ITIF
The Information Technology
& Innovation Foundation

The Road Ahead: The Emerging Policy Debates for IT in Vehicles

BY DANIEL CASTRO | APRIL 2013

Policy decisions about IT in the vehicle should be driven, not by narrow interests and concerns, but rather by a broad government mandate to foster innovation in the transportation sector.

Many industries, from health care to entertainment to retail, have undergone dramatic transformations as firms in these industries use information technology (IT) to automate processes, create more efficient supply chains, and collaborate more efficiently.[1] These technology-driven changes have also created new policy issues and revived old policy debates. For example, widespread use of the Internet and mobile devices by consumers has led to dramatic changes in the distribution and pricing models for movies and music, and introduced new policy challenges such as digital piracy.

While not all industries have undergone the same degree of transformation, as the use of IT continues to grow, it is impacting these lagging industries. The transportation industry, and in particular the automotive industry, are only now beginning to experience some of the more radical changes that IT and the Internet have brought to other industries. These changes are opening up new possibilities for how individuals use transportation, improving the quality and safety of transportation, and creating profound shifts in our society that may ultimately impact how and where individuals work and live.

And just as IT-driven transformations in other industries have created new policy issues, the same will be true in transportation. The automotive industry will likely face some of the same policy debates and challenges previously seen in other industries further along in the technology adoption lifecycle. Chief among these policy debates will likely be concerns about public safety, data privacy and ownership, free speech and decency, liability, and access to wireless spectrum. While this report will not offer answers to all of the questions it raises, it will argue that the policy decisions about IT in the vehicle should be driven, not by narrow interests and concerns, but rather by a broad government mandate to foster innovation in the transportation sector. This will require leadership from both the government and the private sector and cooperation between different stakeholders.

THE EMERGENCE OF IT-ENABLED VEHICLES

As a result of a variety of factors, including low-cost, energy-efficient processors, cheap sensors, and ubiquitous connectivity, IT increasingly has been integrated or "embedded" into previously non-digital products, such as smart meters and smart phones. The same trend is seen in the automotive industry. In 2011, Akio Toyoda, the president of Toyota, unveiled a concept car he described as a "smartphone on wheels."[2] This metaphor is an apt description of the technology changes that are occurring within the automotive industry, where on-board computers and network connectivity increasingly are being integrated into vehicles to create "connected vehicles" that can serve as platforms for new innovation and development.

There are at least four important technology trends shaping the next-generation of vehicles: 1) an increase in machine-to-machine communications, 2) the development of in-vehicle "infotainment" systems, 3) the increased collection and use of vehicle data, especially geo-location data, and 4) vehicular automation.

The first trend is the growth of machine-to-machine communications. Machine-to-machine communications is a principle part of the "Internet of Things", a vision of a world where all devices are networked together to operate more intelligently. The prevalence of machine-to-machine connections is expected to grow from 5 percent of all mobile connections in 2012 to 17 percent of all mobile connections in 2017.[3] Much of this growth in machine-to-machine communications is expected to be driven by the automotive industry with only the healthcare sector expecting to see higher growth.[4]

Currently, one-third of all machine-to-machine communications occurs in the automotive industry.[5] Future growth in machine-to-machine communications will likely be driven by new transportation applications and the increased use of vehicle-to-vehicle and vehicle-to-infrastructure communications.[6] Vehicle-to-vehicle communications involves creating ad-hoc mobile networks to allow communication among vehicles. For example, vehicles may pass along warnings about road conditions or traffic. Vehicle-to-infrastructure communications involves 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.

The second trend is the increased amount of IT found in the dashboard of vehicles, particularly "infotainment" systems that provide consumers access to both information and entertainment content. Automobile manufacturers increasingly include IT systems in vehicles that are capable of providing access to multiple functions, including mobile communications, entertainment (e.g., movies and music), GPS-based navigation, vehicle safety information, traffic information, and other information (e.g., points of interest, gas stations, etc.). These infotainment systems may also serve as a platform for other applications provided by non-OEM developers.

There are two dominant infotainment platforms for vehicles: Microsoft Embedded Automotive and MeeGo. Microsoft Embedded Automotive is used in products such as Ford Sync, Kia UVO, and Fiat Blue & Me. Microsoft Embedded Automotive provides built-in functionality, such as support for SMS messaging, connecting to networks (WiFi, Bluetooth, etc.), multimedia playback, and voice recognition capabilities.[7] Automobile manufacturers can use Microsoft Embedded Automotive as a base system to design custom infotainment solutions for their own vehicles. For example, Ford Sync includes the ability to access data from the Engine Control Unit and display information about the vehicle's health. It can also use these data to detect if an accident has occurred and report this automatically to public safety officials.[8]

MeeGo is an open-source infotainment system built on Linux. Since the platform is open-source, device manufacturers can, if necessary, modify the operating system to work with their devices. MeeGo provides a set of functions similar to Microsoft Embedded Automotive. MeeGo also uses a number of standard software libraries, such as for displaying web content and accessing Bluetooth devices. This allows developers to easily create apps for this platform. The GENIVI Alliance, with support from technology backers such as Intel and Nokia, is the principal backer of the open-source platform and provides a forum for developing standards.[9] BMW, General Motors, Hyundai, Nissan and Renault are all participants in the program, and BMW and Mini Cooper have both implemented MeeGo in some of their vehicles.

