, 2018).

111. Ibid.

112. U.S. National Highway Traffic Safety Administration, "U.S. DOT Proposes Guidelines to Address Driver Distraction Caused by Mobile Devices in Vehicles," press release, November 23, 2016, https://www.nhtsa.gov/press-releases/us-dot-proposes-guidelines-address-driver-distraction-caused-mobile-devices-vehicles, (accessed January 7, 2018).

113. "Visual-Manual NHTSA Driver Distraction Guidelines for In-Vehicle Electronic Devices," *U.S. National Highway Traffic Safety Administration*, (Docket No. NHTSA-2010-0053), February 15, 2012. These guidelines include reducing the complexity and length of time required to complete tasks, limiting operations to those that can be performed with one hand, reducing the need to look away from the road, reducing unnecessary visual information, and limiting the amount of manual input required.

114. "Distracted Driving Information Clearinghouse," *U.S. Federal Communications Commission,* December 7, 2015, https://www.fcc.gov/general/distracted-driving-information-clearinghouse, (accessed January 7, 2018).

115. Ibid.

116. David Silverberg, "Next-Gen 911: First Responders Gear Up for a Whole New Wave of Technology," *GovTech Works*, September 16, 2015, https://www.govtechworks.com/next-gen-911-first-responders-gear-up-for-a-whole-new-wave-of-technology/#gs.RcnUI10, (accessed January 7, 2018).

117. "Connected Vehicle Safety Pilot Program," *Intelligent Transportation Systems Joint Program Office*, November 15, 2012, http://www.its.dot.gov/factsheets/safety_pilot_factsheet.htm, (accessed January 7, 2018).

118. "Automated Driving: Legislative and Regulatory Action," *The Center for Internet and Society,* April 27, 2017, http://cyberlaw.stanford.edu/wiki/index.php/Automated_Driving:_Legislative_and_Regulatory_Action, (accessed January 7, 2018).

119. "Self-driving Vehicles Enacted Legislation," *National Conference of State Legislatures*, January 2, 2018, http://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx, (accessed January 7, 2018).

120. Andy Greenberg, "Hackers Remotely Kill a Jeep On the Highway – With Me In It," *Wired*, July 21, 2015, https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/, (accessed January 7, 2018); Kim Zetter, "Researchers Hacked A Model S, But Tesla's Already Released a Patch," *Wired*, August 6, 2015, https://www.wired.com/2015/08/researchers-hacked-model-s-teslas-already/, (accessed January 7, 2018).

