Brigham Young University Prelaw Review

Volume 32 Article 8

5-2018

Autonomous Cars and the Anonymous Threat: The Immediate Need for Cybersecurity Legislation for Self-Driving Vehicles

Forrest Albiston
forrest.albiston@gmail.com

Autonomous Cars and the Anonymous Threat: The Immediate Need for Cybersecurity Legislation for Self-Driving Vehicles

Forrest Albiston[1]

First, Andy's car fan turned on without him touching it. Soon, Andy lost control of the music, the wipers turned on with the windshield wiper fluid spraying, and the engine shut off. In the middle of the freeway, Andy Greenberg's 2014 Jeep Cherokee had been hacked. Eventually, Andy regained control of his vehicle and quickly pulled over, shouting expletives. Fortunately for Andy, this was a journalistic experiment. The men hacking into the vehicle's systems were not actually making an attempt on his life.[2] But not all hackers have such good intentions.

The Jeep Cherokee, like many vehicles, was accessible to remote hackers because of new and innovative technologies used by many car companies, such as Chrysler's Uconnect system.[3] Some cars come with special cruise control features that help the car stay inside lanes autonomously.[4] For example, Tesla

---

1 Forrest Albiston is a junior at Brigham Young University studying international relations. He plans on attending law school in fall 2019. He wishes to thank the generous efforts of his editors Clarissa McIntire and Garret Meisman. He also wishes to thank the editing board and Kris Tina Carlston for all their help and hard work.

2 Andy Greenberg, *Hackers Remotely Kill Jeep on the Highway—With Me in It*, Wired Mag. (July 2015), https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/.

3 *Id*.

4 *2018 Corolla Features*, Toyota, https://www.toyota.com/corolla/corolla-features/(last visited Jan. 24, 2018).

has been testing an autopilot feature for its vehicles. Uber and Google are testing and supporting self-driving cars.[5] Companies are integrating more technology into cars today than ever before.

Despite technology's benefits, there are always pitfalls. For example, drones have changed the way wars are fought and scientific research is conducted. While drones can be very useful, they have also caused problems for airports and for firefighters combatting forest fires. Drone regulation had to catch up with technology instead of being ahead of it and as a result, the rising industry has had many setbacks. This is the same problem that self-driving cars face: lack of preemptive legislation.

As cars become smarter, there is a need for legislation to ensure the safety and privacy of the American people. We can better understand the threats to vehicle cybersecurity by reviewing past and upcoming legislation, gaining a better understanding of cybersecurity and vehicles, considering possible attackers, and looking at cybersecurity assessments. These insights show the immediate need to fill the legislative hole regarding smart and self-driving vehicles.

Though legislation on the cybersecurity of automated vehicles is largely unprecedented, the advent of smarter and self-driving cars requires the federal legislature to take greater action. To protect consumers from quickly rising cybersecurity threats, the SPY Car Act of 2017 should be immediately enacted with a few changes to its wording and with added definitions to cybersecurity measures. [6]

Part I of this paper will provide background information on the development of the SPY Car Act. Part II will review past legislation on automated vehicles, including acts that are pending before Congress. Part III will consider legislation on drones, a similar technology to smart and self-driving vehicles,

5 Mike Isaac, *Uber Strikes Deal With Volvo to Bring Self-Driving Cars to Its Network*, N.Y. Times (Nov. 20, 2017), https://www.nytimes.com/2017/11/20/technology/uber-deal-volvo-self-driving-cars-.html.

6 SPY CAR Act of 2017, S. 680, 115th Cong. (2017).

as well as the overall status of automated vehicle cybersecurity. Part IV will discuss cybersecurity threats and the difficulties of assessing cybersecurity. Part V will provide an overview of the current cybersecurity status of automated vehicles, while Part VI will give an overview of the SPY Car Act of 2017, and Part VII will recommend alterations to the act. Finally, Part VIII will review the positive and negative aspects of the act and Part IX will review recommended changes to the SPY Car Act as well as the consequences of and immediate need for the act.

