



Free markets. Real solutions.

R STREET POLICY STUDY NO. 118
November 2017

ADDRESSING NEW CHALLENGES IN AUTOMOTIVE CYBERSECURITY

Caleb Watney and Cyril Draffin

EXECUTIVE SUMMARY

As more connected and autonomous vehicles hit the road, new attack vectors emerge for hackers, cyber-criminals and even nation states. If left unaddressed, these cyberattacks can result in physical harm to drivers, bystanders and infrastructure. However, excessive regulation can also delay this important innovation. Accordingly, the present study will discuss the various types of cybersecurity risk and efforts taken by industry stakeholders, federal regulators and Congress to try and reduce it, and will then make recommendations for a policy framework going forward. Rather than force new cybersecurity problems through the traditional Federal Motor Vehicle Safety Standards (FMVSS) process, we recommend embracing a more flexible regulatory approach that aligns manufacturer incentives, promotes the development of cybersecurity best practices, proactively tests their capabilities and holds companies accountable to their promises.

CONTENTS

Executive summary	1
Introduction	1
The automotive cybersecurity challenge	2
Vehicle architecture	3
Cybersecurity risks	4
Industry efforts to improve cybersecurity	6
Risk minimization	6
Proactive vulnerability discovery	6
Development of best practices	7
Current regulatory structure	7
Department of Homeland Security (DHS)	9
National Highway Traffic Safety Administration (NHTSA)	9
Federal Trade Commission (FTC)	10
Effective approaches to future policy	11
Public safety balance	11
Proposed Cybersecurity Legislation	11
The Internet of Things Cybersecurity Improvement Act (IoTICI)	11
SPY Car Acts of 2015 and 2017	12
SELF DRIVE and AV START Acts	12
State efforts	13
A better way forward	14
Additional policy steps	15
Conclusion	15
About the authors	16

FIGURE 1: Smart car assets	3
FIGURE 2: Diagram of federal agency cybersecurity roles	8

TABLE 1: Risk taxonomy of vulnerabilities	5
-------------------------------------------	---

INTRODUCTION

Our automobiles have increasingly begun to act, feel and look like computers. Using myriad sensors and screens, they help us to navigate, communicate, entertain, brake and even steer. Under this broad umbrella of “intelligent vehicles,” there are two separate but overlapping technologies: connected and autonomous driving. Whereas autonomous vehicles (AV) reduce the need for input from human operators, connected vehicles (CV) interface with the internet and with other cars on the road to facilitate information sharing. While almost all autonomous vehicles are in some sense “connected,” not all connected vehicles are automated.¹ Going forward, it seems likely that the overlap between these two technologies will continue to grow. This interconnection presents unique benefits, as well as regulatory challenges.²

The potential benefits offered by both connected and autonomous vehicles are far-ranging and substantial. Most significantly, they provide an opportunity to save thousands of lives a year and to reduce the economic and social costs of auto

1. While autonomous vehicles do not necessarily have to be actively connected, practically speaking, they do have to connect to the Internet at least on a semi-regular basis. This is because without the ability to update key software, maps, traffic patterns or user data via the cloud, they lose much of their functionality.

2. “Shared Mobility on the Road of the Future,” *Morgan Stanley Blue Papers*, June 15, 2016. <https://www.morganstanley.com/ideas/car-of-future-is-autonomous-electric-shared-mobility>.

accidents.³ Drunk, drowsy and distracted driving contributed to 40,000 auto fatalities last year.⁴ Worse still, this number is increasing, as is the urgency to address it. According to the National Highway Traffic Safety Administration (NHTSA), the first half of 2016 experienced a 10.6 percent rise in the number of automobile fatalities compared to the same period of the previous year.⁵ Among young people, vehicle-related fatalities are the nation's single most profound public health crisis. Because an estimated 94 percent of accidents are the result of human error,⁶ autonomous and connected vehicles have the opportunity to save tens of thousands of lives and hundreds of billions of dollars each year.⁷

Additionally, these technologies may increase the economic productivity of drivers⁸ and allow shippers of goods to enhance their services through long-distance, autonomously controlled trucks.⁹ Connected cars may also be cheaper to operate, cut environmental pollution, reduce traffic and create quieter roads.¹⁰ Indeed, if connected autonomous cars could be called on-command and shared by others, the number of parking spaces and parking garages could be shrunk, and the width of roads could be reduced. Changes like these could free-up valuable real estate in urban centers.¹¹ Given all these potential benefits, the connected car market is expected to grow rapidly—from 5.1 million units in 2015 to

37.7 million units by 2022—a growth rate of more than 35 percent.¹²

But as with any complex cyber-physical system, these vehicles have potential cyber vulnerabilities that must be addressed for their benefits to be fully realized. Given the human stakes involved, mistakes will have significant and possibly fatal consequences. For example, if exploited throughout an entire fleet of vehicles, a serious vulnerability in a manufacturer's control system design or software upgrade could pose a nationwide risk if harnessed by a hostile actor.¹³

However, prudent cybersecurity design and systems that diagnose and eliminate potential vulnerabilities could help to mitigate that risk. For leaders in both industry and government, the challenge is determining how to enable the many economic and environmental benefits of connected and autonomous vehicles without endangering public safety or consumer confidence. For this reason, effectively deploying and adopting intelligent vehicles will require continuous, risk-based technological development and a flexible regulatory environment.

THE AUTOMOTIVE CYBERSECURITY CHALLENGE

The increasing technical sophistication of motor vehicles is not a new phenomenon. Onboard electronic information-control systems like fixed-speed cruise control, power steering, auto-braking and tire-pressure sensors have become ubiquitous in traditional automobiles over the past few decades.¹⁴ More recently, other increasingly sophisticated systems are also making their way into vehicles, like electronic interfaces designed to facilitate auto-emissions testing, external sensors used to identify other vehicles,¹⁵ entertainment packages¹⁶ and satellite navigation.¹⁷ Each of these additions have been part of the trend toward a safer, more enjoyable transportation experience. However, along with these desirable innovations in technology has come an associated risk of potential cyberattack. An overview of current

3. Adam Thierer, "Survey of Studies on Life-Saving Potential of Driverless Cars," *The Technology Liberation Front*, June 30, 2017. <https://techliberation.com/2017/06/30/survey-of-studies-on-life-saving-potential-of-driverless-cars>.

4. Ashley Halsey III, "Traffic deaths soared past 40,000 last year for the first time in a decade," *The Washington Post*, Feb. 15, 2017. https://www.washingtonpost.com/local/trafficandcommuting/traffic-deaths-soared-past-40000-last-year-as-economy-continued-to-improve/2017/02/15/fd1e8298-f388-11e6-8d72-263470bf0401_story.html?utm_term=.20229fd47ebc.

5. National Highway Traffic Safety Administration, "Early Estimate of Motor Vehicle Traffic Fatalities for the First Half (Jan-Jun) of 2016," U.S. Dept. of Transportation, October 2016. <https://crashstats.nhtsa.dot.gov/Api/Public/ViewPublication/812332>.

6. National Highway Traffic Safety Administration, "Critical Reasons for Crashes Investigated in the National Motor Vehicle Crash Causation Survey," U.S. Dept. of Transportation, February 2015. <https://crashstats.nhtsa.dot.gov/Api/Public/ViewPublication/812115>.

7. The economic costs of motor vehicle crashes alone are a staggering 910 billion dollars a year, which is the equivalent of six percent of GDP. See, Xavier Mosquet, Michelle Andersen, et al., "A Roadmap to Safer Driving Through Advanced Driver Assistance Systems," The Boston Consulting Group, Inc., and the Motor & Equipment Manufacturers Association, Sept. 29, 2015. <https://www.mema.org/sites/default/files/MEMA%20BCG%20ADAS%20Report.pdf>.

8. Kara Kockelman and Lewis Clements, "Economic Effects of Automated Vehicles," *Transportation Research Record* No. 2602, 2017. http://www.cae.utexas.edu/prof/kockelman/public_html/TRB17EconomicEffectsOfAVs.pdf.

9. Caleb Watney, "Don't shut trucks out of the driverless vehicle future," *The Washington Examiner*, Oct. 4, 2017. <http://www.washingtonexaminer.com/dont-shut-trucks-out-of-the-driverless-vehicle-future/article/2636523>.

10. "Estimated Benefits of Connected Vehicle Applications," U.S. Dept. of Transportation, August 2015. <https://ntl.bts.gov/lib/56000/56200/56238/FHWA-JPO-16-255.pdf>.

11. Sam Lubell, "Here's How Self-Driving Cars Will Transform Your City," *Wired*, Oct. 21, 2016. <https://www.wired.com/2016/10/heres-self-driving-cars-will-transform-city>.

12. "Connected Car Market by Hardware (Semiconductor Components, and Connectivity ICs- Wi-Fi, Bluetooth and Cellular), Application (Telematics, Infotainment, and Combined Telematics & Infotainment), and Geography - Global Forecast to 2022," *Semiconductor and Electronics*, March 2017. https://www.researchandmarkets.com/research/rq92jm/connected_car.

13. David Ward, Ileri Ibarra, et al., "Threat Analysis and Risk Assessment in Automotive Cyber Security," *SAE International Journal of Passenger Cars-Electronic and Electrical Systems* 6(2):507-13, 2013. <https://doi.org/10.4271/2013-01-1415>.