The third trend is the increased collection and use of vehicle data, especially geo-location data. Geo-location information about vehicles (and drivers) is collected using a variety of technologies including roadside sensors (e.g., pneumatic road tubes, piezoelectric sensors, and magnetic loops), floating car data (e.g., GPS-based systems that report back a precise location and cellular-based systems that use triangulation to locate a vehicle), and roadside cameras.[10] While some of the older methods of tracking traffic patterns identify little personal information about drivers, they are more costly and less effective than newer methods. The high adoption rate of smart phones in the United States has created a relatively low-cost, high-density network of vehicle probes. Vehicle location can be reported back either directly over mobile networks or tracked using the MAC address of Bluetooth devices. However, these advanced forms of tracking collect more detailed information about vehicles, such as driving behavior and a precise history of a vehicle's location.[11]

Different businesses may have access to these data. Mobile network operators, such as AT&T and Verizon may have access to cell tower location data; mobile operation system and mobile device makers, such as Apple and Google, may have access to data from smart phones; and intermediaries, including data resellers and data aggregators such as Inrix and AirSage, may have access to third-party data. Vehicle location data may also be collected by the vehicle itself. For example, embedded systems, such as OnStar, may use GPS to determine the vehicle's location to provide roadside assistance, to track a stolen vehicle, or to report a potential accident to public safety officials.[12] Although much of this information is aggregated before it is used, there still may be legitimate concerns about the use of personally identifiable information (PII), especially by law enforcement.[13]

Another technology that is used to collect vehicle location data is automatic license plate readers. These systems use a network of roadside cameras to track the movement of vehicles by photographing license plates. The Drug Enforcement Agency and the Department of Homeland Security both have implemented, or plan to implement, these systems extensively. Only New Hampshire and Maine have restrictions on their use, and there are no restrictions that prevent states and localities from pooling their surveillance data.[14] Red light cameras, which similarly use roadside cameras to monitor driver behavior, also collect similar types of PII. In addition, new technologies such as unmanned aerial vehicles (UAVs) equipped with high-resolution cameras may be used as alternatives to roadside cameras for traffic surveillance. Unlike other traffic surveillance technologies, UAVs do not require access to public infrastructure, and thus can be deployed independently of government by private sector companies.

As the level of detail of information collected about vehicles and drivers increases, thorny questions about the privacy and ownership of this information become more salient. This may be especially true if vehicle tracking is used to implement vehicle miles traveled (VMT) taxes and pay-as-you-go (PAYG) car insurance. Since VMT taxes and PAYG car insurance are examples of uses of IT that disrupt the status quo and create winners (e.g., drivers who would pay less) and losers (e.g., drivers who would pay more), there may be entrenched interests that resist these policies.

VMT taxes have been proposed as an economically more efficient alternative to gasoline taxes to fund highways and roads. However, VMT taxes typically require that information on driving usage be shared with the government (or some other third party intermediary). VMT taxes can also be designed to incentivize more efficient use of highways, for example by charging different rates based on the location and time of day, but these systems necessarily entail the collection of even more detailed data.[15] It may be possible for certain system designs to minimize these privacy risks; for example the systems could report only the tax owed rather than their more privacy-sensitive trip data.

Similarly, PAYG car insurance requires tracking some usage data about vehicles, and this can create its own privacy challenges depending on the system design. Ultimately, however, the rules for car insurance are set by the state insurance commission. Each state has its own insurance commission, and each state can set its own regulations for the insurance industry. However, some types of laws may have the effect of preventing the use of more complex PAYG insurance schemes that are based on more granular tracking of driver behavior by in-vehicle IT systems. For example, California specifies which risk factors insurance companies are allowed to use in their rating systems. In Illinois, insurers can use any risk factors they want as long as they have full transparency. In both cases individual state rules may prevent the adoption of “pay-how-you-drive” insurance. In California, these types of systems simply may not be allowed; in Illinois, insurers may be allowed to offer this product, but would be reluctant to do so because they would be forced to disclose to their competitors their proprietary formulas for calculating risk.[16]

In addition to geo-location data, most vehicles today include embedded systems and sensors that collect information about the vehicle's mechanical condition and performance. Since 1996, all light-weight vehicles in the United States have included on-board diagnostics (OBD) which use a standard electronic interface to communicate information about the condition of the vehicle, such as the reason for a malfunction.[17] While much of this information has been available only to auto technicians, new products such as the Vehicle Diagnostics service offered by Verizon and Delphi allow vehicle owners to connect a device to the OBD port and gain wireless access to their vehicle's diagnostics data. The device also allows drivers to track their vehicle's location and trip history, remotely start their vehicle, and monitor their vehicle's health over time.[18] Finally, many automobile manufacturers are also including event data records (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 occurs, and whether the driver was wearing a seatbelt.[19]

The fourth trend is vehicular automation, or the use of IT to make vehicles autonomous or semi-autonomous. Perhaps the most famous example of this type of technology is Google's self-driving car. These vehicles use technologies such as video cameras, radar sensors, lasers, and ultrasonic sensors, as well as detailed maps and GPS, to detect other cars and obstacles and navigate on the road.[20] As of August 2012, Google's fleet of self-driving vehicles had logged more than 300,000 miles of testing.[21] Much of this initial research was spurred by the Defense Advanced Research Projects Agency (DARPA) Grand Challenge, which offered cash prizes to teams able to develop fully autonomous vehicles capable of completing a course.[22] The competition has been held three times—twice using an off-road course and once using an urban course—and competing teams, such as those at Stanford University and Carnegie Mellon University, have made substantial advancements in creating driverless vehicles.[23]

