THE EMERGING INTERSECTION OF PRODUCTS LIABILITY, CYBERSECURITY, AND AUTONOMOUS VEHICLES

RYAN J. DUPLECHIN[*]

INTRODUCTION 804
I. SELF-DRIVING CARS: A FAR-FLUNG NOTION TURNED REALITY 808
A. Evolution of the Self-Driving Car 808
B. Classifying Modern Autonomous Vehicles 809
II. CONNECTED TECHNOLOGY 811
A. Recent Hacks 813
B. Open Doors to Hacking Connected Cars 814
C. Federal Regulation for Automotive Cybersecurity 816
III. PRODUCTS LIABILITY AND SECURITY BREACHES IN AUTONOMOUS VEHICLES 817
A. The Drawbridge to Products Liability: Software in Traditional "Products" 818
B. Identifying the Defect 820
1. Warning the Defect 820
2. Design or Manufacturing Defect 821
3. The Unidentifiable Defect 823
C. Testing the Defect 826
IV. CYBERSECURITY AND NEGLIGENCE: THREE MAIN BARRIERS 830
V. SCALING THE FINAL BARRIER 833
A. Duty 833
B. Foreseeability and Third-Party Criminal Acts 834
VI. TOWARDS AN AUTOMOTIVE CYBERSECURITY STANDARD OF CARE 837
A. Expert in the Field 838
B. Determining Due Care in Automotive Cybersecurity Cases 839
1. Limited Autonomous Vehicles and Reasonable Care 841
2. Full Self-Driving Vehicles Require a Heightened Standard of Care 843

---

* Mass Torts Section of Beasley, Allen, Crow, Methvin, Portis & Miles, P.C. The author expresses his sincere gratitude to Professor Layne S. Keele for his numerous recommendations and insightful feedback.

CONCLUSION 845

INTRODUCTION

In 2015, Andy Greenberg was driving his 2014 Jeep Cherokee outside St. Louis, Missouri.[1] Suddenly, the car's radio began blaring rap music at full volume.[2] Andy attempted to turn the volume down, but the music kept blaring.[3] Then, the windshield wipers started swinging, and water began spraying all over the windshield.[4] Next, two men appeared on the Jeep's in-dash screen.[5] Finally, with the Jeep traveling seventy miles per hour, the transmission cut and the accelerator quit working.[6] Andy desperately pumped the gas pedal, but the Jeep came to a dead halt.[7] As Andy's Jeep sat incapacitated, cars piled up, honking in frustration.[8] As the two men on Andy's in-dash screen faded from view, an ominous warning came through the speakers: "You're doomed!"[9]

Fortunately, the two men on Andy's in-dash screen were white-hat hackers[10] named Charlie Miller and Chris Valasek, who were conducting a research experiment with their friend Andy Greenberg.[11] Significantly, Miller and Valasek were not out on a test track with white lab coats, remote controls, or crash dummies. The hack occurred on a real highway, disrupting actual traffic flow until Andy's Jeep sat paralyzed in an adjacent ditch.[12] Where were the hackers? Miller and Valasek did all this from their couch at home—using a laptop and smartphone.[13] The hackers explained that, with wireless

---

1. Andy Greenberg, *Hackers Remotely Kill A Jeep on the Highway—With Me In It*, WIRED (July 21, 2015), https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/.
2. *Id.*
3. *Id.*
4. *Id.*
5. *Id.*
6. *Id.*
7. *Id.*
8. *Id.*
9. *Id.*
10. White-hat hackers are professional hackers that are hired to uncover and disclose vulnerable security holes. *See* Elizabeth A. Rowe, *Rats, Traps, and Trade Secrets*, 57 B.C. L. REV. 381, 406–07 (2016). In contrast, "Black Hats access systems to commit a crime, and Grey Hats are between the two, sometimes crossing the line in violating the law, but choosing to report security vulnerabilities." *Id.* at 407.
11. *See* Greenberg, *supra* note 1.
12. *See id.* (displaying a picture of Andy's Jeep in the ditch).
13. *Id.*

control, they could have gained access from anywhere in the country.[14] Following the hack, Miller and Valasek could track and identify "as many as 471,000 vehicles with vulnerable [connectivity] systems on the road."[15] As Andy Greenberg explained, the results show how hackers could target connected vehicles and gain wireless access, solely through the Internet, to "any of thousands of vehicles."[16]

One can only imagine the chaos, ranging from major traffic jams to hundreds of lives lost, had this been a sophisticated attack by hackers motivated to control and crash thousands of connected vehicles, instead of a research experiment. Whether hackers are capable of infiltrating autonomous vehicles is now an outdated question. Miller and Valasek's 2015 hack proves that wireless attacks on connected vehicles are both achievable and real.[17] Now, the questions turn to the range, scope, and severity of hacker capabilities to control autonomous vehicles. Wireless attacks, as opposed to wired-in or proximity attacks, present magnified challenges and dangers.

---

14. *Id.*

15. *Id.*

16. *Id.* At a national conference, in 2013, Toyota, Ford, and other automakers downplayed Miller and Valasek's prior hacks, because they were wired-in attacks and physically present. *Id.* Toyota even boasted that "its systems were 'robust and secure' against wireless attacks." *Id.* Presumably, after the 2015 wireless attack, the hackers now have the automakers' attention.

17. More recently, at a national conference in August 2016, Miller and Valasek "demonstrated that the 2014 Jeep Cherokee they hacked a year ago remains hackable [sic] and to new, potentially more dangerous levels" because they could now steer and accelerate at higher speeds. Carolyn B. Theis, *Mad Hacks: Legal Ramifications of Continued Car Hacking*, LAW360 (Aug. 12, 2016), https://www.law360.com/articles/827379/mad-hacks-legal-ramifications-of-continued-car-hacking.

Threats of cyberattack on autonomous vehicles have captured the attention of law professors,[18] law students,[19] consumers,[20] Congress,[21] and the FBI.[22] Some commentators suggest the risk of cyberattacks on autonomous vehicles "is likely overblown in terms of its severity."[23] Others, however, suggest that "autonomous vehicles being hijacked . . . could lead to terror on the scale of the September 11

---

18. *See, e.g.*, MICHAEL L. RUSTAD, GLOBAL INTERNET LAW 499 (2d ed. 2016) (Professor Rustad explains, "one can easily imagine the danger presented by a vehicle with and [sic] engine and breaking system that can be controlled by a remote hacker in order to deliberately create an accident."); Matthew T. Wansley, *Regulation of Emerging Risks*, 69 VAND. L. REV. 401, 467 (2016) (recognizing legal scholars contemplate "that autonomous vehicles will be hacked by criminals or terrorists"); Neal Katyal, *Disruptive Technologies and the Law*, 102 GEO. L.J. 1685, 1689 (2014) ("Self-driving vehicles would also open the country up to a number of new security concerns. Hackers could tamper with autonomous driving software; terrorists could infiltrate the central transportation system.").

19. *See* Julie Goodrich, *Driving Miss Daisy: An Autonomous Chauffeur System*, 51 HOUS. L. REV. 265, 282–83 (2013) ("Breaching an autonomous vehicle's entry points may do more than just release data; a hacker could potentially take control of the vehicle and cause it to drive to a certain location.").

20. According to University of Michigan researchers, most Americans are concerned that autonomous vehicles "might be hacked to cause crashes, disable the vehicle in some way or even be used as weapons by terrorists. . ." *Americans Worry About Vehicle Hacking*, AUTOMOTIVE FLEET (Feb. 24, 2017), http://www.automotive-fleet.com/channel/safety-accident-management/news/story/2017/02/americans-worry-about-vehicle-hacking.aspx.

21. In September 2017, the House of Representative passed the Safety Ensuring Lives Future Development and Research in Vehicle Evolution ("SELF DRIVE") Act. *See* H.R. 3388: SELF DRIVE Act, 115TH CONGRESS (Apr. 2, 2018), https://www.congress.gov/bill/115th-congress/house-bill/3388/actions. One of the major components of the SELF DRIVE Act mandates protections against cyberattacks on self-driving cars. *See* Ariel Darvish, *The SELF DRIVE Act: Cybersecurity and Cars on Autopilot*, FORDHAM JOURNAL OF CORPORATE & FINANCIAL LAW BLOG (Jan. 15, 2018), https://news.law.fordham.edu/jcfl/2018/01/15/the-self-drive-act-cybersecurity-and-cars-on-autopilot/.

22. The Federal Bureau of Investigation (FBI) has expressed grave concern over autonomous vehicle technology hacks and terrorism. *See* Mark Harris, *FBI Warns Driverless Cars Could Be Used as 'Lethal Weapons'*, THE GUARDIAN (July 16, 2014), http:// www.theguardian.com/technology/2014/jul/16/google-fbi-driverless-cars-leathal-weapons-autonomous; *see also* Aristedes Mahairas, *Manufacturers Must Focus On Securing the Internet of Things*, LAW360 (Sep. 25, 2017), https://www.law360.com/articles/966917/manufacturers-must-focus-on-securing-the-internet-of-things (FBI special agent-in-charge of the FBI's New York Special Operations/Cyber Division stating, "it is only a matter of time before there will be a victim who is able to prove that a cybersecurity event, like the breach of an unsecured IoT device, was the proximate cause of an actual, immediate and foreseeable injury").

23. Adam Thierer & Ryan Hagemann, *Removing Roadblocks to Intelligent Vehicles and Driverless Cars*, 5 WAKE FOREST J.L. & POL'Y 339, 375 (2015). However, Thierer and Hagemann also note, "unanticipated challenges could develop that require flexible, creative solutions. . . ." *Id.* at 389.

attacks."[24] Notwithstanding the speculation of future attacks, researchers have proven that current connected vehicles are vulnerable to cyberattack.[25] Despite this reality, cybersecurity concerns have taken a backseat as manufacturers race to be the first to market a mass-produced autonomous vehicle.

This Article seeks to bring these issues to the forefront by scrutinizing emerging automotive cybersecurity shortcomings through the centuries-old lens of common law tort. Parts I and II offer a brief description of autonomous vehicle technology and modern cybersecurity issues, respectively. Parts III through VI address two areas in which challenges are likely to arise in cases involving the hacking of autonomous vehicles. Part III tackles the challenge of identifying and proving defects in intangible software connected with autonomous vehicles. And Part IV addresses the application of traditional defense doctrines in the specific context of tort-related cybersecurity recovery. Parts V and VI offer a novel approach for courts to analyze a modernized automotive cybersecurity duty and standard of care under a traditional common law framework.

This Article urges courts to draw a distinction between limited autonomous vehicles, which allow for manual driving, and fully self-driving vehicles, which are designed to operate without manual driving components. Under a traditional calculus of risk analysis, cars without human override capabilities create greater risks in the event of foreseeable cyberattacks. The greater risks, coupled with the passenger's complete trust in the vehicle and lack of control, necessitates the highest standard of care known as "utmost care" when manufacturers implement cybersecurity components in self-driving cars.

---

24. William J. Kohler & Alex Colbert-Taylor, *Current Law and Potential Legal Issues Pertaining to Automated, Autonomous and Connected Vehicles*, 31 SANTA CLARA HIGH TECH. L.J. 99, 133 (2015); *see also* Susan W. Brenner & Leo L. Clarke, *Civilians in Cyberwarfare: Conscripts*, 43 VAND. J. TRANSNAT'L L. 1011, 1029–30 (2010) (noting that cyberattacks are likely to target private companies operating national infrastructure).

25. *See* Daniel A. Crane et. al., *A Survey of Legal Issues Arising from the Deployment of Autonomous and Connected Vehicles*, 23 MICH. TELECOMM. & TECH. L. REV. 191, 240 (2017) ("The July 2015 hacking of a Jeep Cherokee by researchers Charlie Miller and Chris Valasek brought wide attention to vehicular cybersecurity threats.").

I. SELF-DRIVING CARS: A FAR-FLUNG NOTION TURNED REALITY

A. Evolution of the Self-Driving Car

Many consider self-driving cars a concept of the future, however, the automated vehicle concept dates back to the late 1930s.[26] During the 1939 World's Fair, General Motors (GM) introduced the "far-flung notion" of cars driving themselves on the open highway.[27] Later, in the 1950s, GM and Radio Corporation of America developed a model highway system allowing electronic steering while maintaining proper distance between vehicles.[28] Although this model never matured, it served as the "foundation of future developments in autonomous navigation."[29]

In 1989, researchers at Carnegie Mellon University began developing sensor-based automated vehicle technology that could navigate the roadway.[30] However, significant technological advances were not made until the twenty-first century.[31] In 2007, the Defense Advances Research Projects Agency (DARPA)[32] sponsored an "Urban Challenge" challenging experts to construct autonomous vehicles that could maneuver through urban areas, including the ability to switch lanes, avoid particular obstacles, and even obey traffic laws.[33] Carnegie Mellon University, along with GM, entered and won the competition.[34] The "Urban Challenge" prompted Google to recruit these experts, along with the second-place team from Stanford University, to develop their own driverless system.[35]

While Google has continuously been at the forefront of autonomous vehicle technology,[36] it is now one of many competitors.[37] Others joining the race to the market, to name a few, include: Tesla,

---

26. Jeremy Levy, *No Need to Reinvent the Wheel: Why Existing Liability Law Does Not Need to Be Preemptively Altered to Cope with the Debut of the Driverless Car*, 9 J. BUS. ENTREPRENEURSHIP & L. 355, 361 (2016).