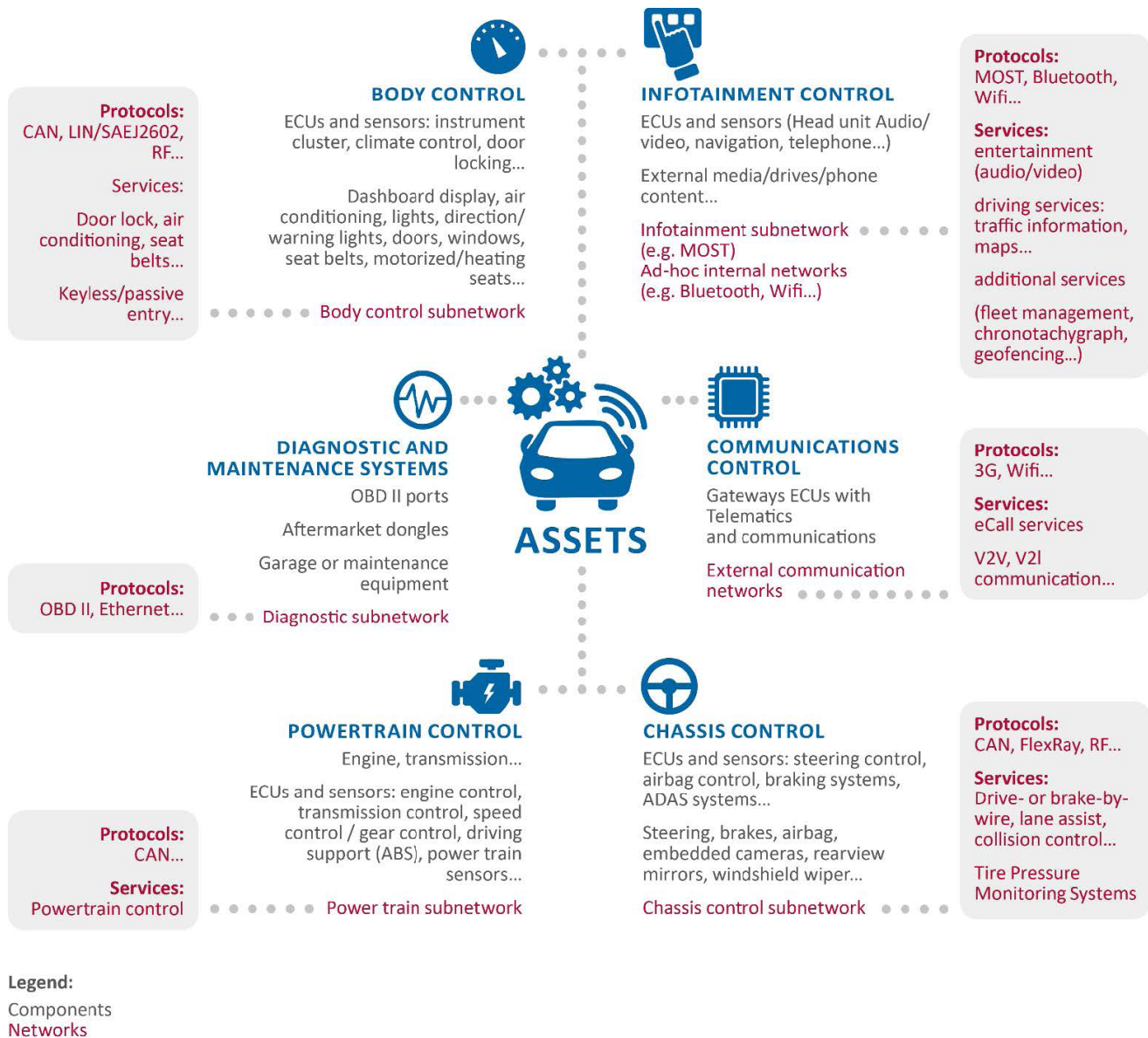
14. See, e.g., Jonathan Petit and Steven E. Shladover, "Potential Cyberattacks on Automated Vehicles," *IEEE Transactions on Intelligent Transportation Systems* 16:2 (April 2015), 546-66. <http://ieeexplore.ieee.org/document/6899663>.

15. This includes both alerts of vehicles in adjoining lanes and spacing between moving cars.

16. These include USB interfaces and streaming capabilities.

17. See, Petit and Shladover. <http://ieeexplore.ieee.org/document/6899663>.

FIGURE I: SMART CAR ASSETS



Source: Enisa¹

1. European Union Agency for Network and Information Security (ENISA), "Cyber Security and Resilience of Smart Cars Report: Good practices and recommendations," Jan. 13, 2017, p.

vehicle architecture thus would be useful to assess the most vulnerable points.

VEHICLE ARCHITECTURE

The internal computational structure of autonomous and connected vehicles is largely coordinated through electronic computing units (ECUs), which are systems embedded within the vehicle that control one or more of its electrical systems. These include the engine, brakes, transmission,

telematics, suspension and powertrain control modules.¹⁸ These ECUs are frequently connected via a controller area network (CAN) "bus," which acts as a type of backbone for electrical signals to pass between ECUs. The architecture of subnetworks and protocols within a CAN may vary from one vehicle to another and can include things like diagnostic interfaces and wireless communications channels. Thus,

18. "Building Flexible, Cost-Effective ECU Test Systems," *National Instruments*, Nov. 4, 2014. <http://www.ni.com/white-paper/3064/en>.

instead of thinking of a connected or autonomous vehicle as a single, undifferentiated cyber target, it is important to recognize that each of these components can also be at risk, and with a variety of related safety, security or privacy concerns (see Figure 1).

In the past, to reduce costs, a single CAN (sometimes without sophisticated encryption) was used to connect all electronic signals within a vehicle.¹⁹ In exchange for the convenience of such an approach, vehicles were rendered hugely vulnerable to penetration. If one vehicle subsystem was compromised, other subsystems also could be accessed.²⁰ Aware of the evolving threat environment, manufacturers have moved away from this practice. Sophisticated connected vehicles now require multiple CANs, each with a different set of ECUs.²¹ For instance, CAN-C is a high-speed bus that connects the brakes, airbags, engine and other safety-critical ECUs, while CAN-IHS is a low-speed one that connects comfort systems like the radio, temperature control and infotainment ECUs.²²

As noted in Figure 1, some of these ECUs also have wireless connectivity for the purposes of providing over-the-air (OTA) software updates, live navigation details or cellular service. As these digital components of the vehicle architecture continue to grow in both capabilities and sophistication, the communication channels they use fall into three overlapping subcategories: communication of data between vehicles (V2V), between vehicles and infrastructure (V2I) or between the vehicle and other connected devices more broadly (V2X). These wireless communication systems are what is popularly thought of as the “connected” part of connected vehicles.

While no manufacturer has yet rolled out a full-scale V2V/V2I/V2X system, some are in the midst of the deployment process or have announced plans to do so in the near future.²³ More advanced versions of this technology—like direct short-range communication (DSRC), 5G or wireless access in vehicular environments (WAVE)—could allow real-time sharing of location and speed data with other vehicles on the road, which in turn can be used to coordinate driving behavior to avoid crashes and reduce traffic congestion. Similar-

ly, wireless communication with infrastructure could alert vehicles or drivers of obstacles on the road miles ahead of their current location or reroute traffic patterns for construction.²⁴

Cybersecurity risks

With increases in the complexity of vehicles and their computer-controlled components, the number of potential vectors a sophisticated attacker could exploit will also continue to grow. This stems not only from the raw number of vehicles on the road, but also from the number of systems susceptible to an attack within each vehicle. Put simply, the more interconnections, the more potential vulnerabilities.

The system assets in the vehicle architecture described above are vulnerable to cyberattack in two broad ways: locally, via the physical connection points inside the vehicle, and remotely, via the external wireless systems with which they connect. While there is some overlap with respect to risk, the distinction is necessary to evaluate the unique vulnerabilities each system presents.

Local attack vectors – The most direct method of attack for these systems are physical connection points like charging stations for electric vehicles, USB ports, infotainment systems and the onboard diagnostic (OBD-II) port.²⁵ All of these ports provide direct access to an ECU, which could then be electrically shorted, or if a vulnerability was discovered, a piece of malware could be delivered via USB drive.

While an attack that relies on local access to a specific internal port may have a higher rate of success, given direct delivery of malware to the intended ECU, its severity will be largely constrained by the time and physical access it takes to reach each port in question.

Remote attack vectors – Alternatively, attackers could try to penetrate one of the external communication systems used by connected cars for information flow. For instance, if a V2V channel like DSRC or a V2X channel like 5G were compromised, an attacker could spoof the location data of that car and cause confusion to other connected vehicles that rely

19. Dan Klinedinst and Christopher King, “On Board Diagnostics: Risks and Vulnerabilities of the Connected Vehicle,” Software Engineering Institute-Carnegie Mellon University, March 2016, 10. http://resources.sei.cmu.edu/asset_files/WhitePaper/2016_019_001_453877.pdf.

20. Ibid.

21. See, e.g., Ward, Ibarra, et al. <https://doi.org/10.4271/2013-01-1415>.

22. See, e.g., Alex Kreilein, “Security Considerations for Connected Vehicles and Dedicated Short Range Communications,” Secure Set, March 29, 2017. <http://glenecho-group.isebox.net/secureaccelerator/dedicated-short-range-communications-dsrc-expose-critical-gaps-in-security-and-privacy>.

23. See, e.g., Andrew J. Hawkins, “Cadillac’s CTS sedans can now ‘talk’ to each other, which may make driving way less deadly,” The Verge, March 9, 2017. <https://www.theverge.com/2017/3/9/14869110/cadillac-cts-sedan-v2v-communication-dsrc-gm>.

24. Brent Skorup, “Driverless Cars Just Need One Thing: Futuristic Roads,” *Wired*, Oct. 10, 2016. <https://www.wired.com/2016/10/driverless-cars-need-just-one-thing-futuristic-roads>.

