NOT EVEN REMOTELY LIABLE: SMART CAR HACKING LIABILITY

Scott L. Wenzel†

Abstract

Automobile laws must change in light of the increasingly popular smart car. Automobiles have dramatically evolved since their introduction to American society in the early twentieth century. Along the way, state and federal legislatures have passed innumerable laws aimed at regulating every facet of the industry. Since the initial regulatory scheme in the 1970s, Congress has been specifically interested in ensuring car safety and reducing the emissions of vehicles. These laws were highly effective in curbing emissions and lowering the mortality rate on the highways of America. Because of their success, the framework of these laws has remained virtually unchanged, signaling a failure to acknowledge the recent introduction of technologically advanced car systems. The legislatures' unquestioned reliance on this framework has never proved to be a problem—until now.

Smart car technology has caused a plethora of problems for consumers ranging from death due to a misplaced reliance on driverless car technology to privacy issues with Internet-"connected" cars. In the summer of 2015, hackers found a weakness in a Jeep's computer system and remotely commandeered the vehicle. They also unwittingly discovered a flaw in the laws assigning liability of defective vehicles. Reliance on the traditional defective automobile laws in cyberattacks would render car manufacturers completely liable, despite the interference of an independent third party. Nobody wins when car manufacturers are burdened with this kind of unbridled liability. In response, manufacturers could choose not to equip their vehicles with sophisticated computers that are prone to hacking events. Those same components, however, play essential roles in car safety and emissions reduction efforts—which both the government and consumers demand.

Smart car technology will continue to evolve—as should our laws. This Article analyzes the current liability scheme for defective automobiles and discusses why laws predicated on physical access and control should not be applicable to remote hacking events. This Article then identifies and analyzes other liability schemes and proposed legislation relating to smart cars. After

† Pace University School of Law, Class of 2017. Managing Editor of 2016–2017 PACE ENVIRONMENTAL LAW REVIEW. My most profound thanks to Professor Leslie Garfield Tenzer for her help, support, and insight with writing and publishing this Article.

concluding that none of the current or proposed laws assigning liability for smart car cyberattacks are sufficient, the Article offers a new, flexible scheme for this novel, ever-evolving technology.

The proposed scheme takes into account, inter alia, public safety, consumer demand, environmental concerns, and blameworthiness. Based on Judge Learned Hand's calculus of negligence, manufacturers would be required to meet a certain standard when producing cars that are susceptible to cyberattacks. Because of the nature of digital technology, this standard cannot be fixed—if it were, it would quickly become obsolete. Manufacturers would only be liable when they fail to meet the appropriate standard. To be sure, given the awareness of potential hacking events and the gravity of harm that can result from a cyberattack, manufacturers have a significant burden in satisfying this standard of care; however, they would not be strictly liable for hacking events. Once this minimum standard is set, much like what happened with the emissions regulations of the 1970s, consumer demand and the market will drive manufacturers to surpass the minimum requirements, ultimately making our roads, and cars, safer.

TABLE OF CONTENTS

I. SMARTER LAWS ARE NEEDED FOR SMART CARS

Advances in technology have transformed cars from large, cumbersome, gas-guzzling Tin Lizzies into extraordinarily efficient, incredibly safe, and remarkably reliable automobiles. Essential to this evolution are onboard computers and Internet-connected features that have become commonplace in modern vehicles. These computers provide myriad benefits ranging from cleaner emissions to safer automobiles, which consumers and the government alike not only encourage, but also demand. However, the current legal framework concerning the potential liability associated with onboard computers will have a chilling effect on future technological advancements in the automotive industry.

Although computers may be able to determine the ideal ratio of gas and oxygen for an engine instantaneously, they are not impenetrable. In fact, all computers—personal computers and high-level government computers alike—are susceptible to cyberattacks.[1] With the advent of devices and features in automobiles that connect to the Internet, computers employed by the automotive industry pose a similar security risk. The threat of hackers breaching an automobile's computer system is real and looming; in fact, onboard computers have already been breached.[2] As cars continue to become more connected to the Internet, the opportunity for remote hackers to commit an array of crimes ranging from theft to murder increases dramatically.

This Article posits that the civil and criminal liability of smart car[3] hacking events should not be placed on the car manufacturer alone. Instead, the primary focus should be on the third-party wrongdoer. The emphasis placed on the wrongdoer is particularly noteworthy in this context because cyberattacks against cars pose a unique problem that easily tempts lawmakers, legal practitioners, and judges to conflate the liability of elusive, malicious hackers with the car manufacturer. Since hackers are difficult to find and bring into a courtroom, often the initial reaction by injured parties is to look to the manufacturer for redress. That blame, however, is misplaced. For example, if someone broke into your car, stole it, and were never apprehended, there would be no case for suing the car's manufacturer because someone was able to break the car's lock. Similarly, suing the manufacturer of your home computer because someone hacked into it would likely prove unsuccessful. However, when the two notions—computers and cars—are combined, there is

1. Damian Paletta, *CIA Director's Private Email Account Was Hacked, News Report Says*, WALL ST. J. (Oct. 19, 2015, 12:57 PM), http://www.wsj.com/articles/cia-directors-private-email-account-was-hacked-news-report-says-1445273851; Emily Glazer & Danny Yadron, *J.P. Morgan Says About 76 Million Households Affected by Cyber Breach*, WALL ST. J. (Oct. 2, 2014, 9:32 PM), http://www.wsj.com/articles/j-p-morgan-says-about-76-million-households-affected-by-cyber-breach-1412283372.

2. Samuel Gibbs, *Jeep Owners Urged to Update Their Cars After Hackers Take Remote Control*, GUARDIAN, (July 21, 2015), http://www.theguardian.com/technology/2015/jul/21/jeep-owners-urged-update-car-software-hackers-remote-control.

3. Throughout this Article, I will use the term "smart car" to refer to automobiles equipped with sophisticated onboard computer systems that have wireless connections, including, but not limited to, Bluetooth, Wi-Fi, cellular, and radio services. The use of the term "smart car" is not in reference to the brand Smart, nor is it limited to electric or hybrid automobiles.

a strong impulse to blame the manufacturer. Unchecked, that urge is likely to lead to burdensome liability that will ultimately have a chilling effect on the implementation and development of future smart car technology.

The argument will be presented in three Parts. Part II provides a brief history of the intersection between computers and cars, outlines the benefits of this technology, and describes some of the liability issues created by smart cars. Part III assesses the current and proposed remedies for cyberattacks on smart cars and explains how they unsuccessfully allocate liability for remote hacking events. Finally, in Part IV, an alternative option is proposed that, while holding the automotive industry to a reasonable standard of care when designing smart cars, encourages manufacturers to continue developing automotive technology that relies on connected computers.

II. BACKGROUND: THE HISTORY OF COMPUTERS AND CARS

The convergence of computers and automobiles first occurred in 1966 to reduce automobile emissions in California.[4] This initial regulation set the stage for Congress to adopt the Clean Air Act of 1970 (CAA), which established national emissions standards for new cars.[5] In response to the newly enacted legislation regulating automobile emissions, car manufacturers sought a way to reduce pollutants in the exhaust that flowed from the catalytic converter into the atmosphere.[6] Central to this development were microprocessor computers known as "engine control units" (ECUs).[7] ECUs perform a variety of functions including gathering data, monitoring system outputs, and regulating vehicle systems, all initially aimed at lowering emissions and ensuring optimal gas mileage.[8] Some scholars have estimated that the modern luxury automobile may have as many as seventy ECUs.[9]

It did not take long for the automotive industry to apply the recently developed emissions monitoring technology to aspects of automobiles not directly related to emissions reduction. Now, manufacturers use sophisticated computer systems for everything from monitoring tire pressure to intelligent "park assist" programs that allow cars to parallel park automatically.[10] Unsurprisingly, computer systems have become an integral part of the modern automobile, playing a vital role in environmental protection efforts while also serving unrelated functional and auxiliary purposes.

