PRIVATE ORDERING: A PROGRESSIVE OUTLOOK ON AUTOMOBILE CYBERSECURITY IN THE UNITED STATES

Sudipto Koner[*]

Abstract

For several years now, cybersecurity hacks have usually been restricted to attacks on our privacy and on cashless modes of payment like credit and debit cards. Nowadays, even car security infringements take place quite often. This essay focuses on the United States of America and begins by providing a concise history of numerous research endeavours to determine the probable risks of car security infringements in Part I. Part II evaluates the current legislations with regards to car hacking and their drawbacks. Part III deals with how laws at present can be relevant to car hacking and establishes how private ordering is the most productive way of setting up cybersecurity benchmarks for the automotive industry. It concludes by stating that no new legislations are required, they are just a burden on the already complicated legislative framework in the United States.

[*]Sudipto Koner is a second-year student of National Law University, Odisha. The author may be reached at 16ba106@nluo.ac.in.

I. INTRODUCTION

For a long time, our privacy was breached in multifarious ways with every cyber hack that occurred; by making illegitimate transactions on our credit cards,[1] reading our confidential documents and emails,[2] and revealing the darkest phases of our otherwise private lives.[3] As we become more dependent on the internet with every passing day,[4] the issue of cybersecurity becomes much more prominent. It becomes more significant when cyberattacks are targeted at automobiles. In this essay, the focus is on automobile cybersecurity in the United States and viable options for the progress of the same.

In the month of July 2015, a reporter named Andy Greenberg was cruising down a St. Louis highway in a Jeep Cherokee.[5] Researchers (or hackers, based on the reader's perspective) Miller and Valasek gained remote access to the Jeep, taking control of the vehicular controls while working at home several miles away.[6] They first disabled the brakes of the vehicle, causing it to fall into a trench.[7] They were also able to trace specific GPS coordinates, find out the speed, and track routes.[8] What appeared like an unlikely concern

[1]Robin Sidel, *Home Depot's 56 Million Card Breach Bigger Than Target's*, THE WALLSTREET JOURNAL (Sept. 19, 2014), https://www.wsj.com/articles/home-depot-breach-bigger-than-targets-1411073571.
[2]Andrea Peterson, *The Sony Pictures hack, Explained*, WASHINGTON 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), https://arstechnica.com/information-technology/2015/08/ashley-madison-hack-is-not-only-real-its-worse-than-we-thought/.
[4]Bill Wasik Gear, *In the Programmable World, All Our Objects Will Act as One*, WIRED (May 14, 2013), https://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 (Jul. 21, 2015), https://www.wired.com/ 2015/07/hackers-remotely-kill-jeep-highway/ (hereinafter Greenberg).
[6]*Id.*
[7]*Id.*
[8]*Id.*

some years ago has now turned out to be a disconcerting reality. These hackers confirmed that cyber-security is no longer restricted to infringements of privacy; hackers can now take charge over the vehicular controls and exploit it to the fullest, mostly resulting in physical harm to the victim.

To this day in the United States (US), many legislations have been incorporated pertaining to cybersecurity measures, with a special focus on car hacking. In July 2015, Senators Edward J. Markey (District Court, Massachusetts) and Richard Blumenthal (District Court, Connecticut) introduced the Security and Privacy in Your Car (SPY Car) Act.[9] This Act was again reintroduced in 2017. In November 2015, Joe Wilson, now Chairman of the House Armed Services Subcommittee on Readiness, and Ted Lieu (CA-33) introduced the SPY Car Study Act[10] (again reintroduced in January 2017), which was preceded by a discussion draft prepared by the House Committee on Energy and Commerce.[11] Critics as well as cybersecurity experts were sceptic about the efficacy of these types of measures,[12] more so because they were cautious about governmental schemes in private businesses.[13] On the contrary, advocates of consumer safety believe that legislation was required to care for unwary motorists.[14]

[9]Security and Privacy in Your Car Act, S. 1806, 114th Cong. (2015) (U.S.).
[10]Security and Privacy in Your Car Study Act of 2015, H.R. 3994, 114th Cong. (2015) (U.S.).
[11]*Id*.
[12]Tim Starks, *Car-hacking feud revs up on the Hill*, POLITICO (Aug. 29, 2015), https://www.politico.com/story/2015/08/pro-cyber-carhacking-starks-213124 (hereinafter Starks).
[13]Eli Dourado & Andrea Castillo, *Why the Cybersecurity Framework Will Make Us Less Secure*, MERCAT. CENT. (2014), https://www.mercatus.org/system/files/Dourado_CybersecurityFramework_v2.pdf (hereinafter Dourado and Castillo).
[14]*See* Starks, *supra* note 12, at 2.

This essay maintains that any new law bringing about new guidelines regarding safety is pointless, and will eventually give rise to more problems. To begin with, there are manifold recognised laws in the US that already mandate what some of these recommend, or tackle the concerns related to hacking of cars. Also, with the constant progress in vehicular technology, new ways and means will be on hand to repair the flaws present in their systems. Finally, the ineffectiveness of the government and its failure to avert its own cyberattacks[15] renders any type of federal directives mandating minimal safety protocols an inconvenient option. Therefore, this essay maintains that private ordering, the act of apportioning regulatory power with private partners,[16] will come in handy when it comes to carrying out of productive security measures.

While driverless cars are close to becoming a reality, such technology evokes several legal issues that is beyond the scope of this essay. Hence, this essay will emphasise on vehicular electronics as they are easily obtainable on the existing market.