121. "Fiat Chrysler Recalls 1.4 Million Cars After Jeep Hack," *BBC*, July 24, 2015, http://www.bbc.com/news/technology-33650491, (accessed January 7, 2018). Zetter, "Researchers Hacked A Model S, But Tesla's Already Released a Patch."
122. "Federal Statutes Relevant in the Information Sharing Environment (ISE)," Justice Information Sharing, *U.S. Department of Justice*, April 3, 2012, http://www.it.jp.gov, (accessed January 7, 2018).
123. "Paperwork Reduction Act: Federal Statutes Relevant in the Information Sharing Environment (ISE)," Justice Information Sharing, *U.S. Department of Justice*, March 20, 2012, http://www.it.jp.gov/default.aspx?area=privacy&page=1289, (accessed January 7, 2018).
124. 18 U.S.C. § 2721.
125. Thomas Fox-Brewster, "Cartapping: How Feds Have Spied On Connected Cars For 15 Years," *Forbes*, January 15, 2017, https://www.forbes.com/sites/thomasbrewster/2017/01/15/police-spying-on-car-conversations-location-siriusxm-gm-chevrolet-toyota-privacy/#12b3c7472ef8, (accessed January 7, 2018).
126. Ibid.
127. United States v. Jones, No 10-1259, U.S. Supreme Court, January 23, 2012. The court was split on whether this was because attaching a device to the vehicle violated the Fourth Amendment or because using GPS to track an individual over a long range violated an individual's expectation of privacy.
128. "Carpenter v. United States." Oyez, January 7, 2018, www.oyez.org/cases/2017/16-402, (accessed January 7, 2018).
129. "Connected Citizen's Program," *Waze*, https://wiki.waze.com/wiki/Connected_Citizens_Program, (accessed January 7, 2018).
130. "Data Security Laws," *National Conference of State Legislatures*, January 16, 2017, http://www.ncsl.org/research/telecommunications-and-information-technology/data-security-laws-state-government.aspx, (accessed January 7, 2018).
131. Ibid.
132. Fixing America's Surface Transportation Act, Public Law 114-94 (2015), 114th Cong. (2015). The DPA was included as part of the FAST Act, which was signed into law in December 2015.
133. Computer Fraud and Abuse Act, 18 U.S.C. § 1030, 1986.
134. "Cybersecurity Practices for Modern Vehicles," *U.S. National Highway Traffic Safety Administration*.
135. Ibid.
136. "Event Data Recorder," *U.S. National Highway Traffic Safety Administration,* https://www.nhtsa.gov/research-data/event-data-recorder, (January 7, 2018).
137. U.S. National Highway Traffic Safety Administration, "Federal Motor Vehicle Safety Standards; V2V Communications," *Federal Register*, January 12, 2017, https://www.federalregister.gov/documents/2017/01/12/2016-31059/federal-motor-vehicle-safety-standards-v2v-communications, (accessed January 8, 2018). For example, see privacy components in the V2V communications NPRM.
138. "Vehicle Data Privacy: Industry and Federal Efforts Under Way, but NHTSA Needs to Define Its Role," *U.S. Government Accountability Office*, July 2017, http://www.gao.gov/assets/690/686817.pdf, (accessed January 7, 2018).
139. The Federal Trade Commission Act, 15 U.S.C. § 41 (1914).
140. During the span of a consent decree—which can last up to 20 years—the company can be subject to an audit by the FTC, and violations can result in steep fines.

141. "Connected Cars: Privacy, Security Issues Related to Connected, Automated Vehicles - Part 1," *Federal Trade Commission*, video, June 28, 2017, https://www.ftc.gov/news-events/audio-video/video/connected-cars-privacy-security-issues-related-connected-automated, (accessed January 8, 2018).

142. "Fostering the Advancement of the Internet of Things," (U.S. National Telecommunication and Information Administration, U.S. Department of Commerce, January 2017), https://www.ntia.doc.gov/files/ntia/publications/iot_green_paper_01122017.pdf, (accessed January 8, 2018).

143. "Multistakeholder Process; Internet of Things (IoT) Security Upgradability and Patching," U.S. National Telecommunication and Information Administration, November 7, 2017, https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-iot-security, (accessed January 8, 2018).

144. Spy Car Act, S. 680 (2015), 114th Cong. (2015).

145. Internet of Things (IoT) Cybersecurity Improvement Act of 2017, S. 1691 (2017), 115th Cong. (2017).

146. Geolocation Privacy and Surveillance Act. H.R. 1062 (2017), 115th Cong. (2017); The Online Communications and Geolocation Protection Act, H.R. 656 (2015), 114th Cong. (2015); Location Privacy Act of 2014, S. 2171 (2014), 113th Cong. (2014); Robert Atkinson, "Testimony Before the Senate Judiciary Committee on Location Privacy Protection Act of 2014," *U.S. Senate Judiciary Committee,* June 4, 2014, https://itif.org/publications/2014/06/04/location-privacy-protection-act-2014; cite all other sources: https://www.gps.gov/policy/legislation/gps-act/, (accessed January 8, 2018). Also see ITIF testimony on the Location Privacy Act of 2014 for more information.

147. "State Data Security Breach Notification Laws," *Mintz Levin*, September 1, 2017, https://www.mintz.com/newsletter/2007/PrivSec-DataBreachLaws-02-07/state_data_breach_matrix.pdf, (accessed January 8, 2018).