---

4. EPA, EPA400-F-92-014, MILESTONES IN AUTO EMISSIONS CONTROL (1994), https://nepis.epa.gov/Exe/ZyPURL.cgi?Dockey=P10001KM.txt.

5. *Id.*

6. Karim Nice, *How Car Computers Work*, HOWSTUFFWORKS (Apr. 11, 2001), http://auto.howstuffworks.com/under-the-hood/trends-innovations/car-computer1.htm.

7. *Id.*

8. *Id.*

9. Stephen Checkoway et al., *Comprehensive Experimental Analyses of Automotive Attack Surfaces*, *in* PROCEEDINGS OF THE 20TH USENIX SECURITY SYMPOSIUM 77, 77–78 (2011), http://static.usenix.org/event/sec11/tech/full_papers/sec11_proceedings.pdf.

10. *Computer Chips Inside the Car: The ECU Computer (Engine Control Unit)*, CHIPSETC., http://www.chipsetc.com/computer-chips-inside-the-car.html (last visited Feb. 22, 2017).

Despite the necessity of equipping cars with computers, these onboard computers pose a serious cybersecurity risk. The "Internet of things"—a phenomenon that continues to permeate every aspect of human life and to which the automotive industry is not immune—is largely the source of this risk.[11] Before the implementation of additional features that required "connectivity" (i.e., a connection to the Internet, the cloud, or even a cellular phone connection), a car's ECU was relatively safe.[12] Before the rise of connected cars, the only way to manipulate a car's computer was to have physical access to the car's computer system.[13] In other words, to access an automobile's ECU, you would need to connect the car's computer to an external computer physically. The need for physical access to the car significantly constrained the opportunity for wrongdoers to tamper with a car's computer system. Under these circumstances, a hacking event was no more likely than someone cutting a car's brake lines.[14]

Thanks to the connectedness of modern cars, physical presence is no longer required to access a car's computer system.[15] Many modern cars employ the use of dozens of ECUs, all of which converge on the Controller Area Network (CAN).[16] The CAN allows cars to offer critical safety features (e.g., automatic crash notification systems) alongside secondary, extraneous features (e.g., curated streaming music).[17] The CAN provides a significant point of access for potential hackers, as the CAN provides a pathway to each of the separate computerized systems within the car.[18] The nature of the CAN's central "network" compounded with various features like onboard Wi-Fi, navigation, and cellular phone services provide hackers with an opportunity to interfere with every component of the car that "communicates" with the CAN.[19] To be sure, remote hackers who successfully breach a car's CAN have access to virtually every component of the car, whether the individual component targeted by hackers is connected or not.[20] This combination of a centralized network and features that connect cars to the Internet has made cars "increasingly indistinguishable from Internet-connected computers in terms of vulnerability to outside intrusion and control."[21]

---

11. Daniel Burrus, *The Internet of Things Is Far Bigger than Anyone Realizes*, WIRED (Oct. 30, 2014), http://www.wired.com/insights/2014/11/the-Internet-of-things-bigger/ (describing the "Internet of things" as "revolv[ing] around increased machine-to-machine communication; it's built on cloud computing and networks of data-gathering sensors; it's mobile, virtual, and instantaneous connection; and they say it's going to make everything in our lives from streetlights to seaports "smart.").

12. Checkoway et al., *supra* note 9, at 90.

13. *Id.* at 77; *see also, e.g.*, Jeremy Laukkonen, *GM's OnStar Service: How Does It Work?*, LIFEWIRE, https://www.lifewire.com/gms-onstar-service-534811 (last updated Apr. 1, 2016) (explaining OnStar provides remote access to car's computer system).

14. Checkoway et al., *supra* note 9, at 77.

15. *Id.*

16. *Id.* at 2; *see also Controller Area Network (CAN) Overview*, NAT'L INSTRUMENTS (Aug. 1, 2014), http://www.ni.com/white-paper/2732/en/ (describing CAN as a "system for networking intelligent devices" originally conceived for automobiles).

17. Checkoway et al., *supra* note 9, at 78.

18. *Id.*

19. *Id.* at 77–78.

20. *Id.* at 78.

21. John Markoff, *Researchers Show How a Car's Electronics Can Be Taken Over Remotely*, N.Y.

As cars have become increasingly connected to the Internet, they have become increasingly susceptible to cyberattacks.[22] In 2011, researchers from the University of California, San Diego, and the University of Washington studied the vulnerability of onboard computer systems.[23] Their discoveries were startling: through their experiments, the researchers were able to successfully hack a parked car remotely.[24] By dialing the telephone number associated with the car, they were able to send files over the cellular connection.[25] This allowed the "hackers" (potential thieves) to use GPS to locate the car, turn on the lights of the car (to indicate to the would-be thief which car was the target), unlock, and start the car (allowing the would-be thief to drive away unnoticed).[26] These findings would make any car owner question the security of his or her vehicle. After all, now car owners are not only vulnerable to traditional "smash and bash" thieves, but also susceptible to remotely based thieves who can operate while drawing little public attention to their criminal activity.

Even more startling is the development that came in July 2015 when researchers successfully hacked into a Jeep Cherokee and took control of its critical components: the engine, brakes, transmission, and steering mechanisms.[27] One of the researchers bluntly stated, "We shut down [the] engine—a big rig was honking . . . because of something we did on our couch. This is what everyone who thinks about car security has worried about for years. This is a reality."[28]

Cars being remotely hacked and commandeered is no longer a distant future concern. Jon Allen, a web security expert, told the New York Times that "[c]ustomers are demanding new capabilities and more technology, so the risk is only going to increase for vehicles."[29] While the problem is only in its nascent stages, it must be dealt with quickly.[30] Gartner, a market research firm, estimates that by the year 2020 there will be a quarter of a billion "connected" cars on the roads.[31] Put bluntly, there will be a quarter of a billion sitting ducks on highways.

To date, there has been only one reported malicious cyberattack on a

---

TIMES (Mar. 9, 2011), http://www.nytimes.com/2011/03/10/business/10hack.html.

22. Checkoway et al., *supra* note 9.

23. *Id.*; *Car-Hacking*, PBS, http://www.pbslearningmedia.org/resource/nvsn6.sci.tech.carhack/car-hacking/ (last visited Feb. 22, 2017).

24. Checkoway et al., *supra* note 9, at 91.

25. *Id.*

26. *Id.*

27. Aaron M. Kessler, *The Web-Connected Car Is Cool, Until Hackers Cut Your Brakes*, N.Y. TIMES (July 23, 2015), http://www.nytimes.com/2015/07/24/business/the-web-connected-car-is-cool-until-hackers-cut-your-brakes.html?_r=0.

28. 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-highway/.

29. Kessler, *supra* note 27.

30. *Id.*

31. Press Release, Gartner, Gartner Says by 2020, a Quarter Billion Connected Vehicles Will Enable New In-Vehicle Services and Automated Driving Capabilities (Jan. 26, 2015), http://www.gartner.com/newsroom/id/2970017.

vehicle.[32] A disgruntled former employee of a car dealership in Austin, Texas, hacked into over one hundred cars the dealership had sold.[33] The cars were equipped with a vehicle immobilization feature the dealership could activate if the owner became past due in his or her car payments.[34] The former employee hacked into the system and "bricked" approximately one hundred vehicles.[35] While this isolated incident was relatively victimless and easily remedied, it serves as a harbinger for how easily hackers can remotely access and control automobiles.

