ADVISEN Productivity & Insight for Insurance Professionals

ZURICH®

Smart cars and connected vehicles

Privacy, security and safety considerations

Introduction

The car, only recently a secluded place, is rapidly becoming a rolling information hub. Increasingly, an automobile is characterized by a sophisticated network of computers linked to one another and to the Internet. Some track and report on internal systems and vehicle usage. Others help govern such functions as steering and braking. Yet others are integral to onboard navigation, communication, information and entertainment systems. Vehicles soon will be equipped with functionality to be in constant communication with surrounding vehicles and transportation infrastructure to improve safety.

Computer technology and the internet are contributing to a safer and more enjoyable driving experience, but there are trade-offs. Electrical control units can improve vehicle performance and enhance diagnostic capabilities, but they have proved vulnerable to hackers. Cars that enhance safety by electronically interacting with other vehicles and the driving environment generate privacy concerns. Advanced infotainment systems provide a wide range of communication, information and entertainment capabilities, but also have many of the same security vulnerabilities as a smartphone or tablet. Additionally, while automobile manufacturers claim that new infotainment technologies are much safer to use than the ways many drivers currently use smartphones and MP3 players, some safety advocates remain unconvinced.

Advances in technology

More than 60 percent of new cars worldwide are expected to have connected capabilities by 2017.

Even a mid-priced automobile today is remarkably "smart." Some modern automobiles have as many as 50 electrical control units (ECUs), many of which are instrumental to systems such as steering and braking. Some cars transmit maintenance and diagnostic information that can be read remotely by the owner or by the manufacturer. Alarms warn drivers of unseen objects behind their vehicle or in their blind spot. On-board GPS systems direct drivers step-by-step to their destination. Entertainment and communication systems are integrated with portable MP3 players or smartphones. The newest generation of automobiles has functionality that enables drivers to receive and send text messages using computerized voice technology.

As technology continues to advance, vehicles will get smarter and more connected. More than 60 percent of new cars worldwide are expected to have connected capabilities by 2017, according to ABI Research.[1]

Some automobile manufacturers are incorporating elements of Apple's iOS operating system in their vehicles, enabling drivers to integrate an iOS device with the in-dash system. Google plans to soon take the concept a step further. Drivers and passengers of vehicles incorporating the Android operating system will have access to traffic data, maps, entertainment, web services and more, all fully integrated with the vehicle's computing and controls. In Google's vision, the car itself becomes a "connected Android device."[2]

"Wearables" – devices such as glasses or watches worn on the body to sense or deliver information – are a new trend in automotive design. Hyundai, Mercedes, BMW and Nissan are among the automakers now offering some form of wearable device for drivers. With wearables, vehicle-to-person interaction levels are expected to become much higher, providing new levels of control and interaction with automobiles.

[1] Chris Woodyard and Jayne O'Donnell, "Your car may be invading your privacy," USA Today (Mar 25, 2013) www.usatoday.com

[2] FAQs, Open Automotive Alliance www.openautoalliance.net

The information rich environment of the modern automobile raises safety concerns, especially as regards distracted driving.

Emerging technologies will directly integrate vehicles within the driving environment. Connected vehicles are in two-way communication with other vehicles, the transportation infrastructure and various devices with the objectives of enhancing safety, improving mobility and reducing the environmental impact. The goal, according to the U.S. Department of Transportation Research and Innovative Technology Administration (RITA), is to develop "a fully connected transportation system that makes the most of multi-modal, transformational applications."[3]

Risk factors

New technologies are intended to make driving safer, more efficient and more pleasurable. As the case with almost all new technologies, however, they are not without risk.

Distracted driving

The information rich environment of the modern automobile raises safety concerns, especially as regards distracted driving. The U.S. Department of Transportation describes distracted driving as a "dangerous epidemic," with many accidents traced back to distractions resulting from mobile phone or smartphone use.