27. Thierer & Hagemann, *supra* note 23, at 341.

28. *Id.* at 341–42.

29. *Id.* at 342.

30. *Id.*

31. Levy, *supra* note 26, at 361.

32. Prior to 2007, DARPA worked with several technology experts to develop driverless technology for military use to reduce the number of physical soldiers exposed to dangerous war zones. *Id.*

33. *Id.*

34. *Id.*

35. *Id.* at 361–62.

36. *Id.* at 363–64.

37. *Id.*

Volvo, BMW, GM, and Ford.[38] Fully self-driving vehicles, requiring no human input besides destination, are not yet available in any consumer market, but it is estimated that consumers will be navigating self-driving cars as early as 2020.[39]

B. Classifying Modern Autonomous Vehicles

The National Highway Traffic Safety Administration (NHTSA) offers well-defined levels of autonomous capabilities. The NHTSA identifies a five-level classification structure for all driver-assistance technologies.[40] These levels of automation include:

- Level 0 (No-Automation): "The driver is in complete and sole control of the primary vehicle controls . . . at all times."[41]
- Level 1 (Function-Specific Automation): Includes vehicles that contain "one or more specific control functions."[42] For instance, Level 1 relates to assisted braking "to enable the driver to regain control of the vehicle or stop faster than possible by acting alone."[43]
- Level 2 (Combined Function Automation): "[A]utomation of at least two primary control functions designed to work in unison to relieve the driver of control of those

---

38. *Id.* at 364; *Ford Invests $1B Toward 2021 Autonomous Vehicle*, AUTOMOTIVE FLEET (Feb. 10, 2017), http://www.automotive-fleet.com/channel/safety-accident-management/news/story/2017/02/ford-invests-1b-in-artificial-intelligence-company.aspx.

39. Benjamin I. Schimelman, *How to Train a Criminal: Making Fully Autonomous Vehicles Safe for Humans*, 49 CONN. L. REV. 327, 330 (2016). ("[P]redictions are that such a vehicle will be available . . . by 2025."); Harry Surden & Mary-Anne Williams, *Technological Opacity, Predictability, and Self-Driving Cars*, 38 CARDOZO L. REV. 121, 136–37 (2016) ("Most experts predict the first consumer sale will occur somewhere between 2020 and 2035."); *see also* Jeffrey K. Gurney, *Crashing into the Unknown: An Examination of Crash-Optimization Algorithms Through the Two Lanes of Ethics and Law*, 79 ALB. L. REV. 183, 189 (2016) ("[F]ully autonomous vehicles . . . will be commonplace by 2040.").

40. *U.S. Department of Transportation Releases Policy on Automated Vehicle Development*, NAT'L HIGHWAY TRAFFIC SAFETY ADMIN., (May 30, 2013), https://www.transportation.gov/briefing-room/us-department-transportation-releases-policy-automated-vehicle-development.

41. *Id.*

42. *Id.*; *see also* Schimelman, *supra* note 39, at 333 (introduced six decades ago, power steering is an example of Level 1 technology).

43. NAT'L HIGHWAY TRAFFIC SAFETY ADMIN., *supra* note 40.

functions[,]" such as "adaptive cruise control in combination with lane centering."[44]

- Level 3 (Limited Self-Driving Automation): Includes self-driving vehicles that operate under "full control" but require the driver to take back "occasional control" in certain situations.[45]
- Level 4 (Full Self-Driving Automation): Driverless cars in which the driver "is not expected to be available for control at any time. . ." requiring driver input solely for destination purposes.[46]

In 2013, at the time the NHTSA released the five-level classification, the Agency was unaware of any level four automated vehicle technology in existence.[47] However, Google's new automated vehicle currently falls within the highest level of automation because the Google prototype lacks a steering wheel, a key component for a driver to take back manual control.[48]

Generally, within the NHTSA's definitions, levels three and four are classified as "autonomous vehicles."[49] The term "autonomous" relates to "computer controlled systems that make important choices about *their own actions* with little or no human intervention."[50] Also, for the purposes of this Article, I will refer to "self-driving" or "driverless" to mean complete automation without monitoring by the human driver.[51]

---

44. *Id.*; *see also* Schimelman, *supra* note 39, at 333 (introduced in 1995, electronic stability control (ESC) only activates the brake system to keep the vehicle consistent with the position of the steering wheel). Also, adaptive cruise control, which adjusts the vehicle's speed to maintain safe distance between vehicles, is an example of Level 2 technology. *Id.* at 334.

45. NAT'L HIGHWAY TRAFFIC SAFETY ADMIN., *supra* note 40.

46. *Id.*

47. Kohler & Colbert-Taylor, *supra* note 24, at 103.

48. *See Id.*

49. Levy, *supra* note 26, at 359.

50. Surden & Williams, *supra* note 39, at 131 (emphasis in original).

51. Many states have defined "self-driving" in a similar manner. *See, e.g.*, CAL. VEH. CODE § 38750(a)(l)-(2)(A) (2015); FLA. STAT. § 316.003(90) (2015); MICH. COMP. LAWS § 257.2b (2014); NEV. REV. STAT. §§ 482A.025, 482A.030 (2013); D.C. CODE § 50-2351 (2013). How are both the federal and state governments simultaneously attempting to regulate the same field? Traditionally, the NHTSA sets federal standards for motor vehicles. On the other hand, States regulate human drivers. What happens when the "driver" becomes the motor vehicle itself? This federalism question is an interesting one, for further discussion on this topic, see Sarah E. Light, *Precautionary Federalism and the Sharing Economy*, 66 EMORY L.J. 333, 392 (2017).

Autonomous vehicle technologies can be further categorized as either sensor-based or connectivity-based. Sensor-based technology uses advanced sensors, such as cameras and radars with control units and integrated software to allow vehicles to oversee and react to the particular setting.[52] Ninety-nine percent of modern consumer cars contain some sensor-based features, such as automated air-bag systems and anti-lock brakes or traction controls.[53] Several commentators have detailed the specifics of sensor-based technology, including Google's use of LiDar systems mounted on the roof to detect obstacles,[54] as well as radars and video cameras.[55] This Article concentrates on connectivity-based technology because connected components present the greatest channel for cybersecurity attacks.[56]

II. CONNECTED TECHNOLOGY

The Internet of Things ("IoT") is a recent and unmistakable surge in the technology arena. Generally, IoT is the notion that everyday products will soon be connected to the Internet.[57] Modern and future IoT devices include retail, healthcare, insurance, "smart" homes, and automobiles.[58] These physical products will all contain connected technology. To avoid confusion relating to the newly fashioned and

---

52. Kohler & Colbert-Taylor, *supra* note 24, at 103.

53. Surden & Williams, *supra* note 39, at 134; *see also* HIGHWAY LOSS DATA INST., Bull. Vol. 28, No. 26, *Predicted Availability of Safety Features on Registered Vehicles* 3 (Apr. 2012) (showing, in 2010, anti-lock brakes were standard on 99% of new vehicles).

54. *See, e.g.*, Surden & Williams, *supra* note 39, at 144–45; Kohler & Colbert-Taylor, *supra* note 24, at 103–04; Levy, *supra* note 26, at 362–63 (LiDar uses sound waves ranging up to 100 meters; in contrast, radar detection uses light).

55. *See* Surden & Williams, *supra* note 39, at 145–46; *see also* Levy, *supra* note 26, at 363 ("Google adds traditional radar and sonar systems in their bumpers to detect the speeds of surrounding vehicles and to better react to potential hazards.").

56. Although sensor-based technology is intriguing, the various sensor-based developments are outside the scope of this Article.

57. Scott J. Shackelford et. al., *When Toasters Attack: A Polycentric Approach to Enhancing the "Security of Things*," 2017 U. ILL. L. REV. 415, 418 (2017).

58. *See id.* at 423 (providing a table with "Current Application" and "Future Scope"); *see also* Swaroop Poudel, *Internet of Things: Underlying Technologies, Interoperability, and Threats to Privacy and Security*, 31 BERKELEY TECH. L.J. 997, 1000 (2016) ("IoT could potentially revolutionize diverse fields such as electric grids, water leakage detection, autonomous vehicles, traffic management, forest fire detection, agriculture, manufacturing, inventory management, and supply chain control.").

ill-defined concept of IoT,[59] this Article will refer to "connected" technology as wireless connections between physical products.[60]

Automotive connectivity is moving from local connected components, such as Bluetooth and Internet, to exterior connectivity, such as components that correspond with other vehicles. Connected capabilities in autonomous vehicles are moving towards vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) programs in autonomous vehicles.[61] In February 2014, the NHTSA announced it would be taking steps to implement V2V communication technology for certain vehicles.[62] The NHTSA explained that "[t]his technology would improve safety by allowing vehicles to 'talk' to each other. . . ."[63] In order for autonomous vehicles to operate effectively on open roads, vehicle manufacturers must create uniform and compatible V2V and V2I technologies.[64] V2V systems, currently in the developmental stages, will allow cars to avoid collision with another vehicle equipped with similar V2V technology.[65] It is estimated V2V communication will be "common in ordinary cars" by 2020.[66] Although increased connectivity brings benefits in efficiency, the notion of a uniform wireless transportation infrastructure is a great concern.[67] Before we overhaul wireless transportation infrastructure, cybersecurity risks in today's vehicles deserve greater scrutiny.

---

59. *See* Poudel, *supra* note 58, at 1000 ("There is no universal definition of IoT because it is a nascent industry whose technology and participants are in a state of great flux.").

60. Kohler & Colbert-Taylor, *supra* note 24, at 103 (connected technology refers to wireless connections).

61. *Id.*

62. *U.S. Department of Transportation Announces Decision to Move Forward with Vehicle-to-Vehicle Communication Technology for Light Vehicles*, NAT'L HIGHWAY TRAFFIC SAFETY ADMIN. (Feb. 3, 2014), https://www.nhtsa.gov/press-releases/us-department-transportation-announces-decision-move-forward-vehicle-vehicle.

63. *Id.*

64. Kohler & Colbert-Taylor, *supra* note 24, at 104.

65. Levy, *supra* note 26, at 363.

66. Surden & Williams, *supra* note 39, at 169.

67. *See*, *e.g.*, Kohler & Colbert-Taylor, *supra* note 24, at 133 ("The remote hijacking of autonomous vehicles presents a very serious risk in a world of fully automated motor vehicles."); Dorothy J. Glancy, *Autonomous and Automated and Connected Cars—Oh My! First Generation Autonomous Cars in the Legal Ecosystem*, 16 MINN. J.L. SCI. & TECH. 619, 664 (2015) ("[T]he potential vulnerability of autonomous cars' automated controls to hackers suggests serious risk of criminal mischief.").

A. Recent Hacks

Today, cybercrime is far too prevalent[68] and connected vehicles create new avenues for intellectual criminals with detrimental motives.[69] Researchers have identified various entry points for cyberattacks, shown which vehicles are more vulnerable than others, and also wirelessly controlled connected vehicles themselves.[70]

Back in 2010, Rutgers and the University of Southern California (USC) researchers were able to access a vehicle's electronic control unit (ECU) through the vehicle's wireless tire pressure monitoring systems.[71] At this time, the Rutgers and USC hacks were notable because they were wireless, proving connected vehicles could be attacked "from adjacent vehicles."[72] Thus, in 2010, attacking a close and "adjacent vehicle" set the bar for accessing autonomous vehicles.

Proximity and related access points create important implications for the potential scale of cyberattacks. Types of access include "supply chain and vendor access, remote access, proximity access, or insider access."[73] Rutgers and USC's wireless hack was accomplished by proximity access because the researchers were close in distance to the subject vehicle. In malicious cyberattacks, proximity access would likely only affect one (or few) vehicles in a limited geographic area since hackers would be close to the vehicle. But remote intrusion creates almost limitless bounds for cyber criminals because remote hacks could be carried out from anywhere in the world.[74] In terms of

---

68. Steve Morgan, *Cybercrime Damages Expected to Cost the World $6 Trillion by 2021*, INT'L DATA GRP. (Aug. 22, 2016), http://www.csoonline.com/article/3110467/security/cybercrime-damages-expected-to-cost-the-world-6-trillion-by-2021.html. While cybercrime costs the world economy $3 trillion in 2015, it is estimated it will cost $6 trillion by 2021. *Id.*

69. There are three primary categories of computer criminals: (1) unsophisticated hackers; (2) sophisticated hackers that are merely curious; and (3) hackers that hack for personal gain or malicious purposes. *See* Jay P. Kesan & Carol M. Hayes, *Mitigative Counterstriking: Self-Defense and Deterrence in Cyberspace*, 25 HARV. J.L. & TECH. 429, 440 (2012).

70. *See infra* Miller & Valasek, note 83.

71. Kohler & Colbert-Taylor, *supra* note 24, at 132–33; *see also* Peter Bright, *Cars Hacked Through Wireless Tire Sensors*, ARS TECHNICA (Aug. 10, 2010), http://arstechnica.com/security/news/2010/08/cars-hacked-through-wireless-tyre-sensors.ars.

72. Bright, *supra* note 71.

73. Kesan & Hayes, *supra* note 69, at 442.

74. *See* Scott L. Wenzel, *Not Even Remotely Liable: Smart Car Hacking Liability*, 2017 U. ILL. J.L. TECH. & POL'Y 49, 54 (2017) ("Thanks to the connectedness

autonomous vehicles, remote intrusions create the most significant risk. Until recently, however, only proximity access into autonomous vehicles had been achieved.

