NOTE

YOU CAN'T HACK THIS: THE REGULATORY FUTURE OF CYBERSECURITY IN AUTOMOBILES

Liz Allison[*]

INTRODUCTION

For many years, cybersecurity hacks have been limited to attacks on our credit cards and privacy. Each cyber hack invaded our privacy in different ways—using our credit cards,[1] reading emails we thought to be

* J.D. Expected 2017, University of Florida.

1. Robin Sidel, *Home Depot's 56 Million Card Breach Bigger than Target's*, WALL ST. J. (Sept. 18, 2014, 5:43 PM), http://www.wsj.com/articles/home-depot-breach-bigger-than-targets-1411073571.

private,[2] and exposing the darkest parts of our private lives.[3] As more parts of our daily lives become connected to the Internet,[4] however, cybersecurity is no longer limited to privacy concerns. Enter Charlie Miller and Chris Valasek.

In July 2015, reporter Andy Greenberg was driving a Jeep Cherokee down a St. Louis highway.[5] Researchers (or hackers, depending on your point of view) Miller and Valasek remotely infiltrated the Jeep, taking charge of the vehicle's controls using a laptop from Miller's house miles away.[6] As part of the experiment, the duo cut the Jeep's brakes, causing the vehicle to slide into a ditch.[7] In addition to manipulating the Jeep's controls remotely, Miller and Valasek could track targeted GPS coordinates, measure speed, and trace routes.[8] What may have once seemed like a far-fetched concern has become an unsettling reality. These researchers demonstrated that cybersecurity is no longer limited to privacy breaches; hackers can cut the breaks of a car and cause physical harm.

To this end, several pieces of legislation have been recently introduced regarding cybersecurity measures with respect to car hacking. Senators Edward J. Markey (D-Mass.) and Richard Blumenthal (D-Conn.) introduced the SPY Car Act in July 2015,[9] Representative Joe Wilson (R-S.C.) introduced the SPY Car Study Act in November 2015,[10] and even the House Energy and Commerce Committee released a discussion draft in October 2015.[11] There is skepticism about the effectiveness of these types of measures from the usual suspects,[12] but also from cybersecurity experts who are wary of governmental initiatives in private industries.[13] Consumer safety advocates, on the other hand, feel

---

2. Andrea Peterson, *The Sony Pictures Hack, Explained*, WASH. POST (Dec. 18, 2014), https://www.washingtonpost.com/news/the-switch/wp/2014/12/18/the-sony-pictures-hack-explained.

3. Dan Goodin, *Ashley Madison Hack is not only Real, It's Worse than We Thought*, ARS TECHNICA (Aug. 19, 2015, 2:22 AM), http://www.arstechnica.com/security/2015/08/ashley-madison-hack-is-not-only-real-its-worse-than-we-thought/.

4. Bill Wasik, *In the Programmable World, All Our Objects Will Act as One*, WIRED (May 14, 2013, 6:30 AM), http://www.wired.com/2013/05/internet-of-things-2/.

5. Andy Greenberg, *Hackers Remotely Kill a Jeep on the Highway—With Me in It*, WIRED (July 21, 2015, 6:00 AM), http://www.wired.com/2015/07/hackers-remotely-kill-jeep-high way/.

6. *Id.*

7. *Id.*

8. *Id.*

9. Security and Privacy in Your Car Act, S. 1806, 114th Cong. (2015).

10. Security and Privacy in Your Car Study Act of 2015, H.R. 3994, 114th Cong. (2015).

11. *Id.*

12. Tim Starks, *Car-Hacking Feud Revs Up on the Hill*, POLITICO (Aug. 29, 2015, 8:42 AM), http://www.politico.com/story/2015/08/pro-cyber-carhacking-starks-213124.

13. Andrea Castillo & Eli Dourado, *Why the Cybersecurity Framework Will Make Us Less Secure* 10, MERCATUS CENTER, Apr. 2014, at 15.

legislation is necessary to protect "unsuspecting motorists."[14]

This Note argues that any new legislation imposing new safety regulations on car manufacturers is unnecessary, and will ultimately create more problems than it solves. First, there are numerous established laws that either already require what some of these propose, or address the issues involved in car hacking.[15] Secondly, as vehicular technology becomes more advanced, so too will the methods available to fix the vulnerabilities within their systems.[16] Finally, the government's inefficiencies[17] and inability to stave off its own cyberattacks[18] makes any type of federal regulations requiring minimum safety protocols a cumbersome option. For these reasons, this Note argues private ordering, the act of sharing regulatory authority with private actors,[19] is the most effective solution to implementing effective cybersecurity measures.

While autonomous or self-driving cars are moving from the realm of science fiction to reality, such technology invokes a range of legal issues that are beyond the scope of this Note. Accordingly, this Note will focus on vehicle electronics as they are readily available on the current market.

This Note begins by providing a brief history of various research efforts to determine the potential dangers of car security breaches in Part I. Part II examines the current legislative proposals relating to car hacking and the shortcomings related to those proposals. Finally, Part III explores how existing laws can be applied to car hacking and sets out how private ordering is the most effective means of establishing cybersecurity standards within the automotive industry.

I. BRIEF HISTORY OF CAR HACKING

In 2010, customers of the Texas Auto Center found their cars not starting or honking uncontrollably.[20] The used car dealer was using a system called Webtech Plus, a remote immobilization system used in lieu of repossessing cars because of delinquent payments.[21] The system allowed car dealers to place a small black box behind a vehicle's

14. *See* Starks, *supra* note 12, at 2.

15. *See infra* Part III.A.

16. *See infra* notes 44–47.

17. *See infra* Part II.B.1.

18. Andrea Peterson & Lisa Rein, *What You Need to Know About the Hack of Government Background Investigations*, WASH. POST (July 9, 2015), https://www.washingtonpost.com/news/federal-eye/wp/2015/07/09/what-you-need-to-know-about-the-hack-of-government-background-investigations/.

