Michigan Telecommunications and Technology Law Review

Volume 23 | Issue 2

2017

New Threats to Vehicle Safety: How Cybersecurity Policy Will Shape the Future of Autonomous Vehicles

Caleb Kennedy
University of Michigan Law School

NOTE

NEW THREATS TO VEHICLE SAFETY: HOW CYBERSECURITY POLICY WILL SHAPE THE FUTURE OF AUTONOMOUS VEHICLES

Caleb Kennedy

Cite as: Caleb Kennedy, Note,
New Threats to Vehicle Safety: How Cybersecurity Policy Will Shape The Future Of Autonomous Vehicles,
23 MICH. TELECOM. & TECH. L. REV. 343 (2017).
This manuscript may be accessed online at repository.law.umich.edu.

ABSTRACT

This note assesses the threat that hacking and related cybersecurity issues will pose to autonomous vehicles. Given the sweeping safety benefits autonomous vehicles will potentially bring to society, protecting against hacking and cyber-threats must be one of the top priorities for industry and public safety officials if autonomous vehicles are to gain widespread acceptance in the market. It proposes a framework for how these concerns should be addressed and how we can mitigate the risks. It addresses both proactive and reactive measures that can be taken by manufacturers, how to incentivize these measures, and the role cyber-insurance can play in filling the remaining risk gaps.

INTRODUCTION

As autonomous vehicle ("AV") technology continues to advance at a breakneck pace, safety is at the forefront of many people's minds.[1] With over 35,000 traffic fatalities each year, AVs have the potential to dramatically improve road safety and save countless lives.[2] This is not inevitable, however, given that autonomous – and often highly interconnected – electronic navigation systems will raise new safety threats of their own.[3] These

1. In one survey, 62% of respondents feared their future vehicles would be easily hacked. Jonathan Vanian, *Should You Worry About Your Car Being Hacked?*, FORTUNE (Mar. 2, 2016), http://fortune.com/2016/03/02/public-car-hacking/.

2. NHTSA, TRAFFIC FATALITIES UP SHARPLY IN 2015 (Aug. 19, 2016), https://www.nhtsa.gov/press-releases/traffic-fatalities-sharply-2015; James Anderson, et al., *Autonomous Vehicle Technology: A Guide for Policymakers*, RAND (Aug. 29, 2016), http://www.rand.org/pubs/research_reports/RR443-2.html.

3. While no one has yet reported a real-world safety incident involving a malicious hack of a vehicle, researchers have demonstrated their vulnerabilities. *See* FBI, FBI PUBLIC SERVICE ANNOUNCEMENT: MOTOR VEHICLES INCREASINGLY VULNERABLE TO REMOTE EXPLOITS (Mar. 17, 2016), https://www.ic3.gov/media/2016/160317.aspx.

threats could range from sophisticated hackers attempting to gain control over an entire network of AVs, or a lone criminal taking advantage of the predictability of the new systems.[4]

One of the hacking incidents that highlights the type of hacking safety officials fear most involves a Jeep Cherokee in 2015. While the Jeep was driving down the interstate at 70 m.p.h., hackers took over vehicle functions as innocuous as the windshield wipers to disabling the accelerator, causing the vehicle to slow to a halt on a crowded interstate highway.[5] All of this was possible by remotely hacking its Uconnect system, an onboard computer that is installed in hundreds of thousands of Fiat-Chrysler vehicles that is intended to control only its entertainment and navigation features.[6] The hackers in this incident were located 10 miles away; but their use of cellular data as a hacking entry point meant they could have potentially reached vehicles across the country.[7] While this hack occurred in a non-autonomous vehicle, the risks will only be amplified as cars become more connected and when there is nobody in the driver's seat to attempt to retake control of a hacked vehicle.[8]

While conventional vehicles can protect themselves by simply limiting connections to the outside world, AVs will not have that luxury. AVs inherently require an array of sensors communicating with other vehicles and infrastructure, and with these additional connections comes added hacking risk. As a result, addressing the new safety threats presented by AVs is a top priority for consumer safety advocates, regulators, and industry officials.[9]

This note argues that specific steps need to be taken now to properly address these new threats. Part I proposes proactive measures that should be implemented. I emphasize the importance of segmenting critical systems and layering security protocols during the initial design process of the vehicles, while also equipping them with robust anti-hacking software. Part II ad-

4. A study from the London School of Economics found that aggressive drivers will be able to take advantage of autonomous vehicles and bully them all over the road. London Sch. of Econ. & Pol. Sci., *Automotive Vehicles: Negotiating a Place on the Road. A Study on How Drivers Feel About Interacting with Autonomous Vehicles on the Road* (2016), http://media.wix.com/ugd/efc875_213cef837dbb42169f6061f585606b46.pdf.

5. At others points in the hack they were able to disable the breaks and track the vehicle using its GPS system. Andy Greenberg, *Hackers Remotely Kill a Jeep on the Highway – with Me in It*, WIRED (July 10, 2017), https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/.