II. INSTANCES OF CAR HACKING IN THE PAST

In February 2010, cars of the customers of the Texas Auto Center refused to start or started honking nonstop.[17] Omar Ramos-Lopez, once a used car dealer, took advantage of a system called Webtech Plus, a remote immobilization system used as an alternative measure

[15]Andrea Peterson & Lisa Rein, *What you need to know about the hack of government background investigations*, WASHINGTON POST (Jul. 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/ (hereinafter Peterson and Rein).

[16]Steven L. Schwarcz, *Private Ordering*, 97 NW. U. L. REV. 319, 320 (2002) (hereinafter Schwarcz).

[17]Kevin Poulsen, *Hacker Disables More Than 100 Cars Remotely*, WIRED (Mar. 17, 2010), https://www.wired.com/2010/03/hacker-bricks-cars/.

against repossessing vehicles for which payments were due.[18] By this system, car dealers mounted a miniature black box under car dashboards that would respond to inputs sent via a central website, and transmit them through a wireless pager network.[19] A dealer was able to switch off the ignition or remotely trigger the horn as an intimation to owners for making payment.[20] Omar infiltrated the system through another employer's account, made a database of all the customers whose cars had been fitted with a black box, and immobilised their cars.[21] Even though it was not fatal from a security breach perspective, this was proof to the fact that any device with an internet connection can be used as an access point.

In the same year, a team of researchers from the University of Washington and the University of California, San Diego tried to find out how much resistance a normal car could have against a virtual attack targeted at its internal machinery.[22] The researchers conducted tests on two cars of the same brand and model in a simulated environment and in actual road tests.[23] The findings of the study revealed that the cars had minimal resistance against cyberattacks.[24] Nonetheless, the study laid emphasis on the question of whether a hacker could infect a car's internal machinery, and not on the manner in which a hacker might do so.[25] The researchers detected several vulnerabilities within the cars and they also established that for each

[18]*Id.*
[19]*Id.*
[20]*Id.*
[21]*Id.*
[22]Karl Koscher et al., *Experimental Security Analysis of a Modern Automobile*, 2010 IEEE SYMPOSIUM ON SECURITY AND PRIVACY (2010), http://feihu.eng.ua.edu/NSF_CPS/year1/w9_1.pdf.
[23]*Id.*
[24]*Id.*
[25]*Id.* at 14.

vulnerability, one could get full command over the vehicular machinery.[26]

It was imminent that Miller and Valasek would come to know about this research and subsequently devoted two years of their time in their pursuit for finding ways to remotely hack a vehicle.[27] They infiltrated the Jeep's internal machinery via a feature called Uconnect—Chrysler's network system that manages the vehicle's entertainment and navigation functions, receives phone calls, and offers a WiFi hotspot.[28] This vulnerability, named as zero-day vulnerability,[29] enabled them to transmit code via the Jeep's entertainment systems to the steering, brake pedals, transmission and dashboard related functions.[30] Besides performing considerably harmless functions like switching on the windshield wipers or toying with the air conditioner, the hackers were capable of completely inactivating the engine at lesser speeds and trigger or disable the brakes at any time.[31] As if their capability to gain access to vehicular controls was not scary enough, they could also trace specific GPS coordinates, and track the route of a particular vehicle.[32] Both of them issued a prior notice to Fiat Chrysler to inform them about their intentions to make their findings public. Thereafter, Fiat Chrysler recalled 1.4 million vehicles

[26]Stephen Checkoway et al., *Comprehensive Experimental Analyses of Automotive Attack Surfaces*, USENIX SECURITY SYMPOSIUM (2011), http://static.usenix.org/events/sec11/tech/full_papers/Checkoway.pdf.
[27]Andy Greenberg, *Hackers Reveal Nasty New Car Attacks—With Me Behind The Wheel (Video)*, FORBES (Jul. 24, 2013), https://www.forbes.com/sites/andygreenberg/2013/07/24/hackers-reveal-nasty-new-car-attacks-with-me-behind-the-wheel-video/.
[28]Greenberg, *supra* note 5.
[29]*See* Kim Zetter, *Hacker Lexicon: What Is a Zero Day?*, WIRED (Nov. 11, 2014), https://www.wired.com/2014/11/what-is-a-zero-day/ (hereinafter Zetter).
[30]*Id.*
[31]Greenberg, *supra* note 5.
[32]*Id.*

and implemented network grade security systems on the Sprint mobile network that operates in its vehicles.[33]

Another duo of researchers, Marc Rogers and Kevin Mahaffey, discovered after several years of research work that they were able to electronically 'hotwire' a Tesla Model S after connecting a laptop via a network cable into the car's driver-side dashboard.[34] They also found out that they could insert a Trojan virus by remote-access in the car's network when they had physical access to it, and afterwards use it to remotely inactivate the engine after disconnecting.[35] The car's infotainment system was operating on an obsolete browser which had an Apple WebKit vulnerability that could make the system accessible to any hacker.[36] They discovered six vulnerabilities in total in the Model S and this was communicated to Tesla thereafter. Tesla worked with the researchers to fix those vulnerabilities.[37] However, contrary to Fiat Chrysler, which had to recall around 1.4 million vehicles, Tesla was able to issue software updates remotely for its vehicles.[38]

These studies were taken into consideration by Senator Edward J. Markey in 2013.[39] Senator Markey dispatched a letter to twenty large