In 2015, as mentioned in the Introduction, Miller and Valasek remotely hacked and controlled a connected vehicle from their couch at home.[75] These white-hat hackers effectively launched the most widely publicized hack on a connected vehicle.[76] Miller and Valasek's hack spoke volumes to cybersecurity concerns, prompting Fiat Chrysler to recall 1.4 million vehicles to install additional security software.[77] Miller and Valasek's hacking experiment has apparently caught the attention of similar hackers. In September 2016, in China, white-hat hackers remotely hacked a Tesla Model S from twelve miles away.[78] The Chinese researchers successfully hacked connected components and then controlled essential driving functions.[79] In addition to toying with the windshield wipers, mirrors, seat adjustments, and door locks, the researchers were able to bring the Tesla to a screeching halt on the open road.[80]

B. Open Doors to Hacking Connected Cars

Experimental cyberattacks have exposed the technological vulnerabilities of autonomous vehicles. As research has shown, the two main avenues to hack an autonomous vehicle are through the vehicle's wireless data systems, such as the ECUs, and the smart road infrastructure. Because smart road infrastructure is still in its nascent stages,[81] the security concerns related to this developing

---

of modern cars, physical presence is no longer required to access a car's computer system.").

75. *See* Greenberg, *supra* note 1.

76. *Id.*

77. *Vehicle Safety News from Reuters*, 36 WESTLAW J. AUTOMOTIVE 10, 1 (Nov. 1, 2016).

78. Rob Price, *Car hackers found a way to trigger a Tesla's brakes from miles away*, BUSINESS INSIDER (Sep. 20, 2016), http://www.businessinsider.com/car-hackers-trigger-tesla-model-s-brakes-unlock-doors-adjust-seats-tencent-keen-security-lab-2016-9.

79. *Id.*

80. *Id.* Within ten days, Tesla released a statement that said they made an immediate update to address "potential security issues." *Id.*

81. Before self-driving cars are widely released on the market, the roads and signs will require redesign for compatibility with V2V and sensors. Patrick Gavin, *Regional Regulation of Transportation Network Companies*, 11 HARV. L. & POL'Y REV. 337, 354 (2017); Kohler & Colbert-Taylor, *supra* note 24, at 133 (explaining traditional traffic signals may become obsolete by the "possibility of coordinating the flow of traffic through intersections").

technology remain to be seen. However, ECUs are presently susceptible to remote attack.[82]

Recent experimental hacks reveal that ECUs are increasingly receptive entry points for attacks.[83] Put simply, ECUs in modern vehicles are like "30 or more computers on wheels."[84] And, some luxury vehicles have over one hundred ECUs.[85] Vulnerable ECUs leave the door open to cyberattack. Over the last few years, many automotive manufacturers have more than doubled the number of ECUs.[86] Hence, they have more than doubled the number of doors by which cybercriminals may gain access. Thus, while manufacturers are fixated on technological advancements, additional connected components pose increasing cybersecurity risks.[87]

Charlie Miller and Chris Valasek, the individuals that remotely hacked the 2014 Jeep Cherokee, explained the steps to access ECUs to physically control a connected vehicle. Generally, the three-stage process includes: (1) identifying an attack surface to gain access to the internal automotive network; (2) injecting messages into the internal network to compromise the targeted ECU; and (3) reverse the engineering code to control the vehicle.[88] ECU entry points vary in vulnerability. In their analysis, the researchers considered Bluetooth components to be "the biggest and most viable attack surfaces" on connected vehicles.[89] Also, the researchers considered "Telematics" and "Wi-Fi" connectivity to be the "holy grail of automotive attacks"

---

82. Kohler & Colbert-Taylor, *supra* note 24, at 133 ("[E]vidence suggests that the ECUs of vehicles currently on the market are not well secured against attack . . . .").

83. *See* Charlie Miller & Chris Valasek, *A Survey of Remote Automotive Attack Services*, at 5 ("ECUs pose the biggest risk to the manufacturer, passenger, and vehicle."), http://illmatics.com/remote%20attack%20surfaces.pdf.

84. Meaning, modern vehicles have more than "thirty microprocessor-controlled devices and electronic control units . . . ." Joel Finch, *Toyota Sudden Acceleration: A Case Study of the National Highway Traffic Safety Administration Recalls for Change*, 22 LOY. CONSUMER L. REV. 472, 481 (2010) (citation omitted).

85. *Id.*

86. For instance, in 2010, Range Rovers contained 41 ECUs. In 2014, only four years later, Range Rovers were equipped with 98 ECUs. Miller & Valasek, *supra* note 83, at 87.

87. *See* Wenzel, *supra* note 74, at 54 ("As cars have become increasingly connected to the Internet, they have become increasingly susceptible to cyberattacks."); *see also* Miller & Valasek, *supra* note 83, at 87 ("The number of different networks in cars (complexity of architecture) has increased over time . . . [t]he addition of ECUs over time is a result of manufacturers requiring more technology . . . . ").

88. *See* Miller & Valasek, *supra* note 83, at 5–6.

89. *Id.* at 16.

because the range is extremely broad via the Internet.[90] Miller and Valasek also explained that the reverse engineering process will require "a large amount of work and will be manufacturer specific."[91] This detail is critically important because, in order to hack autonomous vehicles through ECUs, hackers will most likely tailor their attacks to one specific manufacturer.[92] Considering the increasing reality of automotive cybersecurity threats, recent hacks have sparked interest in Washington D.C.[93]

C. Federal Regulation for Automotive Cybersecurity

NHTSA has expressed its goal of developing baseline requirements to ensure that the ECUs in modern and future autonomous vehicles are secure from cyberattack.[94] In September 2016, the DOT and NHTSA released the Federal Automated Vehicles Policy (FAV Policy), providing guidance in the design, development, and testing of autonomous vehicles.[95] In the FAV Policy, NHTSA stated that all autonomous vehicle manufacturers should "ensure that the vehicle has . . . applied appropriate functional safety and cybersecurity best practices . . . and that consumer education and training have been addressed."[96] Under "Vehicle Cybersecurity," the FAV Policy states:

> Manufacturers and other entities[97] should follow a robust product development process based on a systems-engineering approach to minimize risks to safety, including those due to cybersecurity threats and vulnerabilities. This process should

---

90. *Id.* at 18–19; *see also* Glancy, *supra* note 67, at 648 ("[W]ireless connections to vehicles will, of course, also generate . . . security concerns.").

91. Miller & Valasek, supra note 83, at 6.

92. *See id.* at 6 ("Since each manufacturer (and perhaps each model and even each year) use different data in the messages on the [internal network]"). However, certainly a band of hackers could target several manufacturers through collective efforts.

93. *See* H.R. 3388: SELF DRIVE Act, 115TH CONGRESS (Apr. 2, 2018), https://www.congress.gov/bill/115th-congress/house-bill/3388/actions.

94. Kohler & Colbert-Taylor, *supra* note 24, at 135.

95. *See generally Federal Automated Vehicles Policy: Accelerating the Next Revolution in Roadway Safety*, U.S. DEP'T OF TRANSP. (Sept. 2016), https://www.transportation.gov/sites/dot.gov/files/docs/AV%20policy%20guidance%20PDF.pdf.

96. *Id.* at 13.

97. "Other entities" refers to third party suppliers. *See id.* at 21, n.21 ("Manufacturers should insist that their suppliers build into their equipment robust cybersecurity features.").

> include systematic and ongoing safety risk assessment for the [autonomous vehicle] system, the overall vehicle design into which it is being integrated, and when applicable, the broader transportation ecosystem. The identification, protection, detection, response, and recovery functions should be used to enable risk management decisions, address risks and threats, and enable quick response to and learning from cybersecurity events.
>
> While this is an evolving area and more research is necessary before proposing a regulatory standard, entities are encouraged to design their [autonomous vehicle] systems following established best practices for cyber physical vehicle systems.[98]

Although more defined federal regulations are forthcoming, NHTSA explained that "entities should presently consider and incorporate guidance, best practices, and design principles published by National Institute for Standards and Technology (NIST), NHTSA, SAE International, the Alliance of Automobile Manufacturers, the Association of Global Automakers, the Automotive Information Sharing and Analysis Center (ISAC) and other relevant organizations."[99] As the NHTSA has alluded, cybersecurity is an evolving area and regulations will certainly change. As explained herein, federal regulations will play an important factor in assessing tort liability.

III. PRODUCTS LIABILITY AND SECURITY BREACHES IN AUTONOMOUS VEHICLES

As hackers begin infiltrating autonomous vehicles with substandard cybersecurity, courts will be forced to grapple with potential liability theories against vehicle manufacturers. Tort theories relating to intangible software and data are undeveloped. Courts are seemingly willing to apply tort theories to cybersecurity and data breach cases,[100] however, factual circumstances involving physical injury have not yet been presented to the courts.

---

98. *Id.* at 21.

99. *Id.*

100. *See* In re Sony Gaming Networks & Customer Data Sec. Breach Litig., 996 F. Supp. 2d 942, 966 (S.D. Cal. 2014) (finding Sony had a duty to provide reasonable data security but dismissed on other grounds).

Nonetheless, applying products liability principles to manufacturers and component software developers for personal injuries caused by defective software is a compelling question.[101] This Part addresses product defect theories as they relate to security vulnerabilities in autonomous vehicles. Parts IV and V address traditional negligence theories and the hurdles for constructing a standard of care.

Before delving into products liability in the context of cybersecurity software, a brief primer on product defects is appropriate. There are three distinct types of defects: (1) manufacturing defects, (2) design defects, and (3) warning defects.[102] Manufacturing defects occur when the product fails to meet its intended design and unexpectedly malfunctions.[103] In contrast, design defects arise when a product meets the manufacturer's intended design, and the plaintiff challenges the defectiveness of the entire product line.[104] Thirdly, warning defects arise when the manufacturer fails to provide sufficient warnings or instructions on how to safely use the product.[105] All three defects are likely to be litigated in cybersecurity software vulnerabilities. Although plaintiffs may plead multiple product defect theories,[106] specific evidence may prove one type of defect over another, especially distinguishing between manufacturing and design defects.[107]

A. The Drawbridge to Products Liability: Software in Traditional "Products"

Products liability theories for defective cybersecurity software will likely manifest and evolve through durable products, [108] such as automated and connected vehicles. In the past, products liability law

---

101. 1 OWEN & DAVIS ON PROD. LIAB. § 17:30 (4th ed. 2016) ("Whether manufacturers of computer software should be subject to products liability for personal injuries caused by defective software is an intriguing question.").

102. David G. Owen, *The Puzzle of Comment J*, 55 HASTINGS L.J. 1377, 1378–79 (2004).

103. Douglas A. Kysar, *The Expectations of Consumers*, 103 COLUM. L. REV. 1700, 1709 (2003).

104. *See id.*

105. Owen, *supra* note 102, at 1378–79.

106. David C. Vladeck, *Machines Without Principals: Liability Rules and Artificial Intelligence*, 89 WASH. L. REV. 117, 132 (2014) (commenting that products liability plaintiffs often plead both traditional negligence and products liability claims).

107. Owen, *supra* note 102, at 1380.

108. *See* Rustad, *supra* note 18, at 500 (detailing tort concepts in cyberspace, noting that the "greatest potential" for strict liability or products liability is the Internet connected with durable goods).

has drawn a bright-line distinction between injuries caused by tangible and intangible products.[109] Generally, computer code has been thought of as a "service" and not considered a "product."[110] However, this notion is shifting as software is increasingly implemented into physical machinery, such as the modern connected automobile.[111]

Although statutes may define a "product" for application of products liability, courts must "determine as a matter of law whether something is, or is not, a product."[112] The Restatement (Third) of Torts defines a "product" as "tangible personal property distributed commercially for use or consumption."[113] Further, "[o]ther items, such as real property and electricity, are products when the context of their distribution and use is sufficiently analogous to the distribution and use of tangible personal property."[114] In contrast, services are not "products" sufficient for application of products liability.[115]

Courts may decide computer software is a "product" by drawing comparison under the Uniform Commercial Code (UCC).[116] Under the UCC, software that is mass-marketed is considered a good.[117] In contrast, software developed for specific customers is a "service," thus not applicable in the UCC context.[118] In the early 1980s, in *Saloomey v. Jeppesen & Co.*, the Second Circuit drew this distinction and applied strict products liability to a defective air navigational chart.[119]

---

109. *See* Govind Persad, *Law, Science, and the Injured Mind*, 67 ALA. L. REV. 1179, 1189 (2016).

110. David C. Vladeck, *supra* note 106, at 150 n.52. However, some plaintiffs allege defective software under warranty theories. *See* Motorola Mobility, Inc. v. Myriad France SAS, 850 F. Supp. 2d 878, 880–81 (N.D. Ill. 2012) (alleging defective software pleaded as a breach of warranty); *see also* Daniel B. Garrie, *The Legal Status of Software*, 23 J. MARSHALL J. COMPUTER & INFO. L. 711, 714–20 (2005).

111. *See* Vladeck, *supra* note 106, at 133 n.52 (explaining the "dynamic appears to be changing, as increasingly software systems operate cars, trucks, planes and other machines, that, on occasion, malfunction and injure non-purchaser third parties.").

112. RESTATEMENT (THIRD) OF TORTS: PROD. LIAB. § 19, cmt. a (1998).

113. RESTATEMENT (THIRD) OF TORTS: PROD. LIAB. § 19(a) (1998).

114. *Id.*

115. *Id.* at § 19(b).