19. Steven L. Schwarcz, *Private Ordering*, 97 NW. U. L. REV. 319, 319 (2002).

20. Kevin Poulsen, *Hacker Disables More Than 100 Cars Remotely*, WIRED (Mar. 17, 2010, 1:52 PM). http://www.wired.com/2010/03/hacker-bricks-cars/.

21. *Id.*

dashboard that responds to commands sent through a central website over a wireless pager network.[22] Using this system, a dealer could disable the ignition or remotely honk the horn to remind owners a payment is due.[23] The cars were taken over when a disgruntled former worker of Texas Auto Center used another employee's account to get into the system and disable the cars.[24] Although not catastrophic from a security breach standpoint, the Texas Auto Center hack showed that anything connected to the Internet is a point of entry.

That same year, a research team from the University of California San Diego and the University of Washington set out to "comprehensively assess how much resilience a conventional automobile has against a digital attack mounted against its internal components."[25] The researchers tested two cars of the same make and model in a controlled setting and in live road tests.[26] The study found that the tested automobiles had "little" resilience against attacks.[27] The focus of the study at that point, however, was to determine if a hacker could compromise a car's internal system, not how a hacker might do so.[28] The researchers set out to fill the gap between physically connecting to a car's internal system and possible external attacks[29] after receiving criticism that "presupposing an attacker's ability to *physically* connect to a car's internal network may be unrealistic."[30] The researchers identified several vulnerabilities[31] within the vehicle and discovered that "for every vulnerability . . . demonstrated, [the team was] able to obtain complete control over the vehicle's systems."[32]

---

22. *Id.*

23. *Id.*

24. *Id.*

25. Karl Koscher et al., *Experimental Security Analysis of a Modern Automobile*, 2 (2010), http://www.autosec.org/pubs/cars-oakland2010.pdf.

26. *Id.*

27. *Id.*

28. *Id.* at 14.

29. Checkoway, et al., 1 (2011), *Comprehensive Experimental Analyses of Automative Attack Surfaces*, http://www.autosec.org/pubs/cars-usenixsec2011.pdf.

30. *Id.* at 1.

31. *Id.*

> [W]e demonstrate the ability to compromise a car via, vulnerable diagnostics equipment widely used by mechanics, through the media player via inadvertent playing of a specially modified song in WMA format, via vulnerabilities in hands-free Bluetooth functionality and, finally, by calling the car's cellular modem and playing a carefully crafted audio signal encoding both an exploit and a bootstrap loader for additional remote-control functionality.

Id.

32. *Id.* at 6.

To build off of this academic research of external attacks, Miller and Valasek connected to both a Ford Escape and Toyota Prius to display that "you can do a lot of crazy things once you're inside."[33] The duo showed their ability to cut the brakes, kill power steering, and "violently jerk the Prius' steering at any speed."[34] A Toyota representative, however, was unimpressed with their efforts, intimating that it would be unlikely a real hacker would have direct access to an automobile's data port.[35] The company's focus, therefore, would instead be on preventing wireless attacks.[36]

It is no surprise that Miller and Valasek spent the next two years working towards remotely hacking a vehicle.[37] They were able to access the Jeep's internal computer system through Uconnect—Chrysler's Internet-connected system that controls a vehicle's entertainment and navigation capabilities, enables phone calls, and offers a WiFi hotspot.[38] This weakness, known as zero-day vulnerability,[39] allowed Miller and Valasek to send code through the Jeep's entertainment systems to the dashboard functions, steering, brakes, and transmission.[40] In addition to relatively innocuous actions such as turning on the windshield wipers or playing with the air conditioning, the hackers were able to fully kill the engine at lower speeds and abruptly engage or disable the brakes.[41] While Miller and Valasek's ability to gain physical control over a vehicle was frightening enough, they could also track targeted GPS coordinates, measure speed, and trace the vehicle's route.[42] Miller and Valasek gave Fiat Chrysler advanced notice of their intention to publish their findings, and as a result of their research, Fiat Chrysler issued a recall of 1.4 million vehicles and applied network-level security measures on the Sprint cellular network that communicates with its vehicles.[43]

A separate team of researchers, Kevin Mahaffey and Marc Rogers,

---

33. Andy Greenberg, *Hackers Reveal Nasty New Car Attacks—With Me Behind the Wheel*, FORBES (July 24, 2013, 9:00 AM), http://www.forbes.com/sites/andygreenberg/2013/07/24/hackers-reveal-nasty-new-car-attacks-with-me-behind-the-wheel-video/.

34. *Id.*

35. *Id.*

36. *Id.*

37. *Id.*

38. Greenberg, *supra* note 5.

39. *See generally* Kim Zetter, *Hacker Lexicon: What is a Zero Day?*, WIRED (Nov. 11, 2014, 6:30 AM), http://www.wired.com/2014/11/what-is-a-zero-day/ (defining a zero-day vulnerability as a vulnerability previously unknown to a software vendor and a zero-day exploit as the code used to take advantage of such vulnerabilities) [hereinafter Zetter, *Zero Day*].

40. *Id.*

41. Greenberg, *supra* note 5.

42. *Id.*

43. Aaron M. Kessler, *Fiat Chrysler Issues Recall Over Hacking*, N.Y. TIMES (July 24, 2015), http://www.nytimes.com/2015/07/25/business/fiat-chrysler-recalls-1-4-million-vehicles-to-fix-hacking-issue.html?_r=0.

worked for several years before discovering they could electronically "hotwire" a Tesla Model S by plugging a laptop into the vehicle's driver-side dashboard.[44] The researchers also discovered they could plant a remote-access Trojan in the vehicle's network while they had physical access to the car, and then later use it to remotely cut the engine when no longer connected.[45] They discovered the Model S' infotainment system was running on an out-of-date browser which contained a four-year-old Apple WebKit vulnerability that a potential hacker could use to gain access to the system.[46] In the end, the team found six vulnerabilities in the Model S and worked with Tesla to develop some solutions before Tesla issued a "patch" to every Model S on the road.[47] Unlike Fiat Chrysler, which had to recall over a million vehicles, Tesla was able to remotely deliver software updates to its vehicles.[48]