In 2015, a putative class-action lawsuit was filed in California against General Motors and Toyota.[36] The suit alleged that the defendants' automobiles had computer technology that was vulnerable to malicious hacking.[37] The plaintiffs premised their claim on the notion that hacking is so prevalent that it would only be a matter of time before a car *is* hacked, and despite the defendants' knowledge of the security vulnerabilities, they continued to market their vehicles as safe.[38] Ultimately, the court held that the plaintiffs "fail[ed] to allege that any harm is 'certainly impending' because while it is possible that a potential hacker would in fact attempt to gain control of a vehicle, 'allegations of *possible* future injury are not sufficient.'"[39] Without having suffered actual harm, the plaintiffs lacked standing, and the court dismissed the claim with leave to amend.[40]

This places legislatures in a unique position to be ahead of the rapidly evolving landscape of digital technology. Accordingly, the enacted laws should be proactive in the fight against malicious hackers by immediately implementing appropriate measures to deter such activity, correctly assign liability, and boost the public's perception of the safety of smart cars. While courts must wait for actual damages before they can hear cases, the same is not true for legislatures. They can, and should, proactively enact laws—especially in situations where there is a potential for severe harm and liability is not easily determined.

32. 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/.

33. *Id.*

34. *Id.*

35. *Id.*

36. Cahen v. Toyota Motor Corp., 147 F. Supp. 3d 955 (N.D. Cal. 2015) (dismissed with leave to amend).

37. *Id.* at 958.

38. *Id.* at 959.

39. *Id.* at 967 (quoting U.S. Hotel & Resort Mgmt., Inc. v. Onity, Inc., No. CIV 13-1499(SRN/FLN), 2014 WL 3748639, at *2 (D. Minn. July 30, 2014)).

40. *Id.*

III. EXISTING LIABILITY SCHEMES AND PROPOSED LEGISLATION FAIL TO PROPERLY ASSIGN LIABILITY AND RISK SLOWING THE CONTINUED DEVELOPMENT OF SMART CAR TECHNOLOGY

Should a malicious hacking event occur today, victims would be forced to rely on inadequate traditional legal remedies to resolve a new, technology-based claim. Common law negligence principles would shift liability to the car manufacturer because, due to the recent highly publicized controlled hacking events, car manufacturers should foresee cyberattacks against their connected cars. Along with that foresight comes the duty to guard against the known harm. Similarly, legislation specifically aimed at automobile safety was enacted at a time when cyberthreats were not on the minds of lawmakers. Consequently, current legislation falls short of protecting the public and incorrectly assigns liability in cyberattacks against cars. Finally, proposed legislation and other suggested regulatory schemes centered on smart car technology are too cumbersome to prove effective and ignore the repercussions of reserving the question of who should be liable. None of the current theories of recovery, nor any of the proposed strategies, strike the necessary balance of consumer safety with the continued development of smart car technology.

A. Full Reliance on Traditional Common Law Principles Is Inadequate Because Hacking Events Are Foreseeable

Under a common law action in negligence, the plaintiff is required to show, inter alia, that the defendant was the proximate cause of her damages.[41] The foundation for liability in a negligence action is the sine qua non test: but for one's action (or inaction) the harm suffered would not have resulted; therefore, the wrongdoer is liable for the resulting injury.[42]

Courts have attempted to delineate just how closely the cause must be related to the resulting harm. Often, when an intervening and superseding event breaks the chain of causation, the original actor will be absolved of liability.[43] The intervening cause doctrine operates to relieve a negligent actor from liability "when a new, independent and unforeseen cause intervenes to produce a result that the negligent actor could not have reasonably foreseen."[44] It is likely that a cybercriminal hacking into a car's onboard computer and commandeering its controls would be deemed an intervening cause.

However, the law also demands that these intervening causes be "unforeseen" to exculpate tortfeasors. In *Potter v. Ford Motor Co.*, the court found that the foreseeability requirement is "not so strict as to require the tortfeasor to foresee the exact manner in which the injury takes place, provided

41. *See, e.g.*, Marshall v. Nugent, 222 F.2d 604, 610 (1st Cir. 1955) (explaining requirement of proximate causation).

42. *See, e.g.*, Hayes v. Mich. Cent. R.R. Co., 111 U.S. 228, 241 (1884) (explaining requirement of cause in fact).

43. *See, e.g.*, Potter v. Ford Motor Co., 213 S.W.3d 264, 273 (Tenn. Ct. App. 2006) (explaining intervening cause doctrine).

44. *Id.* (quoting Rains v. Bend of the River, 124 S.W.3d 580, 593 (Tenn. Ct. App. 2003)).

it is determined that the tortfeasor could foresee, or through the exercise of reasonable diligence should have foreseen, the general manner in which the injury or loss occurred."[45] In the context of cyberattacks, the recent, highly publicized controlled hacking events combined with Chrysler's 1.4-million-car recall in response to the controlled July 2015 Jeep hack, would effectively put all car manufacturers on notice as to the risks associated with equipping their cars with connected onboard computers.[46] This knowledge would not only make hacking a foreseeable event but also render car manufacturers liable for damages stemming from a hacking event.

Considering that an impenetrable computer has yet to be developed, it would prove far too large a burden to hold car manufacturers liable for any cyberattack against their cars. This open-ended liability could drive manufacturers to retreat to their pre-Internet days, requiring a physical connection to a car to access its onboard computer systems, which neither manufacturers nor consumers desire. Should the law demand that manufacturers wholly shoulder the liability of cyberattacks on automobiles, the "best-case" result would be a drastic increase in the price of new cars to hedge against the potential exposure to hacking-based liability claims.

While strict adherence to traditional common law negligence principles is inadequate, one of the benefits of common law is that it is not only practical but also malleable, and allows the law to adapt to circumstances, perhaps unexpected by legislators. Judge Learned Hand, in *United States v. Carroll Towing Co.*, recognized this very issue and promulgated the calculus to determine the standard of care required in varying circumstances.[47] Applying Judge Hand's calculus to smart car technology would properly delineate the outer limits of manufacturer liability. If a plaintiff could show that the manufacturer's burden in creating a relatively safeguarded computer system was less than the cost of injury and possibility of occurrence, she would have a successful cause of action.[48] Granted, Hand's methodology is not black and white—there are varying shades of gray. Judge Hand's formula, however, will set a reasonably high standard of care for any car manufacturer because: (1) it is likely that a car might be hacked (a likelihood that grows by the day), and (2) the resulting harm could be nothing short of catastrophic. Accordingly, car manufacturers would not have carte blanche to ignore computer security safety completely. Rather, they would have to make a significant showing that they took adequate steps to protect against remote cyberattacks.

45. *Id.* (quoting McClenahan v. Cooley, 806 S.W.2d 767, 775 (Tenn. 1991)).

46. *Fiat Chrysler Recalls 1.4 Million Cars After Jeep Hack*, BBC NEWS (July 24, 2015), http://www.bbc.com/news/technology-33650491.

47. United States v. Carroll Towing Co., 159 F.2d 169 (2d Cir. 1947).

48. *Id.* (applying Hand's formula).

B. Traditional Principles of Strict Liability Based on Defective Components Is an Inadequate Remedy Because Manufacturers Do Not Have Physical Control of Computers like Other Automobile Components

With the proliferation of automobiles in America, there has been a rise in accidents and automobile-related injuries and deaths. In 1965, automobile accidents became the leading cause of death for Americans under the age of forty-four.[49] This spike in automobile-related deaths led to the passing of the National Traffic and Motor Vehicle Safety Act of 1966 (NTMVSA), which included provisions to protect the public from the "unreasonable risk of accidents occurring as a result of the design, construction, or operation of automobiles."[50] The initial formulation mandated lifesaving shoulder-lap belts, collapsible steering columns, strengthened door latches, shatterproof windshields, and protective dashboards.[51] Subsequent amendments to the NTMVSA have included provisions for airbags and fuel economy requirements.[52]

With the advent of federal safety regulations came increased legal action against automobile manufacturers. The standards outlined in the Federal Motor Vehicle Safety Standards (FMVSS), set forth by the National Highway Traffic Safety Administration (NHTSA), specify the necessary requirements for new cars relating to everything from crash avoidance mechanisms to post-crash standards.[53] If a manufacturer is found to have failed to meet any of the requisite safety standards, the automobile may be considered defective and subject to strict liability[54] for the designing, assembling, or handling of the vehicle if the components in question were unreasonably dangerous.[55] This "defective component" products liability claim is the primary cause of action against automobile manufacturers.[56]

Some practitioners have already distinguished cyberattacks from injuries originally contemplated by the NTMVSA. The NTMVSA guards against "naturally occurring" harm—not *all* harm.[57] Accordingly, because hacking is never "naturally occurring," it should not be subject to the NTMVSA liability scheme. This "naturally occurring" distinction is important because even strict

---

49. Anthony D. Branch, *National Traffic and Motor Vehicle Safety Act*, ENCYCLOPEDIA BRITANNICA, (last updated Nov. 20, 2013), http://www.britannica.com/topic/National-Traffic-and-Motor-Vehicle-Safety-Act.