6. Uconnect offers a Wi-Fi hotspot and is connected to Sprint's cellular network, which allows for remote hacking. Once they gained entrance, they rewrote the firmware to take control of critical vehicle functions such as acceleration and braking. *Id.*

7. *Id.*

8. At one point, the hacking victim was able to regain control of the braking function by turning off and turning back on the engine. *Id.*

9. Rob Toews, *The Biggest Threat Facing Connected Autonomous Vehicles is Cybersecurity*, TECHCRUNCH (Aug. 25, 2016), https://techcrunch.com/2016/08/25/the-biggest-threat-facing-connected-autonomous-vehicles-is-cybersecurity/.

dresses the reactive measures that should be put in place, namely an industry-wide information-sharing network that will be essential in reporting and responding quickly to new safety threats as they emerge. But even with the best proactive and reactive systems in place, some safety risks will inevitably remain. In Part III, I propose cyber-insurance as a key, long-term measure in managing this residual risk.

Part I: Proactive Measures

The National Highway Traffic Safety Administration ("NHTSA") is the primary vehicle regulatory body in the U.S. It defines vehicle hacking as the "unauthorized access to vehicle systems for the purposes of retrieving driver data or manipulating vehicle functionality."[10] White-hat researchers have hacked both autonomous and non-autonomous vehicles on numerous occasions, giving us a better sense of the vulnerabilities that currently exist.[11] In one prominent example, NHTSA purchased an unaltered model-year 2014 vehicle directly from a dealer and attempted to hack into various electronic systems. The results, which were published in a 2015 white paper, revealed that, at low speeds (5-10mph), hackers could remotely shut down the engine, disable the vehicle's brakes, and take control over the steering; and at any speed, hackers could remotely take control over systems including door locks, turn signals, tachometer, radio, HVAC, and GPS.[12]

As a result of this test case, NHTSA determined that the vulnerabilities presented an unreasonable risk to safety given that: (1) they allowed access to and manipulation of critical vehicle control systems; (2) the population of vehicles potentially at risk is enormous; and (3) the likelihood of exploitation is substantial given that researchers were scheduled to publish the bulk

---

10. FBI, Public Service Announcement: Motor Vehicles Increasingly Vulnerable to Remote Exploits (Mar. 17, 2016), https://www.ic3.gov/media/2016/160317.aspx. (I would propose hacking be defined more broadly, particularly to include manipulation of AV sensors like the carjacking hypothetical mentioned above.)

11. Allyson Versprille, *Researchers Hack Into Driverless Car System, Take Control of Vehicle*, Nat'l Def. (May 2015), http://www.nationaldefensemagazine.org/archive/2015/May/Pages/ResearchersHackIntoDriverlessCarSystemTakeControlofVehicle.aspx (researchers at UVA successfully hacked into and took control of an AV); Andy Greenberg, *The Jeep Hackers are Going Back to Prove Car Hacking Can Get Much Worse*, Wired (Aug. 1, 2016), https://www.wired.com/2016/08/jeep-hackers-return-high-speed-steering-acceleration-hacks/ (in 2011, researchers from the University of Washington and University of California-San Diego wirelessly hacked into Jeep vehicles); Kevin Poulsen, *Hacker Disables More Than 100 Cars Remotely*, Wired (Mar. 17, 2010), https://www.wired.com/2010/03/hacker-bricks-cars/ (in a non-research setting, a disgruntled employee at a car dealership hacking into a third party device). *See also* Nat'l Highway Traffic Safety Admin., DOT HS 812 076, Assessment of the Information Sharing and Analysis Center Model (Oct. 2014) (providing a longer list of recent hacks).

12. Chris Valasek & Charlie Miller, *Remote Exploitation of an Unaltered Passenger Vehicle: Technical White Paper*, IOActive Security Services (2015), http://www.ioactive.com/pdfs/IOActive_Remote_Car_Hacking.pdf.

of their work product.[13] NHTSA's test resulted in one of the first major cybersecurity-related vehicle recalls, totaling almost 1.5 million vehicles.[14] In this section, I explain how certain aspects of AVs make them especially susceptible to this type of electronic hacking. As the number of AVs on the road increases, this theoretical hacking threat may become a very real safety threat to every driver on the road.

Part of the threat comes from the increasing interconnectedness of AVs. Internally, nearly all modern automobiles link all of a vehicle's systems and features into one central computer.[15] AVs have the added risk of often being linked to other vehicles, outside infrastructure, or third-party devices.[16] Some of the core benefits of AVs are derived from having a more interconnected fleet through Vehicle-to-Vehicle ("V2V") and Vehicle-to-Infrastructure ("V2I") communication – allowing for a reduction in vehicle collisions and more efficient transportation through concepts such as platooning.[17] Yet, each additional connection is also an additional path in for hackers.