25. See, e.g., Andy Greenberg, “Securing Driverless Cars From Hackers Is Hard. Ask The Ex-Uber Guy Who Protects Them,” *Wired*, April 12, 2017. <https://www.wired.com/2017/04/ubers-former-top-hacker-securing-autonomous-cars-really-hard-problem/>. The OBD-II port is a mandated physical outlet under a car’s dashboard that provides access to the car’s CAN. In particular, it has been flagged as a major vulnerability by security researchers because it was not originally designed with internet connectivity in mind. However, the OBD-II does port with devices used by insurance companies, consumers and fleet managers that utilize wireless cellular connectivity. This creates an access point for would-be attackers. See also, Klinedinst and King. http://resources.sei.cmu.edu/asset_files/WhitePaper/2016_019_001_453877.pdf.

on its signal for navigation.²⁶ This could cause accidents or traffic congestion on a much larger scale than a local attack, because there would be no need for physical access to the vehicles being affected.²⁷

At first glance, this would appear only to affect ECUs that have wireless connectivity functions. However, if the communication bridges between CANs are not robustly protected, an attack on a connected infotainment ECU could be leveraged to affect non-connected, safety-critical functions, such as the brake or engine ECUs.²⁸

Due to the sensational nature of hacking a connected car without direct physical access, whenever they have been demonstrated by security researchers, remote attacks have been heavily featured in the media. Examples of these demonstrated connected-car hacking incidents include:

- A Jeep Cherokee was subjected to a remote attack wherein control was taken, its rate of acceleration was changed and it was forced off the road. This forced 1.4 million cars to be recalled by Chrysler.²⁹
- Security researchers hacked the BMW “Connected-Drive” system and managed to unlock cars remotely. This attack resulted in the recall of 2.2 million cars.
- Attacks on the remote keyless entry systems of many cars—though Volkswagen models produced since 1995 are particularly vulnerable.³⁰
- The operating system of Tesla’s electric vehicles was hacked, which required an OTA software update.³¹
- A teenager remotely unlocked and started a connected car with only \$15 of simple electronics gear.³²

26. See, e.g., Krelein. <http://glenechogroup.isebox.net/securesetaccelerator/dedicated-short-range-communications-dsrc-expose-critical-gaps-in-security-and-privacy>; Cyber Security in the Connected Vehicle Report,” TU Automotive, Ltd., February 2016. <http://www.tu-auto.com/cybersecurity-report>; and Klinedinst and King. http://resources.sei.cmu.edu/asset_files/WhitePaper/2016_019_001_453877.pdf.

27. Ward, Ibarra, et al. <http://papers.sae.org/2013-01-1415>.

28. See, e.g., André Weimerskirch and Ron Gaynier, “An Overview of Automotive Cybersecurity: Challenges and Solution Approaches,” University of Michigan Transportation Research Institute, Sept. 16, 2015. <https://pdfs.semanticscholar.org/0dad/59a91ff57532011d188f3e53bd4387d7dbbf.pdf>.

29. Andy Greenberg, “Hackers Remotely Kill A Jeep On The Highway—With Me In It,” *Wired*, July 21, 2015. <http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway>.

30. Jonathan M. Gitlin, “Almost every Volkswagen sold since 1995 can be unlocked with an Arduino,” *Ars Technica*, Aug. 11, 2016. <http://arstechnica.com/cars/2016/08/hackers-use-arduino-to-unlock-100-million-volkswagens/>.

31. Dave Lee, “Tesla updates software after car hack,” *BBC News*, Sept. 21, 2016. <http://www.bbc.com/news/technology-37426442>.

32. Leo King, “14-Year-Old Hacks Connected Cars With Pocket Money,” *Forbes*, Feb. 23, 2015. <http://www.forbes.com/sites/leoking/2015/02/23/14-year-old-hacks-connected-cars-with-pocket-money>.

While most of these vulnerabilities were quickly neutralized once identified, their existence is a testament to the fact that cyber vulnerabilities are, in some sense, inevitable. Once a system has been compromised, the types of attacks employed can vary dramatically. Ransomware, malware, data exfiltration and traditional distributed denial of service are all possible, but the most immediately dangerous attacks would be those that affect vehicle operability—especially on a mass scale.

Below is a taxonomy of potential vulnerabilities and the various levels of severity that could result:

TABLE I: RISK TAXONOMY OF VULNERABILITIES

Axis of Risk	Severity of Attack		
	Low	Moderate	High
Number of vehicles affected	Localized attack on an individual vehicle	Vulnerability exploited that affects all vehicles of a particular make or model	Common vulnerability found across multiple fleets and manufacturers
ECUs compromised	Isolated to entertainment systems, heating/cooling systems or other auxiliary systems	Parts of the user interface that control fuel gauge, speedometer or navigation	Direct vulnerability to vital safety system like engine, brake or steering functions
Attacking entity	Solo hacker or tinkerer	Coordinated group of sophisticated hackers	Nation state, terrorist organization
Motivation for attack	Experimentation, mischief or boredom	Financial extortion (via ransomware) or industrial espionage	Deliberate intention to harm, cyberwarfare on critical transportation infrastructure
Ability to replicate	Requires immense technical sophistication for each penetration	Moderate-to-low level of technical sophistication required	An automated script that, once created and distributed, would allow anyone access to the same vulnerability
Difficulty to repair	Instant over-the-air (OTA) software update can patch the vulnerability	Overnight OTA update required to patch the vulnerability	Physical recall of the vehicle required to eliminate the vulnerability
Data stolen	Limited, anonymized location datasets	External video feeds, driver behavior data	Personalized location and trip data, internal video/microphone feed, sensitive financial information ¹

1. Sensitive financial information could be compromised if a consumer is using a connected autonomous ridesharing or subscription service.

To ensure the ongoing safe operation of connected cars and autonomous vehicle systems, these automobiles will need to be developed and equipped with defensive capabilities, like

the ability to detect when core software has been unexpectedly tampered with and to come to a full and safe stop on the side of the road using backup systems.³³

INDUSTRY EFFORTS TO IMPROVE CYBERSECURITY

Given the high profile of these technologies and their potential to change society as we know it, the media has been vigilant in its coverage of the details of autonomous and connected vehicle development.³⁴ As the technology gets closer to market, this focus will only intensify. For this reason, connected and automated vehicle manufacturers have a strong incentive to avoid crashes and insecure cybersecurity practices. For the countless companies developing this technology, a public relations nightmare lurks behind every alleged hack and every vehicle collision, irrespective of who is actually at fault.³⁵ This underscores the importance of maintaining public confidence at the early stages of development, particularly as consumers are initially skeptical of the technology.³⁶ After all, if any single company experiences more high-profile accidents or hacks than others, the future of their work in the area will consequently be placed at serious risk.³⁷

Accordingly, companies are taking steps both individually and collectively as an industry to minimize risks, proactively find vulnerabilities and develop cybersecurity best practices.

Risk minimization

Some companies are trying to diminish the cyber risks their vehicles confront by building in system redundancy and by limiting the scope of connectivity. For example, John Krafcik, CEO of Alphabet's self-driving division, Waymo, has revealed that their cars receive limited internet access to minimize the window for hackers to penetrate the system:

Our cars communicate with the outside world only when they need to, so there isn't a continuous line that's able to be hacked, going into the car. When we

33. Waymo claims to have this kind of defensive capability in their new safety report. See, e.g., "On the Road to Fully Self-Driving," *Waymo Safety Report*, Oct. 12, 2017, <https://storage.googleapis.com/sdc-prod/v1/safety-report/waymo-safety-report-2017-10.pdf>.

34. Jordan Golson, "Tesla driver killed in crash with Autopilot active, NHTSA investigating," *The Verge*, June 30, 2016, <http://www.theverge.com/2016/6/30/12072408/tesla-autopilot-car-crash-death-autonomous-model-s>.

35. Andrew Hawkins, "Google's 'worst' self-driving accident was still a human's fault," *The Verge*, Sept. 26, 2016, <https://www.theverge.com/2016/9/26/13062214/google-self-driving-car-crash-accident-fault>.

36. See, e.g., Erin Stepp, "Americans Feel Unsafe Sharing the Road with Fully Self-Driving Cars," AAA, March 7, 2017, <http://newsroom.aaa.com/2017/03/americans-feel-unsafe-sharing-road-fully-self-driving-cars>.

37. Caleb Watney and Ian Adams, "Comments to the FTC on Connected Vehicles Workshop" R Street Institute, April 25, 2017, <http://www.rstreet.org/wp-content/uploads/2017/04/FTC-CV-Comments-RSI-2.pdf>.

say that our cars are autonomous, it's not just that there's not a human driver, but also that there is not a continuous cloud connection to the car.³⁸

Similarly, a recent Waymo report announced that all their connected and autonomous cars will have a redundant secondary computer system with an independent power source that will run in the background to bring the vehicle to a safe stop if it detects a primary system failure.³⁹

Limited windows of connectivity reduce the number of opportunities hackers will have to attempt attacks, while redundancy of key safety systems makes the vehicle substantially more resilient to both local and remote attacks if primary safety systems are infiltrated. In these ways, deliberate redundancy and limited connectivity overlap and reinforce each other to limit most known vectors of cyberattack.

Currently, it is unclear how widespread Waymo's levels of redundancy and limited connectivity are among other manufacturers. However, should such an approach become widespread, there would be tremendous implications for the overall cybersecurity of the industry. Many serious threats to safety are the result of mass vulnerabilities caused by the penetration of wireless communication systems. Accordingly, if connected cars have the ability to operate independently of a wireless connection, then the possibility of mass casualties would be substantially decreased.

Proactive vulnerability discovery

Recognizing that it is impossible to plan for every possible avenue of attack, companies have also turned to computer security specialists or "white hat" hackers to test their defensive capabilities proactively before a malicious hack occurs. To this end, monetary offers for the private disclosure of discovered vulnerabilities—or "bug bounty" programs—have been a popular and effective way for tech giants like Google and Facebook to expose novel attack methods.⁴⁰ A reputation as the safest auto manufacturer with respect to cybersecurity carries a significant competitive advantage. As such, automotive companies have moved to adopt these models established by other tech giants. For example, Chrysler and Tesla both offer financial incentives to any hacker who can

38. Peter Campbell and Patti Waldmeir, "Google keeps self-driving cars offline to hinder hackers" *The Financial Times*, Jan. 10, 2017, <https://www.ft.com/content/8eff8fbed6f0-11e6-944b-e7eb37a6aa8e>.