I. Background

Many parts of the infrastructure of modern cars are vulnerable to attacks. Electronic engine transmission systems, Bluetooth devices, airbags, keyless entry, and even the driver's phone are just a few of the systems that can be used as entry points for a cyber-attack.[7] As technology advances, cars have more and more electronic parts, including tire air pressure sensors. These pieces are vulnerable and require cybersecurity.[8]

Cybersecurity has many components. According to the National Institute of Standards and Technology, those components include identification, protection, detection, response, and recovery.[9] Identification of threats helps companies manage and prioritize cybersecurity risks.[10] The protection of entry points requires the development of safeguards to defend the infrastructure of a system.[11] Detection involves identifying

7 David Clare ET AL, Automotive Security Best Practices 5-7 (Intel, 2015). https://www.autobeatdaily.com/cdn/cms/Intel%20auto%20security%20white%20paper-1.pdf.

8 *Id.*

9 National Institute of Standards and Technology, Framework for Improving Critical Infrastructure Cybersecurity (1.1 ed. 2017). https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf.

10 *Id.*

11 *Id.*

a cybersecurity threat as it is occurring. Then, the response component is to act against the detected threat.[12] Finally, recovery involves repairing any damaged systems from the threat and ensuring that it doesn't happen again.[13] These steps are the basics to ensure that companies and people stay secure. The SPY CAR Act, currently under review in the Senate, focuses on implementing these steps as cybersecurity standards for modern vehicles.[14]

In 2013, Senator Ed Markey of Massachusetts learned about the increasing need for vehicle cybersecurity. Senator Markey then began writing to car manufacturers to discuss what was being done to implement cybersecurity in their vehicles. In July 2015, Charlie Miller and Chris Valasek—two hackers who research carjacking—worked with *WIRED* magazine to show the vulnerability of Chrysler vehicles to remote hacking.[15] That same month, Senator Markey introduced the SPY Car Act of 2015.[16] Miller and Valasek later published more about the vulnerability of Chrysler vehicles.[17] During this time, the SPY Car Act was revised and, in 2017, it was reintroduced in the Senate as the SPY Car Act of 2017.[18]

The SPY Car Act is not the only self-driving car act to be introduced. The SELF DRIVE Act was introduced in 2017 as well.[19] This act focuses more on informing consumers of the

12 *Id.*

13 *Id.*

14 SPY CAR Act of 2017, S. 680, 115th Cong. (2017).

15 Andy Greenberg, *Hackers Remotely Kill Jeep on the Highway—With Me in It*, WIRED MAG. (July 2015), https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/.

16 SPY CAR Act of 2015, S. 1806, 114th Cong. (2015).

17 Andy Greenberg, *The Jeep Hackers Are Back To Prove Car Hacking Can Get Much Worse*, WIRED MAG. (August 2016), https://www.wired.com/2016/08/jeep-hackers-return-high-speed-steering-acceleration-hacks/.

18 SPY CAR Act of 2017, S. 680, 115th Cong. (2017).

19 SELF DRIVE Act, H.R. 3388, 115th Cong. § 30130(a) (2017).

ability of automated vehicles and very little on cybersecurity. There are also other state laws regarding self-driving cars, but those laws regulate the rules of testing these vehicles on the road and keeping people safe during tests. Arizona has an executive order that states necessary precautions should be taken when testing self-driving vehicles.[20] California has the most laws governing self-driving vehicles, including regulations like permits to test vehicles and reporting accidents within ten days.[21] Those regulations do not go into cybersecurity, as they are not designed to govern the purchase of such vehicles, just testing them. For this reason, this review will focus mainly on the SPY Car Act, while also briefly discussing similar technologies and the SELF DRIVE Act to highlight areas of improvement.

II. Similar Legislation

The SELF DRIVE Act[22] is another act of Congress that has yet to pass. The act focuses on ensuring the safety of those using self-driving vehicles and takes into consideration cybersecurity. It is not, however, very descriptive when it comes to stating what automakers' responsibilities would be. The act requires automakers to have a written cybersecurity plan that includes preventing foreseeable intrusions, limiting access to driving systems, and making sure there is a director of cybersecurity in the company.[23] While these are prudent regulations, they make up only a small section of the act.