148. "Privacy of Data From Event Data Recorders," *National Conference of State Legislatures,* December 12, 2016, http://www.ncsl.org/research/telecommunications-and-information-technology/privacy-of-data-from-event-data-recorders.aspx, (accessed January 8, 2018).

149. Department of Motor Vehicles, "DMV Releases Draft Requirement for Public Deployment of Autonomous Vehicles," *State of California*, press release, December 16, 2015, https://www.dmv.ca.gov/portal/dmv/detail/pubs/newsrel/newsrel15/2015_63, (accessed January 8, 2018).

150. Auto Alliance and Global Automakers, "Comments in Response to Consumer Privacy Protection Principles for Vehicle Technologies and Services," *Federal Trade Commission*, November 12, 2014, http://globalautomakers.org/system/files/document/attachments/Global%27s%20and%20the%20Alliance%27s%20FTC%20Letter%20Committment%20and%20Privacy%20Principles%20%282%29.pdf; https://www.automotiveisac.com/best-practices, (accessed January 7, 2018).

151. "DAA Self-Regulatory Principles," *Digital Advertising Alliance*, http://digitaladvertisingalliance.org/principles, (accessed January 8, 2018).

152. "Automotive Cybersecurity Best Practices," *AUTO-ISAC*, July 2016, https://www.automotiveisac.com/best-practices/, (accessed January 8, 2018).

153. "Who Can Join," *AUTO-ISAC*, July 2016, https://www.automotiveisac.com/who-can-join.php, (accessed January 8, 2018).

154. Chance Miller, "Judge throws out lawsuit aiming to put Apple at fault for texting and driving accidents," *9to5Mac*, August 26, 2017, https://9to5mac.com/2017/08/26/apple-responsible-for-texting-while-driving-case/, (accessed January 8, 2018). Matt Richtel, "A Victim's Daughter Takes the Cellphone Industry to Court," *New York Times*, December 6, 2009, http://www.nytimes.com/2009/12/07/technology/07distractedside.html, (accessed January 8, 2018).

155. California Code of Regulations, Title 10, § 2632.5 (2009), https://www.insurance.ca.gov/0250-insurers/0800-rate-filings/upload/PAYDFINALTXTFILED101609.pdf, (accessed January 8, 2018).

156. "Insurance Telematics: US State Regulators Tackle UBI," *Automotive*, June 2, 2012, http://analysis.tu-auto.com/insurance-telematics/insurance-telematics-us-state-regulators-tackle-ubi, (accessed January 8, 2018).

157. The Magnuson-Moss Warranty Act, Public Law 93-637 (1975). The manufacturer can require a vehicle owner to use select repair facilities if the repairs are free.

158. Clean Air Act of 1963, Public Law 101–549 (1990).

159. John Deere, "Comments to Kansas H.B. 2122: Digital Electronic Repair Requirements," *Scribd*, 2017, https://www.scribd.com/document/339340098/John-Deere--letter?irgwc=1&content=10079&campaign=Skimbit%2C%20Ltd.&ad_group=&keyword=ft750noi&source=impactradius&medium=affiliate#from_embed, (accessed January 8, 2018). These comments summarize the argument that owners should not access or tamper with the proprietary code of their vehicles.

160. Lawrence B. Levy and Suzanne Y. Bell, "Software Product Liability: Understanding and minimizing the risks," Berkeley Technology Law Journal, 1990, Vol. 5, No. 1, http://www.law.berkeley.edu/journals/btlj/articles/vol5/Levy.pdf, (accessed January 7, 2018).

161. Russell Hotten, "Volkswagen: The Scandal Explained," *BBC News*, December 10, 2015, http://www.bbc.com/news/business-34324772, (accessed January 7, 2018); David Kravets, "U.S. Regulators Grant DMCA Exemption Legalizing Vehicle Software Tinkering," *Arstechnica*, October 27, 2015, https://arstechnica.com/tech-policy/2015/10/us-regulators-grant-dmca-exemption-legalizing-vehicle-software-tinkering/, (accessed January 7, 2018).

162. Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 37 CFR Part 201, (U.S. Copyright Office, U.S. Library of Congress, 2015) https://copyright.gov/1201/2015/fedreg-publicinspectionFR.pdf, (accessed January 7, 2018).

163. Jason Koebler, "New jersey Becomes the 12th State to Consider Right to Repair Legislation," *Motherboard*, June 2, 2017, https://motherboard.vice.com/en_us/article/newbwd/new-jersey-becomes-the-12th-state-to-consider-right-to-repair-legislation, (accessed January 8, 2018).

164. "Memorandum of Understanding," *Automotive Aftermarket Industry Association, Coalition for Auto Repair Equality, Alliance of Automobile Manufacturers, and the Association of Global Automakers*, January 15, 2014, http://www.autocare.org/workarea/DownloadAsset.aspx?id=1440&gmssopc=1, (accessed January 8, 2018).

165. "Overview," *bIoTope*, http://www.biotope-project.eu/overview, (accessed January 8, 2018).

166. Intelligent Transportation Systems Joint Program Office, "DSRC: The Future of Safer Driving," *U.S. Department of Transportation*, https://www.its.dot.gov/factsheets/dsrc_factsheet.htm, (accessed January 8, 2018). DSRC is a standard developed by the Federal Communications Commission and the International Standards Organization.

167. 47 C.F.R. §§ 90 - 95.

168. 47 C.F.R. § 15.253.

169. Harding et. Al, "Vehicle-to-Vehicle Communications: Readiness of V2V Technology for Application," *U.S. National Highway Traffic Safety Administration*, (Report No. DOT HS 812 014), August 2014, https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/readiness-of-v2v-technology-for-application-812014.pdf, (accessed January 8, 2018).

170. U.S. National Highway Traffic Safety Administration, "Federal Motor Vehicle Safety Standards; V2V Communications."

171. For ITIF's recommendations, *see* Doug Brake, "Comments of ITIF In the Matter of Federal Motor Vehicle Safety Standards: Vehicle-to-Vehicle (V2V) Communications NHTSA-2014-0022" (filing,

Information Technology and Innovation Foundation, Washington, D.C., October 2014), http://www2.itif.org/2014-nhtsa-v2v-comments.pdf.

172. Zac Estrada, "US Set to Drop Proposed Vehicle-to-Vehicle Communications Mandate," *The* Verge, November 1, 2017, https://www.theverge.com/2017/11/1/16592704/vehicle-to-vehicle-communications-mandate-trump, (accessed January 8, 2018); U.S. National Highway Traffic Safety Administration, "V2V Statement," news release, November 8, 2017, https://www.nhtsa.gov/press-releases/v2v-statement (accessed January 8, 2018). While media report suggest that the Trump administration may change or delay the rule, the U.S. Department of Transportation has disputed that claim.

173. Stephen Ezell and Robert Atkinson, "From Chips to Concrete: Bringing the Surface Transportation Reauthorization Act into the Digital Age," (Information Technology and Innovation Foundation, May 2015), http://www2.itif.org/2015-concrete-to-chips.pdf, (accessed January 1, 2018).

174. Ibid.

175. Brian Cronin, "IntelliDriveSM Program Overview," (U.S. Department of Transportation, Research and Innovative Technology Administration [U.S. DOT RITA], November 30, 2010), http://www.its.dot.gov/presentations/pdf/MW_IntelliDrive_Overview.pdf, (accessed January 7, 2018).

176. Rosabeth Moss Kanter, Move: Putting America's Infrastructure Back in the Lead (New York: W.W. Norton & Company, 2015), 162.

177. Office of Management and the Budget (Table 3.2—OUTLAYS BY FUNCTION AND SUBFUNCTION: 1962–2020, Ground Transportation Expenditures; accessed [insert date]), https://www.whitehouse.gov/omb/budget/Historicals, (Accessed May 6, 2015); Ezell and Atkinson, "From Chips to Concrete: Bringing the Surface Transportation Reauthorization Act into the Digital Age."