39. *Waymo Safety Report*, <https://storage.googleapis.com/sdc-prod/v1/safety-report/waymo-safety-report-2017-10.pdf>

40. Andreas Kuehn and Milton Mueller, "Analyzing Bug Bounty Programs: An Institutional Perspective on the Economics of Software Vulnerabilities," *The 42nd Research Conference on Communication, Information and Internet Policy*, April 1, 2014, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2418812.

proactively identify and disclose substantive software flaws in their connected car systems.⁴¹

More coordinated efforts are also underway. For instance, the Automotive Information Sharing and Analysis Center (Auto-ISAC) serves as an information clearinghouse for companies that “represent 99 percent of light-duty vehicles on the road in North America.”⁴² As part of their participation, members flag and submit susceptibilities they encounter to the ISAC, which then pushes out updates to all member organizations as solutions are discovered. In this way, manufacturers can share emerging cyber vulnerabilities with each other in a safe and secure manner.

Development of best practices

In addition to these efforts, standard-setting bodies and industry groups can help cybersecurity best practices become formalized across the industry. To this end, the ISAC publishes regular best practices reports compiled from subject matter experts working within its member organizations.⁴³ With such a large pool of members, the ISAC and groups like it serve as focal points for the adoption of new security standards both internationally and domestically.⁴⁴

Other groups like the Society of Automotive Engineers (SAE),⁴⁵ International Standards Organization,⁴⁶ Alliance of Automobile Manufacturers⁴⁷ and the Center for Internet Security⁴⁸ have each developed, or are currently developing frameworks for automotive cybersecurity best practices and standards of their own. The existence of multiple trade groups and standard-setting bodies is an important sign of health for the industry. Not only does this decrease the odds that any one group overlooks an important facet of cyber-

security, but if different approaches and architectures are championed by each body and adopted by manufacturers, the chances of a single vulnerability affecting the entire industry is reduced.⁴⁹

Third parties like insurance companies are also set to be major players in crafting the industry standards that govern connected and autonomous vehicles. Because individuals and fleet operators are still mandated to demonstrate proof of financial responsibility while operating on public roads, companies that shoulder the risk associated with state requirements also have the ability to encourage best practices via their risk-transfer agreement terms. For instance, insurance companies like Farmers Insurance have been testing and partnering with connected car services to assess the risks of rollout and have then lowered insurance premiums accordingly.⁵⁰ As with past vehicle safety developments, insurance companies will act as powerful coordinators and motivators in the development of industry self-regulatory and safety standards.

All of the aforementioned industry efforts are flexible and responsive, and will continue to evolve and adapt over time. For this reason, it is vital that we consider the ways in which current and future regulatory efforts might stifle or crowd out these forms of “private regulation.”

CURRENT REGULATORY STRUCTURE

Currently, there are more than 50 different federal statutes that address various aspects of cybersecurity, either directly or indirectly. There is thus no single comprehensive legislative framework.⁵¹ On its face, this is not necessarily problematic, as the level of cybersecurity concern and the types of appropriate solutions will vary from one sector to another. However, an overview of the various entities and their approaches helps to explain some of the confusion that arises around regulatory jurisdiction with respect to cybersecurity.

The most significant federal statute that governs the level of internal cybersecurity that executive agencies or national security systems must provide is the Federal Information Security Modernization Act of 2014 (FISMA),⁵² an update

41. See, Dan Lohrmann, “Auto Industry Bug Bounty Programs Point to Our Security Future,” *Government Technology*, July 17, 2016. <http://www.govtech.com/blogs/lohmann-on-cybersecurity/auto-industry-bug-bounty-programs-point-to-our-security-future.html>; “Bugcrowd: Program Details,” Tesla, 2017. <https://bugcrowd.com/tesla>.

42. “Frequently Asked Questions,” Automotive Information Sharing and Analysis Center, 2017. <https://www.automotiveisac.com/faq.php>.

43. *Automotive Cybersecurity Best Practices*, Automotive Information Sharing and Analysis Center, July 2016. <https://www.automotiveisac.com/best-practices>.

44. Consider, for example, the consistent evolution of international cellular standards, which have been modified many times over the past 20 years without specific device mandates. See, e.g. “The Evolution of Mobile Technologies: 1G 2G 3G 4G LTE,” Qualcomm, June 2014. <https://goo.gl/tqDhNH>.

45. *Cybersecurity Guidebook for Cyber-Physical Vehicle Systems*, SAE International, Feb. 19, 2016. <http://standards.sae.org/wip/j3061>.

46. “ISO/SAE AWI 21434 Road Vehicles -- Cybersecurity engineering,” International Organization for Standardization, 2017. <https://www.iso.org/standard/70918.html>.

47. *Framework for Automotive Cybersecurity Best Practices*, Alliance of Automobile Manufacturers and Global Automakers, Jan. 1, 2016. <https://www.globalautomakers.org/system/files/document/attachments/framework.autocyberbestpractices.14jan20161.pdf>.

48. “CIS Controls,” Center for Internet Security, 2017. <https://www.cisecurity.org/controls>.

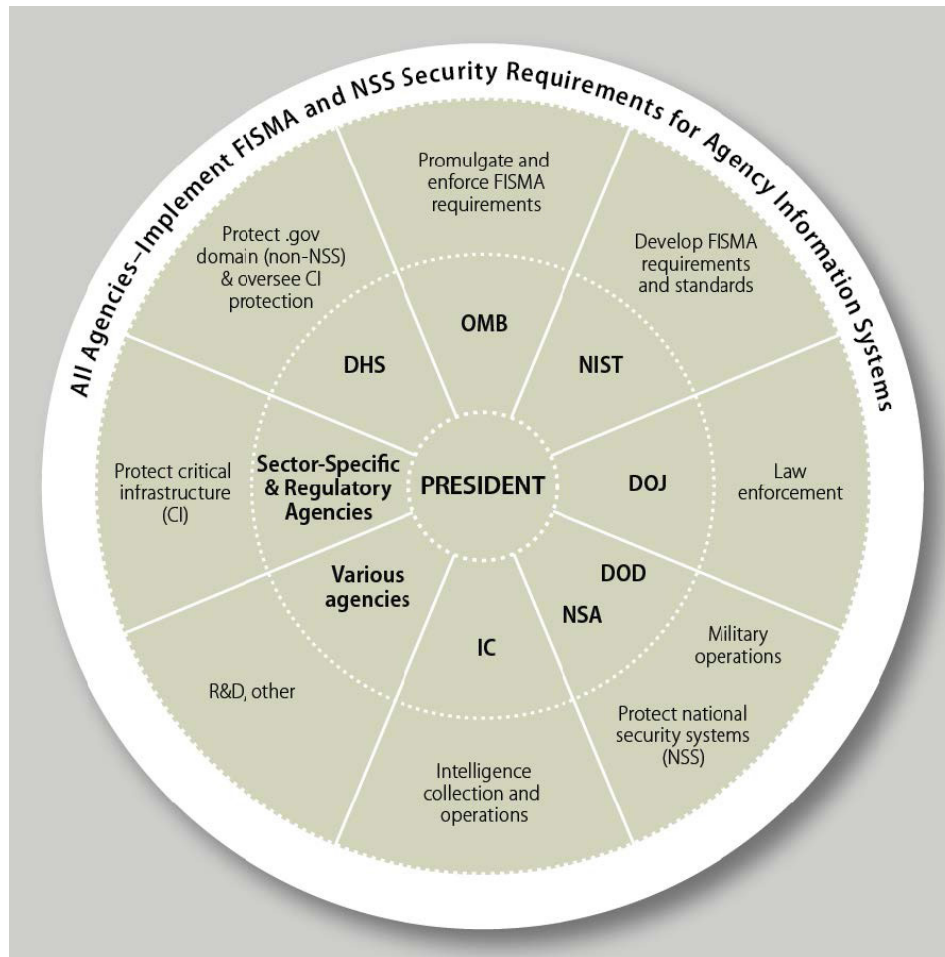
49. “NHTSA and Vehicle Cybersecurity,” *National Highway Traffic Safety Administration*, 2016. <https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/documents/nhtsavehicle-cybersecurity2016.pdf>

50. Danielle Muoio, “Tesla is pushing the insurance industry to prepare for massive disruption,” *Forbes*, May 25, 2017. <http://www.businessinsider.com/how-tesla-self-driving-cars-are-changing-insurance-industry-2017-5>

51. Eric A. Fischer, “Federal Laws Relating to Cybersecurity: Overview of Major Issues, Current Laws, and Proposed Legislation,” Congressional Research Service, 7-5700, Dec. 12, 2014. <https://fas.org/sgp/crs/natsec/R42114.pdf>

52. 44 USC 3551, “Federal Information Security Modernization Act of 2014,” Public Law 113–283. 113th Congress, Dec. 18, 2014. <https://www.congress.gov/113/plaws/publ283/PLAW-113publ283.pdf>.

FIGURE 2: DIAGRAM OF FEDERAL AGENCY CYBERSECURITY ROLES



SOURCE: Congressional Research Service¹

1. Eric A. Fischer, "Cybersecurity Issues and Challenges: In Brief," Congressional Research Service, Aug. 12, 2016. <https://fas.org/sfp/crs/misc/R43831.pdf>.

of the original 2002 law.⁵³ FISMA gives authority to the Office of Management and Budget (OMB) to propagate new cybersecurity processes that must be followed by their fellow agencies, and directs the Department of Homeland Security (DHS) to help other executive agencies develop their own cybersecurity strategies.

FISMA is complemented by Presidential Policy Directive 21 (PPD-21), which designated 16 areas of critical infrastructure and assigns sector-specific agencies (SSAs) to govern the cybersecurity of each part.⁵⁴ Together, FISMA and PPD-21 create a basic federal framework in which all federal agen-

cies have cybersecurity responsibilities that relate to their own internal systems. Many also have sector-specific oversight over a particular part of the economy.