This small section cannot possibly cover the expanse of cybersecurity threats in modern vehicles. Much more

20 Office of the Gov. Doug Ducey, *Executive Order 2015-09: Self-Driving Vehicle Testing and Piloting in the State of Arizona; Self-Driving Vehicle Oversight Committee* (2015), https://azgovernor.gov/file/2660/download?token=nLkPLRi1.

21 Cal. Veh. Div. 16.6 Autonomous Vehicles [38750-38755].

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

23 SELF DRIVE Act, H.R. 3388, 115th Cong. § 30130(a) (2017).

is needed to protect against threats than to state that unauthorized intrusions should be identified, assessed, and mitigated. Such a statement is obvious and provides no real standard for these vehicles. Most automakers already meet these minimum requirements; the purpose of adding the requirements to the SELF DRIVE Act is to ensure a standard of safety to protect not only the consumer, but automakers as well.

Another problem with the SELF DRIVE Act is that it is designed for highly automated vehicles. Because that phrase—"highly automated vehicles"—is largely subject to interpretation, it could be assumed that Andy Greenberg's Jeep did not fall under the highly automated vehicle category. That car only had limited computer capabilities, but it was still hacked into and had its engine shut down. This illustrates how the SELF DRIVE Act is insufficient for the cybersecurity needs of the American people.

The final problem with the SELF DRIVE Act is that it allows automakers to make their own regulations. The Act states that a manufacturer cannot sell an automated or partially automated car "unless such manufacturer has developed a cybersecurity plan that includes . . . a written cybersecurity policy."[24] Some automakers will likely do the bare minimum for the cybersecurity of their vehicles, then point to the law if their cybersecurity protections are challenged. While the law should protect automakers, not just consumers, there should be a higher standard set so all automakers provide more comprehensive protection.

Other legislative efforts on self-driving cars focus on testing regulations. These laws are not significant when considering the cybersecurity needs of self-driving cars. States like California and Arizona have approved testing on their roads and have terms and conditions as stated above.

III. Parallel Technologies

Other breakthrough technologies have also had regulation

24 *Id.*

problems that are a public safety concern. Drones are a prime example of a technology that is not yet regulated well.[25] Lack of regulation resulted in consumers flying drones into buildings and getting drones in the way of helicopters and other manned aircraft.[26] While a few general guidelines are in place, they are not extensive, and the FAA is overwhelmed and far behind on legislation.[27]

Yet, there are some regulations. In 2007, for example, commercial use of drones was banned in certain areas where a federal appeal was needed to use drones commercially.[28] Journalists were also banned from using drones.[29] These blanket ban regulations, passed because progressive legislation is lacking, have hurt the journalism industry and its technological progression. While regulation is needed, just banning something will not resolve the problem. This type of regulation pushes the problem to a future date to be solved. In 2013, Amazon announced plans for drone delivery.[30] This has still not been implemented, and the United States is falling behind other countries on these types of advancements due to lack of regulation.

It is important to have regulations and to not fall behind these new technologies so that years later commercial industries are not struggling to advance. It is also important to have these regulations to protect people from the dangers that can come from new technology. In the case of drones, those dangers include people getting hurt or getting in the way of other flying vehicles. Like drones, self-driving cars are

25 Troy A. Rule, *Drone Zoning*, 95 N.C.L. 133 (2016) (discussing drone regulations and need for specific laws).

26 Arthur Holland Michel and Dan, *Drone Incidents: A Survey of Legal Cases,* Center for the Study of the Drone at Bard College (April 2017), http://dronecenter.bard.edu/files/2017/04/CSD-Drone-Incidents.pdf.

27 Troy A. Rule, *Drone Zoning*, 95 N.C.L. 133 (2016).

28 *Id.*

29 *Id.*

30 *Id.*

still a new technology, and regulations can still be made that will still allow the industry to not fall behind, but advance and keep people safe. Regulations in cybersecurity are an important step in achieving safety for self-driving cars.