Senator Edward J. Markey (D-Mass) took note of these studies as early as 2013.[49] Senator Markey sent a letter to twenty major automobile manufacturers in the United States to learn about security measures that were already in place.[50] The letter included questions on how companies assess potential vulnerabilities from third party equipment, if vehicles contained technology to detect anomalous activity, and what type of driving history information could be collected from technologies in the vehicle.[51] In February 2015, Senator Markey released a report discussing the responses and determined there was a "clear lack of appropriate security measures to protect drivers" against hackers who may seek to control a vehicle or siphon personal data.[52] The report concluded that the responses provided displayed "alarmingly inconsistent and incomplete" security and privacy practices within the industry, and declared a need for the National Highway Traffic Safety Administration (NHTSA) to promulgate new standards to protect modern drivers.[53]

By hacking into a car, researchers demonstrated that cybersecurity

---

44. Kim Zetter, *Researchers Hacked a Model S, But Tesla's Already Released a Patch*, WIRED (Aug. 6, 2015, 6:00 AM), http://www.wired.com/2015/08/researchers-hacked-model-s-teslas-already/ [hereinafter Zetter, *Tesla*].

45. *Id.*

46. *Id.*

47. *Id.*

48. *Id.*

49. Press Release, U.S. Senator for Mass., *As Wireless Technology Becomes Standard, Markey Queries Car Companies About Security, Privacy*, ED MARKEY, U.S. SENATOR FOR MASS. (Dec. 2, 2013), http://www.markey.senate.gov/news/press-releases/as-wireless-technology-becomes-standard-markey-queries-car-companies-about-security-privacy.

50. *Id.*

51. *Id.*

52. STAFF OF SENATOR EDWARD J. MARKEY, TRACKING & HACKING: SECURITY & PRIVACY GAPS PUT AMERICAN DRIVERS AT RISK 1 (2015), http://www.markey.senate.gov/imo/media/doc/2015-02-06_MarkeyReport-Tracking_Hacking_CarSecurity%202.pdf.

53. *Id.* at 2.

now reaches all areas of our lives. As hackers (altruistic and malicious alike) discover more sophisticated ways to infiltrate a car's operating system, the more proposed legislation relating to car hacking there will probably be.

II. CURRENT LEGISLATIVE PROPOSALS RELATING TO CAR HACKING

This Part explores proposed legislation directly addressing car hacking and their respective shortcomings.

A. *Proposed Legislation*

To begin, this Part will examine the SPY Car Study Act of 2015, the SPY Car Act of 2015, and the House Discussion Draft. This Part will then discuss the dilemma of charging the NHTSA with responsibility for promulgating regulations and issues with the government and cybersecurity in general.

1. Spy Car Study Act of 2015

Representative Joe Wilson (R-S.C.) introduced the Security and Privacy in Your Car Study Act of 2015 (SPY Car Study Act) on November 5, 2015.[54] The bill would have required the NHTSA to conduct a study with numerous parties including the Federal Trade Commission (FTC), the Secretary of Defense, SAE International[55], automobile manufacturers and "relevant academic institutions."[56] Preliminary findings of this study would have been presented no later than one year after the enactment of the bill to various committees in the House and Senate, with a final report due no later than six months after that presentation.[57]

However, in 2012, Congress passed the Moving Ahead for Progress in the 21st Century Act (MAP-21),[58] which created a new council within the NHTSA devoted to vehicle electronics requiring the NHTSA to conduct a study regarding safety standards in "electronic systems in

54. SECURITY AND PRIVACY IN YOUR CAR STUDY ACT OF 2015, H.R. Doc No. 3994, at 1 (2015).

55. SAE International is a professional association of engineers, scientists and practitioners that develops safety standards in the automotive, aerospace and commercial vehicle industry, as well as other related initiatives. *See* SAE INTERNATIONAL, http://www.sae.org (last visited Sept. 11, 2016).

56. H.R. 3994 § 2(a)

57. *Id.* § 2(b)

58. Moving Ahead for Progress in the 21st Century (MAP-21) Act, Pub. L. No. 112-141, 126 Stat. 405 (2012).

passenger motor vehicles."[59] Therefore, what the SPY Car Study Act would have mandated was put into law by the MAP-21 Act in 2012.

2. Spy Car Act of 2015

In a more comprehensive take on the issue, Senators Mackey and Blumenthal introduced the Security and Privacy in Your Car Act (SPY Car Act) in July 2015.[60] The bill is broken into three main sections: Cybersecurity Standards in Motor Vehicles, Cyber Dashboard, and Privacy Standards in Motor Vehicles.[61]

If enacted, the first section would require all electronic system entry points in vehicles to be "equipped with reasonable measures to protect against hacking attacks," including "isolation measures" to separate critical software systems.[62] Additionally, data collected by those systems shall be "reasonably secured to prevent unauthorized access" at any point in the collection and storage of the data.[63] Finally, all entry points shall be equipped with capabilities to detect, report and stop data interception or vehicle control.[64]

The second section of the bill, the Cyber Dashboard, would require a label to be affixed to each motor vehicle manufactured two years after the bill is enacted.[65] The label's purpose would be to inform consumers in an "easy-to-understand, standardized graphic" about the specific motor vehicle's protections against cybersecurity and privacy beyond the minimum requirements set forth in the Act.[66]

The bill's third section would mandate privacy standards requiring transparency and consumer control.[67] Vehicles would be required to give "clear and conspicuous" notice of the collection and use of driving data collected by the vehicle.[68] Additionally, owners would be able to opt-out of any such data collection without losing navigation capabilities.[69] In addition to these general guidelines, the SPY Car Act would outsource rulemaking and final regulations to the NHTSA to be enacted no later than three years after the bill's enactment.[70]

Consumers would also be able to opt out of the collection and

59. MAP-21 § 31401–02.
60. Security and Privacy in Your Car Act of 2015, S. 1806, 114th Cong. (2015).
61. *Id.*
62. *Id.* § 30129(a)(1)–(2).
63. *Id.* § 30129(a)(3).
64. *Id.* § 30129(a)(4).
65. *Id.* § 30129(3).
66. *Id.* § 30129(3)(a)(2).
67. *Id.* § 30129(4)(b)–(c).
68. *Id.* § 30129(4)(b).
69. *Id.* § 30129(4)(c)(2).
70. *Id.* § 30129(b)(1)–(2).

retention of "driving data," without losing navigation or other functionalities.[71] As discussed in Part III, this may potentially be in contradiction to the recently enacted Cybersecurity Information Sharing Act.[72] Congress should be wary of allowing consumers to opt out of such data collection as it remains to be seen what type of data monitoring is necessary for car manufacturers and other surveillance companies to truly assess potential risks. Considering researchers have already demonstrated the multitude of ways a hacker could infiltrate a car's system, allowing consumers to decide to terminate driving data collection due to privacy concerns could potentially affect the manufacturer's ability to properly gauge threats to physical safety.