The overall attack surface of newer vehicles is staggering. Within a single car, there can be up to 100 separate and interconnected Electronic Control Units ("ECUs"), each controlling a separate vehicle function, and over 100 million lines of code.[18] Further complicating this, no single entity even owns all of this code, given that a myriad of parts manufacturers provide the individual components of each vehicle.[19]

For example, insurance companies offer dongles that are plugged into a port under a car's dashboard (measuring speed, rapid-breaking incidents, etc.

---

13. *See* FBI, *supra* note 3.

14. "Prior to the research or recall being released, the cell phone network implicated proactively blocked access to a specific port that was used to communicate with other vehicles. Part of the recall involved sending a USB drive to owners of the affected vehicles which contained the security updates. Owners who wished not to manually install the updates were given the option of bringing the vehicle into the dealer." *Id.*

15. *See* FBI, *supra* note 3.

16. One estimate suggests that by 2020, 70 million of the 90 million vehicles projected to ship that year will be connected to an outside network. Kristen Hall-Geisler, *Even Your Connected Car Will Need Antivirus Software*, TechCrunch (May 2, 2016), https://techcrunch.com/2016/05/02/even-your-connected-car-will-need-antivirus-software/.

17. Platooning is the coupling of multiple AVs on a roadway, such that they brake and accelerate simultaneously, allowing for a decrease in distance between cars and trucks. This can both increase the capacity of roads and reduce fuel consumption. Platooning requires wireless communication of each vehicle's position on the road, speed, trajectory, etc. in order to calibrate the platoon's overall movement and ensure the vehicles don't collide. More broadly this could be used outside of platooning; if your vehicle knows the speed/trajectory of other vehicles on the road, they can avoid collisions. James Anderson, et al., *Autonomous Vehicle Technology: A Guide for Policymakers*, Rand (2016), http://www.rand.org/pubs/research_reports/RR443-2.html.

18. Toews, *supra* note 9. For comparison, Facebook has 60 million lines of code and the Large Hadron Collider has 50 million lines. Doug Newcomb, *Could an Open-Source Approach Make Cars Hacker-Proof?*, PC Mag (Jan. 29, 2016), http://www.pcmag.com/article2/0,2817,2498566,00.asp.

19. Newcomb, *supra* note 18.

to study driver risk), while other devices are billed as providing safety features, improved fuel economy, or additional conveniences.[20] Devices such as these that have internet or cellular access and are plugged into diagnostic ports compound this threat, and hackers see these devices as an even softer target than the vehicle itself.[21] Any device that communicates with the outside world would give hackers yet another potential avenue to inject malware into a car's internal network.[22] NHTSA should continue to hold third-party device producers to the same standard as vehicle manufacturers, and both the proactive and reactive measures I propose below should apply equally to third-party device manufacturers.

Hacking vehicles through these outside connections has been a major concern flagged by NHTSA. With the help of the Defense Advanced Research Projects Agency ("DARPA"), regulators have begun to strategize ways to ensure that these communications are secure and protected against potential hacking.[23] One approach would be to protect cars by treating them like a layered network of computers, providing "anti-virus" software to protect individual ECUs (like the steering or braking ECU) with individual firewalls, as well as software that monitors the network as a whole, detecting abnormalities and isolating any threats.[24] In addition to protective software systems such as this, NHTSA's latest automotive cybersecurity guidance addresses other, more structural ways to prevent outside hacks from occurring.

The first, known as segmenting, generally involves separating internal systems when possible (so that a breach of one does not lead to a breach of the system as a whole).[25] This is accomplished through limiting diagnostic

---

20. Hall-Geisler, *supra* note 16.

21. Third-party devices range from the popular vehicle-monitoring devices used by insurance companies, to novel devices like the Comma One that add AV-like features to older cars. The Comma One has drawn scrutiny from NHTSA, and was subsequently withdrawn from the market following a standard safety inquiry from regulators. NAT'L HIGHWAY TRAFFIC SAFETY ADMIN., SPECIAL ORDER DIRECTED TO COMMA.AI (Oct. 27, 2016), https://www.scribd.com/document/329218929/2016-10-27-Special-Order-Directed-to-Comma-ai.

22. Hall-Geisler, *supra* note 16.

23. NHTSA and its partners are developing a Public Key Infrastructure (PKI) based system, termed the "Security Credential Management System" (SCMS), for ensuring trusted and secure V2V and V2I communications. PKI security architectures and methodologies are already used extensively in the auto industry. The SCMS would employ highly innovative methods, encryption, and certificate management techniques to address the challenging task of ensuring trusted communications between entities that previously have not encountered each other—but also wish to remain anonymous (as is the case when vehicles/drivers encounter each other on the road). *See* J. Harding, et al., *Vehicle-to-Vehicle Communications: Readiness of V2V Technology for Application*, NAT'L HIGHWAY TRAFFIC SAFETY ADMIN. (Aug. 2014), http://www.nhtsa.gov/staticfiles/rulemaking/pdf/V2V/Readiness-of-V2V-Technology-for-Application-812014.pdf.