178. Office of Policy and Governmental Affairs, "Fixing America's Surface Transportation Act or 'FAST Act'," *U.S. Department of Transportation*, July 2016, https://www.fhwa.dot.gov/fastact/summary.cfm, (accessed January 1, 2018). To be sure, the FAST ACT also authorizes $418 million per year for five years for research and development of six different programs—only one of which includes ITS systems.

179. Brian Cronin, "IntelliDriveSM Program Overview."

180. U.S. Department of Transportation, "U.S. Department of Transportation Announces up to $42 Million in Next Generation Connected Vehicle Technologies," press release, September 16, 2015, https://www.transportation.gov/briefing-room/us-department-transportation-announces-42-million-next-generation-connected-vehicle, (accessed January 1, 2018).

181. U.S. Department of Transportation, "Notice of Funding Opportunity for the Department of Transportation's Nationally Significant Freight and Highway Projects (INFRA Grants) for Fiscal Years 2017 and 2018," *Federal Register*, July 5, 2017, https://www.federalregister.gov/documents/2017/07/05/2017-14042/notice-of-funding-opportunity-for-the-department-of-transportations-nationally-significant-freight, (accessed January 7, 2018).

182. U.S. Department of Transportation, "U.S. Department of Transportation Launches Infrastructure for Rebuilding America (INFRA) Grant Program, Announces New Funding Opportunities," press release, June 29, 2017, https://www.transportation.gov/briefing-room/dot5217, (accessed January 7, 2018).

183. Wireless Infrastructure NPRM, WT Docket Nos. 17-79 and 15-180 (March 30, 2017, Notice of Proposed Rulemaking, https://transition.fcc.gov/Daily_Releases/Daily_Business/2017/db0330/DOC-344160A1.pdf.

184. Austin Jenkins, "Wireless Industry Lobbies Statehouses For Access To 'Street Furniture'," *National Public Radio*, April 11, 2017, http://www.npr.org/2017/04/11/522246173/wireless-industry-lobbies-statehouses-for-access-to-street-furniture, (accessed January 7, 2018).

185. Colin Gibbs, "Tensions Rise as Officials Struggle to Address Small Cell Deployment Challenges," *FierceWireless*, May 5, 2017, http://www.fiercewireless.com/wireless/tensions-rise-as-officials-struggle-to-address-small-cell-deployment-challenges, (accessed January 7, 2018).

186. Stephen J. Ezell and Robert D. Atkinson, "Explaining International Leadership in Intelligent Transportation Systems" (Information Technology and Innovation Foundation, January 2010), http://www.itif.org/files/2010-1-27-ITS_Leadership.pdf, (accessed January 8, 2018).

187. "Illinois Statewide Intelligent Transportation Systems (ITS) Architecture and ITS Strategic Plan," *Illinois Department of Transportation,* March 2005, http://www.idot.illinois.gov/Assets/uploads/files/Transportation-System/Research/ITS/IL%20SW%20ITS%20Concept%20of%20Operations%201.0.pdf, (accessed January 5, 2018).

188. Ezell and Atkinson, "International Leadership in Intelligent Transportation," 4.

189. Information Technology and Innovation Foundation, "ITIF Comments to Notice of Request for Information on The Strategy for American Innovation," September 23, 2014, http://www2.itif.org/2014-sai-comments.pdf, (accessed January 8, 2018).

190. Ezell and Atkinson, "International Leadership in Intelligent Transportation," 3.

191. Ezell and Atkinson, "From Chips to Concrete: Bringing the Surface Transportation Reauthorization Act into the Digital Age."

192. Ibid.

193. For example, see, "ITS Research 2015-2019 Interoperability White Paper," (Intelligent Transportation Systems Joint Program Office, U.S. Department of Transportation, 2015), https://www.its.dot.gov/research_areas/pdf/WhitePaper_interoperability.pdf, (accessed January 5, 2018).

194. Ezell and Atkinson, "From Chips to Concrete: Bringing the Surface Transportation Reauthorization Act into the Digital Age."