50. *Id.*

51. *Id.*

52. *Id.*

53. 49 C.F.R §§ 571.101–.500 (2015).

54. Strict liability in the traditional sense—if a plaintiff bringing a claim for a defective part shows it failed to meet safety standards, the manufacturer will be liable, regardless of culpability.

55. *See* 63A AM. JUR. 2D *Products Liability* § 982 (last updated Feb. 2017) (discussing product liability as it relates to motor vehicle safety standards).

56. *See* Adams v. Toyota Motor Corp., No. CIV 10-2802(ADM/JSM), 2015 WL 3742898 (D. Minn. June 15, 2015) (finding against Toyota for $11.44 million in a comparative negligence case); *In re* Gen. Motors LLC Ignition Switch Litig., 154 F. Supp. 3d 30 (S.D.N.Y. 2015).

57. Todd Bernhoff, *Automakers Should Not Be Held Strictly Liable for V2V Hacks*, LAW360 (Oct. 29, 2014, 6:04 PM), https://www.law360.com/articles/591695/automakers-should-not-be-held-strictly-liable-for-v2v-hacks.

liability is not equivalent to absolute liability.[58] For example, a criminal may throw a rock off of a bridge, thereby shattering the car's windshield and injuring the driver.[59] Automobile manufacturers are aware that, under normal circumstances, rocks may often come in contact with the windshield, and they are required to ensure their windshields are safe when such contact occurs. Because a rock coming into contact with a windshield—whether thrown by a criminal or, say, falling off of a dump truck—is "naturally occurring," manufacturers are required to guard against it.[60] However, manufacturers are not obligated to equip their cars with windshields that would protect drivers from boulders falling onto the highway because boulders are not "naturally occurring" on the roadways—even if a manufacturer would foresee such an occurrence. Unlike rocks on the roads, there is no "naturally occurring" hacking event.[61] An onboard computer that malfunctions due to fluctuations in temperature or rough roads (i.e., normal driving conditions) would appropriately fall within the bounds of the NTMVSA's strict liability scheme, but the same should not hold true for malicious hacking events. Since there is no such thing as a computer that cannot be hacked and remote hackers are not "naturally occurring" under normal driving circumstances, traditional liability under the NTMVSA strict-liability scheme or a common law action in negligence is improper.[62]

The larger problem with relying on the NTMVSA is the fact that the issues presented by cyberattacks are entirely different from the problems Congress was confronted with in the 1960s. The air quality and safety concerns that were the focus of 1960s automotive legislation related to fixed, physical, and "unconnected" components of the car.[63] When it comes to lowering emissions and ensuring the physical car *itself* was safe, strict liability was—and still is—the prudent path for the legislature to attain its goals.[64] Strict liability was proper because the primary elements of the problem were housed entirely within the car and not subject to the whims of remote actors.[65] Moreover, the manufacturer completely controlled the assembly process.[66]

Building on the example of car windshields, one of the first requirements under the NTMVSA scheme was that windshields be made of tempered glass.[67] These windshields were made and installed at the manufacturing plant. A car's manufacturer, while accounting for typical driving situations, was involved in every step of the design, development, and manufacturing process.

58. *Id.*
59. *Id.*
60. *Id.*
61. *Id.*
62. *Id.*
63. See Arthur C. Stern, *History of Air Pollution Legislation in the United States*, 32 J. AIR POLLUTION CONTROL ASS'N 44, 51–55 (1982) (providing overview of legislation regulating automotive air pollution in the 1960s).
64. *See, e.g.*, Suvada v. White Motor Co., 210 N.E.2d 182, 185–88 (Ill. 1965) (extending concept of strict liability to automobile manufacturers).
65. *Id.*
66. *Id.*
67. 49 C.F.R. § 571.205 (2015).

If a manufacturer failed to account for normal driving situations, or if its products did not, in fact, meet its claims in the real world, the manufacturer could be held strictly liable for its shortcomings.[68] Most importantly, if an owner changed the windshield after she purchased the vehicle, the manufacturer would not be liable for the post-sale modification.[69] A cyberattack is analogous to a post-sale modification in the code of a car's computer. After all, the car's code, when leaving the plant, is operating safely and properly. Once the car has left the plant and the manufacturer no longer has physical control of the car, a third party manipulates the underlying code and causes the car to function differently.

For static, physical components, strict liability schemes are highly effective. More importantly, it makes sense because the automaker has complete control of the process. With control comes liability, and that is precisely where smart cars diverge from the cars of the 1960s. Surely manufacturers would be liable for bad code in vehicles they sold, but requiring them to protect against post-sale modifications of the car's code asks too much of manufacturers.

Car manufacturers are aware of the vulnerability of "connected" computers and the risks posed by potential cyberattacks. Under the NTMVSA scheme, manufacturers could be subject to seemingly endless litigation. This potential gold mine of products liability litigation paired with deep pockets of automotive manufacturers could make for protracted and expensive legal battles. Even worse, it may significantly stunt or even retract some smart car technology because of the automotive industry's understandable wariness to open itself up to unlimited liability. Manufacturers are currently exposed to this sort of litigation; however, because a malicious cyberattack has yet to occur, the threat of litigation has not yet been fully realized. This is not an area where legislatures should "wait and see" what happens when hacking cases eventually reach the courts; the threat is real, and a significant amount of time and resources can be saved by proactively addressing liability.

C. The Proposed SPY Car Act Is Inadequate Because It Fails to Address the Question of Liability for Cyberattacks

While the 114th Congress was locked in a stalemate, two members of the Senate, Senator Markey and Senator Blumenthal, have recognized the potential legal issues that smart cars pose. After Senator Markey learned of the controlled 2015 Jeep hacking event, he solicited information from twenty car manufacturers regarding their current computer security measures.[70] According to Senator Markey, of the twenty automakers that were polled, sixteen automakers confirmed that virtually every vehicle they sell has some sort of wireless connection, including Bluetooth, Wi-Fi, cellular service, and

68. *See, e.g.*, *Suvada*, 210 N.E.2d at 188 (holding that automobile manufactures can be held strictly liable for their defective products).

69. *See id.* (explaining that one of the elements of strict liability is "that the condition existed at the time it left the manufacturer's control").