[33]Aaron M. Kessler, *Fiat Chrysler Issues Recall Over Hacking*, N.Y. TIMES (Jul. 24, 2015), https://www.nytimes.com/2015/07/25/business/fiat-chrysler-recalls-1-4-million-vehicles-to-fix-hacking-issue.html (hereinafter Kessler).
[34]Kim Zetter, *Researchers Hacked a Model S, But Tesla's Already Released a Patch*, WIRED (Aug. 6, 2015), https://www.wired.com/2015/08/ researchers-hacked-model-s-teslas-already/ (hereinafter Zetter, Tesla).
[35]*Id.*
[36]*Id.*
[37]*Id.*
[38]*Id.*
[39]Ed Markey, *As Wireless Technology Becomes Standard, Markey Queries Car Companies About Security, Privacy*, PRESS RELEASE OF THE U.S. SENATOR FOR MASS. (Dec. 23, 2013), https://www. markey.senate.gov/news/press-releases/as-wireless-technology-becomes-standard-markey-queries-car-companies-about-security-privacy.

automobile companies in the United States to know about security measures that were previously implemented.[40] The letter comprised questions on the way companies identify probable vulnerabilities from third party devices, whether vehicles had the technology required to identify unusual behaviour, and what kind of data regarding driving history could be acquired from technologies present in the vehicle.[41] In 2015, Senator Markey showed the report reviewing the responses and came to a conclusion that security measures were grossly inadequate for protecting drivers, especially against hackers who intend to take over a vehicle or tap confidential information.[42] According to the report, the responses given were proof of the fact that privacy and security measures were worryingly inadequate and erratic, and directed the National Highway Traffic Safety Administration ("**NHTSA**") to introduce new norms to protect recent drivers.[43]

What the above establishes, therefore, is that cybersecurity is now an integral part of our lives. As hackers find out more intricate methods to infringe a car's machinery, more laws are likely to be introduced.

III. EXISTING LAWS WITH REGARDS TO CAR HACKING

This section of the essay examines the legislations introduced to solve the issues related to car hacking and the flaws that are associated with them.

[40]*Id.*
[41]*Id.*
[42]Staff of Senator Edward J. Markey, *Tracking & Hacking: Security & privacy gaps put American drivers at risk 1* (2015), https://www.markey.senate.gov/imo/media/doc/2015-02-06_MarkeyReport-TrackingHackingCarSecurity%202.pdf.
[43]*Id.*

A. Schemes of Legislation

There are three legislations dealing with car hacking, namely (i) SPY Car Study Act of 2017, (ii) Spy Car Act of 2017, and (iii) House Discussion Draft. However, the problems lie with the NHTSA because this is mandatory for promulgating ordinances. Later, this part will discuss the problems within the government and cybersecurity at large.

a) Spy Car Study Act of 2017

In January 2017, Congressmen Joe Wilson and Ted Lieu introduced the SPY Car Study Act of 2017.[44] The bill would have mandated the NHTSA to carry out a study with several organizations such as the Secretary of Defense, Federal Trade Commission ("**FTC**"), SAE International, automobile companies and important academic establishments.[45] Initial findings of the study would be submitted within one year of the enactment of this bill to several agencies in the House and Senate, with a concluding report before six months after that submission.[46]

Nonetheless, a few years previously in 2012, Congress ratified the Moving Ahead for Progress in the 21st Century Act (MAP-21).[47] It provided for a new council under the NHTSA committed to automobile electronics mandating the NHTSA to carry out a study pertaining to safety measures in electronic systems in passenger

[44]security And Privacy in Your Car Study Act Of 2017, H.R. Doc No. 701, at 1 (2017) (U.S.).
[45]*Id.* at § 2(a).
[46]*Id.* at § 2(b).
[47]Moving Ahead for Progress in the 21st Century Act, Pub. L. No. 112-141, 126 Stat. 405 (2012) (U.S.) (hereinafter MAP-21 Act).

automobiles.[48] Thus, the requirements of the SPY Car Study Act were already enforced by the MAP-21 Act.

b) Spy Car Act of 2017

By applying a wider perspective on this issue, Senator Edward J. Markey and Richard Blumenthal introduced the SPY Car Act in March 2017.[49] This bill is divided into three primary categories: (i) Cybersecurity Standards in Motor Vehicles (ii) Cyber Dashboard and (iii) Privacy Standards in Motor Vehicles.[50]

If enforced, the first section would mandate every points of access to the electronic systems in automobiles to have satisfactory standards in place to prevent cyberattacks, and the crucial software systems to be segregated.[51] On top of that, the information acquired by these systems shall have adequate protection to foil infiltration during the time of accumulation and storage of that information.[52] Finally, all points of access shall have the technology to identify, inform and prevent interception of information or infiltration on a vehicle.[53]

The next section, the Cyber Dashboard, would made it compulsory for a sticker to be attached to every automobile manufactured two years after the enforcement of the bill.[54] The function of the sticker would be to apprise customers regarding the protections provided by a particular vehicle for cybersecurity and privacy in a way that is simple and graphic-intensive.[55]

[48] *Id.* at § 31401-02.
[49] Security and Privacy in Your Car Act of 2017, S. 680, 115th Congress (2017) (U.S.) (hereinafter Spy Car Act, 2017).
[50] *Id.*
[51] Spy Car Act, 2017, *supra* note 49, at § 30129(a)(1)-(2).
[52] Spy Car Act, 2017, *supra* note 49, at § 30129(a)(3).
[53] Spy Car Act, 2017, *supra* note 49, at § 30129(a)(4).
[54] Spy Car Act, 2017, *supra* note 49, at § 30129(3)(a)(1).
[55] Spy Car Act, 2017, *supra* note 49, at § 30129(3)(a)(2).