3. House Discussion Draft

The House Energy and Commerce Committee also recently released a discussion draft relating to cybersecurity in automobiles, though it has yet to be introduced. Title III—Privacy, Hacking Prohibition, and Cybersecurity would require car manufacturers to develop and implement a privacy policy describing the manufacturer's collection, use, and sharing of certain information connected to consumers.[73] A manufacturer who fails to develop such a policy would be subject to a fine of not more than $5,000 per day and not to exceed $1,000,000 for a single manufacturer.[74] The draft also contains a safe harbor, which provides that manufacturers whose privacy policies comply with the provisions will not be subject to section five of the Federal Trade Commission Act related to unfair practice with respect to privacy.[75]

The draft goes further to declare that it shall be unlawful for "any person to access, without authorization, an electronic control unit or critical system of a motor vehicle, or other system containing driving data for such motor vehicle, either wirelessly or through a wired connection."[76] A person who violates this prohibition will be liable for a fine of not more than $100,000 per violation.[77] The draft additionally calls on the NHTSA to establish the "Automotive Cybersecurity Advisory Council" to develop best practices for manufacturers, with a mandate for manufacturers of significant size to appoint a representative to serve on the Council.[78]

---

71. *Id.* § 30129(4)(c).

72. *See infra* notes 148–154 and accompanying text.

73. Discussion Draft Title III, H.R. 3994, 114th Cong. (2015).

74. *Id.*

75. *Id. See also* 15 U.S.C. § 45(a)(1) (stating unfair or deceptive acts or practices are declared unlawful).

76. Discussion Draft Title III, *supra* note 73.

77. *Id.*

78. *Id.*

Though not yet introduced, the House Energy and Commerce Committee discussion draft would make it unlawful for persons to access a critical control system of a vehicle without authorization. There are two issues with this provision. First, the ambiguous language does not state who is able to give authorization. As Harley Geiger of the Center for Democracy and Technology noted, when a consumer purchases a car, he generally owns the physical parts of the car, while the software embedded in the car is merely licensed to the owner by the manufacturer.[79] Secondly, "unauthorized access" to vehicles has allowed researchers to take notice of a car's vulnerabilities and thereafter work with manufacturers to correct those vulnerabilities, as Mahaffey and Rogers did with Tesla.

Vulnerabilities in systems that hackers are able to exploit but are unknown to vendors are known as zero-day vulnerabilities.[80] Generally speaking, zero-day vulnerabilities are not in and of themselves "bad," as evidenced by Miller and Valasek's zero-day exploit of the Jeep Cherokee. Allowing independent researchers to develop exploitations of current vulnerabilities has already lead to a recall of over a million vehicles[81] and a patch sent to Tesla owners.[82] By making this form of research unlawful, consumers will ultimately be adversely affected. Car manufacturers could decide to withhold authorization from researchers for any number of reasons, suspicious or legitimate. Outside third parties examining vulnerabilities of connected vehicles, however, will only create a larger system of checks-and-balances between experts and car manufacturers.

B. *Pitfalls of Proposed Legislation*

The current proposals all rely heavily on the NHTSA to promulgate regulations. Due to the nature of administrative agency slowness and the NHTSA's recent troubles, this seems like a less than ideal option. Additionally, experts are critical of the government attempting to engage in cybersecurity regulation at all due to their own security failings.

---

79. Harley Geiger, *Draft Car Safety Bill Goes in the Wrong Direction*, CENTER FOR DEMOCRACY & TECH. (Oct. 20, 2015), https://cdt.org/blog/draft-car-safety-bill-goes-in-the-wrong-direction/.

80. Zetter, *Zero Day*, *supra* note 39 (defining a zero-day vulnerability as a vulnerability previously unknown to a software vendor and a zero-day exploit as the code used to take advantage of such vulnerabilities).

81. Aarom *M.* Kessler, *Fiat Chrysler Issues Recall over Hacking*, N.Y. TIMES (July 24, 2015), http://www.nytimes.com/2015/07/25/business/fiat-chrysler-recalls-1-4-million-vehicles-to-fix-hacking-issue.html?_r=0.

82. *See* Zetter, *Telsa*, *supra* note 44.

1. The NHTSA Dilemma

Each of the discussed proposals outsources all or some of the rulemaking authority to the NHTSA. The SPY Car Act, for example, outsources specific rulemaking to the NHTSA,[83] with the NHTSA Administrator issuing a Notice of Proposed Rulemaking within eighteen months of enactment, and final regulations issued no later than three years after the date of the bill's enactment.[84] By mandating a Notice of Proposed Rulemaking, the SPY Car Act leaves the promulgation of cybersecurity standards to the mercy of the rulemaking process.