IV. Current Threats

An important part of understanding the cybersecurity threat to vehicles is understanding where it came from. There are different types of people who would like to hack into a vehicle. Understanding who they are, the threats they pose, and their motives is important context to protecting vehicles.[31]

The first and most dangerous threat comes from other nations. There are many reasons another nation would want to hack into the cars of US citizens: spying, tracking, gathering data about driver habits, causing harm to drivers, disrupting transportation grids, economic chaos, etc. Cyberwarfare can be waged and people can be killed by hackers shutting off braking systems, driving into other cars, etc. There are many ways that other countries can use a cybersecurity breach in a vehicle.[32]

Organized crime groups also pose a threat to vehicle cybersecurity. Whether it be terrorists, gangs, or the mafia, these groups can cause harm to drivers. This category has the broadest spectrum of reasons for committing crimes, and they are a significant threat to the American public. Spying, killing, and threatening are all crimes that organized groups could commit. While they lack the same resources that a nation-state usually does, they are not to be disregarded.[33] Cars have been used in several

31 David Clare ET AL, Automotive Security Best Practices 5-7 (Intel, 2015).

32 *Id.*

33 *Id.*

terrorist attacks, most recently in New York City.[34] If terrorists could control the car without being inside, or turn someone else's car into a weapon, it would be a manageable attack on a country.[35]

The third group, pranksters and hacktivists, pose a much smaller threat. Pranksters pose a small threat, as many pranks are harmless. However, their pranks sometimes go awry and people do get hurt and even die. Hacktivists are often part of a larger community that tries to keep an open forum on hacks. That forum helps build up defense and show automotive companies what their cars' cybersecurity weaknesses are.[36] In 2016, President Obama put out an executive order encouraging private companies to have open forums to help speed along the development of diagnosing cybersecurity risks and protections.[37] This can still be a threat when pranksters, organized crime, and terrorists obtain the data and use it before the appropriate changes are made to defend against it.[38]

The final group is the owners of the vehicles themselves. Vehicle owners have various reasons for hacking their own vehicles, including cheating emissions tests and overriding governors (devices used to regulate speed) to get the most out of their vehicle. These owners are usually trying to make their cars go faster, handle better, etc.[39] This overriding can be dangerous as owners may not know exactly what they are doing or what the consequences of removing certain electronic barriers are. It can also make their vehicles more susceptible to cyberattacks

34 Jonathan Wolfe, *New York Today: A Terror Attack in Manhattan*, N.Y. Times (Nov 1, 2017), https://www.nytimes.com/2017/11/01/nyregion/new-york-today-terror-attack-manhattan.html.

35 David Clare ET AL, Automotive Security Best Practices 5-7 (Intel, 2015).

36 *Id.*

37 Exec. Order No. 13,691, 3 C.F.R. § 271 (2016).

38 David Clare ET AL, Automotive Security Best Practices 5-7 (Intel, 2015).

39 *Id.*

and therefore more dangerous when they are on the road.[40]

V. Cybersecurity Today

To draw attention to the imminent threat that hacking poses, *WIRED* journalist Andy Greenberg planned to be hacked by two hacking researchers as part of an investigative journalism article.[41] This hacking demonstration showed that the 2014 Jeep Cherokee and many other Chrysler vehicles were vulnerable, and forced a massive Chrysler recall[42] so the automaker could patch the system and make it safer. These same hackers also inspired Senator Markey,[43] who began conducting cybersecurity research.

In 2014, Senator Markey began conducting this research on the current cybersecurity status of vehicles.[44] He found that almost all vehicles with some sort of wireless technology were vulnerable, most automakers were unaware of security risks to their vehicles, and only two automakers could describe how they respond to risks in real time. He discovered that most of the measures used to prevent hacking could not do so in real time and were not designed to—a cause for serious concern.[45] He also found that manufacturers collect large amounts of driving data, often without consumer knowledge.[46]

40 *Id.*

41 Andy Greenberg, *Hackers Remotely Kill Jeep on the Highway- With Me in It*, Wired Mag. (July 2015), https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/.

42 Andy Greenberg, *After Jeep Hack, Chrysler Recalls 1.4M Vehicles For Bug Fix*, Wired Mag. (July 2015), https://www.wired.com/2015/07/jeep-hack-chrysler-recalls-1-4m-vehicles-bug-fix/.

43 Ed Markey, Tracking & Hacking: Security & Privacy Gaps Put American Drivers at Risk (2015), https://www.markey.senate.gov/imo/media/doc/2015-02-06_MarkeyReport-Tracking_Hacking_CarSecurity 2.pdf.