The third section of the bill would ensure privacy measures which are unambiguous and under customer control.[56] Vehicles would be mandated to give a proper notice regarding the accumulation and usage of driving information acquired by the vehicle.[57] Moreover, customers could refuse such accumulation of information without getting deprived of the navigation feature.[58] On top of that, the SPY Car Act would delegate the framing of rules and final regulations to the NHTSA to be enforced before three years after the enforcement of the bill.[59] As will be assessed in Part III, this may probably be in conflict with the Cybersecurity Information Sharing Act which was enforced in 2015. The government should be cautious with regard to permitting customers to pull out of such an information accumulation scheme as it is unknown what kind of information surveillance is required for car companies and other surveillance companies to correctly identify probable dangers. Keeping in mind the fact that researchers have already established the variety of ways a hacker could bypass a car's security system, the fact that customers would be permitted to pull out of the accumulation of driving information citing privacy reasons could possibly impair the ability of the company to evaluate security risks.

c) House Discussion Draft

In 2015, The House Committee on Energy and Commerce also issued a discussion draft pertaining to cybersecurity in passenger vehicles. Cybersecurity, Privacy and Hacking Prohibition (Title III) would mandate car companies to devise and enforce a privacy scheme for conveying the company's assimilation, handling and distribution of

[56]Spy Car Act, 2017, *supra* note 49, at § 30129(4)(b)-(c).
[57]Spy Car Act, 2017, *supra* note 49, at § 30129(4)(b).
[58]Spy Car Act, 2017, *supra* note 49, at § 30129(4)(c)(2).
[59]Spy Car Act, 2017, *supra* note 49, at § 30129(b)(1)-(2).

specific information related to customers.[60] A company which is unable to devise such a scheme would be subjected to a fine to the limit of $5000 a day and would not surpass $1,000,000 for a single company.[61] The draft also includes a special provision, which states that companies whose privacy schemes conform to the provisions will be exempted from section five of the Federal Trade Commission Act pertaining to fraudulent practices with regards to privacy.[62]

Further, the draft makes it clear that it shall be illegal for anyone to retrieve, without permission, an electronic control unit or a crucial unit of a vehicle, or other units having driving information for that vehicle, either remotely or via a wired connection.[63] Each time a person is found in contravention of this provision, he/she would be subject to a fine to a limit of $100,000.[64] Also, the draft mandates the NHTSA to set up the 'Automotive Cybersecurity Advisory Council' to formulate superlative practices for companies, with a directive for major companies to elect a delegate for their service on the Council.[65]

Though it was never approved, this draft had its share of problems. First of all, the language was vague and did not mention who could give the approval. Harley Geiger, a former Advocacy Director of the Center for Democracy and Technology, asserted that after a customer buys a car, he normally possesses the physical parts of the car, while the software present in the car is just registered by the car company to the buyer.[66] Also, illegitimate access permitted researchers to identify the vulnerabilities of a car and afterwards work with companies to

[60]Discussion Draft Title III, H.R. 3994, 114th Cong. (2015) (U.S.).
[61]*Id.*
[62]*Id. See also* 15 U.S.C § 45(a)(1).
[63]Discussion Draft Title III, H.R. 3994, 114th Cong. (2015) (U.S.).
[64]*Id.*
[65]*Id.*
[66]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/.

repair those vulnerabilities, similar to the work Mahaffey and Rogers did for Tesla.

Vulnerabilities prevalent in systems which dealers are unaware of but hackers tend to misuse are known as zero-day vulnerabilities.[67] Usually, a zero-day vulnerability is not bad in itself, similar to the way Miller and Valasek misused the system, although their motivations were beneficial. Permitting other researchers to identify ways in which these vulnerabilities can be misused has resulted in the recall of 1.4 million vehicles by Fiat Chrysler[68] and a security patch sent to owners of Tesla cars.[69] By causing this kind of research to be illegal, customers will have to suffer undesirable consequences thereafter. Car companies could accept or reject approval from researchers for a variety of reasons, be it suspicious or genuine. Still, other third parties investigating vulnerabilities of connected vehicles will only lead to a bigger system of counterbalancing influences between experts and car companies.

IV. SHORTCOMINGS IN LEGISLATION SCHEMES

Presently, all the schemes depend on the NHTSA to promote regulations. Owing to the sluggishness of administrative agencies and the NHTSA's problems of late, ideally the NHTSA is not a good option. Also, experts believe that the government is indulging in cybersecurity control as a result of several breakdowns in its own security.

[67]*See* Zetter, *supra* note 29.
[68]*See* Kessler, *supra* note 33.
[69]*See* Zetter, Tesla, *supra* note 34.

A. The NHTSA Controversy

Every scheme mentioned above delegates wholly or partly its power for framing of rules to the NHTSA. For instance, the SPY Car Act delegates exclusive framing of rules to the NHTSA,[70] with the NHTSA Superintendent putting out a Notice of Proposed Rulemaking schemes before eighteen months of enforcement, and final regulations to be brought out within a limit of three years after the enforcement of the bill.[71] By issuing this public notice, the SPY Car Act renders the enactment of cybersecurity norms to the will of the procedure of rulemaking.

It is important to mention that the Administrative Procedure Act[72] oversees the Notice of Proposed Rulemaking. Any individual whose legal right is infringed, or suffers harmful consequences due to the acts of a company within the ambit of the pertinent law, can proceed for judicial review.[73] In this case, the court of review can take a random and impulsive stance with regards to company actions.[74] In *Motor Vehicle Manufacturers Association v State Farm Mutual*,[75] the Supreme Court examined whether the NHTSA acted randomly and impulsively when it annulled the mandate that all vehicles manufactured after 1982 would have some subdued restrictions.[76] The Court viewed that the random and impulsive standard is limited and a court cannot substitute its judgment for the purpose of the company. The Company must provide a reasonable justification for its acts.[77]

[70]*See* Vlasic & Ruiz, *infra* note 81.
[71]Security and Privacy in Your Car (SPY Car) Act of 2015, S. 1806, 114th Cong. § 30129(b) (2015) (U.S.).
[72]5 U.S.C § 553 (2015).
[73]5 U.S.C. § 702 (2015).
[74]5 U.S.C. § 706(2)(a).
[75]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) (U.S.).
[76]*Id.* at 44.
[77]*Id.* at 42.