24. Newcomb, *supra* note 18.

25. NAT'L HIGHWAY TRAFFIC SAFETY ADMIN., CYBERSECURITY BEST PRACTICES FOR MODERN VEHICLES (Oct. 2014), https://www.nhtsa.gov/staticfiles/nvs/pdf/812333_CybersecurityForModernVehicles.pdf.

access to the fewest systems possible, using advanced encryption for communications, as well as employing a type of firewall software.[26] Layering is a more system-wide approach to prevention, focused on five principled functions defined by the National Institute of Standards and Technology: "Identify, Protect, Detect, Respond, and Recover."[27] System-wide anti-virus-like software can serve as an important one of these layers. Most system-wide security software works by performing a heuristic scanning of the vehicle's data traffic, which instead of blocking malware directly, looks for abnormal messages or code, and mitigates the ability of these messages to control critical driving functions (like steering or braking).[28] I anticipate that focusing on isolating critical systems and layering security through encryption and defensive software will help to decrease the likelihood of successful hacks, and diminish the potential damage when such hacks do occur.

One issue not discussed in the NHTSA guidelines or other proposals is a last-resort layer of preventative security that would be available to passengers, or the "driver" of the vehicle, if other security mechanisms fail. If the occupants become aware that their vehicle is being hacked or the AV driving system is not behaving in a normal and safe manner, it might be useful to have a failsafe override feature that would allow occupants to take control of the vehicle, and to disable the vehicle engine in circumstances where that might be the safest option.[29] Such a feature might not be useful in all hacking scenarios (i.e., if the primary purpose of the hack was to disable the vehicle engine) but would potentially help prevent accidents in the case of a hack/glitch where the AV accelerated unnecessarily, refused to stop, or attempted to proceed to a location not intended by the occupants. The presence of a failsafe would allow occupants to retain some form of "control" over the AV even if they are no longer in charge of the primary driving tasks. Not only could this minimize safety risk if AVs malfunction on the road, but I anticipate it would also alleviate consumer fears and help AVs gain more

26. *Id.* at 10 (the full list of recommendations can be found in NHTSA's public cybersecurity guidance).

27. "The automotive industry should follow the National Institute of Standards and Technology's documented Cybersecurity Framework . . . to build a comprehensive and systematic approach to developing layered cybersecurity protections for vehicles." *Id.*

28. Lucas Mearian, *Securing Your Car From Cyberattacks Is Becoming A Big Business*, COMPUTERWORLD (June 9, 2016), http://www.computerworld.com/article/3081467/car-tech/securing-your-car-from-cyberattacks-is-becoming-a-big-business.html (traditional anti-virus software blocks malware directly by seeking out virus signatures; although more accurate, this requires constant updates to remain effective).

29. While disabling a vehicle's engine on a public roadway may also present its own safety risks, this feature would be primarily focused on minimizing relative damage in the case of an AV commandeered by a hacker or when an AVs sensors are malfunctioning, potentially endangering pedestrians or other drivers. Studies would need to be done to determine the least risky means to safety disable an AV system. Requiring non-electronically controlled throttle, braking, and steering back-up systems would likely be prohibitively expensive, so more complex override systems may not be practicable.

widespread acceptance.[30] If the comprehensive anti-hacking systems work as designed, this failsafe would rarely need to be used, but could nonetheless be a useful backup as we gauge the reliability of the protective systems.

To improve cybersecurity, formal legislation or regulation (beyond voluntary guidance) should be introduced to mandate baseline levels of encryption requirements, segmenting protocols, and layering systems that would offer basic protections. Such laws or regulations can be written broadly, such that potential hackers would not have a blueprint of the specific hurdles they must overcome. Just as important as preventative measures, however, will be a robust infrastructure in place to respond to hacks after they happen.

Part II: Reactive Measures

Parallel to some of the hacking concerns raised regarding AVs, the airline industry has also had similar concerns of passengers hacking into the flight controls of an aircraft midflight. One prominent example of a researcher completing a successful hack elevated these fears. After discovering vulnerabilities in their networks and failing to get the attention of airlines, security researcher Chris Roberts hacked into the flight controls of a commercial flight through the in-flight entertainment system and briefly caused the plane to fly sideways according to an investigation by the FBI.[31] There are, however, key differences between the AV and airline industry, and in the next section I will discuss ways to improve the incentive-structure in the automotive industry's ISAC to encourage companies to candidly share vulnerabilities and best practices in real-time. The resulting details of this alleged hacking event were not released, but after the concerns were flagged, Boeing and other airline manufacturers took steps to segment the critical flight functions from the ECUs accessible to passengers. This type of segmenting is commonplace now, and is one of the baseline security measures proposed for AVs.[32] For this reason, NHTSA has encouraged the automotive-industry to follow this model.