44 *Id.*

45 *Id.*

46 *Id.*

In response to Senator Markey's published findings, Intel started designing ways to improve vehicular cybersecurity according to the senator's goals.[47] The Intel White Pages explain that modern cars, not just self-driving ones, have over 100 electronic control units.[48] These units need to be secured against an attack or the car itself becomes vulnerable, unless the unit was designed to make vital parts of the vehicle inaccessible. This has not always been the case and was one of the recommendations for advancing vehicle cybersecurity. This means there are currently over 100 parts of a car that can be susceptible to a cyberattack.

These findings indicate that there is a serious problem with automobile cybersecurity and that car manufacturers are doing little about it. When left to their own devices, car manufacturers are not motivated to do enough, which was the problem with the SELF DRIVE Act. Manufacturers need standards to be accountable for ensuring consumer safety. Without these standards, the problems that Senator Markey found in his research will continue. The Intel White Pages, while a step in the right direction, are just good ideas and not industry standards. For this reason, Senator Markey introduced the SPY Car Act of 2015,[49] which he later revised and reintroduced as the SPY Car Act of 2017.[50]

VI. SPY Car Act

The SPY Car Act of 2017 directs the National Highway Traffic Safety Administration (NHTSA) to create cybersecurity laws that automakers must follow. Those laws are to include electronic controls to manage how and when driving data is collected and stored. The next portion is to have a cyber dashboard attached to the vehicle so it can visibly be seen how the vehicle is equipped

47 David Clare ET AL, Automotive Security Best Practices 5-7 (Intel, 2015).

48 David Clare ET AL, Automotive Security Best Practices 4 (Intel, 2015).

49 SPY CAR Act of 2015, S. 1806, 114th Cong. (2015).

50 SPY CAR Act of 2017, S. 680, 115th Cong. (2017).

to deal with cybersecurity threats and the owner's privacy.[51]

One voiced concern with the act regards the cyber dashboard.[52] The issue here is that if everyone can constantly see what protective measures have been taken, hackers might find it easier to get around them. The dilemma is that consumers should know how they are protected, without hackers knowing what protective measures have been taken against them. The cyber dashboard only shows how far beyond the standards the manufacturer went, and will not actually reveal cybersecurity secrets that protect the vehicle. A consumer has the right to know what protection they have, and it will still be difficult to hack into the vehicle despite an idea of the added protections. This makes the cyber dashboard worth the minimal potential risk it poses.

The act also requires the Federal Trade Commission to ensure that manufacturers notify consumers about data collected, provide consumers the option to terminate this data collection, and prohibit the data from being used for marketing purposes without permission. These regulations do not include black box data collection, which is important during crashes.[53]

The act also sets forth some important cybersecurity guidelines. First, all entry points in a vehicle must be protected against hacking. Second, critical and non-critical software systems need to be isolated. Third, all measures must be updated based on the NHTSA evaluations. Next, the data collected must be secured against cyberattacks. Finally, vehicles must be able to detect, report, and respond to imminent threats.[54]

51 *Id.*

52 Kristen Hall-Geisler, *Senators Reintroduce a Bill to Improve Cybersecurity in Cars*, Tech Crunch (Mar. 2017), https://techcrunch.com/2017/03/23/senators-reintroduce-a-bill-to-improve-cybersecurity-in-cars/.

53 SPY CAR Act of 2017, S. 680, 115th Cong. (2017).

54 *Id.*

VII. Needed Alterations

The act in its current form proposes several necessary regulations of self-driving vehicles, but the vague wording of some sections could cause problems in the future if not changed.

The first area of vague wording that needs to be changed is "reasonable measures."[55] As it stands, the current wording, "to be equipped with reasonable measures of protection," can be interpreted in many ways and does not ensure a clear standard for protection. "Reasonable measures" should be replaced with a standard set of measures. This would ensure that car companies follow the NHTSA standards for cybersecurity.