The Court came to a conclusion that the NHTSA was unable to provide a reasonable justification for annulling the safety norms.[78]

In this situation, should a car company or a business association,[79] feel that they have suffered harmful consequences owing to the NHTSA action, they can go for judicial review wherein the NHTSA must provide a reasonable justification for its acts. The court of review would afterwards employ the same impulsive standard to decide whether the NHTSA provided reasonable justifications or not. As is evident with the hacks conducted by researchers recently, car companies respond to vulnerabilities at once.[80] In a rapidly evolving field such as cybersecurity, even after certain standards qualify for the judicial review, they could still get outdated before the procedure of review gets over.

Amidst the likely indolence of being governed by administrative laws, the NHTSA has been embroiled in some controversies.[81] In 2015, reports were circulated which examined the function the NHTSA performed in General Motors' recalls with regards to flaws in the ignition switch which resulted in the death of at least hundred people.[82] Based on insider inputs, the NHTSA confessed to a failure to spot warning signs that could have notified the agency regarding General Motors' flaw and its reluctance to discharge its full power in punishing them,[83] for which General Motors' cars operated without repairs for several years.[84] This resulted in a restructuring of the

[78]*Id.* at 48.
[79]5 U.S.C. § 551 (2015).
[80]*See* Zetter, Tesla, *supra* note 34.
[81]*See* Bill Vlasic & Rebecca R. Ruiz, *Safety Agency Admits Missing Clues to G.M. Ignition Defects,* N.Y. TIMES (Jun. 5, 2015), https://www.nytimes.com/2015/06/06/business/nhtsa-admits-missing-clues-to-gm-ignition-defects.html (hereinafter Vlasic & Ruiz).
[82]*Id.*
[83]*Id.*
[84]*Id.*

NHTSA, which comprised of a supervisory team of specialists to assist in implementation of those reforms.[85]

Understandably, the NHTSA is the agency for enacting regulations for automobiles. Despite this, car hacking is a cybersecurity concern which calls for an effective approach which can promptly retaliate to technological changes. The NHTSA is not the most reliable agency for enacting regulations with regards to the concern of car hacking, primarily due to the probable deferrals in the rulemaking scheme.

B. Contribution of the Government in the field of Cybersecurity

Another concern with all of the three schemes is entrusting the government with the task of devising cybersecurity regulations for vehicles. The current as well as the previous government's cybersecurity schemes have drawn criticism for quite some time.

The Cybersecurity Framework is one such scheme. The Director of the National Institute of Standards and Technology was to spearhead the growth of this framework in order to minimise cyberattacks to crucial infrastructure, according to Executive order numbered 13636.[86] It comprises guidelines, policies, courses of action and ways to deal with cybersecurity risks with the help of a flexible, merit-based and economical strategy to support owners and administrators of crucial infrastructure in tackling cybersecurity threats.[87] If any of the crucial infrastructure systems (systems and resources, either physical or virtual) in a country (in this case, the US) are adversely affected, it would have a disastrous outcome on matters related to security, financial security and public health security.[88]

[85] *Id.*
[86] Exec. Order No. 13,636, 78 Fed. Reg. 33, at 11, 740-71 (Feb. 19, 2013).
[87] *Id.*
[88] *Id.* at 11739.

The Cybersecurity Framework is divided into three parts: (i) the Framework Core (ii) the Framework Implementation Tiers and (iii) the Framework Profile.[89] The Framework Core contains top-notch methods for every class of crucial infrastructure, which is in turn classified into functions and then subcategories.[90] The Framework Implementation Tiers ensures that every function and category incorporated in the Framework Core are compatible with each other.[91] An organization is scored by the Framework profile with regards to its conformity with the Framework's proposed cybersecurity measures.[92]

The Cybersecurity Framework received responses which were ambivalent at best. Some people believe that the framework was a suitable course of action,[93] while others viewed the Cybersecurity Framework as a bad idea, substituting a dynamic approach of devising cybersecurity norms with a mandate with regards to conformity with prescribed federal norms.[94]

Andrea Castillo and Eli Dourado, both research fellows at the Mercatus Center at George Mason University, viewed that the Internet did not have a cohesive cybersecurity scheme for a long time owing to the associations amongst networks.[95] The Internet devised a policy for itself, such as promptly banning networks that permitted criminals to utilise their resources.[96] Cybersecurity teams were

[89]*See* Dourado and Castillo, *supra* note 13.
[90]*Id.* at 10.
[91]*Id.*
[92]*Id.*
[93]Joab Jackson, *How the NIST cybersecurity framework can help secure the enterprise,* PCWORLD (Feb. 14, 2014), https://www.pcworld.com/article/2098320/how-the-nist-cybersecurity-framework-can-help-secure-the-enterprise.html.
[94]*See* Dourado and Castillo, *supra* note 13.
[95]*Id.* at 6.
[96]*Id.* at 7.

created to keep a check on traffic for malicious activities and notify users of possible security risks.[97] Plausible tactics with regards to botnet activity were created from shared information among organizations.[98] Therefore, private companies had already devised necessary measures to improve cybersecurity standards.[99] However, critics view that the Framework replaces those independent tactics with the impetus to improve the score of their Framework Profile.[100]