70. Greenberg, *supra* note 28.

radio.[71] Senator Markey also found that of the sixteen automakers using wireless technology, only seven companies worked with independent security firms to ensure digital security, and only two companies actively monitored their CANs for malicious code.[72]

These revelations led Senators Markey and Blumenthal to propose the Security and Privacy in Your Car Act of 2015 (SPY Car Act).[73] The proposed SPY Car Act has three major components: (1) cybersecurity standards; (2) privacy standards; and (3) a cyber dashboard.[74] The cybersecurity standards require the NHTSA to cooperate with the Federal Trade Commission (FTC) in developing minimum standards to prevent hacking.[75] Specifically, the bill would require reasonable measures to protect against hacking attacks, to safely store any data collected by the automobile's computer system, and to detect and mitigate attacks in real time.[76] The privacy section of the proposed legislation, again implicating the FTC, would develop privacy standards related to data collection requiring transparency in data collection, an option to opt out of data collection (when feasible), and a prohibition of marketing collected data unless the owner clearly opts in.[77] Finally, the cyber dashboard provision provides for a consumer-friendly window sticker on new cars indicating how well the car protects against cyberattacks and personal data breaches.[78] Given the current political climate, it is unlikely that the SPY Car Act will pass, but "it is an indication of concern about these issues by the bill's sponsors, well-known consumer advocates. Absent other proposals, the bill may become the focus of attention as news stories highlight automotive security and privacy issues," and accordingly, will likely be used to frame future legislation.[79]

The SPY Car Act has been criticized for giving car manufacturers a short time frame to comply with its requirements.[80] The current version of the SPY Car Act gives car manufacturers two years to comply with the cybersecurity standards set forth within it.[81] The worry is that two years is an inadequate amount of time for automakers to comply fully with the promulgated standards.[82] In an effort to adhere to the short time frame, the possibility of quick, superficial "band-aid" fixes may become more appealing to automakers

71. *Id.*
72. *Id.*
73. Security and Privacy in Your Car Act of 2015, S. 1806, 114th Cong. (2015).
74. *Id.*
75. Press Release, Sen. Ed Markey, Sens. Markey, Blumenthal Introduce Legislation to Protect Drivers from Auto Security, Privacy Risks with Standards & "Cyber Dashboard" Rating System (July 21, 2015), http://www.markey.senate.gov/news/press-releases/sens-markey-blumenthal-introduce-legislation-to-protect-drivers-from-auto-security-privacy-risks-with-standards-and-cyber-dashboard-rating-system.
76. *Id.*
77. *Id.*
78. *Id.*
79. *Vehicle Cybersecurity and Privacy Legislation Introduced*, HOGAN LOVELLS (July 29, 2015), http://ehoganlovells.com/cv/6de804a4d5df693a2a5fa80b08ab2cd43f13b22b. As of April 17, 2016, the SPY Car Act has been read twice and is in committee.
80. Gene Carter, *Ramifications of the SPY Car Act*, EMBEDDED COMPUTING DESIGN (July 29, 2015), http://embedded-computing.com/guest-blogs/ramifications-of-the-spy-car-act/#.
81. Security and Privacy in Your Car Act of 2015, S. 1806, 114th Cong. § 2(a)(2) (2015).
82. Carter, *supra* note 80.

to avoid regulatory fines than actually identifying and holistically fixing the underlying security glitches.[83]

While the SPY Car Act acknowledges and properly addresses some of the problems presented by onboard computers and attempts to allay the impending threats, it reserves the question of liability and thus falls short.[84] While a focus on informing consumers and protecting their privacy rights is important, the Act misses the mark when it comes to specifying who is to be responsible if a car (meeting SPY Car Act requirements) is hacked into and damage results.[85] Presumably, the fallback positions previously discussed will establish the standard for liability.[86] Moreover, the SPY Car Act requires coordination with the FTC, which poses a significant hurdle when it comes to efficiency, as discussed in the next Section.[87]

D. Similar Regulatory Approaches Are Inadequate Because of the Magnitude of the Automotive Industry

Senators Markey and Blumenthal are not the only government officials thinking about the flaws in smart car cybersecurity. Regardless of who is trying to assess and remedy the problem, the common thread among all suggested solutions is the size and complexity of the problem. Modern cars have tens of millions of lines of code,[88] which, according to the head of vehicle safety research at the NHTSA, Nat Beuse, is "too gargantuan a task for regulators," especially when considering some "automakers . . . use two or three different versions of code in the same model year."[89] Mr. Beuse suggests that the automotive industry follow a similar protocol to that which the Federal Aviation Administration (FAA) employs with the development of airplane computer systems.[90] Under an FAA-esque regime, regulations would identify "very, very critical systems that affect safety" (e.g., steering, throttle, brakes, and battery systems), and then have a government representative (likely from the NHTSA) directly oversee the software design process for the critical systems.[91] Adding to the challenge is the fact that automakers are "about 20 years behind software companies in understanding how to prevent cyberattacks."[92]

However, there is a foreboding scaling issue with the FAA regime. It begins with the expansive number of automobile makes and models as

83. *Id.*
84. Security and Privacy in Your Car Act of 2015, S. 1806.
85. *Id.*
86. *Id.*
87. *Id.*
88. Checkoway et al., *supra* note 9, at 78.
89. David Gelles et al., *Complex Car Software Becomes the Weak Spot Under the Hood*, N.Y. TIMES (Sept. 26, 2015), http://www.nytimes.com/2015/09/27/business/complex-car-software-becomes-the-weak-spot-under-the-hood.html?_r=0.
90. *Id.*
91. *Id.*
92. Cheryl Dancey Balough & Richard C. Balough, *Cyberterrorism on Wheels: Are Today's Cars Vulnerable to Attack?*, ABA (Nov. 2013), http://www.americanbar.org/publications/blt/2013/11/02_balough.html.

compared to airplanes.[93] An even larger problem is the human resources demanded by such a scheme. The software engineers who would oversee the implementation of complex computer systems in cars are highly specialized, making them scarce and expensive to employ. The FAA has much better access to these specialized resources than does the NHTSA.[94] The FAA has over ten thousand staff members for every one hundred fatalities on commercial aircraft at its disposal.[95] In contrast, the NHTSA has 0.3 staff members for every one hundred fatalities in automobile crashes.[96] The scale and specialization needed to oversee the implementation of onboard computers in all vehicles puts government regulatory agencies in a poor position to ensure adequate smart car cybersecurity.

While synergy between government departments is critical in regulatory schemes that implicate several different sectors (e.g., smart car technology that touches on the development of technology, consumer safety, environmental protection, and national security), it poses a formidable hurdle. The automotive market is oxymoronically expansive yet nuanced. Establishing a system that is adequately resourced, large enough, and sufficiently agile to meet the ever-changing landscape of computer technology as it relates to automobiles is a tall, if not insurmountable, order.

It would be wasteful to put an under-resourced government organization in charge of regulating a highly specialized and dynamic aspect of the automotive industry. Government bureaucracy inhibits a nimble response to what would be rapidly developing changes in the landscape of smart car hacking. Government regulatory action is likely to be dilatory, and perhaps second rate, unless the government can attract and retain top cybersecurity talent. However, acquiring that talent comes at a high price. With limited government resources, relying solely on regulatory schemes is imprudent.

IV. SUGGESTED ALTERNATIVE SCHEMES

Cyberattacks are a threat unlike anything the automotive industry has ever confronted, and thus, require a novel strategy. The first distinguishing characteristic of cyberattacks is the dynamic world of technology itself. Assume, for a moment, that a car manufacturer did the impossible and created an impenetrable onboard computer system. The manufacturer then proceeded to install it in all of its new cars. Because of the fast-moving and ever-shifting nature of technology, hackers would likely quickly develop a method to hack successfully into that car's "impenetrable" computer, immediately rendering the automaker strictly liable (under traditional schemes) for any security breaches. It would be an understatement to classify that kind of liability as an

93. *Compare Total Number of Existing and New Car Models Offered in the U.S. Market from 2000 to 2016*, STATISTA, http://www.statista.com/statistics/200092/total-number-of-car-models-on-the-us-market-since-1990/ (last visited Feb. 22, 2017), *with Modern Commercial Aircraft of the World*, AIRLINES INFORM, http://www.airlines-inform.com/commercial-aircraft/ (last visited Feb. 22, 2017).

94. Gelles et al., *supra* note 89.

95. *Id.*

96. *Id.*

undue burden.