116. *Id.* at 19 cmt. d (Reporters' Note) ("When a court will have to decide whether to extend strict liability to computer software, it may draw an analogy between the treatment of software under the Uniform Commercial Code and under products liability law.").

117. *See, e.g.*, Advent Sys. Ltd. v. Unisys Corp., 925 F.2d 670, 672 (3d Cir.1991); RRX Indus., Inc. v. Lab-Con, Inc., 772 F.2d 543, 546 (9th Cir. 1985).

118. *See, e.g.*, Micro-Managers, Inc. v. Gregory, 434 N.W.2d 97, 100 (Wis. Ct. App. 1988); Data Processing Servs., Inc. v. L.H. Smith Oil Corp., 492 N.E.2d 314, 318 (Ind. Ct. App. 1986).

119. 707 F.2d 671, 676 (2d Cir. 1983).

Notably, the navigational charts were in written form and not navigational software.[120] Even so, navigational charts are analogous because they are "used for their physical characteristics rather than for the ideas contained in them."[121]

Defendant manufacturers will likely attempt to separate cybersecurity software from the tangible autonomous vehicle, arguing that the cybersecurity software is a "service" and not a "product." Similar to the navigational charts in *Saloomey*, software in autonomous vehicles are mass produced.[122] Most importantly, the autonomous vehicle is the overall defective "product." Courts should be unpersuaded by an attempt to separate the two, because the security software is an inseparable component of the durable product. Also, there is no option to purchase a vehicle without the software, thus, the plaintiff is solely relying on that software for protection from unwanted cyber intrusion. Additionally, from the manufacturer's perspective, the connected physical product must also comply with specific regulations or standards. Products liability theories, therefore, will undoubtedly apply to the traditional "product" that contains defective software. Due to cybersecurity components' intangible form, courts and litigants may encounter additional issues when identifying and establishing a defect.

B. Identifying the Defect

1. Warning Defects

Suppose a hacker targets and gains remote access to a vehicle while it is in autonomous mode. The vehicle has limited autonomous features and the driver, at any point, may manually override the autonomous technology.[123] During the remote access, the autonomous technology realizes that an unidentified third party is also connected with the vehicle. Over the next few hours, nothing happens and neither the autonomous vehicle nor manufacturer alerts the drivers. That afternoon, approximately 5:15pm on a Tuesday in Atlanta, twenty-one similar models suddenly break during rush-hour traffic. Multiple cars simultaneously breaking results in a string of crashes

---

120. *See id.* at 672 (explaining the three types of charts: "[e]nroute charts," "[a]rea charts," and "[a]pproach charts").

121. RESTATEMENT (THIRD) OF TORTS: PROD. LIAB. § 19, cmt. d (1998) (Reporters' Note).

122. *See Saloomey*, 707 F.2d at 676.

123. *See supra* Part I.B. (NHTSA classifying limited automated vehicles as level 3 autonomous vehicles).

in the congested roadway. In this scenario, it is clear an adequate warning would have allowed passengers to manually take back control.

Warning defects will be the most recognizable defects. A warning defect arises when a manufacturer breaches its duty to warn by failing to warn at all of a material risk.[124] "A duty to warn actually consists of two duties: One is to give adequate instructions for safe use, and the other is to give a warning as to dangers inherent in improper use."[125] First, front-end instructions may provide information on safe use, such as cautioning owners against installing non-factory or unsecure plug-in devices.[126] Second, pertinent to the scenario above, a warning would have put the driver on notice that an intruder had gained access to the vehicle. The drivers, with this knowledge, could have voluntarily chosen to manually override the autonomous technology. However, if the manufacturer, either manually or through automated warning systems, provided a warning that may apprise the reasonable driver of a need to override the automated technology, then the question turns to adequacy.[127]

2. Design or Manufacturing Defect?

When defects exist in the product development process, distinguishing between a manufacturing and design defect in software technology will present a more strenuous task. Ordinarily, manufacturing and design defects deal with physical components. Defects will be more difficult to pinpoint in security software, due to its intangible form.[128] However, defects may be cognizable after

---

124. *See* Ford Motor Co. v. Gibson, 659 S.E.2d 346, 351 (Ga. 2008) (no warning that rear-end collision could cause fire in fuel tank, that doors could be jammed shut, and driver's seat back could collapse backwards into fire).

125. Ontai v. Straub Clinic & Hosp. Inc., 659 P.2d 734, 743 (Haw. 1983).

126. For instance, in August 2015, University of California at San Diego researchers successfully hacked and shut down a Corvette's brakes by hacking plug-in devices commonly provided by insurance companies, such as the Progressive Snapshot. Andy Greenberg, *Hackers Cut a Corevette's Brakes Via a Common Car Gadget*, WIRED (Aug. 11, 2015), https://www.wired.com/2015/08/hackers-cut-corvettes-brakes-via-common-car-gadget/.

127. Adequacy presents a jury issue to assess the given warning's content and sufficiency. *See, e.g.*, Abbot by Abbot v. Am. Cyanamid Co., 844 F.2d 1108, 1115 (4th Cir. 1988) ("The adequacy of a warning is a question of fact for the jury.") (citations omitted); Altman v. HO Sports Co., 821 F.Supp.2d 1178, 1188 (E.D. Cal. 2011) ("The adequacy of a warning is generally a question of fact.").

128. Dana M. Mele, *The Quasi-Autonomous Car as an Assistive Device for Blind Drivers: Overcoming Liability and Regulatory Barriers*, 28 SYRACUSE J. SCI. & TECH. L. 26, 56 (2013).

adequate investigation and discovery.[129] The complex nature of software development can be broken down into four distinct phases: (1) design, (2) coding, (3) testing, (4) replication and distribution.[130]

During the first design phrase, manufacturers' design choices will certainly be a design defect because it will be implemented in the entire product line.[131] Professor Scott opines that defects in the coding phase are "the most critical issue left open to debate . . . ."[132] However, the coding phase will similarly affect the entire product line.[133] For instance, in *Heartland*,[134] vulnerable coding, written eight years before the attack, created a susceptible avenue for the hackers to gain access to Heartland's network.[135] In the context of connected products, developmental coding will similarly affect the entire car model's security functions.

In contrast, defects in phase four (replication and distribution) should be deemed manufacturing defects. Unlike design and coding, testing and distribution both occur after the completed software program.[136] According to the Fifth Circuit Court of Appeals:

> Manufacturing defect cases involve products which are flawed, i.e., which do not conform to the manufacturer's own specifications, and are not identical to their mass-produced siblings. The flaw theory is based upon a fundamental consumer expectancy: that a mass-produced product will not

---

129. *See* DAVID G. OWEN & MARY J. DAVIS, PRODUCTS LIABILITY AND SAFETY: CASES AND MATERIALS, 52 (7th ed. 2015) (casebook describing products liability cases as "detective stories" because often "neither the injured party nor the manufacturer will have any idea what went wrong . . . . It is a principal responsibility of the lawyers for the parties, and their experts . . . to develop theories of how and why the accident happened, and how it might have been prevented").

130. Michael D. Scott, *Tort Liability for Vendors of Insecure Software: Has the Time Finally Come?*, 67 MD. L. REV. 425, 459 (2008).

131. *Id.* at 459.

132. *Id.*

133. *See* Jeffrey K. Gurney, *Sue My Car Not Me: Products Liability and Accidents Involving Autonomous Vehicles*, 2013 U. ILL. J.L. TECH. & POL'Y 247, 263 (2013) (explaining that most design defect claims in autonomous vehicles will concern the algorithm and coding).

134. *See* Lone Star Bank v. Heartland Payment Sys., 729 F.3d 421 (5th Cir. 2013). *Heartland* is discussed more fully herein. *See infra* Part IV, at p. 31–32.

135. Lawrence J. Trautman, *Managing Cyberthreat*, 33 SANTA CLARA HIGH TECH. L.J. 230, 242 (2017).

136. Jacob Kreutzer, *Somebody Has to Pay: Products Liability for Spyware*, 45 AM. BUS. L.J. 61, 99 (2008).

> differ from its siblings in a manner that makes it more dangerous than the others.[137]

Defects in replication and distribution will undoubtedly present a manufacturing defect.[138] Distribution is the process in which the software is copied and transferred to the end user or product.[139] If a mistake occurs when implementing the software into a vehicle; the mistake will affect that individual vehicle. In these situations, the nonconforming flaws will certainly be manufacturing defects.

At the testing phase, whether the dangerous condition should be a manufacturing or a design defect presents a closer question. Testing involves troubleshooting the completed program and assessing it for vulnerable holes or deficiencies. If a tester inadvertently manipulates the software to cause a defect in the program, then that inadvertent mistake should be a manufacturing defect.[140] However, if a tester discovers the dangerous condition in the testing phase, then a manufacturer will reconcile the software hole through additional coding and return the product to the coding phase.

3. The Unidentifiable Defect

Since pinpointing defects in security software will certainty prove to be complex, situations will arise where the nature of a defective condition is apparent but unidentifiable. For instance, in recent multidistrict litigation cases over Toyota's unintended acceleration, neither plaintiffs nor Toyota were able to pinpoint a defect in the automotive software.[141] The malfunction doctrine could fill the void.

The malfunction doctrine is similar to *res ipsa loquitur* in negligence; however, the malfunction doctrine focuses on the product's

---

137. Casey v. Toyota Motor Eng'g & Mfg. N. Am., Inc., 770 F.3d 322, 329 (5th Cir. 2014) (quoting Green v. R.J. Reynolds Tobacco Co., 274 F.3d 263, 268 (5th Cir. 2001)).

138. Scott, *supra* note 130, at 459 (explaining "there is no debate that a defect introduced into the product at the replication and distribution phase would be deemed a manufacturing defect").

139. Kreutzer, *supra* note 136, at 99.

140. *See* Catalano v. BMW of N. Am., LLC, 167 F. Supp. 3d 540, 554 (S.D.N.Y. 2016) (quoting McCarthy v. Olin Corp., 119 F.3d 148, 154–55 (2d Cir. 1997) (manufacturing defect "results when a mistake in manufacturing renders a product that is ordinarily safe dangerous so that it causes harm").

141. *See* In re Toyota Motor Corp. Unintended Acceleration Mktg., Sales Practices, & Prod. Liab. Litig., 978 F. Supp. 2d 1053, 1100 (C.D. Cal. 2013) (Toyota sought summary judgment on grounds that plaintiff was "unable to identify a precise software design or manufacturing defect"). However, lack of a specific defect was merely inconclusive on either side, thus, creating a triable jury issue. *Id.* at 1102.

condition and does not take into account a manufacturer's fault.[142] In order to prevail under a malfunction defect theory, plaintiff must show that: "(1) the product malfunctioned, (2) the malfunction occurred during proper use, and (3) the product had not been altered or misused in a manner that probably caused the malfunction."[143] Under the doctrine, if plaintiff is unable to prove a specific defect, "the malfunction doctrine may provide relief if the plaintiff is able to show the probability of defect by eliminating other normal causes of such malfunctions."[144] Put simply, the malfunction doctrine lowers a plaintiff's burden to identify and prove a specific defect if circumstantial evidence allows an inference that the product was most likely defective.[145]

Once investigative and discovery measures to ascertain a defect are exhausted, plaintiff may present circumstantial evidence of a defect in the autonomous vehicle's cybersecurity technology.[146] The first element could be proven by presenting evidence of the accident itself.[147] However, the second and third elements are where litigants will likely quarrel. The Supreme Court of Connecticut explained that "[e]vidence as to the second element supports an inference that the defect in the product existed when the product left the manufacturer's control and was not introduced by any other reasonably possible cause outside of its control."[148] To prove the second element, plaintiff "must present sufficient evidence to negate a reasonable possibility that something *or someone* besides the manufacturer caused the defect in

---

142. *See* Kevin Funkhouser, *Paving the Road Ahead: Autonomous Vehicles, Products Liability, and the Need for A New Approach*, 2013 UTAH L. REV. 437, 447 (2013) (explaining "scholars and courts are quick to note that a *res ipsa loquitur* approach is different because it still raises the question of negligence, whereas the malfunction doctrine works under strict liability where negligence is not applicable").

143. David G. Owen, *Manufacturing Defects*, 53 S.C. L. REV. 851, 873 (2002); *see also* Metro. Prop. & Cas. Ins. Co. v. Deere & Co., 25 A.3d 571, 583–84 (Conn. 2011) (Connecticut Supreme Court explaining the malfunction doctrine may be satisfied if plaintiff presents evidence that "(1) the incident that caused the plaintiff's harm was of a kind that ordinarily does not occur in the absence of a product defect, and (2) any defect most likely existed at the time the product left the manufacturer's or seller's control and was not the result of other reasonably possible causes not attributable to the manufacturer or seller.").

144. Owen, *supra* note 143, at 869.

145. Owen, *supra* note 143, at 873–74.

146. *See* Gurney, *supra* note 133, at 259 (under this doctrine, "plaintiff could prove that the accident was caused by a malfunction in the autonomous technology").

147. *Id.*

148. *Metro Prop.*, 25 A.3d at 585.

the product."[149] Addressing the unaltered product component of element three, it is unclear whether plaintiffs will have the opportunity or capability to alter cybersecurity settings. Presumably, if a plaintiff voluntarily shuts off his cybersecurity protections, then that may prevent recovery.[150]

In rebuttal, manufacturers could argue the autonomous vehicle technology was not defective at the time it left the manufacturer's control and any defect arose after it reached the end user.[151] In the context of cybersecurity vulnerabilities, the manufacturer could point to the third-party criminal and allege that a sophisticated hacker actually created the unreasonably dangerous condition. The question then remains whether a sophisticated hacker actually caused the defective condition, or whether the defect was the entry point for a hacker to gain access.