While many automakers are exploring how to further develop autonomous vehicle technology, it will still be many years before this experimental technology is available on the market for high-end vehicles and even longer before it will be available at a price that is affordable for the average consumer. However, automakers are already integrating many new features to make cars on the road today semi-autonomous. These include features like adaptive cruise control, blind spot monitoring, lane departure warnings, automatic parking, enhanced steering control, and automatic braking. According to ABI Research, the market for advanced driver assistance technologies will grow from $10 billion in 2011 to $130 billion in 2016.[24]

COMPETING INTERESTS WILL VIE FOR CONTROL OF THE POLICY DEBATE

Different stakeholders have different priorities. Some of the stakeholders in the transportation field represent the old guard and have been immersed in transportation issues since long before the idea of an intelligent transportation system was even conceived.

Others are newer participants who bring their experiences with IT and disruptive change to the transportation industry. We should expect the concerns from both communities, as well as those of vocal public interest groups, to dominate many of the debates on transportation. These concerns include public safety, data privacy and ownership, free speech and decency, liability, and the allocation of wireless spectrum.

The priorities of the dominant stakeholders will likely shape both the development of the rules governing the use of IT in vehicles and the institutions used to enact and enforce these rules. Other interests may also shape the debate, including private-sector motivations to obtain an advantage over competitors and/or reduce liability for accidents or malfunctions. Finally, external factors, including the saliency of the different issues and the venue of public debate, will likely affect the final policy outcomes.

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).[25] Ensuring that automobile manufacturers build safe vehicles and that policies are in place to prevent accidents remains a priority today.

As vehicles increasingly rely on IT, they face new security risks. For example, researchers have demonstrated that it is possible for hackers to control many aspects of a vehicle, such as disabling the brakes while a car is in motion, jamming the door locks, disabling the windshield wipers, revving the engine, honking the horn, and preventing the car from starting.[26] These attacks are not just theoretical. One disgruntled worker at a car dealership in Austin, Texas used an online tool to disable or trigger the horn to honk continuously on more than a hundred previously-sold vehicles.[27] Concerns about the security of IT systems can dominate many policy discussions, as has happened in other domains such as electronic voting. It is likely that security concerns for IT in vehicles will be prominent in debates about public safety, particularly for autonomous and semi-autonomous vehicles.

Another area of concern over IT in vehicles is distracted driving, which unfortunately ranks as one of the leading causes of accidents. This problem has been exacerbated by the high adoption and use of mobile phones, which present visual, manual and cognitive distractions to drivers.[28] The National Safety Council estimates that in 2010 more than a fifth of accidents (1.1 million accidents) were caused by drivers talking on a cell phone.[29] Other activities, such as texting while driving, have raised new public safety concerns as well.

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.[30] 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. Most states have adopted these policies. According to the Governors Highway Safety Association, as of August 2012, ten states plus the District of Columbia had passed legislation banning the handheld use of cell phones while driving;

thirty-nine states plus the District of Columbia had passed legislation prohibiting drivers from texting while driving; and another thirty-two states plus the District of Columbia ban the use of cell phones for all novice drivers.[31] The drumbeat for a nationwide ban on texting while driving has continued, with many top policymakers, including Secretary of Transportation Ray LaHood and former FCC Chairman Julius Genachowski, citing this as a priority.[32]

Naturally, portable devices are only part of the problem. The increased amount of information presented to drivers from in-vehicle electronics also poses a potential safety hazard. In response to this problem, in 2012 the NHTSA released a set of voluntary guidelines for in-vehicle electronics provided by the manufacturer. These 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.[33] The NHTSA also recommended disabling a number of other in-vehicle electronic devices and features that would be too distracting to the driver, unless these features were exclusively for the passengers or were only enabled when the vehicle is parked.

The Department of Transportation has not eliminated the possibility of issuing additional rules or recommendations related to other devices commonly used in vehicles, such as mobile phones, or voice-activated devices. As explained in a recent NHTSA notice:

> NHTSA is also considering future, Phase II proposed guidelines that might address devices or systems that are not built into the vehicle but are brought into the vehicle and used while driving, including aftermarket and portable personal electronic devices such as navigation systems, smart phones, electronic tablets and pads, and other mobile communications devices. A third set of proposed guidelines (Phase III) may address voice-activated controls to further minimize distraction in factory-installed, aftermarket, and portable devices.[34]

States are also considering additional laws that address the use of IT in vehicles and safety. For example, a West Virginia legislator has proposed a ban on Google Glass for drivers.[35] Of course, not all safety-based rules for IT in vehicles have been developed by the government. The Alliance of Automobile Manufacturers, an industry association, has adopted its own standards for in-vehicle electronics designed to protect public safety.[36]

On the other hand, public safety interests could also motivate greater use of IT in vehicles, such as crash avoidance systems and crash notification systems. Human error is the main cause of accidents, and one of the chief goals of research on autonomous and semi-autonomous vehicles is to improve driving safety.[37] 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.[38] But legislation is required to permit the use of some of this technology. For example, California, Nevada, and Florida have passed laws allowing the use of autonomous vehicles (i.e. driverless cars), albeit with certain restrictions to ensure public safety.[39]

IT can also be used in vehicles to support other public safety priorities. For example, France has implemented a new law that requires drivers to have a breathalyzer kit in their vehicle at all times.[40] While most of the breathalyzer kits are non-digital, single-use tests, in the future this type of device could be integrated directly into the vehicle's on-board IT systems.

