Bloomberg BNA

Privacy and Security Law Report®

Connected Cars

In light of the potential benefits and the rapid technological progress, it is clear that autonomous vehicles will be available to regular consumers in the not so distant future. Though there appears to be a concerted effort, it is still unclear whether governments can pass legislation that adequately addresses cybersecurity concerns relating to autonomous vehicles before they become available to the public, the author writes.

Autonomous Vehicles: Will the Cybersecurity Risks Be Addressed?

Gretchen Ramos

Over the last decade, companies have devoted considerable time and resources to the development of autonomous vehicles. In its August 2016 monthly report, Alphabet Inc.'s Google Inc. reported that its self-driving vehicles had logged nearly two million miles in autonomous mode over the last seven years.

Gretchen Ramos is a partner at Squire Patton Boggs LLP in San Francisco. She counsels companies on three continents on privacy and data security law.

This article represents the views of the author and not necessarily those of the firm.

The potential benefits autonomous vehicles offer society are numerous: from less traffic congestion and increased safety, to greater mobility for the population and possibly even increased digital media revenue. For instance, human error is the cause of 93 percent of road traffic accidents, with 1.3 million fatalities and 50 million injuries globally every year. Experts estimate that replacing human drivers with capable technology will substantially decrease collision rates. A report issued by the Institute of Electrical and Electronics Engineers (IEEE) in 2012 estimated that widespread adoption of autonomous vehicle technology could also increase highway capacity fivefold. Moreover, some predict that autonomous vehicles will provide the population with time to devote to other tasks, and ultimately result in increased digital media revenue. The commercial vehicle industry would also benefit from autonomous vehicles through increased safety since the vast majority of crashes are due to a driver being distracted or tired, which would not occur in an autonomous vehicle.

In light of the potential benefits and the rapid technological progress, it is clear that autonomous vehicles will be available to regular consumers in the not so distant future. Among the many important questions on the minds of consumers is: will autonomous vehicles be safe, or will the use of autonomous vehicles threaten our security?

In last few months, various consumer groups and some legislators have voiced concerns about the lack of legislation addressing security and information privacy issues in connected vehicles. While numerous compa-

 ISSN 1538-3423

nies have devoted endless hours to developing and testing autonomous vehicles, only a few states have enacted laws related to autonomous vehicles, and none of these laws yet relate to privacy and security issues.

In last few months, various consumer groups and some legislators have voiced concerns about the lack of legislation addressing security and information privacy issues in connected vehicles.

The National Highway Traffic Safety Administration (NHTSA) and Department of Transportation (DOT) guidelines on autonomous vehicles were released Sept. 20 and address some of these cybersecurity concerns so that autonomous vehicle companies have a better understanding of the steps they are required to take to protect the consumers' privacy and security, and of course protect themselves from future litigation. These guidelines, which stop short of official regulations, incorporate three key areas into their 15-point safety standard. Whether this will be enough to assure the public of their data privacy and of cybersecurity considerations will wait to be seen.

Hacking: Taking Control of Your Vehicle and Your Data

The concerns heard most often about autonomous cars are the threat of hacking and fear that a third party will take control of their cars. There are numerous reports showing vehicle controls are vulnerable to hacks, and since autonomous vehicles consist of more interconnected components, this increases the ability for a hacker to infiltrate a car's computer system. While the news is peppered with stories of car hacks, to date these hacks have typically been undertaken by security experts hired by the carmakers for research purposes so as to reduce future threats. However, in the last few months there have been reports of crime thefts in Houston where car thieves hack into vehicles' computer control systems.

Taking over the controls of other cars does not just relate to autonomous vehicles—it concerns many of the connected cars that we drive today. In 2012, the Defense and Research Project Agency (DARPA) enlisted security intelligence experts to test car vulnerabilities. One year into their research, they were able to hack into cars by taking control of the horn, cutting the power steering, and spoofing the GPS and the dashboard displays. Three years later, in 2015, the experts figured out how to remotely take control of another car by exploiting a software flaw to shut down its engine while being driven on a highway. This well-publicized hack resulted in a widespread recall.

In the era of big data, a hacker might be more interested in knowing where a driver is located and accessing their personal information rather than in controlling their vehicle.

These scenarios capture the public's attention but, while scary and possible, may not present the biggest cybersecurity issue in relation to hacking. NHTSA has indicated that the hacking of vehicles, on a broader scale, has become one of its highest priorities, apparently recognizing that in the era of big data, a hacker might be more interested in knowing where a driver is located and accessing their personal information rather than in controlling their vehicle. As today's vehicles include more and more components, and autonomous vehicles will contain even more, they are more susceptible to security gaps.