Although courts often assess certain automobile malfunctions under the malfunction theory,[152] it may be difficult for a plaintiff to meet his or her burden to rule out reasonable secondary causes in automotive cybersecurity breaches. Moreover, it is uncertain whether the malfunction doctrine applies to software-related defects.[153] If the malfunction doctrine carries the day, strict liability is appropriate because the malfunction doctrine is a form of proof for manufacturing

---

149. *Id.* (emphasis added); *see also* Rohde v. Smiths Medical, 165 P.3d 433, 439 (Wyo. 2007) (Plaintiff could not rely on malfunction theory because plaintiff "failed to meet his burden to discount reasonable secondary causes of the product's malfunction").

150. However, it is unlikely that autonomous vehicles' cybersecurity technology will operate similar to Norton AntiVirus, requiring the individual to make installations and updates. If the individual is tasked with making updates, manufacturers may likely raise a misuse defense. For instance, it is well-known that computers are more susceptible to cyberattacks when users access risky websites. Since users in autonomous mode will spend considerable time surfing the internet, users could access websites that are more prone to cyber intrusion than others.

151. *See* Alan Calnan, *A Consumer-Use Approach to Products Liability*, 33 U. MEM. L. REV. 755, 816 (2003) ("[S]uch evidence would have to prove clearly and convincingly that the offending product did not leave the factory with a manufacturing flaw.").

152. Owen, *supra* note 143, at 875–76 (detailing automobile cases in which courts have applied the malfunction doctrine, including: unexplainable acceleration, gear changes, air bag deployment failures, and more).

153. Gurney, *supra* note 133, at 259; *see also* Funkhouser, *supra* note 142, at 454 ("It will likely take considerable time for courts to develop a predictable jurisprudence with respect to the malfunction doctrine as applied to autonomous vehicles.").

defects.[154] However, other defects will require a more negligence-based assessment.

C. Testing the Defect

Identifying the defect is vital because it determines the applicable products liability standard. Determining products liability standards, especially in complex products, is one of the most widely debated issues in products liability law.[155] In 1965, the American Law Institute published Section 402A of the Restatement (Second) of Torts.[156] Section 402A established strict liability, which subjects manufacturers and sellers to liability even without negligence.[157] Subsequently, it became clear that strict liability "could not, without considerable difficulty, be applied to design and warning defect cases."[158] In the 1970s, applying strict liability to design and warning defects became problematic, causing courts to "mix" strict liability and negligence principles.[159] In 1998, the American Law Institute released the Restatement (Third) of Torts, which eliminated "strict

---

154. Owen, *supra* note 143, at 870 ("And most courts will certainly want to allow manufacturing defects to be established by the malfunction doctrine and possibly by other forms of proof.").

155. *See, e.g.*, David G. Owen, *Design Defects*, 73 MO. L. REV. 291, 336 (2008) (in determining modern design defects, "most courts" exclusively apply either risk-utility or consumer expectations and "refused to recognize the validity of the other"); James A. Henderson, Jr. & Aaron D. Twerski, *Achieving Consensus on Defective Product Design*, 83 CORNELL L. REV. 867, 882 (1998) (explaining that, in the early 1960s, the Restatement (Second) of Torts' strict liability standard was never intended to apply to design or warning defects).

156. *See* RESTATEMENT (SECOND) OF TORTS § 402A (AM. LAW INST. 1965); *see also* Michael D. Green, *The Unappreciated Congruity of the Second and Third Torts Restatements on Design Defects*, 74 BROOK. L. REV. 807, 812 (2009) ("[S]ection 402A was not a 'restatement' of existing law. Rather, it reflected dissatisfaction with the existing state of the law that posed so many obstacles to establishing liability for dangerous products.").

157. *See* RESTATEMENT (SECOND) OF TORTS § 402A(2) (AM. LAW INST. 1965).

158. James A. Henderson, Jr. & Aaron D. Twerski, *A Proposed Revision of Section 402A of the Restatement (Second) of Torts*, 77 CORNELL L. REV. 1512, 1515 (1992); *see also* Owen, *supra* note 102, at 1378 (In the 1960s, the Restatement Second's strict liability standard offered a vague construction of product defectiveness, however, the need to treat these defects separately is modernly a "well-accepted axiom.").

159. Owen, *supra* note 155, at 336–53 (detailing how courts combined consumer expectations and risk-utility); *see generally e.g.*, Ryan J. Duplechin, *Divided by Design: Reconciling the AEMLD's "Mixed" Design-Defect Approach*, 8 FAULKNER L. REV. 381 (2017) (explaining the evolution of "mixing" the Restatement (Second) of Torts' consumer expectations approach with the Restatement (Third) of Torts' risk-utility standard).

liability" in terms of design and warning defects.[160] Design and warning defects will form the bulk of case law for automotive products liability cases related to cybersecurity, with design defects being the most prevalent.

First, warning defects uniformly apply negligence principles.[161] In warning defect cases, several courts retain the "strict" liability shell while applying negligence law's reasonableness principles.[162] The Restatement (Third) of Torts provides that a product contains a warning defect "when the foreseeable risks of harm posed by the product could have been reduced or avoided by the provision of reasonable instructions or warnings by the seller or other distributor, or a predecessor in the commercial chain of distribution, and the omission of the instructions or warnings renders the product not reasonably safe."[163] Further, comment i provides this is a "reasonableness test," which is "a similar standard for judging the safety of product designs."[164]

Generally, whether a warning or instruction is required considers the foreseeability of the risk and whether a significant number of users are unaware of the specific risk.[165] Providing a warning is usually a cost-effective way to fulfill manufacturer obligations. In a practical sense, autonomous vehicle manufacturers may increase

---

160. John H. Chun, *The New Citadel: A Reasonably Designed Products Liability Restatement*, 79 CORNELL L. REV. 1654, 1681 (1994) (Restatement (Third) of Torts "labored to erase 'strict liability' from thinking on design defect."). Although "strict" products liability has been "echoed by the courts in thousands of courtrooms and written decisions across America for over [four] decades," the Restatement (Third) represented a return to negligence principles in both design and failure to warn cases. David G. Owen, *The Evolution of Products Liability Law*, 26 REV. LITIG. 955, 982 (2007).

161. Hahn v. Richter, 673 A.2d 888, 891 (Pa. 1996) (in drug warning defect cases, negligence is the sole basis of liability); s*ee, e.g.*, Crislip v. TCH Liquidating Co., 556 N.E.2d 1177, 1183 (Ohio 1990) ("[T]he standard imposed upon the defendant in a strict liability claim grounded upon an inadequate warning is the same as that imposed in a negligence claim based upon inadequate warning.").

162. *See* Gourdine v. Crews, 955 A.2d 769, 782 (Md. 2008) ("[N]egligence concepts and those of strict liability have 'morphed together' . . . in failure to warn cases."). *But see* Simonetta v. Viad Corp., 197 P.3d 127, 135 (Wash. 2008) (noting that the court has not "consistently maintained a clear distinction between strict liability and negligence theories in the failure to warn context," yet failing to offer any suggested distinction).

163. RESTATEMENT (THIRD) OF TORTS: PROD. LIAB. § 2(c) (AM. LAW INST. 1998).

164. *Id.* at cmt. i.

165. F. Patrick Hubbard, *"Sophisticated Robots": Balancing Liability, Regulation, and Innovation*, 66 FLA. L. REV. 1803, 1822 (2014) (citing RESTATEMENT (THIRD) OF TORTS: PRODS. LIAB. § 10 (AM. LAW INST. 1998)).

cybersecurity measures for reputational purposes.[166] Unfortunately, by the same token, manufacturers may choose to forgo a specific warning due to reputational concerns and profits. Thus, when cybersecurity threats are known, negligence standards will assess the proper costs and benefits of providing an adequate warning to consumers.

Second, strict liability remains in manufacturing defects.[167] Manufacturing defects result from a fault in the production process that fails to meet the manufacturer's design specifications.[168] Put simply, manufacturing defects are "truly a mistake."[169] Despite increasing cybersecurity threats, no reported decisions have held a software manufacturer strictly liable in tort.[170] Manufacturing defects in automotive cybersecurity components may result from an inadvertent mistake at the software distribution stage. Outside these narrow circumstances, true manufacturing defect cases are unlikely. Rather, defective conditions will more frequently result from substandard construction or omissions in designing security components.

Third, in the early stages of the vehicle development process, risk-utility standards should prevail in design defects. Essentially, risk-utility is purely a negligence standard.[171] Courts use two tests to determine whether a product has a design defect: the consumer expectations test and risk-utility test.[172] Risk-utility is the majority

---

166. *See* Thierer & Hagemann, *supra* note 23, at 377 (suggesting autonomous vehicle manufacturers "have powerful reputational incentives at stake here, which will encourage them to continuously improve the security of their systems.").

167. The standard remains "strict liability" because manufacturing defects are the only type of defect that solely focus on reasonable consumer expectations. *See* Mary J. Davis, *Design Defect Liability: In Search of a Standard of Responsibility*, 39 WAYNE L. REV. 1217, 1235 (1993) ("It is in the context of manufacturing flaws that the intended focus of strict liability on the product, as opposed to the conduct of the manufacturer, makes the most sense.").

168. Owen, *supra* note 155, at 296.

169. Owen, *supra* note 155, at 296.

170. Scott, *supra* note 130, at 469.

171. *See, e.g.*, Ackerman v. American Cyanamid Co., 586 N.W.2d 208, 220 (Iowa 1998) ("a growing number of courts and commentators have found that, in cases in which the plaintiff's injury is caused by an alleged defect in the design of a product, there is no practical difference between theories of negligence."); *S.*; Foley v. Clark Equipment Co. 523 A.2d 379, 388–89 (Pa. Super. 1987) ("The risk/utility analysis is nothing more than a detailed version of the balancing process used in evaluating reasonable care in negligence cases . . . . Because strict liability and negligence employ the same balancing process to assess liability, proof sufficient to establish liability under one theory will in most instances be sufficient under the other.").

172. Owen, *supra* note 153, at 299 ("All courts judge the adequacy of a product's design upon one of two basic standards, or some combination thereof: (1) the 'consumer

standard for design defects.[173] Although design defect approaches vary widely across jurisdictions, the Restatement (Third) requires plaintiffs to prove a safer alternative design.[174] As explained by the Second Circuit, "[t]he purpose of risk/utility analysis is to determine whether the risk of injury might have been reduced or avoided if the manufacturer had used a feasible alternative design."[175]

Safer alternative design issues are unique to design defects.[176] In design defect cases involving cybersecurity software vulnerabilities, the most daunting task will likely be identifying the defect and solution. At the forefront of design defect litigation, numerous experts will delve into the complexities of an alternative cybersecurity design. At present, Miller and Valasek's survey offers a practical and safer approach to safeguarding against automobile cyber intrusion. Their research may supply the groundwork for a safer alternative design.

Miller and Valasek suggest a "layered" approach as a safer design.[177] As explained in Part II(B), hacking an automobile's internal network to physically control the vehicle is a three-stage process. Essentially, hackers gain access through a vulnerable ECU that can send messages to other ECUs with control functions. Vulnerabilities exist when ECUs can easily communicate with other ECUs. For instance, if the Wi-Fi or entertainment functions can communicate with the brakes, an avenue exists to halt those brakes. Therefore, in the most basic sense, blocking cyberattacks requires protective layers at each stage.

---

expectations' test-- whether the design meets the safety expectations of users and consumers, and/or (2) the 'risk-utility' test-- whether the safety benefits of designing away a foreseeable danger exceed the resulting costs.").

173. *See, e.g.*, Branham v. Ford Motor Co., 701 S.E.2d 5, 14 n.11 (S.C. 2010) ("Some form of a risk-utility test is employed by an overwhelming majority of the jurisdictions in this country."); Wright v. Brooke Grp. Ltd., 652 N.W.2d 159, 162 (Iowa 2002) (adopting Products Liability Restatement § 2(b)); Ford Motor Co. v. Miles, 967 S.W.2d 377, 386 (Tex. 1998) (instruction conflicted with "the risk versus utility analysis that lies at the core of products liability design defect law"); Warner Fruehauf Trailer Co., Inc. v. Boston, 654 A.2d 1272, 1276 (D.C. 1995) ("In design defect cases, most jurisdictions decide [strict liability in tort] by applying some form of a risk-utility balancing test."); Banks v. ICI Americas, Inc., 450 S.E.2d 671 (Ga. 1994); Sperry-New Holland v. Prestage, 617 So.2d 248, 255 (Miss. 1993) ("Risk-utility has become the trend in most federal and state jurisdictions.").

174. RESTATEMENT (THIRD) OF TORTS: PROD. LIAB. § 19 (AM. LAW INST. 1998).

175. McCarthy v. Olin Corp., 119 F.3d 148, 155 (2d Cir. 1997).

176. *See* Wankier v. Crown Equip. Corp., 353 F.3d 862, 867 (10th Cir. 2003) ("In neither duty-to-warn claims nor manufacturing defect claims does the issue of a safer alternative design logically arise.").

177. *See* Miller & Valasek, *supra* note 83, at 87.