Automakers claim that new technologies reduce distractions and even can make driving safer by feeding drivers valuable information about the route, the immediate environment and the vehicle itself. They claim that new applications of smartphone technology will lead to safer roads, easier navigation and generally smarter drivers. Others are not yet convinced. Some safety advocates claim that the new technologies do little to address certain underlying safety factors. They further claim that automobile infotainment systems are being developed faster than independent researchers can analyze their effects.[4]

The National Highway Traffic Safety Administration (NHTSA) has published guidelines "to encourage automobile manufacturers to limit the distraction risk for in-vehicle electronic devices."[5] Some safety advocates are concerned, however, that the NHTSA guidelines don't go far enough. They point to existing studies on distracted driving to support their concerns about new technologies. A study by the American Automobile Association and the University of Utah, for example, concluded that drivers who engage in complex multitasking have a decrease in brain function and reaction time and an increase in crash risk.[6] Proponents of the new technology counter with a study conducted by the Virginia Tech Transportation Institute and funded by the NHTSA, which found that distracted driving risks were mainly due to visual and manual distractions.[7] They claim that the new technologies reduce these distractions.

Wearables are an important part of the next generation of human-machine interface and will involve such things as eye control, gesture recognition and Augmented Reality (AR). AR uses optical devices, such as Google Glass, to provide enhanced information. Proponents of this technology claim it offers drivers the ability to keep their eyes on the road while interacting with maps, dashboard displays, collision safety alerts and various smartphone functions.[8]

As might be expected, the use of wearables for accessing and interacting with information also raises safety concerns in some quarters. Google Glass is the most highly touted wearable in today's market, but legislation banning Google Glass and similar eyewear is being considered in several states and in the UK. The AAA has come out against the use of computer powered glasses, claiming that something that requires the "preoccupation of one of your eyes" should never be used while operating a car.[9]

[3] "Connected Vehicle Research," RITA www.its.dot.gov

[4] Hands-Free Infotainment Isn't The Solution To Distracted Driving, Researchers Warn Webcast News Room (Feb 5, 2014) www.webcastnewsroom.com

[5] "U.S. Department of Transportation Proposes 'Distraction' Guidelines for Automakers," NHTSA www.nhtsa.gov

[6] David L. Strayer, Joel M. Cooper, Jonna Turrill, James Coleman, Nate Medeiros-Ward, and Francesco Biondi, Measuring Cognitive Distraction in the Automobile (June 2013), University of Utah www.aaafoundation.org

[7] Fitch, G. A., Soccolich, S. A., Guo, F., McClafferty, J., Fang, Y., Olson, R. L., Perez, M. A., Hanowski, R. J., Hankey, J. M., & Dingus, T. A. (2013, April). The impact of hand-held and hands-free cell phone use on driving performance and safety-critical event risk. (Report No. DOT HS 811 757). Washington, DC: National Highway Traffic Safety Administration. www.nhtsa.gov

[8] "Insights Into The Future Of The Auto Industry And The Connection Mobile Will Play," AutoMotion www.automotiontv.com

[9] Erik Ortiz, "Driving while wearing Google Glass: Could the futuristic device join handheld cell phones, texting as illegal?" New York Daily News www.nydailynews.com

Cars that digitally communicate with one another and with infrastructure, such as bridges or freeway on-ramps, to avoid accidents hold tremendous potential for improving highway safety, but they raise red flags with privacy watchdogs.

Perils of the connected vehicle

Consumer privacy is regulated to varying degrees when it comes to banking transactions, medical records, and phone and Internet use. Data generated by cars, for the most part, is not. As a result, consumers have little control over who can see their data and how it can be used.

Information produced by a vehicle and transmitted over the Internet can be intercepted. Ultimately, it ends up on servers, making it a potential target for law enforcement officials, trial lawyers and hackers. That information also may be sold or otherwise used for purposes never contemplated by the automobile owner.