A major disapproval of the current as well as the previous government's efforts to enact cybersecurity regulations arises because of the government's own susceptibility to being hacked and otherwise bad reputation regarding cybersecurity. In 2014, the US Department of Justice confirmed around 3600 cases of data infringements, which was followed by malicious software being downloaded onto computers of various companies roughly around 180 times.[101] The very next year, the United States Office of Personnel Management was targeted by hackers, resulting in the breach of confidential information of 21.5 million people.[102] Recently, the emails of around 350 blue-chip clients of accountancy giant Deloitte were targeted by hackers.[103] These 350 clients comprise of four US government departments, the United Nations and a few of the world's biggest corporations like FIFA and three airline companies amongst others. Insider inputs believe that the breach occurred only in the US, and the hackers got access to the IP addresses, usernames, passwords,

[97]*Id.* at 8.
[98]*Id.* at 9.
[99]*Id.* at 6.
[100]*Id.* at 15.
[101]Eli Dourado & Andrea Castillo, "*Information Sharing": No Panacea for American Cybersecurity Challenges*, MERCAT. CENT. (2015), https://www.mercatus.org/system/files/Dourado-Information-Sharing-Cybersecurity-MOP.pdf.
[102]*See* Peterson and Rein, *supra* note 15.
[103]Nick Hopkins, *Deloitte hack hot server containing emails from across US government*, THE GUARDIAN (Oct. 10, 2017), https://www.theguardian.com/business/2017/oct/10/deloitte-hack-hit-server-containing-emails-from-across-us-government.

architectural models for businesses and healthcare, and secret security and design data of those blue-chip clients.[104] Therefore, a situation may arise wherein the NHTSA enacts regulations that would drive companies to make an effort towards conforming to federally prescribed regulations rather than devising suitable standards for technological changes.

C. Addressing the Legislative Inadequacies with regards to Car Hacking

As is the case with any security risk, car hacking has led to a rift amongst business insiders, supervisors, and consumer activists. There should be two primary objectives to be achieved. First, car companies have to create a blueprint for proceeding with appropriate conventions that protect their vehicles against imminent cyberattacks. Second, customers have to be safeguarded. Consumer activist groups along with Senators Markey and Blumenthal contend that the most appropriate way to accomplish these objectives is to enact laws that exclusively tackles car hacking, like the SPY Car Act.[105] Nevertheless, car companies believe that the new conventions will only hamper development of appropriate security standards and were reluctant to be held accountable for the acts of hackers when they have acted with sincere intentions.[106] Also, the automobile industry has encouraged information-sharing schemes, like the Cybersecurity Information Sharing Act ("**CISA**"), with General Motors advising the Senate to enforce the CISA.[107]

Even though the discussed proposals are introduced with good faith, they are ultimately unnecessary. Many subsisting legislations contain

[104] *Id.*
[105] *See* Starks, *supra* note 12.
[106] *Id.*
[107] *Id.*

most of the issues concerned with car hacking, rendering new legislations as surplusage. To address the concern in a more convenient way, private ordering should be used as a tool to facilitate the automobile industry to implement its own standards with the purpose of keeping up with the technological changes more effectively.

a) Current Legislations associated with car hacking

Most of the concerns related to car hacking are already dealt with by current laws such as automotive safety norms, cybersecurity regulations and accountability of car companies. For instance, the NHTSA has been enacting motor vehicle safety regulations under confederate order[108] from the year 1967.[109] The function of these regulations is to minimise traffic mishaps and death by performing requisite research in the field of safety and development.[110] Product accountability and other tort-based litigations have dictated the culpability of automobile companies for several years. On top of that, MAP-21 issues an additional mandate to the NHTSA to explore safety issues with regards to connected vehicles.[111]

Undoubtedly, car hacking is within the ambit of the Computer Fraud and Abuse Act (CFAA).[112] The law includes acts like deliberately inducing harm to a secured computer by means of a transfer of a codified program,[113] deliberately infiltrating a secured computer by bypassing authentication and impulsively bringing about damage and loss.[114] A secured computer refers to a computer which is used in the

[108]Motor Vehicle Safety, 49 U.S.C. § 30101 (2016) (U.S.).
[109]*See* Federal Motor Vehicle Safety Standards And Regulations, U.S. DEPT. OF TRANSP. (1998) (U.S.).
[110]*Supra* note 108.
[111]MAP-21 Act, *supra* note, at § 31401-02.
[112]18 U.S.C. § 1030 (2015).
[113]*Id.* at § 1030(a)(5)(A).
[114]*Id.* at § 1030(a)(5)(C).

process of carrying out regional or overseas trade.[115] The CFAA states that the word 'computer' also includes an information storage or transmissions service functioning directly or in combination with that service.[116] As a result, this is definitely a way to penalise hackers who illegitimately access a vehicle.

In spite of this, the CFAA has also drawn criticism for quite some time. Few people contend that this Act is abused by prosecutors to torment and threaten security scientists by using the 'unauthorised access' phrase.[117] Others contend that the phrase 'unauthorised access' is very wide and ambiguous and should therefore be made unconstitutional.[118] It is thus not difficult to comprehend that the analogous usage of 'without authorization' phrase by the House Discussion Draft is complicated while making efforts to penalise prospective hackers.