195. Adam Thierer, Permissionless Innovation (Arlington, VA: Mercatus Center at George Mason University, 2014), 3, http://permissionlessinnovation.org/wp-content/uploads/2016/04/PI_Blueprint_040716_final.pdf, (accessed January 8, 2018).

196. Daniel Castro and Alan McQuinn, "How and When Regulators Should Intervene," (Information Technology and Innovation Foundation, February 2015), http://www2.itif.org/2015-how-whenregulators-intervene.pdf, (accessed January 8, 2018).

197. Daniel Castro, "Benefits and Limitations of Industry Self-Regulation for Online Behavioral Advertising," (Information Technology and Innovation Foundation, December 2011), http://www.itif.org/files/2011-self-regulation-online-behavioral-advertising.pdf, (accessed January 8, 2018).

198. Ibid.

199. Castro and McQuinn, "How and When Regulators Should Intervene."

200. Auto Alliance and Global Automakers, "Comments in Response to Consumer Privacy Protection Principles for Vehicle Technologies and Services."

201. Alan McQuinn, "The Economics of 'Opt-Out' Versus 'Opt-In' Privacy Rules," *Information Technology and Innovation Foundation,* October 6, 2017, https://itif.org/publications/2017/10/06/economics-opt-out-versus-opt-in-privacy-rules, (accessed January 7, 2018). This resource provides more information on how limiting data collection can harm innovations.

202. "Search Vehicle Safety Ratings," *U.S. National Highway Traffic Safety Administration*, https://www.nhtsa.gov/ratings, (accessed January 7, 2018).

203. Center for Data Innovation, "CDI Comments to in response to the National Highway Traffic Safety Administration's (NHTSA) request for comments on its Federal Automated Vehicles Policy," November

21, 2016, http://www2.datainnovation.org/2016-federal-automated-vehicle-policy.pdf, (accessed January 7, 2018).

204. "Vehicle Data Privacy: Industry and Federal Efforts Under Way, but NHTSA Needs to Define Its Role," *Government Accountability Office*.

205. Fred Lambert, "Tesla Reduces Price of the 75 kWh Battery Upgrade by 22% for Some Model S Owners," *Electrek*, January 13, 2017, https://electrek.co/2017/01/13/tesla-price-75-kwh-battery-upgrade, (accessed January 7, 2018).

206. Joshua New, "Data-Driven Differential Pricing Benefits Consumers and Companies Alike," *Center for Data Innovation*, April 28, 2015, https://www.datainnovation.org/2015/04/data-driven-differential-pricing-benefits-consumers-and-companies-alike/, (accessed January 7, 2018).

ACKNOWLEDGMENTS

The authors wish to thank Rob Atkinson for providing input to this report. Any errors or omissions are the authors' alone.

ABOUT THE AUTHORS

Alan McQuinn is a research analyst at ITIF. His research areas include a variety of issues related to emerging technology and Internet policy, such as cybersecurity, privacy, virtual currencies, e-government, and commercial drones. Prior to joining ITIF, McQuinn was a telecommunications fellow for Representative Anna Eshoo (D-CA) and an intern for the Federal Communications Commission in the Office of Legislative Affairs. He graduated from the University of Texas at Austin with a B.S. in public relations and political communications.

Daniel Castro is vice president of ITIF. His research interests include health IT, data privacy, e-commerce, e-government, electronic voting, information security, and accessibility. Before joining ITIF, Castro worked as an IT analyst at the Government Accountability Office, where he audited IT security and management controls at various government agencies. He has a B.S. in foreign service from Georgetown University and an M.S. in information security technology and management from Carnegie Mellon University.

ABOUT ITIF

The Information Technology and Innovation Foundation (ITIF) is a nonprofit, nonpartisan research and educational institute focusing on the intersection of technological innovation and public policy. Recognized as the world's leading science and technology think tank, ITIF's mission is to formulate and promote policy solutions that accelerate innovation and boost productivity to spur growth, opportunity, and progress.

FOR MORE INFORMATION, VISIT US AT WWW.ITIF.ORG.