The Notice of Proposed Rulemaking is controlled by the Administrative Procedure Act.[85] A person who suffers a legal wrong, or is adversely affected or aggrieved by agency action within the meaning of a relevant statute, is entitled to judicial review.[86] The reviewing court will use an arbitrary and capricious standard for agency actions.[87] In *Motor Vehicle Manufacturers Association v. State Farm Mutual*,[88] the Supreme Court explored whether the NHTSA "acted arbitrarily and capriciously" when it revoked the requirement that all new vehicles made after September 1982 would be equipped with passive restraints.[89] The Court stated the arbitrary and capricious standard "is narrow and a court is not to substitute its judgment for that of the agency" but that an agency must "articulate a satisfactory explanation for its actions."[90] The Court found that the NHTSA failed to provide an adequate reason for rescinding the safety standard.[91]

In this scenario, should a car manufacturer or industry association[92] feel they have been adversely affected by NHTSA action, it would be entitled to judicial review in which the NHTSA would need to provide a satisfactory explanation for its actions. The reviewing court would then apply the arbitrary and capricious standard to determine whether or not the NHTSA provided adequate reasons for its cybersecurity standards. As seen with the recent hacks performed by researchers, car

---

83. It is interesting to note here that Sen. Blumenthal, the co-sponsor of this bill, called the NHTSA a "failing agency" merely a month before the bill was introduced, and yet proscribes control of the regulatory specifics to the Agency nonetheless. *See* Ruiz & Vlasic, *infra* note 94.

84. Security and Privacy in Your Car (SPY Car) Act of 2015, S. 1806, 114th Cong. § 30129(b) (2015).

85. 5 U.S.C. § 553 (2015).

86. 5 U.S.C. § 702 (2015).

87. 5 U.S.C. § 706(2)(a).

88. Motor Vehicle Mfrs. Ass'n of U.S., Inc. v. State Farm Mut. Auto. Ins. Co., 463 U.S. 29, 43, 103 S. Ct. 2856, 2867, 77 L. Ed. 2d 443 (1983)

89. *Id.* at 44.

90. *Id.* at 42.

91. *Id.* at 48.

92. 5 U.S.C. § 551 (2015) (defining "person" to include corporations and associations).

manufacturers respond to vulnerabilities quickly.[93] In a rapidly changing environment such as cybersecurity, even if specific standards pass this judicial review, they could be rendered obsolete by the time the review process has concluded.

Beyond the potential sluggishness of being subject to administrative laws, the NHTSA has been in hot water recently.[94] In summer 2015, reports were released assessing the role the NHTSA played in General Motors' (G.M.'s) recalls relating to ignition switch defects linked to at least one hundred deaths.[95] According to internal reports, the NHTSA admits to missing clues that would have alerted the agency to G.M.'s defect and failing to use its full authority in disciplining G.M.[96] Members of Congress were critical of this failure,[97] which allowed G.M. cars to go unrepaired for decades.[98] This led to a reorganization of the NHTSA, which included an "oversight team of outside experts to help put the changes into effect."[99]

The NHTSA is the logical agency to promulgate regulations for vehicles. However, car hacking is a cybersecurity issue that requires a dynamic system which can quickly respond to changes in technology. The NHTSA is not the best agency for setting standards for the car hacking issue because of the potential delays in the Proposed Rulemaking process and the agency's current restructuring.

2. Government's Role in Cybersecurity

A separate problem with all three proposals is putting the federal government in charge of setting cybersecurity standards for automobiles. The government's cybersecurity initiatives have been roundly criticized in recent years.

One such initiative is the Cybersecurity Framework. Executive Order 13636 instructed the Director of the National Institute of Standards and Technology to lead the development of the Cybersecurity Framework needed to "reduce cyber risks to critical infrastructure."[100] Participation in the Framework is voluntary.[101]

The Cybersecurity Framework includes "standards, methodologies,

---

93. *See* Zetter, *Tesla*, *supra* note 44.

94. *See* Rebecca R. Ruiz & Bill Vlasic, *Safety Agency Admits Missing Clues to G.M. Ignition Defects*, N.Y. TIMES (June 5, 2015), http://www.nytimes.com/2015/06/06/business/nhtsa-admits-missing-clues-to-gm-ignition-defects.html?_r=0.

95. *Id.*

96. *Id.*

97. *Id.*

98. *Id.*

99. *Id.*

100. Exec. Order No. 13,636, 78 Fed. Reg. 33, at 11,740–71 (Feb. 19, 2013).

101. *Id.*

procedures and processes" that address cyber risks through a flexible, performance-based, and cost-effective approach to help owners and operators of critical infrastructure manage cyber risk.[102] The Order defines critical infrastructure as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."[103] Critical infrastructure is divided into sixteen sectors, each with unique characteristics and a federal agency, known as a Sector-Specific Agency, responsible for "providing institutional knowledge and specialized expertise" to individual sectors.[104] Vehicle manufacturing falls within the Critical Manufacturing Sector[105] overseen by the Department of Homeland Security.[106]

The Cybersecurity Framework has three parts: the Framework Core, the Framework Implementation Tiers and the Framework Profile.[107] The Framework Core contains best practices for each critical infrastructure category, divided into functions and then subcategories.[108] The Framework Implementation Tiers measures compliance with each function and category developed in the Framework Core.[109] The Framework Profile gives a participating organization's "score" of compliance with the Framework's recommended cybersecurity protections.[110]

The Cybersecurity Framework has been met with mixed reviews. Some view the Framework as a step in the right direction, laying out a process of "risk-based approach" to improving security.[111] Others view the Cybersecurity Framework as "the wrong approach," replacing a dynamic process of developing cybersecurity standards with "rigid

---

102. *Id.*

103. *Id.* at 11,739.

104. Presidential Policy Directive 21, *Critical Infrastructure Security and Resilience* 4, 12, (Feb. 12, 2013), https://fas.org/irp/offdocs/ppd/ppd-21.pdf.

105. Critical Manufacturing Sector, DEPT. OF HOMELAND SECURITY, Oct. 14, 2015, http://www.dhs.gov/critical-manufacturing-sector.

106. Exec. Order No. 13,636, *supra* note 100, at 11,739.

106. Presidential Policy Directive 21, *Critical Infrastructure Security and Resilience* 4, 12, Feb 12, 2013, https://fas.org/irp/offdocs/ppd/ppd-21.pdf.

107. Andrea Castillo & Eli Dourado, *Why the Cybersecurity Framework Will Make Us Less Secure* 10, MERCATUS CENTER, Apr. 17, 2014.

108. *Id.* at 10.