Moreover, the Federal Trade Commission ("**FTC**") may well have the power to control automobile cybersecurity referred to under the 'unfair acts' section of the FTC Act.[119] In the case of *FTC v Wyndham Worldwide Corporation*,[120] the Third Circuit decided that the FTC has the power to initiate proceedings against a company for its recurring inability to protect itself against cyberattacks in a small period of time.[121] Here, in between the year 2008 and 2009, Wyndham was targeted by hackers thrice, all of them happening in a similar manner,

[115]*Id.* at § 1030(e)(2)(B).
[116]*Id.* at § 1030(e)(1).
[117]Sam Gustin, *U.S. "Hacker" Crackdown Sparks Debate over Computer-Fraud Law*, TIME (Mar. 19, 2013), http://business.time.com/2013/03/19/u-s-hacker-crackdown-sparks-debate-over-computer-fraud-law/.
[118]Tim Wu, *Fixing the Worst Law in Technology*, NEW YORKER (Mar. 18, 2013), https://www.newyorker.com/news/news-desk/fixing-the-worst-law-in-technology.
[119]15 U.S.C. § 45(a) (2015).
[120]F.T.C. v. Wyndham Worldwide Corp., 799 F.3d 236, 259 (3d Cir. 2015) (U.S.) (hereinafter F.T.C. v. Wyndham).
[121]*Id.* at 241–42.

by gaining access to an administrator account.[122] The FTC suspected that Wyndham was involved in fraudulent cybersecurity practices that were unjust and pointless, such as exposing consumers' confidential information to illegitimate access and theft and also suspected that Wyndham was unsuccessful in employing firewalls or taking suitable steps to identify and thwart illegitimate access.[123] The court dismissed these claims stating that the absence of a firewall and a third attack in a like manner would put Wyndham on a warning that it failed to comply with the norm of the cost benefit analysis[124] stated in a different section of the Act.[125] While this was an interim appeal, and therefore no conclusion was arrived at with regards to its merits,[126] it unofficially made companies aware of the fact that the FTC has the authority to initiate legal proceedings against those it believes lack adequate cybersecurity measures.

Furthermore, CISA[127] was enacted as an addition to an omnibus budget bill.[128] CISA permits private parties[129] to inspect their own data system for cybersecurity reasons.[130] It also safeguards legal responsibility as against private parties for inspecting a data system under section 104(a).[131]

This Act also provides for companies to give out information related to cybersecurity risks with the government[132] and grants extra

[122]*Id.*
[123]*See Id.* at 240–41.
[124]15 U.S.C. § 45(n) (2015).
[125]F.T.C. v. Wyndham, *supra* note 120, at 256.
[126]*Id.* at 240.
[127]Cybersecurity Information Sharing Act of 2015, Pub. L. No. 114-113, 161 Stat. 1729 (2015) (U.S.).
[128]Andy Greenberg, *Congress Slips CISA into a Budget Bill That's Sure to Pass*, WIRED (Dec. 16, 2015), https://www.wired.com/2015/12/congress-slips-cisa-into-omnibus-bill-thats-sure-to-pass/.
[129]Consolidated Appropriations Act, P.L. No. 114-113, § 102(4), 129 Stat. 2242 (2016) (U.S.).
[130]*Id.* at § 104(a)(1)(A).
[131]*Id.* at § 106(a).
[132]*Id.* at § 105.

protection of legal responsibility from litigations arising due to this sharing of information.[133] For future laws that may mandate sharing of information, CISA's protection makes it certain that car companies will be more likely to inspect their data systems and share information with the government to get the best possible protection given by law. For any legislation that is introduced, like the SPY Car Act of 2015, that permits customers to refuse this collection of information, car manufacturers may draw attention to CISA, arguing that they are permitted to inspect the data systems of their automobiles. Excluding car hacking from other cybersecurity legislations will result in conflicting policies.

It is evident that there are plenty of legislative schemes available to legislators to create safety regulations for car companies, initiate legal proceedings against those they believe are falling short of providing reasonable protection to customers, and penalise malicious hackers in future. Enacting more laws governing this field of law will only create more problems in an already congested legislative scenario.

b) Private Ordering is the answer

Private ordering will permit automobile companies to implement their own cybersecurity regulations. A good example of a private ordering system is the Internet Corporation for Assigned Names and Numbers (ICANN) which manages the Internet domain structure.[134] Moreover, Moody's Investors Service and Standard & Poor's Ratings Service had the authority to hand out credit ratings, in addition to other duties.[135] The credit card sector is a case in point with regards to private ordering in the industrial sector which addresses its own cybersecurity concerns.

[133]*Id.* at § 106(b).
[134]*See* Schwarcz, *supra* note 16, at 319, 320.
[135]*See Id.* at 326.

D. The role of private ordering in the Credit Card Industry

Private ordering has been in operation in the credit card industry to help devise the Payment Card Industry Data Security Standards ("**PCI DSS**").[136] Private ordering is concerned with different methods for regulating behaviour and addressing disputes which are distinct from legislations brought forward by the government and implemented by the judiciary.[137] In the year 2004, five big card brands joined hands to issue the first renewal of the PCI DSS, which provided for an organised methodology to increase productivity with the help of 'shared security knowledge.'[138] The PCI Data Security Council ("**PCI DSC**") enforces regulations that must be adhered to by the various levels of the whole industrial sector.[139] Professors Vasant Raval and Edward Morse view that expertise pertaining to industry security regulations is presently shared by the means of the PCI SSC.[140] By sharing the expertise with the help of this private ordering scheme, the knowledge that is shared amongst the regulated industry and those who have the intention of regulating it come in conflict with each other.[141] This gives rise to major concerns regarding efforts at regulatory intervention by the government.