The fact of the matter is that cybersecurity, especially as it relates to onboard computer systems in automobiles, is a new and developing technology that requires an equally forward-thinking legal standard and regulatory scheme to ensure consumer safety and cultivation of technology.

A. Third-Party Wrongdoers Should Be Held Liable for Their Unlawful Actions

Congress enacted the NTMVSA with one aim: to hold automobile manufacturers responsible for their wanton or even merely reckless actions.[97] After all, laws are supposed to hold the person responsible for an act (or a failure to act) liable.[98] Accordingly, the correct party to be held liable for the damages stemming from a cyberattack on an automobile is the hacker herself. To be sure, the "mere act of hacking into the control system of someone else's car can be analogized to stealing a car, and ultimately carjacking, should the car then take off with an unsuspecting passenger."[99] Much like a boulder falling or a party changing a car's windshield after purchasing a car, nobody would seek to hold car manufacturers liable for such actions.

There is, however, resistance to relying solely on the criminal party for liability in automotive cyberattacks. First, the surreptitious nature of hacking often makes it extremely difficult to identify, let alone prosecute, the perpetrators. Remote hacking, especially, is unique in that it can be done from anywhere in the world—provided there is an Internet connection. Indeed, parties outside of the United States could hack into cars that are driving on American roads and harm American citizens. The hurdles are obvious in these circumstances: (1) finding the wrongdoer, no matter where in the world she may be; (2) extraditing her to the United States; and (3) successfully prosecuting her in American courts. This is no small task for the Department of Justice or the American legal system as a whole.

Additionally, hackers often use proxy Internet protocol (IP) addresses, fully cloaking their actual location. Astute hackers that utilize proxy IP addresses are virtually impossible to find, exacerbating the already difficult problem of apprehending and prosecuting hackers.[100] Proxy IP addresses are just one of several options in a hacker's playbook used to mask the hacker's identity, making it easier to elude law enforcement officials.[101]

Finally, hackers likely have less money to satisfy a lawsuit than automobile manufacturers. Surely, a company worth $20 billion is a preferred

97. Branch, *supra* note 49.

98. *President Johnson Signs the National Traffic and Motor Vehicle Safety Act*, HISTORY, http://www.history.com/this-day-in-history/president-johnson-signs-the-national-traffic-and-motor-vehicle-safety-act (last visited Feb. 22, 2017) (describing the automotive safety crisis as one that automakers either could not or were not able to fix and the impetus behind the law).

99. Frank Douma & Sarah Aue Palodichuk, *Criminal Liability Issues Created by Autonomous Vehicles*, 52 SANTA CLARA L. REV. 1157, 1165 (2012).

100. Alan Woodward, *Viewpoint: How Hackers Are Caught Out by Law Enforcers*, BBC NEWS (Mar. 12, 2012), http://www.bbc.com/news/technology-17302656.

101. *Id.*

defendant compared to a computer hacker (whose assets may be ill-gotten and would likely be frozen upon arrest).[102] However, just because hackers are difficult to locate and not easily prosecuted does not mean that we should turn a blind eye to the actual criminal enterprises and make the automotive industry shoulder the burden of hackers' actions just because they are available and have relatively full coffers. Liability premised on convenience, though appealing, is misplaced and would have a chilling effect on important technology.

Cross-department synergy might prove cumbersome and inefficient for regulatory purposes,[103] but it is an indispensable tool when it comes to identifying and locating rogue hackers. Hacking has become more prevalent across nearly every sector.[104] In fact, it is hard to go a day without hearing something related to hacking on the news, or even learning that you, yourself, have been hacked—after all, nearly half of American adults have been victims of hacking.[105]

Furthermore, hacking is not likely to be a short-lived phenomenon. Former Defense Secretary Leon Panetta has warned of a possible "cyber-Pearl Harbor" attack.[106] With the growing risk of hacking incidents, now is not the time for the automotive industry (or any other industry for that matter) to shy away from attempting to identify and prosecute criminal hackers. It is narrow minded to allow the automotive industry to shoulder the liability for smart car hacking simply because it is difficult to track, apprehend, and prosecute the hackers. Instead, it provides the perfect opportunity for several different sectors to come together and make significant progress on a difficult problem that must be addressed.

Since every industry that connects to the Internet is at risk, the more prudent solution would be a cross-sector effort to develop methods to identify the criminals perpetrating the cybercrimes. This would require bringing in the experts in each sector to help ensure the security of connected computers and pooling resources to defend against and investigate cyberthreats.[107]

---

102. Zachary Shahan, *Tesla Motors Worth $20 Billion (About 42% GM's Worth), & the One Reason Why*, CLEAN TECHNICA (Aug. 29, 2013), http://cleantechnica.com/2013/08/29/tesla-motors-worth-20-billion-about-42-gms-worth-the-one-reason-why/.

103. *See supra* Section III.D.

104. Orr Hirschauge & Nicole Hong, *Accused Mastermind of J.P. Morgan Hack a Product of Israel's Internet Underbelly*, WALL ST. J. (Nov. 21, 2015, 5:33 AM), https://www.wsj.com/articles/accused-mastermind-of-j-p-morgan-hack-a-product-of-israels-internet-underbelly-1448101982 (discussing hacking in the financial sector); Chris Isidore, *Target: Hacking Hit Up to 110 Million Customers*, CNN (Jan. 11, 2014, 6:20 PM), http://money.cnn.com/2014/01/10/news/companies/target-hacking/ (discussing hacking in the retail sector); Bruce Schneier, *We Still Don't Know Who Hacked Sony*, ATLANTIC (Jan. 5, 2015), http://www.theatlantic.com/international/archive/2015/01/we-still-dont-know-who-hacked-sony-north-korea/384198/ (discussing hacking in the entertainment sector); Steve Weisman, *Another Health Care Data Breach*, USA TODAY (July 25, 2015, 9:02 AM), http://www.usatoday.com/story/money/personalfinance/2015/07/24/steve-weisman-health-care-data-breach/30593661/ (discussing hacking in the healthcare sector).

105. Jose Pagliery, *Half of American Adults Hacked This Year*, CNN: TECH (May 28, 2014, 9:25 AM), http://money.cnn.com/2014/05/28/technology/security/hack-data-breach/.

106. Christopher Versace, *2014's Hacking Pain Is Cyber Security's Gain*, FORBES (Jan. 22, 2014, 9:42 AM), http://www.forbes.com/sites/chrisversace/2014/01/22/2014s-hacking-pain-is-cyber-securitys-gain-for-symc-feye-pawn-keyw-csco-cuda-ftnt-impv/.

107. *See infra* Section IV.D (discussing possible public-private partnerships).

Addressing the daunting issues of finding remote hackers and bringing them to justice is decidedly beyond the scope of this Article. However, it is clear that there is much opportunity for cross-sector collaboration to shine the light more brightly on hackers. A challenge such as hacker anonymity is no reason to place the blame on a non-blameworthy party—as convenient as it may be.

B. Proper Legislation Should Provide an Exception to Encourage the Further Development of Smart Car Technology

While myopic consumers might not be so easily persuaded, there is much more at stake when assigning cyberattack liability than driver and passenger safety alone. Even in light of the potentially catastrophic consequences of smart car hacking, the technological advances found in smart car technology are penetrating, and they play a fundamental role in technology development as a whole. While at first glance many features may seem superficial and superfluous, several technologies employed by smart cars are aimed at increasing automobile safety, and play a significant role in environmental protections.[108] These technologies should be encouraged and incentivized, not obstructed and hindered by potentially unlimited liability.

This is not the first time that Congress has been faced with the issue of new technology precipitating unexpected potential for harm. A similar issue arose in 1996 in connection with the Communications Decency Act (CDA), in which Congress favored the development of technology over the possibility of some personal harm.[109] The CDA was a part of the larger Telecommunications Act of 1996, which updated its predecessor (the Communications Law of 1934), and included modern provisions for the Internet.[110] The CDA provides a helpful template in updating and adapting legislation for new, developing technologies.