109. *Id.*

110. *Id.*

111. Joab Jackson, *How the NIST Cybersecurity Framework Can Help Secure the Enterprise*, PCWORLD (Feb. 14, 2014, 2:00 PM), http://www.pcworld.com/article/2098320/how-the-nist-cybersecurity-framework-can-help-secure-the-enterprise.html (quoting Andrew Wild, the Chief Security Officer of Qualys, an IT security firm).

incentive toward compliance with recommended federal standards."[112] Andrea Castillo and Eli Dourado argue that the Internet has existed thus far without a unified cybersecurity plan due to the relationships between networks.[113] The Internet has developed a system of self-policing, such as quickly "shunning" networks that allow malicious criminals to use their resources.[114] Groups of computer security teams have formed to "monitor traffic for destructive activities and warn parties of potential security threats."[115] Best practices regarding botnet activity have developed from shared information among organizations.[116] Thus, private firms already have intrinsic incentives in place to develop cybersecurity standards.[117] Critics argue the Framework replaces these self-interested incentives with the incentive to increase their Framework Profile score.[118]

A major criticism of the federal government's attempt to promulgate cybersecurity regulations stems from the government's own propensity to being hacked and otherwise poor track record of cybersecurity.[119] Just this summer, the Office of Personnel Management was hacked into, resulting in 21.5 million people being affected in some fashion.[120] In 2014, the Department of Justice reported 3,604 incidents of security breaches, with malicious software downloaded onto agency computers 182 times.[121] It is not difficult to imagine a scenario in which the NHTSA implements regulations that cause manufacturers to work towards meeting federally mandated standards instead of developing dynamic protocols for changing technology.

III. SOLVING THE LEGISLATIVE ISSUES RELATING TO CAR HACKING

As with any high-stakes security issue, car hacking has created a divide between industry insiders, regulators, and consumer advocates.

112. *See* Castillo & Dourado, *supra* note 13, at 15.
113. *Id.* at 6.
114. *Id.* at 7.
115. *Id.* at 8.
116. *Id.* at 9.
117. *See id.* at 6.
118. *Id.* at 15.
119. This factor, however, should not be a concern in the car hacking context as it is difficult to argue a car in the government's hand as a greater likelihood of being hacked because the point of entry comes from the manufacturer, not government systems.
120. Andrea Peterson & Lisa Rein, *What You Need to Know About the Hack of Government Background Investigations*, WASH. POST (July 9, 2015), https://www.washingtonpost.com/news/federal-eye/wp/2015/07/09/what-you-need-to-know-about-the-hack-of-government-background-investigations/.
121. Eli Dourado & Andrea Castillo, *Information Sharing: No Panacea for American Cybersecurity Challenges*, *in* MERCATUS ON POLICY 1, 4 (2015).

When discussing legislation or any other initiative related to car hacking, there should be two main goals. The first is for car manufacturers to establish expectations for moving forward with proper protocols that secure their vehicles from external cyberattacks. The second, of course, is to protect consumers. Consumer advocate groups and those in Congress like Senators Markey and Blumenthal believe the best way to achieve these separate goals is to pass legislation that specifically addresses car hacking, such as the SPY Car Act.[122] Car manufacturers, however, feel that new regulations will only bog down development of effective security measures and do not want to be liable for hackers' activities when they have acted in good faith.[123] The automotive industry has also supported information-sharing proposals, such as the Cybersecurity Information Sharing Act (CISA), with General Motors recently urging the Senate to pass CISA.[124]

Although the discussed proposals are well-intentioned, they are ultimately unnecessary. Many existing laws cover all of the issues relating to car hacking, so new legislation is redundant. To better solve the issue, private ordering should be used to allow the automotive industry to set its own standards in order to meet the changes in technology more efficiently.

A. *Existing Laws as Applied to Car Hacking*

Ultimately, many car hacking issues are already covered by existing laws including automotive safety standards, car manufacturer liability, and cybersecurity measures. For example, the NHTSA has been issuing motor vehicle safety standards since 1967[125] under federal mandate.[126] The purpose of the Motor Vehicle Safety chapter is to "reduce traffic accidents and death," by "prescribe[ing] motor vehicle safety standards" and "carry[ing] out needed safety research and development."[127] Product liability and other tort-based lawsuits have controlled automakers' liabilities for decades. MAP-21 provides yet another directive to the NHTSA to investigate safety concerns in connection with connected vehicles.[128]

Car hacking most certainly falls within the purview of the Computer

---

122. *See* Starks, *supra* note 12 (quoting Catherine Chase of Advocates for Highway and Auto Safety as stating bills such as the SPY Car Act are the "next wave of protection").

123. *Id.*

124. *Id.*

125. *See* FED. MOTOR VEHICLE SAFETY STANDARDS AND REGULATIONS, FOREWORD (1999), http://www.nhtsa.gov/cars/rules/import/FMVSS/.

126. Motor Vehicle Safety, 49 U.S.C. § 30101 (2016).

127. *Id.*

128. *See supra* notes 58–59 and accompanying text.

Fraud and Abuse Act (CFAA).[129] The statute covers actions such as intentionally causing damage to a protected computer through the transmission of a program or code,[130] intentionally accessing a protected computer and recklessly causing damage,[131] or intentionally accessing a protected computer without authorization and causing damage and loss.[132] A protected computer is defined, in part, as a computer "which is used in or affecting interstate or foreign commerce."[133] The CFAA defines computer broadly as an "electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device."[134] Therefore, there is already a means available to punish hackers who infiltrate a vehicle.

It is important to note, however, that the CFAA has been widely criticized in recent years. Some have said that the Act is used by prosecutors to "bully and intimidate" security researchers with the "unauthorized access" language.[135] Others have argued the phrase "unauthorized access" is so broad and vague that it must be unconstitutional.[136] Thus, it is easy to understand how the House discussion draft's use of similar "without authorization" language[137] is problematic in attempting to punish potential hackers.