---

30. Products used to remotely disable stolen vehicles, as well as emergency in-car engine-disabling systems, already exist. They are relatively inexpensive, and have not raised significant safety concerns. *Vehicle Disabling Systems*, North American Transp. Ass'n, http://www.ntassoc.com/uploads/FileLinks/be1d5f8106d64e0198d776625e0f31aa/Vehicle%20Disabling%20Systems.pdf (last visited Apr. 10, 2017).

31. Kim Zetter, *Feds Say that Banned Researcher Commandeered Plane*, Wired (May 15, 2015), https://www.wired.com/2015/05/feds-say-banned-researcher-commandeered-plane/. There is evidence already that automakers are responding more quickly to these types of white-hat researcher hacks on their cars; in a recent Tesla example, by the time they issued a press release downplaying one of these hacks by a researcher in China, Tesla had already issued an over-the-air security patch that fixed the problem. Kim Zetter, *Researchers Hacked a Model S, but Tesla's Already Released a Patch*, Wired (Aug. 6, 2015), https://www.wired.com/2015/08/researchers-hacked-model-s-teslas-already/.

32. 14 C.F.R. pt 25 (2013).

Airlines address these cybersecurity risks primarily through the Aviation Information Sharing and Analysis Center ("A-ISAC"), which requires companies to quickly tell each other about breaches to their respective networks, and allows all airlines to rapidly update their algorithms to contain the problem and prevent similar breaches.[33] This framework has been largely effective, demonstrating how evolving cybersecurity concerns in a critical transportation industry can be effectively dealt with.[34] NHTSA has flagged this as a well-established and effective system to react to cyber threats.[35]

NHTSA's 2016 AV guidelines emphasized the important role the Automotive Information Sharing and Analysis Center ("auto-ISAC") will play as a "central hub for gathering intelligence to help the industry analyze, share, and track cyber threats."[36] The auto-ISAC, officially formed in July 2015, became operational in January of 2016 and, like the aviation-ISAC, will play a critical role in modeling cybersecurity best practices within the industry.[37] Like the airline industry, the automotive industry produce technologically complex and high-automated products. Within each industry, the products from each manufacturer are similar enough that they often face common challenges regarding security threats. But unlike other industries, carmakers are always at risk of being targeted with potentially costly recall orders from NHTSA.[38] For this reason, revealing potential vulnerabilities quickly and publicly is not a practice the industry has made a habit of in the past.[39]

One possible solution to encourage automakers to more quickly address vulnerabilities would be to create a less-intrusive and expensive recall standard for over-the-air security updates compared to the current system for issuing traditional safety recalls. Currently, NHTSA issues a safety recall if there is non-compliance with any Federal Motor Vehicle Safety Standard ("FMVSS") or if a product contains a defect related to motor vehicle

33. Aviation Information Sharing & Analysis Center, *About the Aviation ISAC*, http://www.a-isac.com/aboutus.

34. J. Harding et al., *supra* note 25, at 13. NHTSA has proposed a similar function for the automotive industry's equivalent organization, the auto-ISAC.

35. *Id.* (NHTSA Cyber best practices). Aviation Information Sharing & Analysis Center, *supra* note 33.

36. FBI, *supra* note 3. Automakers are encouraged to use this information to collaborate on best practices for enhancing the cyber resiliency of motor vehicle electronics and associated in-vehicle networks. *Id.*

37. In July, 2016, they released their first report on industry best practices specifically targeted to automotive cybersecurity. *Automotive Cybersecurity Best Practices*, AUTO-ISAC (July 21, 2016), https://www.automotiveisac.com/best-practices/.

38. U.S. DEP'T OF TRANSP., NHTSA SAFETY RECALL COMPENDIUM (2016), http://www-odi.nhtsa.dot.gov/recalls/documents/recompendium.pdf.

39. The Cooper Firm, PERS. INJURY BLOG, http://thecooperfirm.com/vw-spent-two-years-trying-to-cover-a-security-flaw/ (last visited April 24, 2017).

safety.[40] Manufacturers have a duty of notice and recall, and they get five days to notify NHTSA if they find a defect and sixty days to notify consumers.[41] Large civil penalties can stem from a delay or failure to report; this, along with the cost of the recall itself might dissuade manufacturers from reporting vulnerabilities to the auto-ISAC[42] Such a hesitation would defeat, or at least largely diminish, the purpose and effectiveness of the auto-ISAC. Many cybersecurity vulnerabilities will be software-based. Instead of requiring recall notices to be sent out and vehicles brought into a dealership, regulators could simply require prompt notification of NHTSA and the auto-ISAC, along with a requirement to implement an over-the-air security patch as soon as one can be made available.[43] For this to adequately address safety concerns these security updates should be: (1) compulsory for manufacturers across the industry; (2) install automatically as soon as it is safe to do so; and (3) compulsory for consumers who should not be able to opt-out. Over-the-air security patches are gaining popularity among car manufacturers, so these requirements will likely face minimal industry pushback.[44] For reactive security measure to be effective, regulators should do whatever is necessary to ensure that proper incentives are in place to encourage timely, honest participation in the auto-ISAC and providing remedies for security vulnerabilities.[45]

Part III: Remaining Risk Gaps

As long as there are connected cars on the road, we must acknowledge up front that there is no policy that will entirely eliminate the risk of hacking in AVs. Cybersecurity regulation concerning AVs should minimize risk as

40. U.S. Dep't of Transp., *supra* note 38, at 5. Defect is defined as a non-de minimis number of failures in normal operation. *See U.S. v. General Motors*, 518 F.2d 420 (D.C. Cir. 1975).