Data Privacy and Ownership

As described earlier, information about the location, speed, and occupancy of vehicles, among other data, is collected through many different technologies, some of it by the public sector and some of it by the private sector. Different rules govern this information depending on who collects it and for what purpose. This information is enormously valuable for transportation planners, drivers, and businesses, but questions regarding data privacy and ownership will likely shape how different entities can use the data.

Multiple federal laws govern the use of personally identifiable information (PII) by government agencies. Three laws in particular, the Privacy Act of 1974, the Paperwork Reduction Act of 1980, and the E-Government Act of 2002, set requirements for how government agencies handle PII.[41] The Privacy Act limits the information that federal agencies can collect and distribute, especially PII. Federal agencies must specify the purpose of collecting information and limit collection to those purposes. The Privacy Act also requires agencies to follow certain fair information practices, such as allowing individuals to review information in their own records and to request corrections to inaccurate information. The Paperwork Reduction Act seeks to minimize the burden from government collection of information. The Act requires agencies to seek comment on proposed information collection activities and have an independent review process in place for information collection requests.[42] The E-Government Act requires federal agencies to conduct Privacy Impact Assessments to analyze what PII is stored in government systems. The E-Government Act also requires agencies to implement certain security controls to protect this information.

Government access to private location data is also restricted by the Fourth Amendment, which protects against unreasonable search and seizure. 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 (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).[43] 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.

Federal and state lawmakers have also expressed interest in enacting broad privacy legislation to better protect consumers, such as by creating a consumer privacy "Bill of Rights", and these laws would likely affect vehicle data.[44] In addition, most states have implemented data breach notification laws that require businesses and government agencies to notify individuals if PII has been lost or stolen.[45] Congress has also considered multiple proposals to implement national data breach legislation as well as other privacy legislation, such as to restrict the use of geo-location data.[46] These existing and proposed laws would likely apply to vehicle location information and other related PII. States have also considered privacy laws specific to drivers. For example, as of 2012, at least thirteen states have passed legislation governing the use of data from event data recorders.[47]

Within the broader debate about privacy, the specific issue of privacy as it relates to advertising may also impact vehicle information systems. There is little in-vehicle advertising in most vehicles on the road today (although there is a long history of on-vehicle advertising). However, this may change, especially if vehicle manufacturers adopt an "app store" model for in-vehicle information systems and allow ad-supported apps. (It is also possible to have in-vehicle ads included at the factory or dealership. For example, ads could be shown to bring in a car for maintenance to the dealer.)

App stores create a central location for consumers to find apps from different developers. These apps may be available to consumers for a charge or for free. Some of the free apps are made available as a "freemium" app (i.e., a limited functionality app that the user may pay to upgrade by unlocking additional functionality). For example, a new car may include a free year of real-time traffic information; after the first year is up, the owner must purchase a subscription to continue using the service. Other apps are made available to consumers for free, but contain advertising. For example, TeleNav, which makes a popular navigation system for the iPhone, provides ads on some of its products.[48]

These apps would run on the in-vehicle information system and deliver in-vehicle ads. Depending on how the app ecosystem evolves and the types of apps that are allowed on in-vehicle information systems, it is possible that in the future ad-supported in-vehicle apps will be as common as ad-supported websites are on the Internet. If this is the case, then it is likely that the same types of policy debate about online advertising will cross over to vehicles. This includes debates about the use of behavioral (or targeted) advertising and advertising standards for children. These debates will be particularly relevant since many of the same advertisers and advertising networks involved in online advertising would likely be participating in in-vehicle advertising.

There exist multiple avenues for potential regulation based on how this policy issue plays out for online advertising. The Federal Trade Commission (FTC) enforces related laws on the Internet, such as the Children's Online Privacy Protection Act (COPPA), which is intended to regulate online practices, including advertising targeted at children. Similarly, the FTC is responsible for ensuring that companies follow their stated privacy policies. It is likely that the FTC would also have authority to ensure that developers of in-vehicle apps adhere to their stated terms of services, especially if some apps run on platforms outside of the vehicle, such as a mobile device. There likely will also be debate about how to disclose privacy notices to drivers most effectively, without distracting them. Safety regulators with the U.S. Department of Transportation would likely provide input on this. In addition, state legislatures may craft their own legislative requirements or guidelines for in-vehicle advertising, as they have for mobile online advertising. Alternatively, rules on in-vehicle advertising could be set through voluntary processes. For example, the National Telecommunications and Information Administration (NTIA) in the Department of Commerce currently leads a multi-stakeholder process to develop voluntary industry codes of conduct for consumer privacy.[49] In addition, various industry and non-profit associations, including the Direct Marketing Association, the Digital Advertising Alliance, and the Better Business Bureau are developing a voluntary self-regulatory program for online advertising. Automotive industry associations, or their advertisers, might also develop their own industry codes of conduct (e.g., not advertising alcohol to drivers).