Many commentators have expressed grave concerns about Dedicated Short-Range Communication (DSRC) technology incorporated into many cars today. The DSRC technology, which will form part of all autonomous and ''connected cars'' in the future, helps to avoid collisions and offers commercial services. Numerous public interest groups and some legislators have recently requested the Federal Communications Commission (FCC) halt the use of this technology and have requested that the FCC rather than the DOT or the Department of Commerce be responsible for regulating the DSRC technology. These consumer organizations fear DSRC technology will not only create a ''Computer on Wheels'' but also will result in significant cybersecurity issues due to increased connectivity. If a DSRC system was hacked, the perpetrator could falsify vehicle safety messages or disable the communication of the device, which could lead to catastrophic results. Thus, consumer groups are pushing to have rules established that would require data transparency and breach notification and have companies submit privacy and cybersecurity plans before activating DSRC systems.

Some groups disagree. In comments that the State of California Department of Transportation (Caltrans) submitted to the FCC, it notes that:

> Neither the use of the 5.9GHz band, nor the use of standards based protocols developed by the IEEE and Society of Automotive Engineers, pose a unique vulnerability for vehicle safety or user privacy. Actually, the security and privacy measures implements by following the standards make sure of the 5.9 GHz band less vulnerable to hackers.

Caltrans went on to note that the petition seeking delay of DSRC technology does not identify any specific vulnerabilities ''but rather preys on fear of zombies to derail a well designed and tested system.''

Neither State Nor Federal Law Exists That Addresses Consumers' Cybersecurity Concerns

While the public and the industry recognize the risks, and there is industry agreement on information privacy

  PVLR ISSN 1538-3423

best practices, the vast majority of states have yet to adopt legislation related to autonomous vehicles. Although California and other states have passed legislation addressing the testing of autonomous vehicle technology, Nevada is the only state to have regulations concerning the implementation of autonomous vehicle technology on its roads. There are currently no state laws in place addressing the security and privacy issues stemming from autonomous vehicles.

To date, these state regulations have failed to address the privacy issues associated with the collection, use, and storage of data stemming from autonomous vehicle use. In December 2015, the California Department of Motor Vehicles released draft regulations that, among other things, proposed that autonomous vehicles be equipped with self-diagnostic capabilities that detect and respond to cyber-attacks or other unauthorized intrusions, alert the operator, and allow an operator override.

At the federal level, several bills have been proposed that relate to autonomous vehicles and security. In July 2015, the Security and Privacy in Your Car Act (SPY Car Act) was introduced. The SPY Car Act seeks to launch a cross-sector investigation into vehicle cybersecurity. Among other things, under the SPY Car Act, NHTSA would be required to issue regulations that would require that vehicles with accessible data or control signals be equipped to detect, report and stop any attempts to intercept driving data or control the vehicle itself. The SPY Act was referred to and remains with the Committee on Commerce, Science and Transportation.

In November 2015, the Security and Privacy of Your Car Study Act of 2015, and the Autonomous Vehicle Privacy Protection Act of 2015 were proposed. The Car Study Act would require NHTSA to conduct a one year study, consulting with other government agencies and industry leaders as well as universities, to recommend a framework for regulating car automated software safety, cybersecurity and privacy regulations. The Autonomous Vehicle Act would require the U.S. Comptroller General to provide a public report that assesses the readiness of the DOT to address vehicle technology challenges, including consumer privacy protection. Both of these bills were referred to committees, and currently remain there. However, as explained below, it appears that much of what these bills propose is actually being undertaken by the NHTSA already.

The role of industry-led collaboration should not be discounted.

NHTSA and the Auto Industry Are Establishing Cybersecurity Guidelines

Federal law already requires NHTSA to issue Federal Motor Vehicle Safety Standards (FMVSS) and regulations to which manufacturers of motor vehicles must conform and certify compliance. NHTSA and the autonomous vehicle industry recognize the importance of cybersecurity and in the last several years have devoted considerable resources to developing recommended cybersecurity practices. In March 2016, the FBI, DOT and NHTSA put out a public service announcement warning the public and the automobile industry of cybersecurity vulnerabilities that exist in cars today and in the future.

Recognizing the possible risks autonomous and connected cars present, in 2012 NHTSA created a new division of Electronic Systems Safety Research to conduct research on the safety, security and reliability of complex, interconnected, electronic vehicle systems. The Electronics Council was also established to collaborate more broadly on these issues, and to reach out to other government agencies, vehicle manufacturers, suppliers, and the public to identify cybersecurity risks and develop best practices to inform any future federal policy and regulatory activities.

A year later, NHTSA released a preliminary statement on autonomous vehicles in an effort to help states in regulating. At that time, however, NHTSA noted that it believed that the regulation of the technical performance of automated vehicles was premature and did not want to stifle ''the evolution toward increasingly better vehicle safety technologies''.