One of the CDA's aims was to regulate obscenity available to children on the Internet.[111] However, Congress provided a unique carve-out for Internet service providers (ISPs).[112] In an effort to preserve the "vibrant and competitive free market" of ideas on the Internet, Congress chose not to hold ISPs liable for actions third parties took on their websites.[113] Courts have broadly construed this exception. For instance, in *Doe II v. MySpace Inc.*, a California court held that the social website MySpace was immune from tort claims brought by young women who were sexually assaulted by men they met on MySpace.[114]

108. *See, e.g.*, Josh Clark, *Will Your Next Car Wake You Up When You Fall Asleep at the Wheel?*, HOWSTUFFWORKS (May 27, 2008), http://auto.howstuffworks.com/car-driving-safety/safety-regulatory-devices/car-wake-you-up.htm (describing how "drowsy driver" alerts work).

109. 47 U.S.C. § 151 (2012).

110. *Id.*

111. *Id.* § 230.

112. *Id.* § 230(c)(1).

113. *Id.* § 230(b)(2), (c)(1).

114. Doe II v. MySpace Inc., 96 Cal. Rptr. 3d 148, 149–50 (Cal. Ct. App. 2009).

The CDA attempted to balance parents' ability to restrict their "children's access to objectionable or inappropriate online material" with the desire to "promote the continued development of the Internet and other interactive computer services and other interactive media."[115] The CDA effectively draws a line between ISPs and the actual publisher or speaker of the information provided.[116] This broad exception effectively "immunizes providers of interactive computer services from liability for the dissemination of third-party content."[117]

The congressional finding that in some situations the development and promotion of technology for the public at large supplants interests of wronged individuals is telling; moreover, it is applicable to smart car technology. A similar exception should apply to smart car technology because the government, itself, has recognized the benefits of smart car technology.

In fact, the federal government has already challenged automakers to develop smart technologies that could potentially help drivers avoid accidents.[118] One such technology the federal government is exploring and encouraging is vehicle-to-vehicle communication systems (V2V). Essentially, V2V is a "crash avoidance technology, which relies on communication of information between nearby vehicles to potentially warn drivers about dangerous situations that could lead to a crash."[119]

It would be contradictory to acclaim (let alone incentivize) the benefits of smart cars, and then place weighty liability on those attempting to advance that very technology. If the federal government recognizes the profound impact that smart car technology has on vehicle emissions and the safety of our roads, it should also recognize the hypocrisy of saddling car manufacturers with complete liability related to those systems. Some fields require well-thought-out exceptions to cultivate and develop technology that in the long run provides a significant benefit to society. Smart car technology is such an area.

C. Car Manufacturers Should Be Held to a Reasonable Standard of Care

Automobile manufacturers should not be free of all liability when it comes to their utilization of smart car technology. Since these manufacturers are best positioned to guard against hacking events, they owe a duty to their customers and the public to ensure their cars are reasonably secure. A more prudent approach than a strict liability scheme or obsolescent regulatory requirements would be a flexible and evolving standard similar to Judge Hand's standard of care formula.[120] The potential harm posed by a cyberattack

115. 47 U.S.C. § 230(b)(1), (4).

116. *Id.* § 230(c)(1).

117. Claudia G. Catalano, Annotation, *Validity, Construction, and Application of Immunity Provisions of Communications Decency Act, 47 U.S.C.A. § 230*, 52 A.L.R. Fed. 2d 37 (2011).

118. Nedra Pickler, *"Smart Car" Tech Encouraged in U.S.*, ABC NEWS (July 19, 2000), http://abcnews.go.com/Technology/story?id=119657.

119. U.S. DEP'T OF TRANSP., NAT'L HIGHWAY TRAFFIC SAFETY ADMIN., VEHICLE TO VEHICLE COMMUNICATION TECHNOLOGY (Oct. 14, 2014), http://www.safercar.gov/staticfiles/safercar/v2v/V2V_Fact_Sheet_101414_v2a.pdf.

120. United States v. Carroll Towing Co., 159 F.2d 169 (2d Cir. 1947).

coupled with the probability of a hacking incident actually occurring would place a demanding duty on car manufacturers to equip their cars with secure connected onboard computer systems. Accordingly, any manufacturer found to have failed to meet that standard of care would be liable for resulting damages.

The downside of Judge Hand's formula, however, is that it is vague and subjective in nature. There is not a bright line delineating adequate digital security. While this is unsatisfactory for consumers, attorneys, and judges, standards governing evolving technologies must be elastic and provide for flexibility because of the dynamic nature of the underlying technology. Technology advances more rapidly than the law does, and it would be shortsighted for legislatures to tie themselves to bright-line rules that could quickly become obsolete as a result of subsequent technological developments.

A variable standard, although somewhat bothersome, is key because liability, related to ever-changing technology, should be determined in real time by the fact finder at trial. Plaintiffs' lawyers will have little problem identifying all of the measures that manufacturers could or should have taken to prevent a cyberattack against their cars. Likewise, car manufacturers could demonstrate how seriously they approached the security of their onboard computers (e.g., utilizing independent red teams to assess the security of their computers or air gapping critical components).[121] The fact finder would then determine if the manufacturer sufficiently guarded against cyberattacks and then allocate liability accordingly.

While the proposed standard is a moving target, it is not nebulous. Several factors would help manufacturers gauge their risk of liability long before they are ever brought into a courtroom. The Environmental Protection Agency (EPA), in its regulation of stationary source polluters, is faced with a similar difficulty of aligning effective regulation with changing technologies. To ensure that stationary source polluters utilize the newest pollution-lowering technologies, the EPA has developed a scheme under which "new source" polluters must obtain a permit before building a plant that will increase emissions by a significant amount.[122] One of the primary considerations in issuing a permit is whether the proposed plant utilizes the best available control technologies (BACTs).[123] Under the guidance of the EPA, a "BACT is determined by state permitting agencies on a case-by-case basis, taking into account a proposed control measure's energy, environmental, and economic impacts."[124] This holistic, fact-intensive permitting process could serve as a model for the NHTSA in its efforts to regulate onboard computers.

---

121. Kim Zetter, *Hacker Lexicon: What Is an Air Gap*, WIRED (Dec. 8, 2014, 10:15 AM), https://www.wired.com/2014/12/hacker-lexicon-air-gap/ (stating that air gapping is not infallible).

122. *Basic Information*, EPA, https://www3.epa.gov/ttncatc1/rblc/htm/welcome.html (last visited Feb. 22, 2017).

123. LARRY PARKER & JAMES E. MCCARTHY, CONG. RESEARCH SERV., R41505, EPA'S BACT GUIDANCE FOR GREENHOUSE GASES FROM STATIONARY SOURCES 2 (Nov. 22, 2010), http://nationalaglawcenter.org/wp-content/uploads/assets/crs/R41505.pdf.

124. *Id.*

While the NHTSA is poorly positioned to regulate smart car technology single handedly,[125] it can play an important role in defining whether a manufacturer has met the requisite standard of care. A regulatory scheme that mirrors the EPA's New Source Review process is impracticable in the context of automobiles—there are simply too many manufacturers and models of cars that would require individual permitting to implement the *same* scheme as the EPA. There is ample room, however, for the NHTSA to set general standards that can help establish a minimum standard that manufacturers must meet to avoid liability. Once the NHTSA establishes general "best available technologies" to prevent cyberattacks against automobiles, compliance with those standards can serve as evidence that the manufacturer met its standard of care in developing its smart car technology. Conversely, failure to comply with the NHTSA's standards can provide evidence that the manufacturer failed to fulfill its duty, rendering it liable. To be sure, failure to satisfy the NHTSA's requirements would also render the manufacturer strictly liable under the traditional NTMVSA scheme.