Cars that digitally communicate with one another and with infrastructure, such as bridges or freeway on-ramps, to avoid accidents hold tremendous potential for improving highway safety, but they raise red flags with privacy watchdogs. The concerns multiply with the number of connected systems in a vehicle. In addition to recording factors such as how fast a driver is driving and where she is going, intelligent automobiles also know such things as the frequency of her texts, who she is texting and who is texting her.

Not surprisingly, local and state highway police departments already have expressed an interest in monitoring such information for speed control, stolen vehicle recovery and other purposes. Motorists may be pleased that first responders can be automatically alerted to accidents or other emergencies, or that the police can more easily find a stolen car, but information broadcast by vehicles also may provide police and other government officials with knowledge that citizens consider private and, in some cases, which may raise constitutional issues. The line between respecting the privacy of individual drivers and identifying law breakers is not always clear.

Developers of a proposed nationwide system of connected cars say they are sensitive to privacy concerns and are trying to build in safeguards. According to the Vehicle Infrastructure Integration Coalition, a cooperative effort between Federal and State departments of transportation and automobile manufacturers, the system will be designed to assure driver anonymity.[10] Other observers note that most of the data generated during vehicle-to-vehicle communication is transient and the opportunity for a privacy breach is very short lived.[11] Nonetheless, history has shown that when there is valuable information to be had, someone will devise a way to get to it.

Even information not intended to be seen or used outside a vehicle's internal systems poses security issues. Many cars now have wireless networks to transmit information throughout a vehicle. Researchers point out that the privacy and security implications of such in-car networks are not yet well understood. A team of researchers from the University of South Carolina and Rutgers University found that they could "eavesdrop" on internal systems from more than 120 feet away.[12]

Some devices that collect or transmit information from a vehicle are not built in by manufacturers, but are introduced into vehicles by drivers or are added after the vehicle has been purchased. These include transponders for automatically paying tolls and devices to track and report on driving practices for insurance purposes.

Transponders can enable cars to breeze through toll booths, but also can – and are – used to track driving patterns and for other purposes. Presenting his findings at hacker

[10] Chris Woodyard and Jayne O'Donnell, "Your car may be invading your privacy," USA Today (Mar 25, 2013) www.usatoday.com

[11] Joe Barkai, "Connected Cars: Conduit vs. Content" www.joebarkai.com

[12] Ishtiaq Rouf, Rob Miller, Hossen Mustafa, Travis Taylor, Sangho Oh, Wenyuan Xu, Marco Gruteser Wade Trappe, Ivan Seskar; Security and Privacy Vulnerabilities of In-Car Wireless Networks: A Tire Pressure Monitoring System Case Study, University of South Carolina and Rutgers University www.cse.sc.edu

conference Defcon, a hacker known as Puking Monkey rigged his E-Z Pass to alert him every time it was read. He then drove through New York City and found his device was tagged multiple times on the short drive between Time Square and Madison Square Garden.[13]

Automobiles and trucks increasingly rely on computer technology for diagnostics and to improve vehicle performance. As a result, many features of modern vehicles are susceptible to being hacked.

Even when used for its intended purposes, auto owners cannot assume information produced by automated toll paying systems is private. Several states have provided electronic toll information in response to court orders in civil cases.[14] Some observers also have raised concerns that automated toll-paying systems, which now are also used for paying at parking lots and fast food drive-through windows, provide one more hackable access point to credit card information.[15]

Telematic devices are increasingly used to compile and sometimes transmit information about driving habits, vehicle performance and even the mental and physical acuity of drivers. A growing number of insurance companies install devices that enable the company to identify safe drivers and reward them with lower premiums. The privacy implications are obvious, prompting Progressive, a pioneer in telematics insurance, to stop monitoring vehicle locations, and to remove their devices after six months.[16]

Vehicles do not necessarily have to transmit information to raise privacy concerns. Electronic data recorders (EDRs) – widely known as "black boxes" – which compile the critical details leading up to a crash, are now built into 96 percent of new cars. EDRs can help make cars safer by providing critical information about crashes, but the data is increasingly used by attorneys in lawsuits involving drivers. While some attorneys claim black boxes are "dispassionate and reliable witnesses," others question the reliability of the data.[17]

NHTSA guidelines state that EDR information belongs to a vehicle's owner and can be used only with consent in most cases, but in many cases it can be obtained through a court order. Eleven U.S. senators recently introduced a bipartisan bill that makes it clear that the owner of a vehicle is also the owner of any information collected by an EDR.