Nevertheless, in 2014, NHTSA published four cybersecurity reports describing its initial work, which set the stage for cybersecurity guidelines that NHTSA is scheduled to release this month. In January 2016, the DOT and NHTSA issued policy guidance updating the Preliminary Statement of Policy Concerning Automated Vehicles, identifying certain initiatives that include the development of a best practices guide for the deployment of autonomous vehicles and a model state policy on automated vehicles. NHTSA has now proposed a model policy for the states to adopt so as to prevent a patchwork of state laws in the future and has identified which aspects of autonomous vehicle regulation should be left to the states' discretion.

Meanwhile, automakers established an Automotive Information Sharing and Analysis Center (Auto-ISAC) in 2015 to assist in the sharing of threat information. In July, the Auto-ISAC released an overview of comprehensive Automotive Cybersecurity Best Practices (''Best Practices'') to improve vehicle cybersecurity. Developed over a five month period, the Best Practices does not prescribe specific technical or organizational solutions, and are only recommendations that incorporate established cybersecurity resources and standards from organizations such as the International Organization for Standardization (ISO) and National Institute of Standards and Technology (NIST). The Best Practices include seven functions, each of which includes several recommendations around:

(1) governance;

(2) risk assessment and management;

(3) security by design;

(4) threat detection and protection;

(5) incident response;

(6) training and awareness; and

(7) collaboration and engagement with appropriate third parties.

The role of industry-led collaboration should not be discounted. Indeed, the newly released NHTSA guidelines outlines the need for ever greater collaboration within the sector and points to Auto-ISAC as a group to promote learning and information exchange.

In relation to concerns raised about DSRC technology, the DOT announced a commitment to developing advanced technologies that could enhance highway safety. Since 2014, NHTSA has been working on a rule addressing vehicle-to-vehicle communications technology standards, including safety, privacy and security issues. That rule is currently under review by the White House Office of Management and Budget.

One of the initiatives undertaken by NHTSA in the last year was to test the safety of DSRC technology designed to share the section of the radio spectrum reserved for vehicle safety applications such as Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communications. Moreover, during the last decade various organizations, including the Collision Avoidance Metrics Partnership (CAMP) and the Vehicle Safety Communications (VSC) consortium, have dedicated significant resources to ensuring DSRC is secure and protects privacy through the Security Credentials and Management System (SCMS), and via the establishment of security specifications.

In the highly anticipated NHTSA and DOT guidelines for autonomous vehicles released Sept. 20, the agency set out a framework rather than a prescribed set of safety regulations. The guidelines note that the ''identification, protection, detection, response, and recovery functions should be used to enable risk management decisions, address risks and threats, and enable quick response to and learning from cybersecurity events.'' DOT will utilize a 15-point security standard to independently evaluate each vehicle. Three of these points relate exclusively to data privacy and cybersecurity:

- ***Data Recording and Sharing***, requiring that manufacturers have a documented process for testing, validation, and collecting vehicle data;
- ***Privacy***, requiring that manufacturers protect consumer privacy by having privacy policies and practices that ensure transparency, choice, context, minimization of the retention of data, data security, and access to such data and accountability; and
- ***Vehicle Cybersecurity***, requiring that manufacturers and their suppliers have a fully-documented process that minimizes risks to safety due to cybersecurity threats and vulnerabilities.

In the explanatory notes of the new guidelines, the DOT and NHTSA make clear that the cybersecurity requirements relate to the entire supply chain in the design and development stages. As they note, ''manufacturers should insist that their suppliers build into their equipment robust cybersecurity features. Manufacturers should also address cybersecurity, but they should not wait to address cybersecurity until after they have received equipment from a supplier.'' Autonomous vehicle manufacturers will therefore have to set out that they have met such standards within the 15-point standard but also potentially that their suppliers have as well.

These new guidelines, while providing further guidance, are just the beginning to defining an exact set of cybersecurity practices that manufacturers and their suppliers will need to follow. As noted in a White House fact sheet issued on Sept. 20, NHTSA will continue to solicit feedback including through a public comment period, workshops, and expert review and update the guidelines annually. The DOT will also be releasing more specific but complementary cybersecurity best practices for the whole automobile industry in the near future.

Thus, the private sector and government stakeholders are attempting to take the necessary steps to ensure adequate security measures are in place prior to making autonomous vehicles available to the public.

Conclusion

Consumers' fears about the potential security issues that autonomous vehicles pose are valid. Fortunately, key government stakeholders and companies active in the autonomous vehicle industry are taking such concerns seriously and are working towards cybersecurity guidelines and privacy principles that could shape future regulations and alleviate such concerns. We will await to see whether the NHTSA safety standard puts a further spotlight on manufacturers and suppliers.

This does not mean autonomous vehicles will not be hacked once they are available to the public, but it does mean that a process is in place and moving forward to minimize such risks. Though there appears to be a concerted effort, time will tell whether federal and state governments can pass legislation that adequately addresses these cybersecurity concerns relating to autonomous vehicles before they become available to the public or if, as with other emerging technologies, lawmakers will be playing catch-up.

  PVLR ISSN 1538-3423