41. U.S. Dep't of Transp., *supra* note 38, at 4, 8.

42. *See* The Cooper Firm, *supra* note 39 (VW attempted to cover up a cybersecurity flaw for two years).

43. *See* Alex Brisborne, *Tesla's Over-the-Air Fix: Best Example Yet of the Internet of Things?*, Wired (Feb. 2014), https://www.wired.com/insights/2014/02/teslas-air-fix-best-example-yet-internet-things (Tesla's approach to recalls and updates contrasted to the traditional industry approach).

44. BMW decided to encrypt wireless communication via an over-the-air patch after its vehicles were vulnerable to hackers wirelessly unlocking vehicles. Paul, *BMW Fixes ConnectedDrive Flaw with Over the Air Patch*, The Security Ledger (Feb. 2, 2015), https://securityledger.com/2015/02/bmw-fixes-connecteddrive-flaw-with-over-the-air-patch/. Other companies have partnered with software companies to handle their over-the-air security updates. Bob Sorokanich, *Ford Partners With Microsoft for Over-The-Air Sync Infotainment Updates*, Car & Driver (Mar. 17, 2015), http://blog.caranddriver.com/ford-partners-with-microsoft-for-over-the-air-sync-infotainment-updates/.

Other companies have partnered with software companies to handle their over-the-air security updates. http://blog.caranddriver.com/ford-partners-with-microsoft-for-over-the-air-sync-infotainment-updates/.

45. *See* The Cooper Firm, *supra* note 39.

much as possible, without delaying the growth of an industry that is anticipated to bring many significant, life-saving benefits with it. In addition to regulation, the specter of costly litigation has a very real effect on industry behavior. We are already starting to see hints of what form it might take, and the risk it may pose to AVs. In *Cahen v. Toyota Motor Corp.* 147 F. Supp. 3d 955 (N.D. Calif. 2015), a class action suit was filed against Ford, G.M., and Toyota, alleging that the electronic systems in place in their vehicles were susceptible to hacking by third parties and put their privacy rights at risk.[46] Although this case was built on a claim of risk to privacy (rather than physical safety), the Controller Area Network Bus ("CAN Bus") that allegedly exposed consumers to the privacy risk controls *all* of the internal ECU connections in a vehicle, including those that operate critical driving tasks such as the steering, acceleration, brakes, etc.[47] While the court noted a lack of real injury in fact, counsel for the plaintiffs argued that,

> "We shouldn't need to wait for a hacker or terrorist to prove exactly how dangerous this is before requiring car makers to fix the defect. Just as Honda has been forced to recall cars to repair potentially deadly airbags, Toyota, Ford and GM should be required to recall cars with these dangerous electronic systems."[48]

The case was dismissed for lack of Article III standing, but nonetheless serves as a reminder of the broad types of litigation threats AV systems might be facing in the future. Manufacturers and technology companies could face huge costs relating to litigation stemming from hacking incidents once they occur. But now, if a court finds argument made in Cahen compelling, they might even face liability relating to the *potential* of their vehicles to be hacked.

Those companies that take cybersecurity seriously, adhering closely to the auto-ISAC guidelines (or exceeding the standards), would likely have the lowest liability risk compared to those manufacturers that fall below the industry standard for cybersecurity architectures.[49] This could be a helpful

---

46. *Cahen v. Toyota Motor Corp.*, 147 F. Supp. 3d 955 (N.D. Calif. 2015). Although dismissed on jurisdictional grounds, the plaintiff's case was never likely to win on the merits (given the technology it targeted is nearly ubiquitous in all vehicles made in the past 25 years). More successful future cases might target a unique AV feature that may or may not meet auto-ISAC best practices, for example.

47. J. Harding et al., *supra* note 25; Lucas Mearian, *Securing Your Car From Cyberattacks Is Becoming A Big Business*, COMPUTERWORLD (Jun. 9, 2016), http://www.computerworld.com/article/3081467/car-tech/securing-your-car-from-cyberattacks-is-becoming-a-big-business.html.

48. Aebra Coe, *Ford, GM, Toyota Slammed with Suit Over Hacking Risks*, LAW360 (Mar. 10, 2015), http://www.law360.com/articles/629544/ford-gm-toyota-slammed-with-suit-over-hacking-risks.