Two recent executive orders (EOs) have reinforced this general division: both have focused primarily on cybersecurity process reform internal to the executive agencies and have reaffirmed the need for oversight of critical infrastructure by SSAs.⁵⁵ Along with PPD-21, these executive orders give fairly broad discretion to the SSAs to determine what forms of oversight might be necessary to maintain critical infrastructure. However, they do so without assigning any new statutory authorities to them.

53. H.R. 3844, "Federal Information Security Management Act of 2002," Public Law 107-347 107th Congress, Dec. 17, 2002. <https://www.congress.gov/bill/107th-congress/house-bill/3844>.

54. Office of the Press Secretary, "Presidential Policy Directive -- Critical Infrastructure Security and Resilience," The White House, Feb. 12, 2013. <https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil>.

55. See, e.g., Office of the Press Secretary, "Executive Order—Improving Critical Infrastructure Cybersecurity," The White House, Feb. 12, 2013. <https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity>; Office of the Press Secretary, "Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure," The White House, May 11, 2017. <https://www.whitehouse.gov/the-press-office/2017/05/11/presidential-executive-order-strengthening-cybersecurity-federal>.

The core contribution of these EOs was the initial development of the National Institute of Standards and Technology (NIST) Cybersecurity Framework (in the 2013 EO) and the later mandate that executive branch agencies document and follow the NIST Framework (in the 2017 EO).⁵⁶ Created as a collaboration between industry groups and government officials, the framework consists of guidelines, standards and practices for the promotion and protection of critical infrastructure. While significant in its own right, the framework has also been used as the basis and/or starting point for many subsequent best practice documents from standard-setting organizations and private companies.⁵⁷

With this understanding of the overarching regulatory landscape of general cybersecurity, we can turn more specifically toward that associated with connected vehicles. These reside under the “transportation” designation of critical infrastructure. As such, they fall under the co-SSA assignment of the DHS and the U.S. Transportation Department (DOT).⁵⁸ However, the Federal Trade Commission also plays an adjacent role to protect the cybersecurity of stored data.

Department of Homeland Security (DHS)

While the DHS has issued occasional guidance documents and has participated in ongoing cybersecurity task forces, they have largely allowed the DOT to set the direction for day-to-day cybersecurity enforcement in the domain of connected vehicles. Their most relevant, recent document was the 2015 “Transportation Systems Sector Cybersecurity Framework Implementation Guidance,” and its companion workbook, which provides practical advice and commentary on applying the NIST Framework within the transportation industry. However, neither of these contributions specifically addresses motor vehicles or issues any binding requirements.⁵⁹

In the event of a coordinated cybersecurity attack by a hostile nation-state or terrorist organization, DHS would be most relevant under their authority from the Cybersecurity Information Sharing Act (CISA) of 2015. CISA also gives the DHS statutory authority to “(1) issue emergency directives to agencies in response to a substantial information security

threat, vulnerability, or incident; or (2) authorize intrusion detection and prevention capabilities to secure agency information systems in the case of an imminent threat.”⁶⁰

Until such time as a direct national security attack occurs, DHS has delegated its part of the co-SSA responsibilities to its sub-agencies the Transportation Security Administration (TSA) and the U.S. Coast Guard (USCG). DOT, TSA and the USCG jointly perform the co-SSA functions through a steering group and co-leadership of government coordinating councils.⁶¹

National Highway Traffic Safety Administration (NHTSA)

The DOT’s NHTSA is the federal regulator charged with vehicle safety more broadly. As such, it has played an important coordinating role between other federal agencies and the vehicle manufacturers themselves.⁶² Given the comparative expertise and relevant skillsets of NHTSA, it has been positioned through the co-SSA steering group as the primary regulator of motor vehicle cybersecurity, both as it pertains to the safe operation of motor vehicles and in its capacity as a piece of critical national infrastructure.

Thus far, NHTSA’s most overarching work on connected and autonomous vehicles has been the creation and subsequent update—in 2016 and 2017, respectively—of the Federal Automated Vehicle Policy (FAVP).⁶³ The policy is intended as a nonbinding and evolutionary document for stakeholders from all interested industries.⁶⁴ It includes a 12-point voluntary safety self-assessment that manufacturers can use to open lines of communication with NHTSA and to give them an overview of their strategies for validation testing, crash

56. *Framework for Improving Critical Infrastructure Cybersecurity*, National Institute of Standards and Technology, Feb. 12, 2014. <https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf>.

57. For instance, the Auto-ISAC mentions that the NIST Framework was one of the baselines from which it developed its own cybersecurity best practices. See, e.g., “Automotive Cybersecurity Best Practices,” Automotive Information Sharing and Analysis Center, July 2016. <https://www.automotiveisac.com/best-practices>.

58. “Presidential Policy Directive -- Critical Infrastructure Security and Resilience,” <https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil>.

59. *Transportation Systems Sector Cybersecurity Framework Implementation Guidance*, U.S. Dept. of Homeland Security, June 26, 2015. https://www.dhs.gov/sites/default/files/publications/tss-cybersecurity-framework-implementation-guide-2016-508v2_0.pdf.

60. The purpose of CISA was “[t]o improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes.” Accordingly, it requires the Director of National Intelligence and the Departments of Homeland Security, Defense and Justice to share cybersecurity threat information with private entities, states and nonfederal government agencies in scenarios where they might be at risk. See, S.754, 114th Congress, Oct. 28, 2015. <https://www.congress.gov/bill/114th-congress/senate-bill/754>. It was later incorporated and passed in H.R.2029, as the “Consolidated Appropriations Act, 2016,” Public Law No: 114-113, 114th Congress, Dec. 18, 2015. <https://www.congress.gov/bill/114th-congress/house-bill/2029>.

61. *Transportation Systems Sector-Specific Plan*, Department of Homeland Security and Department of Transportation, 2015. <https://www.dhs.gov/sites/default/files/publications/nipp-ssp-transportation-systems-2015-508.pdf>.

62. Most recently, NHTSA was reauthorized as an agency through the MAP21 Act. H.R.4348, “Moving Ahead for Progress in the 21st Century Act,” Public Law No: 112-141, 112th Congress, July 6, 2012. <https://www.congress.gov/bill/112th-congress/house-bill/4348/text>.

63. National Highway Traffic Safety Administration, *Federal Automated Vehicles Policy*, U.S. Dept. of Transportation, September 2016. <https://www.transportation.gov/sites/dot.gov/files/docs/AV%20policy%20guidance%20PDF.pdf>; and National Highway Traffic Safety Administration, *Automated Driving Systems 2.0: A Vision for Safety*, U.S. Dept. of Transportation, September 2017. https://www.nhtsa.gov/sites/nhtsa.dot.gov/files/documents/13069a-ads2.0_090617_v9a_tag.pdf.

64. Examples include original equipment manufacturers, component manufacturers and insurers (among others).

worthiness, cybersecurity, data recording and other related areas.

In October 2016, NHTSA released another guidance document concerning cybersecurity. The “Cybersecurity Best Practices for Modern Vehicles” document⁶⁵ was the result of a multiyear development process. It is incorporated by reference into the FAVP and thus is similarly intended to be nonbinding. However, unlike the FAVP’s treatment of cybersecurity, the best practices document offers concrete recommendations for manufacturers to follow as they develop their vehicles.⁶⁶

In addition to these significant guidance documents, the NHTSA has actively convened roundtables with security researchers and industry experts, tested the safety of various wireless communication technologies through pilot programs, and issued extensive technical reports on the capabilities and threats of various electronic systems used in motor vehicles.⁶⁷

NHTSA’s primary method of regulatory enforcement is through its post-market compliance testing of Federal Motor Vehicles Safety Standards (FMVSS) and through its recall authority.⁶⁸ Essentially, the NHTSA lays out the specific technical standards a manufacturer must meet in order to deploy a vehicle legally. Manufacturers self-certify that they meet these standards and the NHTSA selectively tests the deployed vehicles to ensure that they are, in fact, in compliance. If a manufacturer is found to be not in compliance with a specific FMVSS or otherwise poses an unreasonable risk to consumer safety, the NHTSA uses its broad recall authority to force it to fix the defect or to remove the car from circulation. However, most decisions to conduct a recall and remedy a safety defect are made voluntarily by manufacturers before any involvement by NHTSA.⁶⁹

To date, the NHTSA has not issued any specific FMVSS that pertain to cybersecurity, which has led some legislators to question whether the agency is taking the issue seriously enough.⁷⁰ However, the NHTSA’s approach is an apt recognition of the

pace of technological change and the difficulty of using traditional regulatory models to govern emerging technologies.⁷¹ As NHTSA Administrator Mark Rosekind has explained:

A traditional approach to regulating these new technologies would be to engage solely in rulemaking process, writing new regulations that prescribe specific standards. Our view is that approach would stymie innovation and stall the introduction of these technologies [...] Any rule we might offer today would likely be woefully out-of-date by the time it took effect, given the pace of technological development.⁷²

This may help to explain NHTSA’s reliance thus far primarily on voluntary guidance and the promotion of cybersecurity best practices.⁷³

Federal Trade Commission (FTC)

For issues of cybersecurity that do not relate specifically to the safe operation of a motor vehicle, regulatory jurisdiction falls to the FTC, which has frequently used its authority under Section 5 of the FTC Act to prosecute companies it deems are using unfair or deceptive acts and practices as a form of cybersecurity enforcement.⁷⁴ For instance, if an auto manufacturer suffers a data breach that includes sensitive consumer information, it would be incumbent upon the FTC to hold them accountable. The FTC’s recently announced investigation into the Equifax data breach of 2017 serves as an example of this after-market regulatory approach.⁷⁵

In summary, the current policy framework primarily regulates executive agencies in their cybersecurity efforts through FISMA, but also assigns specific regulators for criti-

71. For more on the pacing problem see: Adam Thierer, “Wendell Wallach on the Challenge of Engineering Better Technology Ethics,” *The Technology Liberation Front*, April 20, 2016. <https://techliberation.com/2016/04/20/wendell-wallach-on-the-challenge-of-engineering-better-technology-ethics>.