Free Speech and Decency

Policy makers at all levels of government have long had an interest in regulating the appropriateness of content, both in the digital and pre-digital eras, based on community standards. For example, the Federal Communications Commission (FCC) has used decency standards to restrict radio and television broadcasts and has issued rules and levied fines on broadcasters for content that it deemed to be inappropriate. Policy makers also have tried to regulate decency on the Internet with laws such as the Communications Decency Act (CDA) and the Child Online Protection Act (COPA). These types of policies often come into conflict with the First Amendment's guarantee of freedom of expression. As a result, some of these laws and policies have been struck down by the U.S. Supreme Court as unconstitutional.[50]

The increased use of the Internet in places outside of the home and workplace is raising new opportunities for policy makers to debate these issues again. While many libraries have resisted restrictions on content, casting themselves in the role of guardians against censorship, other venues for accessing content may be more willing to restrict access to certain content. For example, many restaurants, coffee shops, and airlines provide Internet access to their customers, and all of these businesses could potentially impose restrictions on what online content users can access through their networks. These restrictions could be imposed either at the network level or through policies put in place to require their customers to restrict their viewing to only non-objectionable content. For example, Delta Airlines has a policy of not allowing passengers to view offensive material.[51] As with most of the debates about decency, the exact definition of what is considered to be offensive is typically elusive.

Companies that restrict access to content deemed inappropriate can become targets of political protest by offended groups. For example, Apple has faced criticism for the software it makes available in the iTunes Apps store, and Facebook has faced criticism for blocking certain images on its site, such as photos depicting breastfeeding.[52]

Policy makers are beginning to debate the decency of content in vehicles. This debate is driven primarily by the increased availability of infotainment systems in vehicles. Large, high-resolution displays in the dashboard or mounted for viewing by passengers in the backseat may be highly visible, including by passengers in other vehicles. While many policy makers would not object to parents showing their children the latest Disney movie on DVD on a long road trip, they have raised objections to the display of pornographic material in vehicles both because the content may be a distraction to other drivers, and because the content may be offensive.[53]

Restrictions of content at the network level may raise questions of network neutrality. It is not entirely clear if blocking access to legal websites for in-vehicle systems would be a violation of the FCC's Open Internet rules. This would likely depend on which rules the FCC applied to the situation. Currently, the FCC does not apply its Open Internet rules to premise operators (i.e., bookstores, coffee shops, etc.).[54] However, while mobile operators are exempt from some of the Open Internet rules, they may not block lawful websites.

This distinction may also depend on the technology that is adopted in vehicles. There are two different models for connectivity in vehicles: using embedded systems and using mobile phones. Embedded systems connect to the Internet using network services integrated into the vehicle. This service may be packaged with the vehicle or billed based on usage. Alternatively, a vehicle may use the wireless connection of a mobile phone. Automobile manufacturers necessarily have more control over embedded systems. In addition, since these systems are being used exclusively while in the vehicle, they may fall under multiple regulatory jurisdictions. Some of the regulatory decisions may ultimately depend on whether the connectivity is provided by existing mobile operators directly to consumers or whether it is being resold by the auto makers.

Policy decisions relating to decency of in-vehicle information could be made in a number of different policy arenas, including federal and state law makers. For example, the New Jersey state legislature is considering a bill that would criminalize the display of obscene materials in vehicles and similar legislation has been passed in Tennessee, Louisiana, and Virginia.[55] And interest groups, such as the anti-pornography group "Morality in Media", will likely continue to push for further restrictions on the availability of certain content.[56]

As discussed previously, the National Highway Transportation Safety Administration could issue rules to address the safety of in-vehicle electronics, including infotainment systems that could cause distracted driving. This debate could also be shaped by civil courts if there is a case where the driver of a vehicle showing objectionable content is found liable for an accident caused by a distracted driver. This, in turn, would likely put market pressure on vehicle owners to forgo certain types of infotainment systems if they came with higher insurance rates. Until the legal implications of viewing potentially objectionable material in vehicles is resolved this policy issue will likely continue to grow as the availability of Internet connectivity in the vehicle increases. Ubiquitous connectivity means that the same content that is available online, including objectionable content, will also be available in the vehicle.

Liability

The issue of liability will also be an important policy issue that will affect the development and deployment of IT systems in vehicles. For example, which companies, if any, should be liable if a driver causes an accident while distracted by a vehicle's infotainment system? Many companies, including mobile network operators, computer hardware manufacturers, app developers, and automakers could all face legal claims that they are liable for accidents caused by the use of their products. Wireless carriers and handset makers have already faced claims of negligence for vehicular accidents involving their products.[57]

Similar liability questions arise from other uses of IT in vehicles. For example, automakers are generally responsible for defects in their vehicles if they result in operational failures. 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. Already some automakers have issued major recalls of vehicles for the sole purpose of updating software.[58] This may also create the need to develop different testing methods to ensure that critical software used in vehicles is reliable and secure.