49. One piece of legislation proposes a ranking system for cybersecurity, akin to the current crash-test safety rating featured prominently in car advertisements. Staff of Senator

non-regulatory incentive to ensure the voluntary best practices become the de facto baseline. Although, in the event of a particularly large cybersecurity breach, AV companies may still face crippling costs if a jury finds their precautions inadequate from either a risk-utility or consumer expectations standpoint.[50] While still a very underdeveloped market at this time, cyber-insurance may offer one avenue to mitigate the potential costs of litigation.

Given the strong probability of a successful hack of an AV or AV-network, the need for cyber-insurance at some level will be an almost certain part of any regulatory scheme.[51] Cyber-insurance is a nascent industry and trying to price the risk is challenging at this stage.[52] There is very little data on how big the scope of the risk related to vehicle hacking is and what it will look like in the future. While researchers have proven that it is possible, it remains to be seen how prevalent a problem it will be given that the only fully-autonomous AVs currently on the road are those being tested by manufacturers.[53] Since the risk may range from single vehicles to potentially much larger networks of linked autonomous vehicles, valuating that risk may continue to be vexing for the foreseeable future.[54]

The need for cyber-insurance is also highlighted by the unique threats faced by AVs that even the best anti-hacking software may be unable to prevent. In a hypothetical scenario, a carjacker could step in front of an AV, forcing it to stop, while she or a fellow carjacker takes control of the vehicle or commits a robbery of its occupants.[55] While a human driver might recognize the threat and drive away, an AV likely would not. Unoccupied AVs in remote locations might make particularly attractive targets for criminals given the low likelihood of being caught. Even non-malicious pranksters or

---

Edward Markey, *Tracking and Hacking: Security and Privacy Gaps Put American Drivers at Risk* (Feb. 2015), http://www.markey.senate.gov/imo/media/doc/2015-02-06_MarkeyReport-Tracking_Hacking_CarSecurity%202.pdf.

50. Gary Marchant & Rachel Lindor, *The Coming Collision Between Autonomous Vehicles and the Liability System*, 1321 SANTA CLARA L. REV. 1324, 1333 (2012).

51. Jemina Kiss, *Your Next Car Will Be Hacked*, THE GUARDIAN (Mar. 13, 2016), https://www.theguardian.com/technology/2016/mar/13/autonomous-cars-self-driving-hack-mikko-hypponen-sxsw.

52. Though relatively new, the cyber-insurance industry is growing rapidly. One industry leader predicts the market will grow from $2.5bn in 2015 to a predicted $7.5bn in 2020. *Id.*

53. The earliest forecasted AV will become available next year. *See Forecasts*, DRIVERLESS FUTURE, http://www.driverless-future.com/?page_id=384 (last visited Apr. 10, 2017).

54. "One of the factors that could increase premiums is the cyber exposure because there is no real cyber product being purchased in relation to auto today," said Mike Scrudato, head of Munich Re's mobility operations. Alex Webb, *Cybersecurity is Biggest Risk of Autonomous Cars, Survey Finds*, BLOOMBERG (July 19, 2016), https://www.bloomberg.com/news/articles/2016-07-19/cybersecurity-is-biggest-risk-of-autonomous-cars-survey-finds.

55. A participant in one of their focus groups from the U.K. described just such a concern, saying, "[The AVs are] going to stop, so you're going to mug them right off. They're going to stop and you're just going to nip round." Rob Price, *Aggressive Drivers Are Going to Bully Self-Driving Cars*, BUSINESS INSIDER (Oct. 17, 2016), http://www.businessinsider.com/aggressive-drivers-bully-self-driving-cars-autonomous-vehicles-study-lse-goodyear-2016-10.

children might conceivably find amusement in deceiving AVs and taking advantage of their predictable behavior with regard to avoiding collisions, creating a number of potentially hazardous scenarios. These types of manipulations of properly working sensors may be impossible for engineers to solve, given that a carjacker and errant pedestrian standing in the road would look the same to a vehicle's sensors.

The larger scale risk of a system-wide hack, terrorist-related hack, or other widespread electronic disabling of vehicles is both unknown, and a risk that would potentially be incredibly difficult to insure early on. One option to ensure these costs do not stifle the development of the industry would be for the federal government to grant immunity to AV manufacturers from liability arising from AV hacking.[56] Although this could be a tempting incentive, given the massive safety benefits many industry and government officials expect AVs to deliver, eliminating risk entirely for manufacturers might create a perverse incentive to cut corners on best practices, especially features that add significant cost.[57]

Another mechanism to protect against unwieldy costs rising from litigation could be a federal fund to compensate victims of AV hacking. Hacking will likely be inevitable; even the most secure, state-of-the-art systems get hacked, and to open manufacturers to potentially massive liability even if they are following best practices would detrimentally dampen innovation in the industry and curtail many of the benefits.[58] A compensatory fund for victims may or may not be paired with an immunity provision, and could potentially help speed implementation of AVs in the short-term if liability concerns grow.