A "hackable asset"

Automobiles and trucks increasingly rely on computer technology for diagnostics and to improve vehicle performance. As a result, many features of modern vehicles are susceptible to being hacked.

In 2010, researchers affiliated with the Center for Automotive Embedded Systems Security (CAESS), a partnership between the University of California San Diego and the University of Washington, demonstrated how it is possible to take over all of a car's vital systems by plugging a device into the OBD-II port under the dashboard.

The following year, the same CAESS researchers demonstrated how to remotely take control of an unnamed vehicle through its telematics system. In a report, they also reveal that it is theoretically possible to hack a car with malware embedded in an MP3 and with code transmitted over a Wi-Fi connection.

While basic risk management practices call for separation between the infotainment and vehicle-centric safety systems, the trend has been towards greater integration at certain levels. The CAESS researchers show that MP3 hosted malware can infect many different functions of a vehicle because the dozens of independently operating computers spread throughout modern vehicles are all connected through an in-car communications network known as a controller-area-network bus, or CAN bus.[18]

[13] Kashmir Hill, "E-ZPasses Get Read All Over New York (Not Just At Toll Booths)," Forbes (Sept 12, 2013) www.forbes.com

[14] Chris Newmarket, "E-ZPass records out cheaters in divorce court," AP (Oct 10, 2007) www.nbcnews.com

[15] "Drive-Thru Lets Fast Food Customers Pay with EZ-Pass," The Internet Patrol www.theinternetpatrol.com

[16] "How's my driving?" The Economist (Feb 23, 2013) www.economist.com

[17] Chris Woodyard and Jayne O'Donnell, "Your car may be invading your privacy," USA Today (Mar 25, 2013) www.usatoday.com

The vulnerability of automobiles to hacking is sufficiently troublesome that the Defense Advanced Research Projects Agency (DARPA), a research arm of the Pentagon, is financing research into security weaknesses. DARPA-sponsored researchers have uncovered yet more vulnerabilities.[19]

Fortunately, at this point in time, only a few cybercriminals are skilled enough to hijack a vehicle using only a laptop, according to computer security firm Trend Micro. However, as automobiles become more thoroughly wired into the "Internet of things," it will become increasingly simple for criminals to wreak havoc on the roadways. According to Trend Micro, automobiles "should be regarded as potentially hackable assets that, if compromised, could result in actual loss of life."[20]

Automakers have taken steps to secure onboard networks, but the threat is continuously evolving. Some researchers claim that automobile manufacturers have not done enough to counter the threat. One CAESS researcher claims his team was able to exploit the types of vulnerabilities found on PCs in the early to mid-1990s.[21]

Risk management and underwriting considerations

The unending cat-and-mouse game between hackers and security experts has found a new playing field, but how much car companies are willing to invest in additional security remains to be seen. According to the Auto Alliance, an association of 12 automobile manufacturers, "cyber-security is among the industry's top priorities and the auto industry is working continuously to enhance vehicle security features."[22] Some critics, however, are skeptical.

In any event, even the best defended networks have proved vulnerable to hackers. It never can be assumed that anything connected to the Internet is impregnable. As Trend Micro advises, automobiles should always be treated as if they are potentially hackable. Individual automobile owners probably can do little more than to take commonsense precautions as they would with their PC or smartphone, but commercial fleet owners should incorporate their vehicles within their companies' overall network security strategies.