Software companies typically try to limit their exposure to monetary damages from software that does not perform as expected, and questions of liability become more complicated if third-party software is running on a vehicle or if drivers can modify the software that is pre-installed on their vehicle.[59] For example, drivers 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. Depending on whether such software changes are permitted by the automaker, these actions could also be potential violations of the Digital Millennium Copyright Act (DMCA), which prevents unauthorized circumvention of certain technical measures. Alternatively, the U.S. Copyright Office could choose to exempt these technologies from the anti-circumvention rules.[60]

Autonomous and semi-autonomous vehicles create additional liability issues. For example, car owners may be liable for the actions of a vehicle they are not driving, and companies providing navigation and map data may be responsible for incorrect information. Many of these types of questions may be resolved with legislation and insurance, but different stakeholders will seek different outcomes. In addition, federal, state, and local governments may also face liability for accidents caused by failures in vehicle-to-infrastructure communications or failure to deploy these technologies on known dangerous roads.

Access to Wireless Spectrum

The successful adoption of in-vehicle IT systems will likely not succeed if vehicles do not have access to the bandwidth they need. As connectivity issues become more important to the transportation industry, it will likely find itself competing against other interests for access to wireless spectrum. In this regard, the Federal Communications Commission (FCC) will have a significant impact on the IT used in vehicles as a result of its authority to manage spectrum in the United States. The FCC manages spectrum that is important for at least three applications: vehicle-to-vehicle and vehicle-to-infrastructure communications; vehicular radar technologies communications; and transmission of traffic data to vehicles. In addition, the FCC sets the rules for certain service fees associated with wireless connections. Depending on how they are assessed, these fees could disproportionately affect the transportation industry and discourage connectivity in the vehicle.[61]

Spectrum is necessary for short-range vehicle-to-vehicle communications and vehicle-to-infrastructure communications. The FCC has initiated rulemaking to make spectrum available for this purpose. In 2003, the FCC allocated 75 megahertz in the 5.9 gigahertz band for dedicated short range communications (DSRC). This decision came six years after ITS America, a trade association, petitioned the FCC for this allocation and five years after

Congress passed the Transportation Equity Act for the 21st Century, which directed the FCC to consider the spectrum needs for intelligent transportation systems.[62]

Spectrum is also used for collision avoidance technologies. In 1995, the FCC adopted rules to allow the use of the 76-77 gigahertz band for vehicular radars. The FCC imposed certain use restrictions, such as limiting the average power when a vehicle is at rest, and the direction of radar, because of uncertainties about the possible consequences to human health of exposure to radiofrequency radiation. In 2012 the FCC modified its rules at the request of automakers to remove these restrictions.[63]

Finally, spectrum is important for transmitting traffic data to in-vehicle navigation systems. There are two principle methods for this: over mobile networks (e.g., 3G or 4G wireless networks) or over FM radio using the Traffic Message Channel (TMC). Both of these methods of communication rely on spectrum and licensing regulated by the FCC.

CONCLUSION

The rapid advancement of IT creates many new opportunities to leverage technology to improve the transportation system. However, as described in this report, there are various policy issues raised by the increased use of IT in vehicles, and the policy debates about IT that we have seen in other domains will likely be relevant to the transportation industry. Attempts to address these policy issues may put different stakeholders, both in the public and private sectors, at odds with one another when different priorities come into conflict. While there are not always simple solutions to all of these challenges, neither are these challenges insurmountable. The fact is that technology creates new risks and policy makers should expect many interest groups to draw attention to these risks. But the greater risk for citizens is that they will not obtain the benefits of emerging, innovative technology. Thus, policymakers should be strong advocates for the development and deployment of IT in the transportation industry.