72. “Hearing: Disrupter Series: Self-Driving Cars,” House Energy and Commerce Subcommittee, Nov. 16, 2016. <https://energycommerce.house.gov/hearings/disrupter-series-self-driving-cars>.

73. In early 2017, NHTSA did propose a new FMVSS (No. 150), which would mandate the inclusion of V2V communications for new light vehicles and standardize the message and format of V2V transmissions through DSRC. The proposed rule is complex and covers a wide range of areas, some of which are outside of the agency’s traditional regulatory boundaries. NHTSA is not certain whether the estimated costs for DSRC-based proposals would be comparable to that of alternative interoperable technologies. Given pushback from industry and security researchers on the potential harms of mandating a technology that could quickly become out-of-date, NHTSA has since delayed the implementation of this rulemaking. See, e.g., Joshua Higgins, “NHTSA delays regulation for connected cars amid industry’s cybersecurity concerns,” *Inside Cybersecurity*, Sept. 1, 2017. <https://insidecybersecurity.com/daily-news/nhtsa-delays-regulation-connected-cars-amid-industrys-cybersecurity-concerns>.

74. “A Brief Overview of the Federal Trade Commission’s Investigative and Law Enforcement Authority,” U.S. Federal Trade Commission, July 2008. <https://www.ftc.gov/about-ftc/what-we-do/enforcement-authority>.

75. Brian Fung and Hamza Shaban, “The FTC is investigating the Equifax breach. Here’s why that’s a big deal,” *The Washington Post*, Sept. 14, 2017. <https://www.washingtonpost.com/news/the-switch/wp/2017/09/14/the-ftc-confirms-its-investigating-the-equifax-breach-adding-to-a-chorus-of-official-criticism>.

65. National Highway Traffic Safety Administration, “U.S. DOT issues Federal guidance to the automotive industry for improving motor vehicle cybersecurity,” U.S. Dept. of Transportation, Oct. 24, 2016. <https://www.nhtsa.gov/press-releases/us-dot-issues-federal-guidance-automotive-industry-improving-motor-vehicle>.

66. See, Adams. <https://www.bna.com/internet-things-era-n73014449118>.

67. National Highway Traffic Safety Administration, *Automotive Cybersecurity: Overview*, U.S. Dept. of Transportation, 2017. <https://www.nhtsa.gov/crash-avoidance/automotive-cybersecurity>.

68. NHTSA receives its statutory regulatory authority to issue FMVSS and corresponding recalls from 49 U.S. Code Chapter 301.

69. National Highway Traffic Safety Administration, “Safety Issues & Recalls,” U.S. Dept. of Transportation 2017. <https://www.nhtsa.gov/recalls>.

70. Sens. Ed Markey, D-Mass., and Richard Blumenthal, D-Conn., have criticized the agency for not developing new FMVSS specifically for privacy and cybersecurity. This is discussed in detail below.

cal infrastructure under PPD-21. In the case of transportation, this falls to the DOT and DHS. In practice, however, the NHTSA is the primary regulator for automotive cybersecurity, DHS assists during coordinated national security attacks and the FTC covers the cybersecurity of related data while it is held in company storage.

EFFECTIVE APPROACHES TO FUTURE POLICY

While the current regulatory framework adequately covers many of the existing risks, there is room for improvement and a robust, open and coordinated effort is necessary in order to realize the potential of connected cars. Accordingly, the government needs better general cyber hygiene, a simplified policy framework and a way of reconciling NHTSA's traditional after-market oversight with the unique challenges of cybersecurity. A successful policy approach should result in a speedy rollout of connected and autonomous vehicles, strengthened cybersecurity systems and a reduction in human fatalities on the road.

Public safety balance

First, it is important to frame the discussion not in an ideal situation where autonomous cars never make mistakes and connected vehicles never suffer from cyber vulnerability, but rather in the messy status quo we inhabit today. At its heart, the need for AV/CV technology addresses a significant public safety problem. Accordingly, every policy action that pertains to connected and autonomous vehicles should be judged by how quickly it moves us away from the current baseline of 40,000 auto fatalities a year,⁷⁶ as each day of unnecessary delay is deadly. For this reason, it is important to balance the costs of unwarranted regulatory delay on the one hand, with the potential for cybersecurity to be underprovided or overlooked on the other.

Regulatory delay can occur both when the path to deployment is slowed by explicit regulatory barriers, or more subtly, when technical mandates require unnecessary systems that increase the per-unit cost and thus reduce the number of consumers able to purchase the vehicle or service. A recent study issued by the Mercatus Center found that with a delay in deployment of these vehicles by even 5 percent, we could see an additional 15,000 fatalities over the next 30 years.⁷⁷

On the other side of this balance is the potential for cybersecurity to be chronically underprovided by the industry or

for particular actors within the market to overlook its provision. There is some theoretical backing for this idea, at least as it pertains to traditional internet companies.⁷⁸ However, traditional regulatory approaches tend to be ineffective at fixing this kind of problem, given the difficulty of measuring security and the rapid pace of change that standards require to stay up to date.

Furthermore, when variables like product liability, tort law, standard-setting bodies, cyber insurance and potential publicity scandals come into the picture, the incentives for any given manufacturer can be nudged in favor of more cybersecurity investment.⁷⁹

All of this should lead us to the conclusion that, while cybersecurity is certainly important, there is some margin at which additional levels of cyber-safety are actually counterproductive to the larger policy goal of reducing auto fatalities. It is hard to know exactly where this line is, but it is clear that we nudge closer to a balanced regulatory approach when manufacturers have incentives to provide appropriate cybersecurity themselves, rather than relying on regulators to forecast a single "correct" strategy.⁸⁰

PROPOSED CYBERSECURITY LEGISLATION

While NHTSA has largely been content to focus on the continued development of best-practice documents and cybersecurity guidance, some legislators at both the state and national levels have been pushing for government regulators to do more in the realm of automotive cybersecurity legislation. These proposals range from specific technical standards, to general cyber hygiene, to better information-sharing efforts. Below, we evaluate these ongoing legislative efforts.

Internet of Things Cybersecurity Improvement Act (IoTCI)

Sponsored by Sens. Mark Warner, D-Va., Cory Gardner, R-Colo., Ron Wyden, D-Ore., and Steve Daines, R-Mont., the Internet of Things Cybersecurity Improvement (IoTCI) Act of 2017, if passed, would be a good step toward general cyber

76. See, Halsey III. https://www.washingtonpost.com/local/trafficandcommuting/traffic-deaths-soared-past-40000-last-year-as-economy-continued-to-improve/2017/02/15/fd1e8298-f388-11e6-8d72-263470bf0401_story.html?utm_term=.20229fd47ebc.

77. Adam Thierer and Caleb Watney, "Comment on the Federal Automated Vehicles Policy," *Mercatus Center Public Interest Comments*, Dec. 5, 2016. <https://www.mercatus.org/publications/comment-federal-automated-vehicles-policy>.

78. Alfredo Garcia and Barry Horowitz, "The Potential for Underinvestment in Internet Security: Implications for Regulatory Policy," University of Virginia, February 2006. <http://webcache.googleusercontent.com/search?q=cache:http://weis2006.econinfosec.org/docs/24.pdf>

79. Institute for Legal Reform, "Torts of the Future: Addressing the Liability and Regulatory Implications of Emerging Technologies," U.S. Chamber of Commerce, June 14, 2017. <http://www.instituteforlegalreform.com/research/torts-of-the-future->

80. For more on the potential for cybersecurity market failures and market responses see, Eli Dourado, "Is There a Cybersecurity Market Failure," *Mercatus Working Paper*, Jan. 23, 2012. https://www.mercatus.org/system/files/Cybersecurity_Dourado_WP1205_0.pdf.

hygiene by the federal government.⁸¹ This would require all “internet of things” (IoT) devices purchased by the government to be compliant with the NIST Best Practices framework. Potentially, this could have positive spillover effects for various regulated industries, particularly if the agencies in question have greater levels of technical sophistication about their own cybersecurity systems.⁸²

SPY Car Acts of 2015 and 2017

In 2015, Sen. Ed Markey, D-Mass., issued a report that purported to demonstrate there was a lack of appropriate security measures to protect drivers against hackers who may be able to take control of a vehicle, or against those who may wish to collect and use personal driver information.⁸³ Accordingly, Markey and fellow Sen. Richard Blumenthal, D-Conn., called for binding FMVSS to be set for both cybersecurity and for the privacy of connected and autonomous vehicles.⁸⁴ This legislation did not attempt to list specific cybersecurity standards to be made into FMVSS, but instead directed NHTSA to consult with the FTC and develop standards for hacking protection, data security and hacking mitigation, as well as for the creation of a few additional privacy standards within two years.

While this specific legislative effort failed, the impetus to enshrine specific cybersecurity technical mandates within the FMVSS has continued to be a significant political force. Most recently, Rep. Joe Wilson, R-S.C., introduced a very similar bill in the House in 2017.⁸⁵

As the NHTSA has recognized, the problem with this approach is that FMVSS enforcement of cybersecurity would be too slow and too rigid a process to keep up with the quickly evolving world of cybersecurity.⁸⁶ Even if the NHTSA were able to precisely choose the optimal level of cybersecurity provision, it could become quickly out-of-date—perhaps even before the rule could take effect. Each time the NHTSA seeks to add or modify an FMVSS, they must go through a lengthy notice-and-comment rulemaking

process whereby the public is allowed to give input on the proposed rule. It frequently can take over a year between the drafting of the rule, comment period and final publication. At minimum, the process would have to incorporate the traditional 60-day comment period.⁸⁷ If it were discovered that some new exploit required an immediate change to cybersecurity standards to prevent future vulnerabilities, the slow FMVSS update process would be ill-equipped to handle it.