In weighing the cost and feasibility of an alternative design, some commentators suggest that rewriting code in software will be cheap and easy.[178] For instance, "what is often needed for software containing security-related flaws is not an extensive redesign of the entire software package, but merely the rewriting of a small portion of the code to remove the vulnerability."[179] Others, however, suggest there are additional and costlier implications.[180] Professor Rustad explains that while cost of encrypting data may be relatively low, other costs include "enhanced employee training, outside security consultancies, data monitoring, and security audits of every party in a data transmission stream."[181] Even so, a product is defectively designed if the safety benefits of the alternative design *outweigh* the costs of alleviating the danger.[182] Once an alternative design is offered, the overarching question remains "whether the product *qua* product meets society's standards of acceptability."[183] In a narrower sense, the issue is "whether, given the risks and benefits of and possible alternatives to the product, we as a society will live with it in its existing state or will require an altered, less dangerous form."[184] When presented with an alternative design, juries will decide whether the danger of automotive cyberattacks can be squared with a particular increase in a manufacturer's monthly production costs.

IV. CYBERSECURITY AND NEGLIGENCE: THREE MAIN BARRIERS

Establishing cybersecurity tort principles will both provide redress to consumers and encourage manufacturers to invest in cybersecurity safety measures.[185] The preceding Part detailed litigation challenges relating to identifying and proving defects in software-driven cars. In addition to identifying and proving defects, plaintiffs must surpass three barriers in order to successfully maintain a tort action related to cybersecurity.

---

178. Scott, *supra* note 130, at 468.

179. *Id.*

180. RUSTAD, *supra* note 18, at 488.

181. *Id.*

182. *See* Owen, *supra* note 155, at 311 ("A product's design is 'defective' under a risk-utility test if the costs of avoiding a particular hazard are foreseeably less than the resulting safety benefits.").

183. William A. Donaher et. al., *The Technological Expert in Products Liability Litigation*, 52 TEX. L. REV. 1303, 1307 (1974).

184. *Id.*

185. *See* George L. Priest, *The Current Insurance Crisis and Modern Tort Law*, 96 YALE L.J. 1521, 1553 (1987) ("One of the objectives of the tort system is to create incentives for appropriate investments in preventing injury.").

According to Professor Rustad, in modern software security cases, an individual seeking to recover for negligence faces three "insurmountable barrier[s]."[186] The three main barriers include: (1) the economic loss doctrine; (2) present injury requirements; and (3) the lack of a judicially created duty to protect software and data intrusion.[187] In the autonomous-vehicle context, these barriers are present, but not insurmountable. Past software-related negligence cases have never dealt with a physical injury scenario.[188] But autonomous-vehicle cybersecurity cases may involve physical injuries or property damage, in which case the first two barriers will be significantly lowered.

The economic loss doctrine, the first modern barrier, states that unless a plaintiff suffers physical injury or property damage,[189] that person cannot recover in tort actions such as negligence and products liability.[190] In data breach cases, courts have routinely barred cases based on the economic loss doctrine;[191] however, in *Lone Star Bank v. Heartland Payment Systems*,[192] the Fifth Circuit articulated an "exception to the economic loss rule" in the large data breach context.[193] If courts follow the Fifth Circuit, data breach victims may have a route to recovery for purely financial loss.[194]

---

186. *See* RUSTAD, *supra* note 18, at 481.

187. *Id.*

188. *See id.* at 503.

189. Only product defects that result in harm to property *other than* the product itself are actionable in tort. *See* E. River S.S. Corp. v. Transamerica Delaval, Inc., 476 U.S. 858, 868 (1986).

190. *See, e.g.*, Am. United Logistics, Inc. v. Catellus Dev. Corp., 319 F.3d 921, 928 (7th Cir. 2003) (upholding dismissal of failure to warn claim because economic loss rule precluded recover for commercial loss); Werwinski v. Ford Motor Co., 286 F.3d 661, 674 (3d Cir. 2002) (barring claims against automotive manufacturer because claims premised on purely economic loss).

191. *See, e.g.*, In re Target Corp. Data Sec. Breach Litig., 66 F. Supp. 3d 1154, 1176 (D. Minn. 2014) (dismissing plaintiffs' negligent data breach claims under Alaska, California, Illinois, Iowa, and Massachusetts law;); *In re Sony Gaming Networks & Customer Data Sec. Breach Litig. (Sony II)*, 996 F. Supp. 2d 942, 967 (S.D. Cal. 2014).

192. 729 F.3d at 423–24.

193. Colin J.A. Oldberg, *Organizational Doxing: Disaster on the Doorstep*, 15 COLO. TECH. L.J. 181, 199 (2016); RUSTAD, *supra* note 18, at 488 (*Heartland* was a "significant decision" in cybersecurity tort cases).

194. RUSTAD, *supra* note 18, at 488. Whether tort suits related to denial of service attacks will surpass the economic loss doctrine is a thought-provoking question. For instance, Miller and Valasek analyzed the Smart Key ECU in a 2010 Toyota Prius and concluded they are susceptible to a denial of service attack from a range of five to twenty meters. Miller & Valasek, supra note 83, at 13–14. Also, hackers may be more easily identifiable after short range cyberattacks. However, the issue is beyond the scope of this Article.

Present injury requirements, the second barrier to recovery, relates to plaintiffs' standing.[195] This obstacle often arises in economic-based class actions. In order to satisfy constitutional standing, a plaintiff must show: (1) he or she has suffered an "injury in fact" that is concrete and particularized, actual or imminent, and not conjectural or hypothetical; (2) that the injury is fairly traceable to the challenged action of the defendant; and (3) that it is likely that the injury will be redressed by a favorable decision.[196] In 2013, in *Clapper*, the United States Supreme Court held that a plaintiff must show harm that is "certainly impending" to sufficiently allege a cognizable injury for Article III standing.[197]

Interestingly, plaintiffs recently filed a class action complaint for a design flaw in Chrysler's 2013–2015 vehicles—the subject of Miller and Valsek's 2015 hacking experiment.[198] In attempt to satisfy present injury requirements, plaintiffs argued the "vulnerabilities have exposed them to an increased risk of injury or death if their vehicles were hacked and that they suffer anxiety and fear because of that possibility."[199] The court held plaintiffs' allegations failed to satisfy *Clapper*'s standing requirements.[200] Under *Clapper*, risk of future injury and the fear of that injury does not create standing "absent a 'substantial' risk that the feared injury will come to bear."[201] The court reasoned that no "real world hacker" has ever hacked the Chrysler's system to cause injuries.[202] These recent class actions are only the beginning of cybersecurity-related litigation for connected and automated products.[203]

When cybersecurity tort cases involve physical injuries, those cases will easily overcome economic loss and present injury

---

195. *See* Clapper v. Amnesty Int'l USA, Inc., 133 S. Ct. 1138, 1143 (2013); *see also* Davis v. Fed. Elec. Comm'n, 554 U.S. 724, 734 (2008) (standing is evaluated on an injury-by-injury basis).

196. Lujan v. Defs. of Wildlife, 504 U.S. 555, 560–61 (1992).

197. 133 S. Ct. at 1143.

198. Flynn v. FCA US LLC, 2016 WL 5341749, at *1 (S.D. Ill. Sept. 23, 2016).

199. *Id.* at *2.

200. *Id.* (citing *Clapper*, 133 S. Ct. at 1147 & n.5).

201. *Flynn*, 2016 WL 5341749 at *2.

202. *Id.*; *see also* Cahen v. Toyota Motor Corp., 147 F. Supp. 3d 955, 958 (N.D. Cal. 2015) (dismissing plaintiffs' automotive cybersecurity class action against GM and Toyota because plaintiffs failed to satisfy present injury requirements).

203. *See* Bryant Walker Smith, *Automated Driving and Product Liability*, 2017 MICH. ST. L. REV. 1, 44 (2017) (describing the dismissed class actions against automakers and suggesting "these claims foreshadow some of the technical and legal issues that could accompany the combination of increasing automation and increasing connectivity").

barriers.[204] However, the third barrier remains unscaled. Faced with the first cybersecurity tort case involving physical injuries, courts must devote considerable time to crafting a new duty and standard of care for cybersecurity. This Article attempts to lay the groundwork for that endeavor.

V. SCALING THE FINAL BARRIER

A. Duty

"Duty is central to the law of torts."[205] A legal duty to exercise care may be imposed by both common law and statutes.[206] Presently, the scope of negligence liability for autonomous vehicle manufacturers is untested and unclear. Where statutes may come up short, common law principles can adapt to future and emerging technologies. In the common law context, the theories of where a duty originates are well-documented, often injecting philosophy, social customs, and natural law.[207] And an automobile manufacturer's duty to consumers is well-established. According to the Restatement (Second), comment i:

> [T]he manufacturer of an automobile, intended to be driven on the public highway, should reasonably expect that, if the automobile is dangerously defective, harm will result to any person on the highway, including pedestrians and drivers of other vehicles and their passengers and guests; and he should also expect danger to those upon land immediately abutting on the highway.[208]

Although the Restatement (Second)'s drafters, in 1965, likely did not contemplate self-driving automobiles, the duty of care owed by an autonomous vehicle manufacturer persists to a wide variety of

---

204. This Article does not offer a proposal for cases, often class actions, in which there are no physical injuries or property damage. For an analysis in the analogous data breach context, *see* Daniel Bugni, *Standing Together: An Analysis of the Injury Requirement in Data Breach Class Actions*, 52 GONZ. L. REV. 59, 60 (2017).

205. David Owen, *Duty Rules*, 54 VAND. L. REV. 767, 767 (2001).

206. Vincent R. Johnson, *Cybersecurity, Identity Theft, and the Limits of Tort Liability*, 57 S.C. L. REV. 255, 263–64 (2005).

207. *See* Owen, *supra* note 205, at 767.

208. RESTATEMENT (SECOND) OF TORTS § 395, cmt. i (1965) (comment entitled "[p]ersons endangered by use").

persons.[209] The foreseeability doctrine raises the most significant question to whether an autonomous vehicle manufacturer will owe a duty to plaintiffs injured by cybersecurity flaws.

B. Foreseeability and Third-Party Criminal Acts

The scope of a duty "depends on the relationship to plaintiffs, whether plaintiffs were within a zone of foreseeable harm, and whether the harm was within the class of reasonably foreseeable hazards that the duty exists to prevent."[210] Foreseeability is a liability limitation.[211] Over the years, courts have employed an expansive or restrictive approach to foreseeability.[212] At the duty level, the foreseeability function should be distinguished from proximate cause.[213] For instance, foreseeability should be assessed on a categorical basis, rather than delving into the particular facts of each case.[214]

In modern tort law, both individuals and companies may reasonably assume that third parties will not commit intentional criminal acts upon innocent parties.[215] However, a duty may arise in extraordinary circumstances.[216] There is no legal presumption in the

---

209. *See, e.g.*, Gourdine v. Crews, 955 A.2d 769, 782 (Md. 2008) (duty "is an essential element" of plaintiff's negligence claim for failure to warn); Satterfield v. Breeding Insulation Co., 266 S.W.3d 347, 355 (Tenn. 2008) ("duty has become an essential element of all negligence claims"); Hamilton v. Beretta U.S.A. Corp., 750 N.E.2d 1055, 1060 (N.Y. 2001) (this is "[t]he threshold question in any negligence action").

210. In re Sept. 11 Litigation, 280 F. Supp. 2d 279, 295 (S.D.N.Y. 2003) (citing Sanchez v. State of New York, 784 N.E.2d 675, 678 (N.Y. 2002)).

211. 1 OWEN & DAVIS ON PROD. LIAB. § 2:9 (4th ed. 2016) (foreseeability is not a basis of liability).

212. *See* Owen, *supra* note 205, at 774–77.

213. *See* Owen, *supra* note 205, at 777–78.

214. *See* Owen, *supra* note 205, at 777–78.

215. *See* Perry v. S.N., 973 S.W.2d 301, 306 (Tex. 1998) ("At common law there is generally no duty to protect another from the criminal acts of a third party or to come to the aid of another in distress."); RESTATEMENT (SECOND) OF TORTS § 302B, cmt. d ("Normally the actor has much less reason to anticipate intentional misconduct than he has to anticipate negligence. In the ordinary case he may reasonably proceed upon the assumption that others will not interfere in a manner intended to cause harm to anyone. This is true particularly where the intentional conduct is a crime, since under ordinary circumstances it may reasonably be assumed that no one will violate the criminal law."); *see also* Gaines–Tabb v. ICI Explosives USA, Inc., 995 F. Supp. 1304 (D. Okla. 1996) (holding that fertilizer and blasting cap manufacturers were not liable for Murrah Federal Building bombing, as they were entitled to believe that third parties would not engage in intentional criminal conduct).