ENDNOTES

1. Robert D. Atkinson and Daniel D. Castro, “Digital Quality of Life: Understanding the Personal and Social Benefits of the Information Technology Revolution,” October 2008, The Information Technology and Innovation Foundation, http://www.itif.org/files/DQOL.pdf.
2. Hans Greimel, “Toyota unveils ‘smartphone on wheels' concept car for Tokyo show,” November 28, 2011, Autoweek, http://www.autoweek.com/article/20111128/TOKYO/111129928.
3. “Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2012–2017,” Cisco, February 6, 2013, http://www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/ns827/white_paper_c11-520862.pdf.
4. Ibid.
5. Kevin O’Brien, “Talk to Me, One Machine Said to the Other,” The New York Times, July 29, 2012, http://www.nytimes.com/2012/07/30/technology/talk-to-me-one-machine-said-to-the-other.html, (accessed August 4, 2012).
6. Intelligent Transportation Systems Joint Program Office, “Trends in Machine-to-Machine Communications,” October 2011, http://www.its.dot.gov/research/techscan_m2m.htm.
7. Mukund Ghangurde, “Ford’s SYNC and Microsoft Windows Embedded Automotive Make Digital Lifestyle a Reality on the Road,” SAE International, 2011.
8. Tarik Al-Ani, “Android In-Vehicle Infotainment System,” University of Otago, June 2011.
9. Graham Smethurst, “Changing the In-Vehicle Infotainment Landscape,” GENIVI Alliance, 2010.
10. Guillaume Leduc, “Road Traffic Data: Collection Methods and Applications,” Work Papers on Energy, Transport and Climate Change, JRC Technical Notes, 2008.
11. Jean-Pierre Hubaux, Srdjan Capkun and Jun Luo, “The Security and Privacy of Smart Vehicles,” IEEE Security & Privacy, May-June 2004, p. 49 – 55.
12. “Our Privacy Practices,” OnStar, January 1, 2011, http://www.onstar.com/web/portal/privacy.
13. For example, in *United States v. Jones*, Justice Sotomayor notes, “With increasing regularity, the Government will be capable of duplicating the monitoring undertaken in this case by enlisting factory- or owner-installed vehicle tracking devices or GPS-enabled smartphones.” Available at http://www.supremecourt.gov/opinions/11pdf/10-1259.pdf.
14. Kade Crockford, “What We Know About License Plate Tracking, What We Don’t, And Our Plan to Find Out More,” American Civil Liberties Union, July 30, 2012, http://aclu.org/blog, (accessed August 4, 2012).
15. “Alternative Approaches to Funding Highways,” Congressional Budget Office, March 2011, http://www.cbo.gov/publication/22059, (accessed August 4, 2012).
16. “Insurance telematics: US state regulators tackle UBI,” Telematics Update, June 2, 2012, http://analysis.telematics.update.com/print/35496 (accessed August 4, 2012).
17. “Basic Information,” U.S. Environmental Protection Agency, n.d., http://www.epa.gov/obd/basic.htm.
18. “Vehicle Diagnostics by Delphi,” Verizon Wireless, n.d., http://shop.verizonwireless.com/?id=vehicle-diagnostics (accessed March 29, 2013) and Brian Heater, “Delphi / Verizon's Vehicle Diagnostics hands-on,” Engadget, January 8, 2013, http://www.engadget.com/2013/01/08/delphi-verizons-vehicle-diagnostics-hands-on-video/.
19. 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.
20. Sebastian Thrun, “What we’re driving at,” Google Blog, October 2010, http://googleblog.blogspot.com/2010/10/what-were-driving-at.html.

21. “The self-driving car logs more miles on new wheels,” August 7, 2012, Google Blog, http://googleblog.blogspot.com/2012/08/the-self-driving-car-logs-more-miles-on.html.
22. Erico Guizzo, “How Google’s Self-Driving Car Works,” IEEE Spectrum, October 18, 2011, http://spectrum.ieee.org/automaton/robotics/artificial-intelligence/how-google-self-driving-car-works.
23. For details see “History”, DARPA, n.d., http://www.darpa.mil/About/History/Archives.aspx.
24. Russ Juskalian, “Europe’s Driverless Car (Driver Still Required),” MIT Technology Review, January 20, 2012, http://www.technologyreview.com/news/426651/europes-driverless-car-driver-still-required/.
25. 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.
26. Karl Koscher et al., “Experimental Security Analysis of a Modern Automobile,” IEEE Symposium on Security and Privacy, 2010, http://www.autosec.org/pubs/cars-oakland2010.pdf.
27. Kevin Poulsen, “Hacker Disables More Than 100 Cars Remotely,” Wired, March 17, 2010, http://www.wired.com/threatlevel/2010/03/hacker-bricks-cars/.
28. “Understanding the distracted brain,” National Safety Council, March 2012, http://distracteddriving.nsc.org (accessed August 4, 2012).
29. Ibid.
30. “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 August 4, 2012).
31. “Cell Phone and Texting Laws,” Governors Highway Safety Association, August 2012, http://www.ghsaw.org/html/stateinfo/laws/cellphone_laws.html (accessed August 4, 2012).
32. Jessica Meyers, “Groups rally against texting while driving,” Politico, September 19, 2012, https://www.politicopro.com/story/tech/?id=14265.
33. “Visual-Manual NHTSA Driver Distraction Guidelines for In-Vehicle Electronic Devices,” Docket No. NHTSA-2010-0053, National Highway Traffic Safety Administration, February 15, 2012.
34. “U.S. Department of Transportation Proposes ‘Distraction’ Guidelines for Automakers,” U.S. Department of Transportation, February 16, 2012, http://www.dot.gov/affairs/2012/nhtsa0212.html, (accessed August 4, 2012).
35. Matt Burns, “West Virginia Lawmaker Seeks To Ban Drivers From Wearing Head Mounted Displays Like Google Glass,” TechCrunch, March 24, 2013, http://techcrunch.com/2013/03/24/west-virginia-lawmaker-seeks-to-ban-drivers-from-wearing-head-mounted-displays-like-google-glass/.
36. “FCC Encyclopedia: Distracted Driving Information Clearinghouse,” Federal Communications Commission, n.d., http://www.fcc.gov/encyclopedia/distracted-driving-information-clearinghouse (accessed August 4, 2012).
37. General Accounting Office, “Highway Safety: Research Continues on a Variety of Factors That Contribute to Motor Vehicle Crashes,” March 2003, http://www.gao.gov/new.items/d03436.pdf.
38. “Connected Vehicle Safety Pilot Program,” Intelligent Transportation Systems Joint Program Office, November 15, 2012, http://www.its.dot.gov/factsheets/safety_pilot_factsheet.htm.
39. See “Automated Driving: Legislative and Regulatory Action” at the Center for Internet and Society for an updated list of state legislation and regulatory action. Available at http://cyberlaw.stanford.edu/wiki/index.php/Automated_Driving:_Legislative_and_Regulatory_Action.