There is also the need to prevent a homogeneous security monoculture. Because all manufacturers must certify they meet the FMVSS before deploying vehicles on the road, there will inevitably be more similarities in vehicle architectures and defensive capabilities between manufacturers. Essentially, when all automakers are required to meet specific, technical cybersecurity requirements, the likelihood increases that a given vulnerability will affect all manufacturers simultaneously.⁸⁸ As previously mentioned, one of the single most reliable determinants of the severity of a cyber-attack is the sheer number of vehicles affected. A scenario in which every single car is potentially compromised is dire indeed. In view of this, a better approach would use the different recommendations of various standard-setting bodies to increase the level of overall security without putting all of our eggs into one regulatory basket.

In spite of these factors, the NHTSA may still determine that there are occasional times when ensuring some level of lowest-common-denominator security or coordination is worth the trade-offs of slow response times and security homogeneity.⁸⁹ But these identified regulatory issues should certainly prevent the NHTSA from making FMVSS the primary mechanism for automotive cybersecurity enforcement, which is the SPY Car Acts recommend.

SELF DRIVE and AV START Acts

To date, the most significant push for a federal legislative framework specifically for connected and autonomous cars has come this year with the House’s SELF DRIVE Act⁹⁰

81. S.1691, “Internet of Things (IoT) Cybersecurity Improvement Act of 2017,” Sen. Mark Warner, 115th Congress, Aug. 1, 2017. <https://www.congress.gov/bill/115th-congress/senate-bill/1691/text?format=txt>.

82. Nicholas Weaver, “The Internet of Things Cybersecurity Improvement Act: A Good Start on IoT Security,” *Lawfare*, Aug. 2, 2017. <https://www.lawfareblog.com/internet-things-cybersecurity-improvement-act-good-start-iot-security>.

83. Office of Senator Edward Markey, *Tracking & Hacking: Security & Privacy Gaps Put American Drivers at Risk*, February 2015. https://www.markey.senate.gov/imo/media/doc/2015-02-06_MarkeyReport-Tracking_Hacking_CarSecurity_2.pdf.

84. S.1806, “SPY Car Act of 2015,” Sen. Edward Markey, 114th Congress, July 21, 2015. <https://www.congress.gov/bill/114th-congress/senate-bill/1806>.

85. H.R. 701, “SPY Car Study Act of 2017,” Rep. Joe Wilson, 115th Congress, Jan. 24, 2017. <https://www.congress.gov/bill/115th-congress/house-bill/701/text>.

86. As noted in the NHTSA section, see former NHTSA administrator Dr. Mark Rosekind’s comments here: “Hearing: Disrupter Series: Self-Driving Cars,” House Energy and Commerce Subcommittee, Nov. 16, 2016. <https://energycommerce.house.gov/hearings/disrupter-series-self-driving-cars>.

87. National Highway Traffic Safety Administration “Rulemaking Process,” U.S. Dept. of Transportation, 2017. <https://www.transportation.gov/regulations/rulemaking-process>.

88. See, e.g., Bruce Schneier, “The Dangers of a Software Monoculture,” *Schneier on Security*, November 2010. https://www.schneier.com/essays/archives/2010/11/the_dangers_of_a_sof.html; and Kreilein. <http://glenechogroup.isebox.net/secure-taccelerator/dedicated-short-range-communications-dsrc-expose-critical-gaps-in-security-and-privacy>.

89. For instance, if all manufacturers agree to communicate V2V using a wireless 5G network, the benefits of coordination may outweigh the additional cybersecurity risks that come from homogeneity. However, it also seems likely that industry standard-setting bodies could make this tradeoff with more flexibility and local knowledge than the NHTSA.

90. H.R.3388, “SELF DRIVE Act,” 115th Congress, July 25, 2017. <https://www.congress.gov/bill/115th-congress/house-bill/3388>.

and the Senate's AV START Act.⁹¹ Each proposal is broadly aimed at clearing regulatory hurdles for the deployment of autonomous vehicles and both include specific sections with respect to cybersecurity.

In exchange for broad pre-emption from state and local regulations on the security, design and performance of autonomous vehicles, both of these bills take the voluntary safety self-assessment letter that NHTSA developed as part of its FAVP and make it mandatory. In addition, they each require written cybersecurity plans from auto manufacturers that "cover a process for identifying, assessing, and mitigating reasonably foreseeable vulnerabilities from cyber attacks or unauthorized intrusions, including false and spurious messages and malicious vehicle control commands."⁹² Additionally, the AV START Act's cybersecurity section requires manufacturers to answer a few additional questions about their cybersecurity practices and authorizes the DOT to create incentives for voluntary disclosure of vulnerabilities. However, the bills are fairly consistent in their overall content.

If one of these bills (or a unified version which emerges from a conference committee) becomes law, it would not be a radical departure from the NHTSA's existing cybersecurity approach. It would certainly be the first time that auto manufacturers are required to submit a full cybersecurity plan before deploying connected vehicles, but the NHTSA would be barred from keeping cars off the road based solely on their answers to those cybersecurity questions. Practically speaking, this would be more of an information-sharing arrangement than a traditional regulatory one. There could certainly be scenarios where manufacturers change their practices or behavior because they know their answers are being read by regulators, but this process would look more like an experiment in soft law than hard law.⁹³

If adopted, the overall effect of this new cybersecurity provision will likely depend more on what the NHTSA decides to do with all this new information, rather than on its mere collection. If the agency centralizes all the sensitive cybersecurity details in a single digital location, it will become an attractive target for would-be hackers. Further, if the NHTSA uses the data to implement specific cybersecurity standards as FMVSS, they could quickly become out of date. Alternatively, if the NHTSA uses the information to facilitate a more productive dialogue about the weak points of the

industry's cybersecurity strategies, then it could be a positive step forward.

State efforts

Faced with ambiguity from the federal government, some states have elected to take legislative and regulatory steps specifically related to the cybersecurity of connected vehicles. To this end, Massachusetts⁹⁴ and Pennsylvania⁹⁵ have each introduced legislation directing state regulatory bodies to promulgate regulations that set standards to ensure the security of vehicle cyber systems. While neither of these legislative efforts have yet been passed into law, they nevertheless represent a potentially troubling trend.

States and cities care and want to be involved in the development, deployment and governance of autonomous vehicles. Yet when it comes to cybersecurity, a multiplicity of state and city rules would be both cumbersome and costly to monitor and to comply with. Furthermore, the level of technical sophistication required to be an effective cybersecurity regulator is something that even federal agencies with substantially more financial resources struggle to keep up with. To imagine that all the various state and local regulators—with little, if any, experience in cybersecurity policy—will be able to manage the nuanced network of challenges seems overly optimistic, to say the least.

If some version of the federal pre-emption laid out in the AV START or SELF DRIVE Act makes it into law, this discussion will become moot, because the NHTSA will have sufficient authority to overrule attempted cybersecurity policies that would interfere with the performance of motor vehicles. However, if a unifying federal framework fails to be adopted, the issue of regulatory uncertainty could come to the forefront, as additional states continue to pursue their own, potentially conflicting, automobile cybersecurity frameworks.⁹⁶

Among these various legislative efforts, the IoTCI Act and some version of the SELF DRIVE/AV START acts seem likely to have a positive effect on the cybersecurity of the indus

91. S.1885, "AV START Act," 115th Congress, Sept. 28, 2017. <https://www.congress.gov/bills/115/congress/senate-bill/1885>.

92. H.R.3388. <https://www.congress.gov/bills/115th-congress/house-bill/3388>.

93. For more on the distinction between hard and soft law and the way these concepts are developing within NHTSA, in particular see e.g., Adam Thierer, "DOT's Driverless Cars Guidance: Will 'Agency Threats' Rule the Future," *The Technology Liberation Front*, Sept. 20, 2016. <https://techliberation.com/2016/09/20/dots-driverless-cars-guidance-will-agency-threats-rule-the-future>.

94. House No. 1829, "An Act to Promote the Safe Integration of Autonomous Vehicles into the Transportation Systems of the Commonwealth," In the One Hundred and Ninetieth General Court, Feb. 24, 2017. https://custom.statenet.com/public/resources.cgi?id=ID:bill:MA2017000H1829&ciq=AsteigenHAV&client_md=de0c7elfcccd35da566b7a8e318fada4&mode=current_text.

95. Senate Bill No. 427, "An Act Amending Title 75 (Vehicles) of the Pennsylvania Consolidated Statutes, in operation of vehicles, providing for highly automated vehicles and platooning testing," The General Assembly of the Commonwealth of Pennsylvania, Feb. 24, 2017. https://custom.statenet.com/public/resources.cgi?id=ID:bill:PA2017000S427&ciq=AsteigenHAV&client_md=161c1654ee34c8b8236a55923b6172f5&mode=current_text.

96. For a longer discussion of the problems with regulatory uncertainty and the need for federal preemption, see Watney and Adams. <http://www.rstreet.org/wp-content/uploads/2017/04/FTC-CV-Comments-RSI-2.pdf>.

try, while the SPY Car Act and a state patchwork of cybersecurity standards could do more harm than good.

A BETTER WAY FORWARD

Cybersecurity of connected cars is a more recent challenge than vehicle safety writ large, but with some tweaks, established regulatory procedures can be used to address contemporary cybersecurity challenges. The principal regulatory mechanism that the NHTSA uses to enforce FMVSS is founded in its post-market recall authority and the related steps associated with its enforcement. Since its inception 60 years ago, the recall system has successfully balanced the competing needs of public safety and innovation, particularly in comparison to alternative regulatory approaches like the pre-market approval structure used by the Federal Aviation Administration.⁹⁷ For this reason, while the FMVSS regulatory structure has substantial drawbacks when used for cybersecurity, the post-market recall authority may be a more fruitful policy instrument.