216. *See* James v. Meow Media, Inc., 300 F.3d 683, 694 (6th Cir. 2002).

context of third-party criminals—the issue requires an ordinary balancing of the risk.[217] Factors to be considered are: (a) the "known character, past conduct, and tendencies" of the third party; (b) the "temptation or opportunity" to act in misconduct; (c) the severity of the potential resulting harm; and (d) the possibility that some other person will assume the responsibility for preventing the conduct or the harm. These factors are considered with the burden of safeguarding against these risks.[218]

Suppose cyber criminals infiltrate and control hundreds of connected automobiles from a remote location. On balance, these factors should give rise to a duty of care in this context. In balancing the foreseeability factors, the "known character, past conduct, and tendencies"[219] of cybersecurity hacks on private corporations are highly prevalent.[220] Also, new software-driven technology certainly creates greater opportunity and vulnerabilities.[221] As Professor Rustad alludes, cyber terrorists continuously focus on "soft targets."[222] Connected components in autonomous vehicles, as modernly constructed, create accessible avenues for cyberattacks.[223] Thirdly, the severity of harm risked by remote control of autonomous vehicles is enormous.[224]

When determining whether cyberattacks on autonomous vehicles are foreseeable to create a duty, the Southern District of New York's decision in *In re September 11 Litigation* is instructive.[225] In *In re September 11 Litigation*, the court addressed whether the scope of

---

217. RESTATEMENT (SECOND) OF TORTS § 302B, cmt. f (1965). As explained in the Restatement Second, "stat[ing] definite rules as to when the actor is required to take precautions against intentional or criminal misconduct" is impossible.

218. *Id.*

219. *Id.*

220. *See* Kesan & Hayes, *supra* note 69, at 450 ("In 2002, the Computer Security Institute of San Francisco compiled statistics with the FBI indicating that ninety percent of surveyed companies had their computer security breached.").

221. RUSTAD, *supra* note 18, at 486 ("The failure to implement reasonable cybersecurity poses great risks to our networked society. Increasingly, the world's infrastructure is software-driven and networked which creates new vulnerabilities.").

222. *Id.*

223. Glancy, *supra* note 67, at 664 (explaining that current controls in autonomous vehicles "suggests serious risk of criminal mischief" by hackers); K.C. Webb, *Products Liability and Autonomous Vehicles: Who's Driving Whom?*, 23 RICH. J.L. & TECH. 9, 65 (2017) ("[H]acking is a foreseeable risk, the consequences of which are potentially catastrophic.").

224. *See* Kohler & Colbert-Taylor, *supra* note 24, at 133 (suggesting cyberattacks on autonomous vehicles could potentially cause mass harm on the scale of the 9/11 terrorist attacks).

225. 280 F. Supp. 2d at 295.

duty was foreseeable to "ground victims" that lost their lives and suffered physical injury as a result of the terrorists attacks on September 11th.[226] The airline security companies argued that the terrorist attack was not reasonably foreseeable to create a duty because "terrorists had not previously used a hijacked airplane as a suicidal weapon to destroy buildings and murder thousands."[227] The court rejected this argument, explaining that "[i]n order to be considered foreseeable, the precise manner in which the harm was inflicted need not be perfectly predicted."[228] The court held the airplane crashes were "within the class of foreseeable hazards resulting from negligently performed security screening."[229] Further, the court explained:

> While it may be true that terrorists had not before deliberately flown airplanes into buildings, the airlines reasonably could foresee that crashes causing death and destruction on the ground was a hazard that would arise should hijackers take control of a plane. The intrusion by terrorists into the cockpit, coupled with the volatility of a hijacking situation, creates a foreseeable risk that hijacked airplanes might crash, jeopardizing innocent lives on the ground as well as in the airplane.[230]

Also, the court rejected a similar argument by Boeing, the airplane manufacturer, and held that Boeing had a similar duty as a matter of law.[231] *In re September 11 Litigation* clearly shows the potentially expansive application of the foreseeability doctrine as it relates to third-party criminal acts.[232] The foreseeability determination for a duty of care is analogous when third-party cyber criminals act from a remote location, being physically absent from the scene of the incident. Similar to *In re September 11 Litigation*, in the duty context,

---

226. *See id.* at 295.
227. *Id.*
228. *Id.*
229. *Id.* at 296.
230. *Id.*
231. *In re Sept. 11 Litig.*, 280 F. Supp. 2d at 307. Ultimately, six years later, the wrongful death actions in *In re September 11 Litigation* were settled. *See In re* Sept. 11 Litig., 600 F. Supp. 2d 549 (S.D.N.Y. 2009).
232. Elaine D. Solomon & Dina L. Relles, *Criminalization of Air Disasters: What Goal, If Any, Is Being Achieved?*, 76 J. AIR L. & COM. 407, 444 n.218 (2011).

cyberattacks on autonomous vehicles should be foreseeable as a matter of law.[233]

As Professor Owen explains, the duty determination is not a mechanism for judges to decide "how wide or narrow the law of negligence should be based upon their personal predilections."[234] Although cyberattacks on automobiles are a recent phenomenon, the nature of cyberattacks is certainly a risk manufacturers reasonably contemplate. Once plaintiffs prove the automotive manufacturer has a duty to exercise reasonable care in security, the next issue is setting the standard of care.

VI. TOWARDS AN AUTOMOTIVE CYBERSECURITY STANDARD OF CARE

A cybersecurity standard of reasonableness is a new and evolving concept, especially in the automotive industry. Constructing a cybersecurity standard of care may be difficult for courts due to the "ever-changing nature of the problem and sheer number of actors involved."[235] Nevertheless, when faced with the task, courts may rely on well-established tort principles to construct a workable and effective standard of care. Recently, Professor Bryant Walker Smith, one of the leading scholars in automation, suggested cybersecurity vulnerabilities in motor vehicles could lead to "expanded tort duties and higher standards of reasonable care."[236] This Article goes further by suggesting the standard of care should be based on the physical attributes of the motor vehicle, particularly whether the manufacturer is designing limited or fully automated vehicles.

As detailed below, the standard of care autonomous vehicle manufacturers owe to consumers and passengers should depend on the vehicle's level of automation. Specifically, the standard of care should turn on whether the vehicle can be manually controlled by the

---

233. However, proximate cause may wield a different result under a fact-specific foreseeability analysis. At this stage, addressing a proximate cause analysis may be overly speculative since intervening and superseding cause questions are highly uncertain. *See* Montgomery Elevator Co. v. McCullough, 676 S.W.2d 776, 779 (Ky. 1984) ("There is no area of tort law that has generated more confusion than the question of superseding or intervening cause . . . where the claim is based on products liability.").

234. Owen, *supra* note 205, at 777.

235. Scott J. Shackelford, et. al., *Toward A Global Cybersecurity Standard of Care?: Exploring the Implications of the 2014 NIST Cybersecurity Framework on Shaping Reasonable National and International Cybersecurity Practices*, 50 TEX. INT'L L.J. 305, 312 (2015); s*ee also* RUSTAD, *supra* note 18, at 480 (suggesting formulating a duty is the most difficult element to prove in "cybertort" cases).

236. Smith, *supra* note 203, at 51.

human driver or whether the vehicle is fully self-driving. If the autonomous vehicle can be manually overridden, the standard of care for designing cybersecurity components should be reasonable ordinary care. In contrast, if the autonomous vehicle does not have a manual override function, manufacturers should be held to the heightened standard of utmost reasonableness.

A. Expert in the Field

Both limited autonomous vehicle manufacturers and full self-driving vehicle manufacturers will be held to the level of an expert in their particular field.[237] The "expert in the field" standard requires manufacturers to be well-acquainted with scientific knowledge, technical discoveries, and devices used by others in the trade.[238] A manufacturer, with respect to the specific product it purposefully markets and produces, is "presumed to be an expert in the field in which it has chosen to do business."[239] The "expert in the field" doctrine weighs an actor's conduct against that of a reasonable manufacturer that is an expert in manufacturing that particular type of product.[240]

Through connected and autonomous vehicle developments, automotive manufacturers have entered the internet-based technology arena. Thus, manufacturers will be required to stay informed on evolving automotive cybersecurity developments.[241] This will require traditional automobile manufacturers, such as Ford and

---

237. *See, e.g.*, Alcala v. Emhart Industries, Inc., 495 F.3d 360, 364 (7th Cir. 2007) ("[T]he jury may presume that the manufacturer has the skill and knowledge that other manufacturers at the time possessed."); O'Hare v. Merck & Co., 381 F.2d 286, 291 (8th Cir. 1967) ("A manufacturer is held to the skill of an expert in its particular field of endeavor, and is obligated to keep informed of scientific knowledge and discoveries concerning that field."); Guffie v. Erie Strayer Co., 350 F.2d 378 (3rd Cir. 1965) (manufacturer is held to the standard of an expert in regards to its own product).

238. *See* Huggins v. Stryker Corp., 932 F. Supp. 2d 972, 987 n.14 (D. Minn. 2013) ("A manufacturer is held to the skill of an expert in its particular field of endeavor, and is obligated to keep informed of scientific knowledge and discoveries concerning that field.").

239. 1 OWEN & DAVIS ON PROD. LIAB. § 2:8 (4th ed. 2016).

240. *See* Trull v. Volkswagen of America, Inc., 320 F.3d 1, 8 (1st Cir. 2002) (reasonable "automobile manufacturer").

241. One relevant limitation to defectiveness is the "state of the art" defense. The "state of the art" defense is a developing doctrine, and definitions vary widely across jurisdictions. *See* 2 OWEN & DAVIS ON PROD. LIAB. § 10:12 (4th ed. 2016) ("In products liability law, 'state of the art' is an unrefined concept whose meaning and role continue to evolve."). If adopted by the relevant jurisdiction, "state of the art" may deserve the court's attention as a defense.

GM, to stay abreast of cybersecurity technology developed by internet-savvy manufacturers, such as Google and Uber. The necessary care required of manufacturers to implement such evolving automotive cybersecurity measures will depend on the nature of the autonomous vehicle.

B. Determining Due Care in Automotive Cybersecurity Cases

In products liability cases premised on negligence, most courts apply an all-encompassing standard of care that is defined simply as "reasonable" or "ordinary" care.[242] Some courts refine these reasonableness principles to specific product manufacturers.[243] Other courts further refine the standard prevailing in that particular product industry.[244] Moreover, in premise liability cases, courts have simply employed a "reasonable security" standard of care.[245] By a similar token, if an automotive manufacturer owes a duty to keep its occupants safe in the event of foreseeable cyberattacks, the question remains: what is "reasonable cybersecurity?"

Reason requires the type and amount of care to be determined by the "magnitude of the risk" measured against the particular costs of precautions that may have prevented the risk.[246] "[M]agnitude of the risk" includes the "type, likelihood, and degree of harm."[247] This

---

242. *See e.g.*, Weigle v. SPX Corp., 729 F.3d 724, 734 (7th Cir. 2013) (defective design sounding in negligence "must establish that the manufacturer or seller failed to exercise reasonable care under the circumstances in designing the product"); *Stahlecker v. Ford Motor Co.*, 667 N.W.2d 244, 253 (Neb. 2003) (in a products liability negligence action, the issue is "whether a manufacturer's conduct was reasonable in view of the foreseeable risk of injury").

243. *See, e.g.*, Nichols v. Union Underwear Co., 602 S.W.2d 429, 433 (Ky. 1980) (in a negligence action, the standard was "a prudent manufacturer exercising ordinary care"); Back v. Wickes Corp., 378 N.E.2d 964, 971 (Mass. 1978) (explaining "standard of the ordinary, reasonably prudent manufacturer in like circumstances . . . was a correct statement of the law.").

244. *See, e.g.*, Alcala v. Emhart Indus., Inc., 495 F.3d 360, 365 (7th Cir. 2007) (under Illinois law, the question is whether "the defendant deviated from the standard of care that other manufacturers in the industry followed at the time the product was designed"); Sumnicht v. Toyota Motor Sales, U.S.A., Inc., 360 N.W.2d 2, 17 (Wis. 1984) (conformity of "design to the practices of other manufacturers in its industry at the time of manufacture").

245. *See* Farooq ex rel. Estate of Farooq v. MDRB Corp., 498 F. Supp. 2d 284, 287 (D.D.C. 2007) (deciding whether defendant's acts or omission met the standard of care for reasonable security); *see also* McClung v. Wal-Mart Stores, Inc., 270 F.3d 1007, 1011 (6th Cir. 2001) (reversing summary judgment because whether Wal–Mart had a duty to provide reasonable security presented a jury question).

246. *See* 1 OWEN & DAVIS ON PROD. LIAB. § 2:10 (4th ed. 2016).

247. *Id.*

method of balancing is known as calculus of risk, or the Hand Formula, which Judge Learned Hand most famously articulated in *United States v. Carroll Towing Co.*[248] In *Carroll*, Judge Learned Hand simplified his formula by "designating likelihood of injury as probability, seriousness of injury as loss and the interest sacrificed burden."[249] Recently, Professor Rustad offered a Hand Formula-based approach in the cybersecurity context.[250] Professor Rustad suggests the "best analytical approach" for creating a new standard of care should ask "whether the burden of a comprehensive security solution is less than the magnitude of the damages caused by lost or stolen data, multiplied by the probability of occurrence."[251] This is a sound rendition of the Hand Formula applied to data breach cases.[252] A similar Hand Formula-based approach can prove workable in the automotive cybersecurity context. However, one important difference is the "magnitude of risk."

Potential risks in data breach cases relate primarily to economic or financial losses. In automotive cybersecurity cases, however, hackers may gain access to an automobile's primary driving functions and cause serious physical harm to the vehicle's occupant and to many others on the road. The magnitude of potential harm from a hacked autonomous navigation system differs depending on whether the vehicle's occupant can override the hacked autonomous system and take manual control of the vehicle. If not, then the hackers will be able to wreak unmitigated havoc on the road as long as the hacked vehicle can move, with the hapless occupant of the vehicle helpless to do anything other than endure the ride. Thus, in constructing a standard of care for designing cybersecurity components in autonomous vehicles, courts will look to the vehicle's level of automation.