Privacy concerns will continue to be a thorny issue for all organizations that compile, analyze, share or sell the enormous amount of information now available digitally, including information produced by and about automobiles and their drivers. This is a rapidly developing area where law and regulation struggle to keep pace with changing technology and the privacy expectations of citizens. Automakers and the various companies that provide technology and services around the transmission, collection and use of data need to develop robust systems, processes and policies to assure information integrity and confidentiality, as well as to govern information retention and disposition. Transparency is important. Even when the uses of data do not run afoul of existing privacy laws, companies risk backlash from customers and others who object to how their personal information is collected and used.

"The individualism and the freedom of the automobile and the open road are [central] to American culture," according to one writer on car culture.[23] But Americans also love their technology, which increasingly is a cornerstone of modern culture. The clash between individualism and freedom on the one hand, and the uses of technology and data on the other hand, will be played out on America's highways. However, the rate of change in automobile-based information, entertainment, communication and computer-enabled

[18] "Hack to the Future," Car and Driver (August 2011) www.caranddriver.com

[19, 21] "Hackers Reveal Nasty New Car Attacks – With Me Behind The Wheel," Forbes (Aug 12, 2013) www.forbes.com

[20] "Automobiles: A new frontier in hacking and cybersecurity," Trend Micro http://blog.trendmicro.com

[22] "Cyber-Security," Auto Alliance www.autoalliance.org

[23] United States: Home of Car Culture, EMBARQ www.embarq.org

safety technologies means that exposures are multiplying faster than the risks can be fully analyzed and quantified. Risk managers and underwriters will continue to be challenged to respond with creative solutions to this complex and constantly shifting risk landscape.

Smart risk management for smart cars: What your company should be considering

Smart car technologies and connected vehicles are capturing the attention of companies that manage their own fleet. These technologies offer companies a new set of tools that can help improve safety, reduce fleet operational cost, increase efficiency and improve productivity. Consider these possibilities:

- Driving patterns of individual drivers can be detected, allowing you to address unsafe behaviors with appropriate supervisory and management-related actions.
- Monitoring fleet vehicles, driving patterns and routing can help reduce costs associated with fuel, maintenance and insurance, and discourage employee drivers from using company vehicles for personal reasons.
- Vehicle data can be shared with insurance providers for the purpose of refining rates and coverage costs.
- Technologies can help law enforcement locate and recover stolen vehicles.

While these advantages may be clear, the potential risks are still hazy. As vehicle owners, companies have some challenging questions to think about, particularly those surrounding the issues of privacy and liability, such as:

- What information do you have a right to collect?
- How long should you keep the information?
- What are the consequences and potential liabilities of not monitoring drivers and vehicles?
- Could a plaintiff's attorney sue your company for not exercising "reasonable control" or for negligence?

While the liability issues will continue to unfold in the courtroom, one thing is certain: Smart car technology is here to stay, and like all emerging risks, the key will be to optimize the potential advantages while building a solid risk management strategy around the potential exposures.

Zurich
1400 American Lane, Schaumburg, Illinois 60196-1056
800 382 2150 www.zurichna.com

The information in this publication was compiled from sources believed to be reliable for informational purposes only. All sample policies and procedures herein should serve as a guideline, which you can use to create your own policies and procedures. We trust that you will customize these samples to reflect your own operations and believe that these samples may serve as a helpful platform for this endeavor. Any and all information contained herein is not intended to constitute legal advice and accordingly, you should consult with your own attorneys when developing programs and policies. We do not guarantee the accuracy of this information or any results and further assume no liability in connection with this publication and sample policies and procedures, including any information, methods or safety suggestions contained herein. Moreover, Zurich reminds you that this cannot be assumed to contain every acceptable safety and compliance procedure or that additional procedures might not be appropriate under the circumstances. The subject matter of this publication is not tied to any specific insurance product nor will adopting these policies and procedures ensure coverage under any insurance policy.