Professors Raval and Morse found out that the private schemes of regulation in the payment card industry were created because it was necessary to gain the trust of customers and traders regarding the usage of this mode of payment.[142] A chain of trust relationships exists which are integral to this industry.[143] To enhance the trust of

[136]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) (hereinafter Morse & Vasant Raval).
[137]*Id.* at 214.
[138]*Id.* at 229.
[139]*Id.* at 230.
[140]*Id.* at 235.
[141]*Id.*
[142]*Id.* at 221.
[143]*Id.*

customers, customers are safeguarded from illegal transactions performed on the network of any card issuer by not acquiring any accountability from such transactions.[144] Although there are a few laws which mandate customers to accept liability to the limit of 50 dollars, companies are focusing on their own self-interest by giving more protection than the minimal requirement.[145] By reducing, or completely eradicating customers' apprehensions regarding illegal transactions, payment card companies have amassed a great fortune.[146]

Likewise, in the automobile industry, customers should be able to rely on the cars they own that they will be safe for regular use and car companies should have faith that their product will not be used for creating harm in any manner. Car companies will also be operating in their own self-regard by enforcing safety regulations. If customers are unable to bestow their faith on a specific company's vehicles, they will shift to a company which they find more reliable.

Back in 2012, governmental interventions in the payment card sector had no significant impact.[147] One such intervention was the Fair and Accurate Credit Transaction Act of 2003 ("**FACTA**"), which contained a provision mandating only the final five digits and the complete abolition of expiration dates on every computer generated bill.[148] It turned out to be under-inclusive as well as over-inclusive in a few ways.[149] A criminal hypothetically would choose insecure electronic information over paper receipts, which FACTA does not focus on. An infringement of the FACTA provision could result from revealing the first and the last card numbers and hiding the numbers

[144]*Id.* at 223.
[145]*Id.* at 223–24.
[146]*Id.*
[147]*Id.* at 253.
[148]*See* Morse & Vasant Raval, *supra* note 136, at 253-54.
[149]*Id.* at 254–55.

in the middle, thus generating billions of permutations to determine the exact number of the card.[150] This kind of infringement is not much of a concern, minus other information.[151] Ultimately it leads to higher litigation expenses, owing to the large number of class action lawsuits brought under the realm of FACTA, thereby causing inconvenience to customers.[152]

Reviews of the PCI DSS suggest that the trader community mostly does not conform to its regulations.[153] This concern is possibly not prevalent in the automobile industry sector since the companies themselves will most likely be liable for enforcing the safety regulations in the end. The payment card industry is a case in point regarding private ordering, and the inadvertent outcomes of controlling an industry that has the impetus for self-regulation. Permitting the automobile industry to self-regulate with the assistance of cybersecurity specialists will tackle inadvertent undesirable consequences on customers.

E. The importance of private ordering with respect to car manufacturers

Just like in the credit card industry, car companies will implement safety regulations owing to market pressure, which includes ensuring the safety of customers. By now, car companies have started to devise private ordering systems. One of the most prominent groups in the US within the automobile sector is the Auto Alliance.[154] The Auto Alliance instituted the Automotive Information Sharing and Analysis Center ("**Auto-ISAC**") in order to make progress on collective

[150]*Id.* at 255.
[151]*Id.*
[152]*Id.* at 255–56.
[153]*Id.* at 238.
[154]There are twenty members of the Auto Alliance, which include Mercedes-Benz USA LLC, Volkswagen Group of America, General Motors, Volvo Car USA, and other major players. *See* Participating Members, AUTO ALLIANCE, https://autoalliance.org/connected-cars/automotive-privacy/participating-members/.

efforts.[155] The Auto-ISAC is a public body for conveying important security information to the automobile industry. It collects and circulates information about cybersecurity threats faced by interconnected vehicles across the globe. Information is obtained from its own members, administrative agencies, scholarly articles, open-source and other reliable sources. After a detailed examination by cybersecurity experts, the information is compiled into intelligence reports and shared through its secure Auto-ISAC Portal. With these stats, the automobile industry is better equipped to react to security threats, vulnerabilities and other similar events so that members of the interconnected vehicular network can best deal with their business risks.

Other initiatives undertaken by the automobile sector include founding the Vehicle Electrical System Security Committee, which was set up by the Society of Automotive Engineers (SAE).[156] It was set up to issue regulations and convenient practices and to target cybersecurity measures in sectors like medicine and aviation. Such initiatives are proof of the fact that the automobile industry is conscious about security risks and is striving towards enhancing the standards of security for their vehicles. By formally passing on the duty of implementation of cybersecurity standards to the car companies, the government will be in favour of the initiatives already undertaken by the automobile sector.

[155]Press Release, *Auto-ISAC Announces Board of Directors*, GLOBAL AUTOMAKERS (Oct. 21, 2015), https://www.globalautomakers.org/posts/press-release/auto-isac-announces-board-directors/.

[156]Alliance of Automobile Manufacturers, *Auto Cyber-Security: Continual Testing, Checks and Balances*, AUTO ALLIANCE (Jul. 10, 2014), https://www.autoalliance.org/auto-innovation/cyber-security/.

V. CONCLUSION

As the world becomes more interlinked, the risk of car hacking turns out to be more prominent than ever. Hacks of vehicular machinery amongst other things serve as a reminder to people that even if they have physical control over their car, it is just moments away from being infiltrated by a resourceful hacker who then gains complete control over the vehicle. It is not just about mere breaches of privacy, it can put to risk innocent lives as well.

The anticipated legislation exclusive to car hacking is not required in the present legal scenario of the US. Current laws already deal with the kind of offences regarding car hacking, and making more regulations will just create more problems in an already congested legislative scenario. Parting with the NHTSA or any other organization to enforce norms through the course of regulation disregards the way technology progresses and evolves steadily. Instead of switching to confederate regulations, legislators should take into consideration the significance of private ordering schemes like the PCI DSS. A private ordering system will permit car companies to enforce norms with the aid of specialist researchers for the purpose of keeping pace with evolving technology.