---

248. 159 F.2d 169, 173 (2d Cir. 1947); *see also* William M. Landes & Richard A. Posner, THE ECONOMIC STRUCTURE OF TORT LAW 85–86 (1987) (suggesting calculus of risk had "long been used to decide negligence cases" and "Hand was purporting only to make explicit what had long been the implicit meaning of negligence").

249. Lawrence A. Cunningham, *Traditional Versus Economic Analysis: Evidence from Cardozo and Posner Torts Opinions*, 62 FLA. L. REV. 667, 676 (2010). It is worth noting that the Hand Formula's seemingly rigorous framework concentrates on social wealth or utility maximization, which could come at the "expense of other values tort law may advance."

250. RUSTAD, *supra* note 18, at 483–84.

251. *Id.*

252. In data breaches, hackers access a company's computer network system to intercept or steal data, such as financial or personal information.

1. Limited Autonomous Vehicles and Reasonable Care

Automotive manufacturers should be held to a standard of reasonable care in designing cybersecurity functions if the vehicle at issue, according to the NHTSA's classifications,[253] operates on a level of automation between Level 0 (No Automation) and Level 3 (Limited Self-Driving Automation). Although "reasonableness" is easily stated in the abstract, this standard will operate within traditional risk-utility factors. In determining whether a design was reasonable, risk-utility factors generally assess relevant compliance with federal regulations; design choices to install or change certain components; the manufacturer's knowledge of the dangerous condition; whether an alternative design was available on the market; whether that alternative design was cost effective; and several other broad examinations into the design process.[254] Cybersecurity-related risks in autonomous vehicles, as illustrated below, vary depending on the designed level of automation.

Suppose, in the spring of 2027, Sarah's 2026 Ford Fusion is driving her in automation mode from Dallas to Houston for business. Meanwhile, in the basement of an abandoned warehouse, a band of intelligent hackers are launching a remote hack they had been planning for weeks. Their goal is to gain access through a vulnerable ECU and send a 3,500 pound machine down the wrong way of Interstate 45. Suddenly, the radio in Sarah's car goes silent. Sarah immediately clicks the volume button three times to no avail. A few seconds later, Sarah's car abruptly veers from the right lane to the left lane and hits a mid-sized sedan, causing both cars to spin out into the grass median. While Sarah is still in shock, holding her broken arm, she notices her car is continuing to accelerate across the grass median heading towards oncoming traffic. Promptly, Sarah opts for manual override—cutting off all automated functions. Sarah is able to take back control and manually stop her car before it heads into oncoming traffic.

Sarah brings a products liability action against Ford Motor Company, specifically for design defects in Ford Fusion's ECUs and cybersecurity components. The court, as a matter of first

253. *U.S. Dep't of Transp.*, *supra* note 40.
254. *See* Kysar, *supra* note 103, at 1709.

impression,[255] is faced with determining a standard of care applied to Ford Motor Company in designing cybersecurity components in its 2026 Ford Fusion. After determining that the Ford Fusion had manual override, the court should apply a standard of reasonableness.[256] But what is reasonable in designing cybersecurity components?

In shaping reasonableness for negligent design, courts rightly look to statutory and regulatory compliance. NHTSA's September 2016 guidance, explained in Part II of this Article, relates to design, development, and testing of automated vehicles. The guidance documents state that manufacturers should develop cybersecurity software based on a "systems-engineering approach."[257] This approach includes: continuous safety assessment; design implications consistent with the uniform transportation system; and risk management recovery programs to ensure immediate response to cybersecurity events.[258] Additionally, the September 2016 guidance explained that autonomous vehicle manufacturers should "appl[y] appropriate functional safety and cybersecurity best practices."[259]

Best practices relate to industry standards and custom. Similarly, from the famous *T.J. Hooper* case, industry practice or custom is compelling—but not conclusive—evidence of reasonableness, since the industry as a whole may fail to adopt adequate procedures.[260] Certainty, whether the manufacturer breached this duty of care will be highly fact-intensive to the particular circumstances. However, in

---

255. The fact that this hypothetical case arises in 2026 is for argument's sake only. I do not offer an estimation as to when the first automotive cybersecurity case will arise because it is impossible to estimate when cyberattacks will occur.

256. *See* 5 Star, Inc. v. Ford Motor Co., 759 S.E.2d 139, 141 (S.C. 2014); *see also* Bilotta v. Kelley Co., 346 N.W.2d 616, 626 n.2 (Minn. 1984) ("The manufacturer has a duty to use due care to design a product that does not create an unreasonable risk of harm.").

257. *Federal Automated Vehicles Policy: Accelerating the Next Revolution in Roadway Safety*, U.S. DEP'T OF TRANSP. (Sept. 2016) at 21, https://www.transportation.gov/sites/dot.gov/files/docs/AV%20policy%20guidance%20PDF.pdf.

258. *Id.*

259. *Id.* at 13.

260. *See* The T.J. Hooper, 60 F.2d 737, 740 (2d Cir. 1932) ("[I]n most cases reasonable prudence is in fact common prudence; but strictly it is never its measure; a whole calling may have unduly lagged in the adoption of new and available devices. It never may set its own tests . . . . Courts must in the end say what is required; there are precautions so imperative that even their universal disregard will not excuse their omission."); *see also* Trautman, *supra* note 135, at 242–43 (Discussing the Heartland breach, explaining Heartland had been "certified by network-approved quality security assessors . . . and, in fact received this certification several times during the period in which the vulnerability had been present").

the event a plaintiff occupied a full self-driving car, proving breach may be less demanding if the self-driving car manufacturer is held to the highest level of care.

2. Full Self-Driving Vehicles Require a Heightened Standard of Care

Remote hijacking of full self-driving cars poses risks that require the highest level of care. In the past, consumers have reasonably expected that automobile manufacturers would design a car that is safe for them to drive. In the near future, consumers will have to trust that automobile manufacturers will design a car that is safe to drive them. In situations where a human occupant elects to switch from manual to autonomous mode, this higher level of trust requires a higher level of care. Full self-driving cars, without any kind of manual control, naturally necessitates full confidence and trust in the driverless vehicle itself. This full and complete trust requires the highest level of care. Thus, the standard of care an automotive manufacturer should owe to protect consumers from cyberattacks on full self-driving cars should be one of utmost care.

Utmost care is the highest degree of due care.[261] Courts generally require utmost care for common carriers.[262] The primary reason that courts have required utmost care for common carriers is that the passengers of common carriers are fully dependent on the carrier—they must fully trust the carrier for safe transport.[263] In these situations, utmost care is required because of the one-sided control one party has in the activity and the essential trust by the other party.[264] In *Railroad Co. v. Lockwood*, the United States Supreme Court imposed this heightened standard of care based on three considerations: (1) the unequal footing of the parties, (2) the passenger's lack of control, and (3) the carrier's obligation to the public.[265]

---

261. Davis, *supra* note 167, at 1272.

262. *See, e.g.*, Am. Orient Exp. Ry. Co., LLC v. Surface Transp. Bd., 484 F.3d 554, 557 (D.C. Cir. 2007); USAir Inc. v. U.S. Dep't of Navy, 14 F.3d 1410, 1413 (9th Cir. 1994); Markwell v. Whinery's Real Estate, Inc., 869 P.2d 840, 841 (Okla. 1994) (requiring common carriers to "exercise the utmost care for the safety of their passengers").

263. Davis, *supra* note 167, at 1225. Trust is the "assured reliance on the character, ability, strength, or truth of someone or something." MERRIAM-WEBSTER'S ONLINE DICTIONARY (Jan. 31, 2017), https://www.merriam-webster.com/dictionary/trust.

264. N.Y., N. H. & H. R. Co. v. Nothnagle, 346 U.S. 128, 136 (1953); Davis, *supra* note 167, at 1225.

265. 84 U.S. 357, 379–81 (1873).

Self-driving cars will inevitably require a higher level of trust from consumers. Full self-driving cars, on NHTSA's 5-Part classification chart, fall within Level 4, the highest level of automation.[266] Under Level 4, "[s]uch a design anticipates that the driver . . . is not expected to be available for control at any time during the trip."[267] Currently, Google and Ford plan to construct self-driving vehicles without steering wheels or pedals.[268] In an effort to shape future regulations, Google wrote the NHTSA to urge the Agency not to require steering wheels or essential driving devices in self-driving cars because, as Google suggests, such self-driving vehicles will be safer without human intervention.[269] However, in the event of foreseeable cyberattacks, passengers may face uncontrollable danger when a vehicle lacks manual override.

Recall, in the hypothetical above, Sarah was able to thwart the cyberattack by switching into manual driving mode and escaped with only a broken arm. Suppose now that Sarah's 2026 Ford Fusion is a full self-driving car with no steering wheel or brake pedal. After Sarah spins out in the median, the remote hackers continue to accelerate her car towards oncoming traffic. The hackers are successful in their malicious act of terrorism, causing mass injuries, casualties, and havoc on Interstate 45.

Undoubtedly, once hackers gain access to an autonomous vehicle, damages will be amplified if a driver cannot take back manual control. This higher and more serious degree of risk requires a heightened standard of care. When a vehicle is fully self-driving, without the option for human control, the sheer trust occupants will have in the vehicle itself creates a special relationship that requires utmost care. Whether an autonomous vehicle manufacturer ultimately breached the duty of utmost care will be a question reserved for the trier of fact.[270] As evidence is produced and juries render decisions,

---

266. *See supra* note 40 and accompanying text.

267. *Id.*

268. Jacob D. Walpert, *Carpooling Liability?: Applying Tort Law Principles to the Joint Emergence of Self-Driving Automobiles and Transportation Network Companies*, 85 FORDHAM L. REV. 1863, 1869 (2017).

269. For a discussion on Google's suggestions and the NHTSA's responses, see Jerry L. Mashaw, David L. Harfst, *From Command and Control to Collaboration and Deference: The Transformation of Auto Safety Regulation*, 34 YALE J. ON REG. 167, 268 (2017). Of course, if Google's assertions are to be believed, there may be other risks involved in including a manual override. However, a full risk-benefit analysis on that particular issue is outside the scope of this Article.

270. *See* Markwell v. Whinery's Real Estate, Inc., 869 P.2d 840, 841 (Okla. 1994) ("The determination of what constitutes "utmost care" . . . is a question to be resolved by the trier of fact."); Parlato v. Conn.Transit, 434 A.2d 322, 323 (Conn. 1980) ("Strictly

manufacturers will likely curtail their efforts to responsibly protect consumers against foreseeable cyberattacks.[271]

CONCLUSION

Cybersecurity measures must take priority in emerging autonomous vehicle technology. In the seminal products liability case *MacPherson v. Buick*, Justice Cardozo distinguished automobile cases "from the days of travel by stage coach."[272] But he then stated the tort "principle . . . does not change, but the things subject to the principle do change. They are whatever the needs of life in a developing civilization require them to be."[273] In a software-driven world, cybersecurity protections are a need of developing society. If cybersecurity measures continue as a second-rate concern for the automotive industry, established tort principles will bring those concerns to light.

Self-driving and autonomous vehicles will undoubtedly reduce traditional automobile crashes, however, increased connectivity ushers in the legitimate threat of cyberattacks. This Article provides a framework through the lens of well-established tort principles for courts and litigants to approach emerging challenges and hurdles in automotive cybersecurity cases. In determining the applicable standard of care, courts should draw a distinction between limited autonomous vehicles and self-driving cars without manual override. In the former, automotive manufacturers should use a high degree of reasonable care under the circumstances. In full self-driving vehicles, consumers will be required to fully trust in the vehicle itself to protect

---

speaking, a conclusion of negligence is ordinarily one of mixed law and fact, involving the determination of the standard of care required and its application to the facts of the particular case . . . if there is room for a reasonable disagreement the question is one to be determined by the trier as matter of fact.").

271. For a current suggestion: Technology experts suggest that, to sufficiently protect against cyberattacks, automotive manufacturers must hire hackers, such as Miller and Valasek, the white-hat hackers that gained remote control of the 2014 Jeep Cherokee. *See* Andy Greenberg, *5 Lessons from the Summer of Epic Car Hacks*, WIRED (Oct. 8, 2015), 2, https://www.wired.com/2015/10/five-car-hacking-lessons-we-learned-this-summer/. Miller, over the last few years, has worked with autonomous vehicle manufacturers such as Uber and Didi, a Chinese company emerging in the autonomous vehicle industry. Andy Greenberg, *Securing Driverless Cars from Hackers is Hard. As the Ex-Uber Guy Who Protects Them*, WIRED (Apr. 12, 2017), https://www.wired.com/2017/04/ubers-former-top-hacker-securing-autonomous-cars-really-hard-problem/. According to Miller, "now's the time to work on the problem . . . before cars become more automated and make the problem far more real."

272. 111 N.E. 1050, 1051 (N.Y. 1916).

273. *Id.*

them from cyber intrusions, which necessitates a standard of utmost care. The common carrier relationship is most like the relationship between driverless cars and passengers because the one-sided control the carrier has and reliance on the vehicle itself. Self-driving cars will demand the passenger's complete trust to safely drive and protect him or her from foreseeable dangers. Both proposed standards of care will prove malleable and workable as automotive cybersecurity measures advance. In the eyes of tort law, automation and connectivity components are merely new bells and whistles on traditional products. Technology has undoubtedly evolved over the past century and products liability law will continue to prove it is capable to handle the complications presented by this automated technology.