These standards set by the NHTSA, however, must only serve as the floor for liability. Flexibility—particularly in an upward direction—is necessary for the law to keep pace with evolving technology. Any standard set by the NHTSA will quickly become obsolete, and accordingly, the NHTSA's standards alone should not be used to allocate liability. The NHTSA's "best technologies" guidance serves merely as a guidepost to the finder of fact at trial. This ensures that pressure remains on manufacturers to continue to develop newer and safer technologies in addition to remaining vigilant in protecting and updating systems already on the market as technology advances.

Another guidepost that may be used at trial to show whether a manufacturer has met its required standard of care is participation in public-private partnerships aimed at advancing automotive cybersecurity as a whole. For example, in July 2015, the automotive industry created the Automotive Information Sharing and Analysis Center (Auto-ISAC).[126] Through its network of manufacturers, cybersecurity experts, and academics, the Auto-ISAC develops "best practices" that emphasize risk management for car manufacturers.[127] The proposed best practices encompass a wide range of elements, including but not limited to: (1) risk assessment and management; (2) security by design; (3) threat detection and prevention; (4) incident response and recovery; and (5) collaboration with appropriate third parties (e.g., the NHTSA and the Department of Homeland Security).[128]

In recognition of the continually evolving technology involved with smart car technology, the Auto-ISAC's best practices "provide forward-looking guidance without being prescriptive or restrictive," and they are "committed to updating [them] over time as the motor vehicle ecosystem's risk landscape

125. *See supra* Section III.B.
126. AUTO-ISAC, https://www.automotiveisac.com (last visited Feb. 22, 2017).
127. *Id.*
128. *Id.*

evolves."[129] Courts would also consider participation in such a partnership when determining whether it should hold a manufacturer liable for a cyberattack against one of its cars. Compare a manufacturer that decides not to join the Auto-ISAC with one that not only joined, but also adopted several of the center's proposed best practices. That sort of evidence would clearly help a court determine if a manufacturer failed to satisfy its duty of care.

However, much like compliance with NHTSA guidelines, membership in such an organization is not dispositive—it is considered as part of the total mix of evidence relating to the manufacturer's actions. When the stakes are so high, more must be demanded of manufactures than simply meeting minimum requirements and then coasting. The variable standard proposed keeps that upward pressure on manufacturers to remain vigilant and innovate in order to continue to ensure their cars are safe from remote cyberattacks.

Not only would this proposed scheme properly assign liability, as technology continues to evolve, it will also inherently ratchet up the manufacturer's duty to safeguard against cyberattacks. Once the minimum duty is established, market demand will take over and drive developments in smart car security further. This is not a new concept. The emissions standards established in the CAA increased market demand for cleaner cars, causing industry benchmarks to surpass government-imposed standards.[130] When emissions standards were first introduced, they were initially resisted by automakers.[131] However, once the regulations were in place, they eventually transformed the automotive industry because the market demanded cars that were more efficient than what the government mandated.[132]

Today, car buyers demand efficient and "clean" vehicles.[133] While their motivations are varied (although the demand is largely attributed to economic incentives[134]), consumers are now (at least until the recent drop in gas prices) demanding "clean" cars. The automotive industry has responded by not only producing cleaner cars but also by focusing its marketing and advertising campaigns on the emissions and efficiency of cleaner cars.[135] This trend has penetrated the entire automotive market to the extent that Tesla has even gone so far as to build an entire brand on premium electric cars alone.[136]

---

129. *Automotive Cybersecurity Best Practices*, AUTO-ISAC (July 21, 2016), https://www.automotiveisac.com/best-practices/.

130. *Auto Research and Regulation*, CQ RESEARCHER (Feb. 23, 1979), http://library.cqpress.com/CQResearcher/document.php?id=cqresrre1979022300.

131. *Id.*

132. *Id.*

133. Brad Tuttle, *All of a Sudden, There Aren't Enough Electric Cars to Keep Up with Demand*, TIME (June 18, 2013), http://business.time.com/2013/06/18/all-of-a-sudden-there-arent-enough-electric-cars-to-keep-up-with-demand/.

134. Press Release, Ass'n for Convenience & Fuel Retailing, Consumers Like "Green" Car Options—As Long As Green Means Money (Nov. 15, 2013), http://www.nacsonline.com/news/press_releases/2013/pages/pr111413.aspx; *see also* Eric Morath, *Gas-Price Drop Takes Americans' Interest in Fuel Economy Down with It*, WALL ST. J. (Sept. 4, 2015, 2:26 PM), http://blogs.wsj.com/economics/2015/09/04/gas-price-drop-takes-americans-interest-in-fuel-economy-down-with-it/ (discussing American interest in fuel economy).

135. *Honda Hybrid Car 2000*, BERKLEY ELEC. ENG'G & COMPUT. SCI., http://www.eecs.berkeley.edu/~hu/car_00.html (last visited Feb. 22, 2017) (depicting an advertisement for a hybrid car).

136. TESLA, https://www.tesla.com (last visited Feb. 22, 2017).

The relationship is even more pronounced with hacking safety than it is with emissions standards. While car buyers are keen on finding a car that gets good gas mileage to save money at the gas pump (or to do their part in reducing greenhouse gasses), the thought of having their car hacked and commandeered is far more worrisome. The government does not need to enact stringent, strict liability legislation mandating cybersecurity for cars, because the market will inherently demand it. Once there is a demand for digitally secure smart cars, manufacturers will *have* to figure out a way to supply it, or risk losing their market share. This demand is amplified by the fact that the "Internet of things" will only continue to grow, effectively requiring every automaker to address the demand for secure computer systems in its cars.

Additionally, automakers are much better positioned to adapt to the ever-changing nature of technology. Private companies are better situated to attract top cybersecurity talent, which allows automakers to employ better software engineers and to find and hire independent agencies to assess and develop strategies to develop smart car cybersecurity. That is not to say there is no room for government involvement. Several proposed sections of the SPY Car Act are complementary to the suggested liability scheme. Consumer identity protection measures in addition to clear and full disclosures about a car's features can and should be mandated by law. But, extending common-sense mandates like those to liability because of third-party interference should not go unquestioned. Liability for cyberattacks on cars should be imposed only once it is shown that an automaker fell below a reasonable standard of care.

Once this minimum standard has been established, the market will complete the task. Companies that fail to satisfy the standard of care test will not only be held liable for their shortcomings, but they will also likely be driven out of business, losing their market share to manufacturers that focus on cybersecurity. There is not a car manufacturer today that would revert to a 1950s-esque car if environmental and safety standards were abrogated. It is simply not commercially feasible. The best way to ensure that both our cars and roads are safer is to allow market forces to take effect and catalyze cybersecurity competition within the automotive industry.

V. CONCLUSION

The automotive industry has come a long way since the heavy, gas-guzzling, inefficient, emission-spewing machines that America fell in love with in the early 1960s. Our laws regulating automobiles should reflect those same developments. Strict liability regulations in the 1960s were necessary to make the roads safer and the air cleaner. They were also effective—so effective that the automotive market now demands (and manufacturers hang their hat on) automobiles that *exceed* government-imposed safety and environmental standards. The cybersecurity concerns that plague automobiles today cannot be remedied by the same mechanisms used in the 1960s because it is an entirely different animal—an animal that was ironically brought to life by the first regulations that increased automobile safety and efficiency. An animal that has less to do with the physical components of cars, and more to do

with protecting cars from a completely external, invisible, and remote threat. Because car hacking is such a different beast than previous risks encountered in the automotive industry, it requires an entirely different strategy. The most prudent path is one that, through common law principles of negligent standard of care, fixes the floor of liability for manufacturers, while simultaneously driving a competitive market to transcend that ground level, all while pursuing the actual wrongdoers and holding *them* liable so as to ensure the continued development of technology.