40. “France orders breathalyser for motorists,” BBC News, July 1, 2012, http://www.bbc.co.uk/news/world-europe-18662555 (accessed August 4, 2012).
41. “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 August 4, 2012).
42. “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 August 4, 2012).
43. United States v. Jones, No 10-1259, U.S. Supreme Court, January 23, 2012.
44. “Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy,” The White House, February 2012, http://www.whitehouse.gov/sites/default/files/privacy-final.pdf (accessed August 4, 2012).
45. “Senators Float National Data Breach Law, Take Four,” InformationWeek, June 25, 2012, http://www.informationweek.com/news/security/attacks/240002651 (accessed August 4, 2012).
46. Ibid.
47. “Privacy of Data from Event Data Recorders: State Statutes,” National Conference of State Legislatures, January 7, 2013, http://www.ncsl.org/issues-research/telecom/privacy-of-data-from-event-data-recorders.aspx.
48. “Will ‘freemium’ work for telematics apps?” Telematics Update, November 4, 2011, http://analysis.telematicsupdate.com/other/will-‘freemium’-work-telematics-apps, (accessed August 4, 2012).
49. “First Privacy Multistakeholder Meeting: July 12, 2012,” National Telecommunications and Information Administration (NTIA), June 15, 2012, http://www.ntia.doc.gov/other-publication/2012/first-privacy-multistakeholder-meeting-july-12-2012, (accessed August 4, 2012).
50. Sue Ann Mota, “The U.S. Supreme Court Addresses the Child Pornography Prevention Act and Child Online Protection Act in Ashcroft v. Free Speech Coalition and Ashcroft v. American Civil Liberties Union,” Federal Communications Law Journal (55) 1, 2002, p. 85 - 98.
51. “He’s Watching That, in Public? Pornography Takes Next Seat,” The New York Times, July 21, 2012, http://www.nytimes.com/2012/07/21/us/talets-and-phones-lead-to-more-pornography-in-public.html (accessed August 4, 2012).
52. “Facebook clarifies breastfeeding photo policy,” ZDNet, February 7, 2012, http://www.zdnet.com/blog/facebook/facebook-clarifies-breastfeeding-photo-policy/8791 (accessed August 4, 2012).
53. For example, Tennessee and Virginia prohibit the display of pornographic material in cars. See Matt Sundeen, “Cell phones and Highway Safety,” March 2007, National Conference of State Legislators, http://www.ncsl.org/print/transportation/2006cellphone.pdf.
54. “In the Matter of Preserving the Open Internet Broadband Industry Practices, FCC 10-201,” Federal Communications Commission, December 21, 2010, http://hraunfoss.fcc.gov/edocs_public/attachmatch/FCC-10-201A1_Rcd.pdf (accessed August 4, 2012).
55. “He’s Watching That, in Public? Pornography Takes Next Seat,” The New York Times, July 21, 2012, http://www.nytimes.com/2012/07/21/us/talets-and-phones-lead-to-more-pornography-in-public.html (accessed August 4, 2012).
56. Ibid.

57. 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/07distracted-side.html

58. See, for example, Dale Jewett, "Ford Escape, Fusion get software fix," Autoweek, December 11, 2012, http://www.autoweek.com/article/20121211/carnews/121219975 and "Honda recalls 2.5 million vehicles on software issue," Reuters, August 5, 2011, http://www.reuters.com/article/2011/08/05/us-honda-recall-idUSTRE77432120110805.

59. 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.

60. "Section 1201 Exemptions to Prohibition Against Circumvention of Technological Measures Protecting Copyrighted Works," U.S. Copyright Office, n.d., http://www.copyright.gov/1201/.

61. Brooks Boliek, "Toyota: Put the brakes on wireless fee rules," Politico, August 7, 2012, https://www.politicopro.com/story/tech/?id=13289.

62. "Dedicated Short Range Communications (DSRC) Service," December 7, 2004, http://wireless.fcc.gov/services/index.html?job=about&id=dedicated_src (accessed August 4, 2012).

63. "Amendment of Sections 15.35 and 15.253 of the Commission's Rules Regarding Operation of Radar Systems in the 76-77 GHz Band Amendment of Section 15.253 of the Commission's Rules to Permit Fixed Use of Radar in the 76-77 GHz Band," Federal Communications Commission, July 3, 2012, http://www.fcc.gov/document/toyotaera-76-77-ghz-band (accessed August 4, 2012).

ACKNOWLEDGEMENTS

The author wishes to thank the following individuals for providing input to this report: Rob Atkinson, Stephen Ezell, and Sue Wunder. Any errors or omissions are the author's alone.

ABOUT THE AUTHOR

Daniel Castro is a Senior Analyst with the Information Technology and Innovation Foundation. His research interests include health IT, data privacy, e-commerce, e-government, electronic voting, information security, and accessibility. Before joining ITIF, Mr. Castro worked as an IT analyst at the Government Accountability Office (GAO) 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 Washington, D.C.-based think tank at the cutting edge of designing innovation strategies and technology policies to create economic opportunities and improve quality of life in the United States and around the world. Founded in 2006, ITIF is a 501(c) 3 nonprofit, non-partisan organization that documents the beneficial role technology plays in our lives and provides pragmatic ideas for improving technology-driven productivity, boosting competitiveness, and meeting today's global challenges through innovation.

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