Additionally, the Federal Trade Commission may have the authority to regulate cybersecurity in automobiles under the "unfair acts" section of the Federal Trade Commission Act.[138] In a recent decision, *FTC v. Wyndham Worldwide Corporation*,[139] the Third Circuit ruled that the FTC has the authority to bring a suit against a company for repeated failures to safeguard against cyberattacks within a short period of time.[140] Wyndham was hacked three separate times between 2008 and 2009, all three of which occurred in similar fashions by infiltrating an

129. 18 U.S.C. § 1030 (2015).

130. *Id.* § 1030(a)(5)(A).

131. *Id.* § 1030(a)(5)(B).

132. *Id.* § 1030(a)(5)(C).

133. *Id.* § 1030(e)(2)(B).

134. *Id.* § 1030(e)(1).

135. Sam Gustin, *U.S. "Hacker" Crackdown Sparks Debate over Computer-Fraud Law*, TIME.COM (Mar. 19, 2013), http://business.time.com/2013/03/19/u-s-hacker-crackdown-sparks-debate-over-computer-fraud-law/.

136. Tim Wu, *Fixing the Worst Law in Technology*, NEW YORKER (Mar. 18, 2013), http://www.newyorker.com/news/news-desk/fixing-the-worst-law-in-technology.

137. *See* discussion *infra* Part II.A.

138. 15 U.S.C. § 45(a) (2015).

139. F.T.C. v. Wyndam Worldwide Corp., 799 F.3d 236, 259 (3d Cir. 2015).

140. *Id.* at 241–42.

administrator account.[141] The FTC alleged Wyndham engaged in unfair cybersecurity practices that "unreasonably and unnecessarily exposed consumers' personal data to unauthorized access and theft" and alleged, among other things, that Wyndham failed to use firewalls or deploy reasonable measures to detect and prevent against unauthorized access.[142] Wyndham offered several arguments as to why this particular suit exceeds the FTC's authority, most pertinently, that the FTC failed to give fair notice of the specific cybersecurity standards under the Act and that Wyndham was entitled to "ascertainable certainty" of the standards required under section 45(a).[143] The court rejected these arguments, specifically noting that the lack of any firewalls and a third attack in a similar fashion would put Wyndham on notice that it fell short of the cost-benefit analysis standard[144] provided in another section of the Act.[145] While this was an interlocutory appeal, and thus no decision was reached on the merits,[146] it effectively put companies on notice that the FTC has standing to bring suit against those it deems lack reasonable cybersecurity protections.

Further, CISA[147] was recently signed into law as an amendment to an omnibus budget bill.[148] CISA allows private entities to monitor, for cybersecurity purposes,[149] an "information system of such private entity."[150] CISA provides liability protection against private entities for monitoring an information system under § 104(a).[151]

The Act also allows for companies to share cybersecurity threat information with the federal government[152] and provides additional liability protection from lawsuits resulting from such sharing.[153] For potential legislation that may call for information sharing, CISA's passage ensures car manufacturers will be more than willing to monitor

---

141. *Id.*

142. *Id.* at 240–41.

143. *Id.* at 252

144. 15 U.S.C. § 45(n) (2015).

145. *Wyndham*, 799 F.3d at 256.

146. *Id.* at 240.

147. Cybersecurity Information Sharing Act of 2015, Pub. L. No. 114-113, 161 Stat. 1729 (2015).

148. Andy Greenberg, *Congress Slips CISA into a Budget Bill That's Sure to Pass*, WIRED (Dec. 16, 2015, 12:24 PM), http://www.wired.com/2015/12/congress-slips-cisa-into-omnibus-bill-thats-sure-to-pass/.

149. Consolidated Appropriations Act, P.L. No. 114-113, § 102(4), 129 Stat. 2242 (2016) (defining cybersecurity purpose as "the purpose of protecting an information system or information that is stored on, processed by, or transiting an information system from a cybersecurity threat or security vulnerability").

150. *Id.* § 104(a)(1)(A).

151. *Id.* § 106(a).

152. *Id.* § 105.

153. *Id.* § 106(b).

their information systems and share information with the federal government to obtain the maximum protections provided by law. For any proposed legislation, such as the SPY Car Act of 2015, that calls for consumers to have the ability to opt out of data collection, car manufacturers may point to CISA, claiming they are able to monitor the information systems of their automobiles. Considering car hacking in isolation from other cybersecurity laws will lead to contradictory policies.

It is clear, then, that there are already legislative measures available for lawmakers to create safety standards for car manufacturers, bring suit against those they feel are failing to adequately protect consumers, and punish potential malicious hackers. Enacting additional laws regulating this area will only serve to complicate an already crowded legislative landscape.

B. *Private Ordering as a Solution*

Private ordering will allow for automotive manufacturers to establish their own cybersecurity standards. Private ordering is not a new concept. The Internet Corporation for Assigned Names and Numbers (ICANN) is a private ordering scheme handling the Internet domain system.[154] Additionally, Standard & Poor's Ratings Service and Moody's Investors Service were given the power to issue credit ratings, among other responsibilities.[155] The credit card industry provides an example of private ordering within an industry dealing with its own cybersecurity issues.

1. Private Ordering in the Credit Card Industry

The credit card industry has used private ordering to develop the Payment Card Industry Data Security Standards (PCI DSS).[156] Private ordering refers to solutions for governing behavior and resolving disputes separate from laws advanced by the government and enforced by the judiciary.[157] In 2004, five major card brands came together to release the first iteration of the PCI DSS, which offered a coordinated approach to improve efficiency through "shared security expertise."[158] The PCI Data Security Council (PCI DSC) promulgates standards that must be met throughout different levels of the entire industry.[159] Professors Edward

154. Steven L. Schwarcz, *Private Ordering*, 97 NW. U. L. REV. 319, 320 (2002).

155. *Id.* at 326.

156. Edward A. Morse & Vasant Raval, *Private Ordering in Light of the Law: Achieving Consumer Protection Through Payment Card Security Measures*, 10 DEPAUL BUS. & COM. L.J. 213, 216 (2012).

157. *Id.* at 214.

158. *Id.* at 229.

159. *Id.* at 230.