As questions about cybersecurity become more pertinent to the safe operation of motor vehicles via autonomous and connected technologies, extending the NHTSA recall model may provide policymakers and consumers with the confidence necessary to forestall the adoption of overly prescriptive alternative measures. Steps could include:

1. The NHTSA requires manufacturers (by a fixed date) to provide written in-depth answers to questions on the capabilities and characteristics of their cybersecurity plans, the types of attacks they should be able to thwart, various levels of redundancy and layered defenses they have installed, and how their vehicles should perform if attacked.
2. The NHTSA makes nonsensitive/nonconfidential answers available to the public. This will allow intra-industry competition for more comprehensive and effective cyber security plans. Answers that include specific trade secrets or information that should not be disclosed publicly would be carefully controlled, maintained by NHTSA and used only for internal assessments.
3. The NHTSA then would selectively test these manufacturer claims in a manner similar to, and inspired by, its current post-market oversight. They may also contract with white-hat hacker groups to more proactively test the robustness of cybersecurity systems. If a vulnerability is found that is inconsistent with a representation published in the manufacturer's cybersecurity plan and subsequent answers to ques-

tions (either those publicly disclosed or held internally by the NHTSA), the agency would be able to use its existing recall authority to rectify the issue.

There are several advantages to taking such an approach. First, this is an enforcement process with which industry groups and manufacturers are already familiar, which should reduce the level of regulatory uncertainty associated with compliance. Second, it allows the level of cybersecurity enforcement that companies are held responsible for to evolve over time as companies update their publicly available cybersecurity plans. Further, manufacturers have an incentive to tell the public that they have a more rigorous cybersecurity plan than competitors, but also to be honest about their current level of security. The desired end result is that manufacturers will feel an internal compulsion to bring their level of cybersecurity enforcement closer toward current "best practices" in order to stay competitive.

In contrast with the SPY Car Act's suggested FMVSS approach, this approach is significantly more flexible, as it does not require the agency go through the lengthy notice-and-comment rulemaking process every time they seek to update the level of enforced cybersecurity standards. Additionally, because manufacturers may choose to base their cybersecurity plans on a wide selection of available best practice strategies, the level of homogeneity in both vehicle architecture and defensive strategies should be reduced as well. Finally, because manufacturers have more local knowledge about the necessary cybersecurity capabilities of their vehicles and about consumer sensitivity to an increase in prices, they are better able to manage the balance between sufficient cybersecurity defenses and a speedy deployment process.⁹⁸

It is also worth noting that such an approach would be especially compatible in the event that some version of the SELF DRIVE or AV START acts becomes law. Companies would already be required to submit cybersecurity plans to the NHTSA before deployment and to answer specific questions about their capabilities as part of the safety self-assessment letter from the FAVP. The NHTSA could announce their intention to hold companies to the promises listed in their cybersecurity plans via their recall authority and to give manufacturers sufficient time to update their plans accordingly.

98. This overall approach is quite similar to that used by the FTC in their enforcement of cybersecurity in the credit card industry. All major credit card companies have publicly agreed to follow the industry-developed "Payment Card Industry Data Security Standards (PCC-DSS)," which is then enforced by the FTC using their Section 5 "unfair and deceptive practices" authority. Some security researchers have suggested such an approach be used in automotive cybersecurity as well, but this runs into regulatory jurisdiction issues as the FTC is not the designated SSA for transportation. For more on the PCC-DSS model of enforcement and calls to adopt it in automotive cybersecurity, see, Kreilein. <http://glenechogroup.isebox.net/secureaccelerator/dedicated-short-range-communications-dsrc-expose-critical-gaps-in-security-and-privacy>.

97. See, e.g., Thierer and Watney. <https://www.mercatus.org/publications/comment-federal-automated-vehicles-policy>.

This would not require any additional regulatory authority, as the NHTSA's current authority allows it to issue recalls if "a motor vehicle or replacement equipment contains a defect related to motor vehicle safety," where motor vehicle safety is defined as "the performance of a motor vehicle or motor vehicle equipment in a way that protects the public against unreasonable risk of accidents occurring because of the design, construction, or performance of a motor vehicle."⁹⁹ Certainly it would be an "unreasonable risk of accident" if consumers are sold vehicles that do not include the level of cybersecurity promised to them in the manufacturer's public cybersecurity plan.

Furthermore, the government already has experience contracting with white-hat hackers to test the viability of their own cybersecurity systems.¹⁰⁰ In principle, there is no reason the NHTSA could not mirror these programs to test the stated capabilities of the entities they regulate.¹⁰¹

The specific questions that the NHTSA would ask and ultimately adopt as part of this enforcement strategy should be carefully crafted through a multistakeholder model that includes members from the NHTSA, manufacturers, standard-setting bodies, trade associations, independent cybersecurity experts and civil society groups. It is unclear whether the traditional notice-and-comment rulemaking process would have to be undertaken on the specific questions that are agreed upon, but it would most likely be wise. This could act, in effect, as a replacement for specific cybersecurity FMVSS.

Additional policy steps

In addition to the approach listed above, the NHTSA should continue to update their guidance documents on cybersecurity issues (such as their October 2016 report on cybersecurity best practices for modern vehicles)¹⁰² and nonbinding cybersecurity standards. As connected cars interface with intelligent transportation-management systems, electric-charging stations and so forth, NHTSA could expand these standards to address changing technology. NHTSA should

also continue to convene industry roundtables to facilitate data-sharing agreements and the development of best practices.

The Federal Communications Commission (FCC) has a role as a facilitator in spectrum allocation, but should not privilege specific technical standards in V2V communications like DSRC.¹⁰³ Flexible and evolving industry intervehicle communication standards are preferable to fixed and slow-to-change regulatory automotive communications standards.

As recommended by the privacy section of the SELF DRIVE Act, the Federal Trade Commission is well-positioned to hold companies accountable to their claims with regard to privacy and data collection.¹⁰⁴

Procurement regulations like those in the IoTCI Act can be used to promote cyber hygiene and insist that information technology systems delivered to government are more secure. With safer systems available, vendors may be able to offer them to the broader marketplace as well.

States should not attempt to create a patchwork of connected car cybersecurity standards, but rather should encourage the federal government to take necessary action. Cities and states could more productively spend their time developing voluntary data-sharing agreements with manufacturers to start preparing local infrastructure for the future needs of autonomous and connected cars.

CONCLUSION

Connected cars, especially when autonomous, present enormous opportunities for our economy and for public safety. But new risks arise alongside new benefits. The speed of technological innovation means traditional regulatory tools may not be able to keep up. Rather than force new cybersecurity problems through the traditional Federal Motor Vehicle Safety Standards process, we recommend embracing a more flexible regulatory approach that aligns manufacturer incentives, promotes the development of cybersecurity best practices, proactively tests their capabilities and holds companies accountable for their promises.

Legislative and regulatory efforts should focus on support-

99. 49 U.S. Code § 30118, "Notification of defects and noncompliance." <https://www.law.cornell.edu/uscode/text/49/30118>

100. See e.g., Dan Lohrmann, "Why Offering Bug Bounties Will Be Widespread, Even in Government," *Government Technology*, July 16, 2017. <http://www.govtech.com/blogs/lohmann-on-cybersecurity/why-offering-bug-bounties-will-be-widespread-even-in-government.html>;

Mark Rockwell, "Why bug bounty programs are worth the risk," *FCW Magazine*, March 30, 2017. <https://fcw.com/articles/2017/03/30/bug-bounties-gsa-dod.aspx>.

101. Amit Elazari, "Bug Bounty Programs as a Corporate Governance 'Best Practice' Mechanism," *Berkeley Technology Law Journal Blog*, March 22, 2017. <http://btjlj.org/2017/03/bug-bounty-programs-as-a-corporate-governance-best-practice-mechanism>.

102. See, e.g., "U.S. DOT issues Federal guidance to the automotive industry for improving motor vehicle cybersecurity," <https://www.nhtsa.gov/press-releases/us-dot-issues-federal-guidance-automotive-industry-improving-motor-vehicle>.

103. Joe Kane, "For connected cars, let the best technology win," *R Street Institute*, Oct. 2, 2017. <http://www.rstreet.org/2017/10/02/for-connected-cars-let-the-best-technology-win>.

104. See section 12 here: H.R.3388, "SELF DRIVE Act," 115th Congress, July 25, 2017. <https://www.congress.gov/bill/115th-congress/house-bill/3388>. Potential harm from sensitive data breaches and privacy violations from connected cars are outside of the scope of this paper, but as R Street has discussed in previous comments to NHTSA, the current FTC framework should be sufficient when updated. See, e.g., Marc Scribner, Ian Adams, et al., "Comments of the Competitive Enterprise Institute, R Street Institute, and TechFreedom," 81 Fed. Reg. 65703, Docket No. NHTSA-2016-0090, Nov. 22, 2016. <http://www.rstreet.org/wp-content/uploads/2016/12/CEI-et-al-NHTSA-FAVP-guidance-comments.pdf>.

ing market-based security mechanisms, such as fostering independent research, bug bounty programs and general cyber hygiene. They should also empower standard-setting bodies to proactively address cybersecurity issues, promote industry-led certification and testing efforts, share cyber and physical threat information, and encourage collaboration between stakeholders.

ABOUT THE AUTHORS

Caleb Watney is a technology policy associate at the R Street Institute, where he leads R Street's work on emerging technologies, including autonomous vehicles, artificial intelligence, drones, robotics and medical tech. In this role, he regularly meets with policy-makers, files regulatory comments, writes op-eds and manages a technology policy working group.

Cyril Draffin has been project adviser to the MIT Energy Initiative since 2015. He evaluates the cybersecurity of electric utilities: solar, wind, coal, gas and nuclear energy systems; information technology and strategy. He is U.S. representative to the International Energy Agency International Smart Grid Action Network Academy, was cybersecurity lead for the MIT Energy Initiative "Utility of the Future" study, is a mentor at the Mach 37 cybersecurity accelerator and is a member of the Maryland Cybersecurity Council.