Prior to a successful case being brought against a manufacturer, it remains to be seen what posture courts will take toward cybersecurity liability,

---

56. So far industry-officials are moving forward without such a scheme in place, with Volvo's CEO going as far as preemptively accepted all liability for accidents cause by their AVs. *See* Pete Bigelow, *Can't accept autonomous liability? Get out of the game, says Volvo*, AUTOBLOG (Oct. 9, 2015), http://www.autoblog.com/2015/10/09/volvo-accept-autonomous-car-liability/. But if liability costs accelerate in the future, government indemnification for vital industries that may face crippling liability is not without precedent. *See, e.g.*, Price-Anderson Nuclear Industries Indemnity Act, 42 U.S.C. § 2210.

But if liability costs accelerate in the future, government indemnification for vital industries that may face crippling liability is not without precedent, see, e.g., Price-Anderson Nuclear Industries Indemnity Act, 42 U.S.C. § 2210.

57. One insurance industry official predicted AVs could reduce traffic accidents by as much as 80% by 2030; if these projections pan out, there could be a strong government incentive to facilitate the industry if it encounters obstacles. Kiss, *supra* note 51.

58. *See* Ellen Nakashima, *Powerful NSA Hacking Tools Have Been Revealed Online*, WASH. POST (Aug. 16, 2015) (Victims of malicious hacking include the NSA, OPM, and IRS), https://www.washingtonpost.com/world/national-security/powerful-nsa-hacking-tools-have-been-revealed-online/2016/08/16/bce4f974-63c7-11e6-96c0-37533479f3f5_story.html; *See also* Josue Ledesma, *How Big is the U.S. Government Cybersecurity Problem?*, SECURITY SCORECARD (Apr. 14, 2016). http://blog.securityscorecard.com/2016/04/14/big-us-government-cybersecurity-problem/.

and whether following industry best practices is enough to protect against claims. Until the scope of actual liability and cost is determined, I would recommend against any federal immunity provision or compensation fund. The industry seems more than willing to absorb the risk at this stage, and a private cybersecurity insurance market will likely be able to more efficiently price risk in the long-term.

Conclusion

Cybersecurity is only as strong as its weakest link. In order to succeed, they must become a fundamental part of the entire design process, not merely an afterthought. There must be both strong incentives for designing cybersecurity systems in AVs using best practices through the auto-ISAC and implementing them without delay. The worst-case scenario that the industry should prepare for is a large-scale coordinated attack on connected vehicles, but even isolated safety incidents would be a public relations nightmare and could set back public confidence in AVs significantly. This underscores why we must focus on proactive measures just as much as reactive measures when it comes to preventing hacks. Given the large number of cars that already feature semi-autonomous functions (like adaptive cruise control), and the anticipated rollout of fully autonomous vehicles in the near future, this is a challenge that needs to be addressed immediately industry-wide.

So far, federal regulators have moved quickly, taking seriously the safety risk posed by hackers by offering voluntary guidance, but they have yet to issue any new FMVSSs related to cybersecurity or mandate that AVs follow best practices.[59] While nothing can be done to eliminate risk entirely, if the following steps are taken, we can be more confident in both the cybersecurity of our vehicles and the continued viability of the AV-industry overall:

1) Proactive measures should be implemented now, and there is room for agency or legislative pressure to ensure basic encryption standards are being met, internal vehicle systems are segmented when possible, and multiple layers of security protocols are built into the design process. The NHTSA Cybersecurity guidelines offer a good initial framework for what these proactive measures should look like. Isolating and containing vulnerabilities will both dissuade hackers and limit potential damage.
2) Better incentives need to be created to ensure compliance with industry best practices, and real-time, honest reporting of vulnerabilities to the auto-ISAC. One method would be creating a less-burdensome category for safety recalls, specifically to ad-

59. *See* Nat'l Highway Traffic Safety Admin., *supra* note 25.

dress over-the-air security patches to vehicle software. Any over-the air updates should be mandatory and uploaded as soon as practicable. Given the risk to the safety an AV presents to others, opting-out of these security updates should not be allowed.

3) Tort liability related to hacks may present a concern for the industry. However, it can also serve a useful purpose in incentivizing close adherence to industry best-practices. A broad federal immunity provision for manufacturers should be avoided at this time. Instead, a more robust cyber-insurance industry can instead fill the vital role of mitigating some of the inherent risks that remain for the industry.

That being said, these recommendations should remain flexible as the industry is likely to undergo rapid changes. We should be cautious not to limit our concern to traditional types of electronic hacking. Like the hypothetical scenario laid out at the beginning of this note revealed, there are numerous and inventive ways individuals will attempt to take advantage of autonomous vehicles. AVs will still need traditional lock-and-alarm security systems, along with some form of insurance, but they will also need adaptive algorithms that can think more like a human driver if AVs are going to see truly widespread viability in the market and deliver their promised safety benefits. While we should welcome the anticipated benefits the AV-era will offer to society, we should take steps now – with every tool available – to ensure we are not creating new and greater safety risks, just as we eliminate the risks of the past.