Morse and Vasant Raval note that knowledge regarding industry security standards is currently shared through the PCI SSC.[160] By sharing knowledge through this private ordering infrastructure, a knowledge asymmetry is created between the "regulated industry and those who seek to regulate it."[161] This poses significant issues for any attempts at regulatory interference by the government.

Professors Morse and Raval establish that private systems of regulation in the payment card industry were developed out of the necessity for the trust of consumers and merchants in using this method of payment.[162] There is a "network of trust relationships inherent in the industry."[163] To facilitate consumer trust, consumers are protected from fraudulent transactions conducted on a card issuer's network by not incurring any liability from such transactions.[164] Although there are federal laws requiring consumers bear no more than $50 in liability, firms within the industry are acting in their own self-interest by offering better protection than the mandated minimums.[165] By minimizing, or altogether eliminating, consumers' fears of fraudulent transactions, payment card firms are increasing their profits.[166]

The same can be said of the automobile industry. Consumers must be able to trust the cars they are purchasing will be safe to use and manufacturers must trust their product will not be used in a malicious fashion. Likewise, car manufacturers will be acting in their own self-interest by implementing safety protocols. If consumers cannot trust a particular company's vehicles, they will turn to a brand they deem more trustworthy.

Attempts at federal intervention in the payment card marketplace added little, if any, value as of 2012.[167] The Fair and Accurate Credit Transaction Act of 2003 (FACTA) includes a provision requiring that no more than the last five digits, and the blocking of expiration dates entirely, on all electronically printed receipts.[168]

This provision proved to be both under and over-inclusive in certain ways.[169] A criminal theoretically would prefer unencrypted electronic data over paper receipts, which FACTA does not cover. A FACTA violation could occur from displaying the first and last card numbers and

---

160. *Id.* at 235.
161. *Id.*
162. *Id.* at 221.
163. *Id.*
164. *Id.* at 223.
165. *Id.* at 223–24.
166. *Id.*
167. *Id.* at 253.
168. Morse, *Private Ordering in Light of the Law: Achieving Consumer Protection Through Payment Card Security Measures*, 10 DEPAUL BUS. & COM. L.J. 253–54 (2012).
169. *Id.* at 254–55.

blocking the middle blocked, thus creating millions of permutations to find the correct card number.[170] This type of violation presents "no appreciable risk to consumers" absent other information.[171] The result leads to increased litigation costs, due to the high amount of class action suits brought under FACTA, creating an actual harm to consumers.[172]

Assessments of the PCI DSS indicate that "significant noncompliance exists within the merchant community."[173] This concern is probably not present within the automotive industry because the manufacturers themselves will presumably be the ones that are responsible for implementing the safety protocols in the end.[174] The payment card industry offers an example of private ordering, and the unintended effects of regulating an industry that has incentives to self-regulate. Allowing the auto industry to self-regulate with the help of cybersecurity experts will combat unintentional adverse effects on consumers.

2. Private Ordering for Car Manufacturers

As in the credit card industry, car manufacturers will develop safety standards due to market forces, namely, keeping customers safe. Car manufacturers have already begun forming the foundation of a private ordering scheme. One of the more influential interest groups within the auto industry is the Alliance of Automobile Manufacturers (Auto Alliance).[175] The Auto Alliance has already established the Automotive Information Sharing and Analysis Center (Auto-ISAC) in an effort to move "forward on collaborative efforts."[176] Additional measures taken by the automobile industry include establishing the Vehicle Electrical System Security Committee by the Society of Automotive Engineers (SAE)[177] to draft standards and best practices and to benchmark other

170. *Id.* at 255.

171. *Id.*

172. *Id.* at 255–56.

173. *Id.* at 238.

174. It is plausible, however, that manufacturers could leave the implementation of certain safety protocols to dealerships before cars are sold, in which case, the noncompliance of merchants may become an issue. It is likely, however, that dealerships are more likely to comply with manufacturer requirements as they are directly connected to specific car manufacturers (*e.g.*, Ford), as opposed to merchants who generally accept multiple brands of payment cards.

175. There are twelve members of the Auto Alliance, which include BMW Group, Fiat Chrysler U.S. LLC Motor Co., Ford Motor Company, GM, Mercedes-Benz, and other major players. *See* Members, AUTO ALLIANCE, http://www.autoalliance.org/members (last visited Sept. 14, 2016).

176. *Auto-ISAC Announces Board of Directors*, AUTO ALLIANCE (Oct. 21, 2015), http://www.autoalliance.org/index.cfm?objectid=2A25D140-7826-11E5-997E000C296BA163 (last visited Sept. 14, 2016).

177. The committee's charter states the committee is responsible for developing and maintaining recommended practices and information reports. Patrick Ponticel, *SAE Committee*

cybersecurity initiatives in industries such as aviation and medicine.[178] These initiatives make clear the auto industry is cognizant of security issues and working towards heightened security standards in their vehicles. By officially delegating cybersecurity standards to car manufacturers, the government will be supporting the initiative already underway by the automotive industry.

CONCLUSION

As our world becomes more interconnected, hacking becomes a more significant threat with each passing day. Hacks of personal emails and backgrounds put individuals on notice that what we deem to be private is just a few clicks away from an enterprising hacker. Plus, the recent research into car hacking proves that hacks are no longer simply invasions of privacy.

The proposed legislation specific to car hacking is unnecessary in the current legal landscape. Existing laws cover the range of offenses inherent in car hacking, and creating more regulations will just cloud an already crowded regulatory field. Leaving the NHTSA or another agency to create standards through the regulatory process ignores the way technology develops and changes quickly. Before jumping to federal regulations, legislators should take note of private ordering systems such as the PCI DSS. A private ordering system will allow car manufacturers to set standards with the assistance of expert researchers in order to keep up with dynamic technology.

Busy Developing Standards to Confront the Cybersecurity Threat, SAE INT'L (Jan. 5, 2015, 3:28 PM), http://articles.sae.org/13809/ (last visited Sept 14, 2016).

178. *Auto Cyber-Security: Continual Testing, Checks and Balances*, AUTO ALLIANCE (July 10, 2014).