These standards should be written into the act and used to clarify the meaning of "reasonable measures." This clarification should be based on the current best standards brought forth by Intel in their white pages, but should focus specifically on vehicular cybersecurity. These include:

- Security techniques – Message Authentication Codes
- Trusted Platform Module
- Systems and software engineering – Software life cycle processes
- Evaluation criteria for IT security
- Functional safety for road vehicles
- Information Security Management System
- Code of Practice – Security
- Code of Practice – Handling PII / SPI (Privacy)
- Application security techniques
- Privacy architecture framework
- Software testing standard
- Industrial Network and System Security
- Dedicated Short Range Communication (DSRC) Minimum Performance Requirements
- Cybersecurity Guidebook for Cyber-Physical Vehicle

55 *Id.*

Systems
- Requirements for Hardware-Protected Security for Ground Vehicle Applications[56]

This is only part of the list that Intel provides. There should be further research to see if other standards should be added.

The next vague phrasing in the SPY Car Act says that measures "shall be evaluated for security vulnerabilities."[57] Part D of the Act says that all other parts should be updated based on this evaluation. The problems here lie in the questions of who checks the evaluation, how often should it be checked, and who is being evaluated. Manufacturers should be evaluating their vehicles and standards. The NHTSA should then evaluate this process.

The evaluation by automakers, per part D, should be sent to the NHTSA. This can be a method for reporting the results of this kind of testing to hold manufacturers accountable. If it is the first evaluation and there are problems, then the NHTSA can respond saying that that vehicle is not fit for the road. If the vehicle passes all tests the first time, no more evaluations would be needed.

These evaluations should be done with every new vehicle on the automaker's side, as well as once a year, ensuring that no new weaknesses have been discovered. They should also be re-evaluated if a potential weakness has been shown or an attack has taken place. The NHTSA should also yearly review all its standards ensuring that the "best security practices"[58] are the standard.

The final vague section parallels the problem of "reasonable measures." It says that vehicles should be "reasonably secured."[59] Again, this language is vague and its meaning is up to interpretation. The phrase should be changed or clarified to reflect that it follows the standards

56 David Clare ET AL, Automotive Security Best Practices, 16 (Intel, 2015).

57 SPY CAR Act of 2017, S. 680, 115th Cong. (2017).

58 *Id.*

59 *Id.*

created under this act. This clarification will ensure the law is clearly protecting both consumers and manufacturers.

VIII. Implications

One negative aspect of this act is that it requires manufacturers to do more. While this does provide safety and privacy, the increased workload, parts, departments, development, and possibly employees will likely drive up prices on vehicles. This will increase many people's expenses as vehicles become increasingly more expensive to maintain and eventually need to be replaced.

Another negative aspect of this act is that it will take time to get the standards set and followed by car companies. This act will not have final regulations for three years—a long time, considering that Senator Markey's research showed problems back in 2014. This timing means that if the act passes this year, 2018, there will be regulations by 2021. Vehicular cybersecurity is a national security threat, since cars are ubiquitous. Everyone is surrounded by vehicles. This means that everyone is at risk to foreign and domestic attacks. Although it is hard to speed up this research and standard making, it is important that the act be passed quickly so manufacturers can adopt the national cybersecurity standards as quickly as possible.

There are many positive sides of this act. The act will set standards for safety and ensure consumer privacy. Cyberwarfare is a reality (there are even jobs in the Air Force dedicated to cyberwarfare).[60] The safety of United States citizens should not be taken lightly. Cybersecurity of the cars Americans use every day is indeed a national security issue.

60 Air Force Careers: Computers & Computer Science, https://www.airforce.com/careers/browse-careers/computers-computer-science (last visited Jan. 25, 2018).

The act will keep people safer and help them decide what data collected about them is shared with the world. These protections also profit both consumers and manufacturers.

IX. Conclusion

With self-driving cars quickly advancing, it is important to adapt federal law to protect this new technology. The lack of legislation governing drone use has shown the need for legislation to not fall behind on rapidly developing technologies, including self-driving cars. Self-driving and smart cars will be an asset to society: they can help the disabled and the elderly, and they can be a convenience to many people. However, without laws to govern cybersecurity, self-driving cars can be a hazard to all who are on the road. The SPY Car Act can provide some of that necessary cybersecurity legislation to prevent hazards. Some safety concerns associated with self-driving cars cannot be avoided, as with all vehicles, but the act will increase security measures to eliminate many of those safety concerns. The SPY Car Act needs to be amended and passed immediately to ensure the safety of United States citizens.