Santa Clara Law Review

Volume 60 | Number 1 Article 6

5-6-2020

THE SELF DRIVE ACT: AN OPPORTUNITY TO RE- LEGISLATE A MINIMUM CYBERSECURITY FEDERAL FRAMEWORK FOR AUTONOMOUS VEHICLES

Green, Alexandra

THE SELF DRIVE ACT: AN OPPORTUNITY TO RE-LEGISLATE A MINIMUM CYBERSECURITY FEDERAL FRAMEWORK FOR AUTONOMOUS VEHICLES

*Alexandra Green**

"Hacking" began as a concept where individuals used their technical skills to improve computers. Over time, however, the term hacking has become associated with hackers gaining unauthorized access to manipulate systems with malicious intent. Autonomous vehicles have the ability to produce a vast amount of in-vehicle, environment, and driver and passenger data. This data ranges from acceleration records to GPS information. Legislators and leaders in the auto manufacturing industry have concerns about the risk of hackers gaining access and manipulating autonomous vehicles' systems and networks, which could lead to detrimental harms on consumers. At the time of writing this Note, there continues to be a lack of federal legislation and regulation to protect consumers' safety in connection with autonomous vehicles.

This Note discusses the background of The Safely Ensuring Lives Future Deployment and Research in Vehicle Evolution Act ("SELF DRIVE Act"), a bill that died in Congress. This Note will address how the SELF DRIVE Act was designed to ensure the safety of autonomous vehicles with respect to the design, construction, and performance within their deployment and testing. To understand the background of the SELF DRIVE Act, it is also critical to be aware of the history of self-driving cars, how hacking has advanced over the years, and best practices within security and privacy. Finally, this Note proposes how the seven foundational principles of Security by Design can help form a minimum cybersecurity federal framework in autonomous vehicles.

* B.A., University of Washington, 2015. J.D., Santa Clara University School of Law, 2020.

TABLE OF CONTENTS

I. Introduction 218
II. Background 221
A. The SELF DRIVE Act 221
B. Who is NHTSA? 222
C. History of Self-Driving Cars 223
D. Hacking in General 226
E. Security Vulnerabilities in Self-Driving Cars 228
F. Security by Design 230
1. Proactive not Reactive; Preventative not Remedial 231
2. Default Setting 232
3. Embedded into Design 233
4. Positive-Sum 234
5. End-to-End Security 234
6. Visibility and Transparency 236
7. Respect for the User 237
III. Identification of Legal Problem 237
IV. Analysis 238
A. Current Flaws of the SELF DRIVE Act 239
B. The Benefits for Manufacturers of a Federal Framework 240
C. State Concerns Raised by a Federal Framework 241
D. Soft Law and Best Practices under NHTSA 242
V. Proposal 244
A. Proactive not Reactive; Preventative not Remedial 244
B. Default Setting 245
C. Embedded into Design 245
D. Positive Sum 247
E. End-to-End Security 248
F. Visibility and Transparency 250
G. Respect for the User 251
VI. Conclusion 251

I. INTRODUCTION

Imagine a scenario, from the not too distant future in which you are riding in a self-driving vehicle[1] and hackers seize control of your vehicle while taking you to an unknown location.[2] The hackers then torture you for ransom by disabling your windows and locking the door, while

1. "Self-driving" and "highly automated" vehicles are defined as "a motor vehicle equipped with an automated driving system; and does not include a commercial motor vehicle." "Automated driving system" is defined as "the hardware and software that are collectively capable of performing the entire dynamic driving task on a sustained basis, regardless of whether such system is limited to a specific operation design domain." SELF DRIVE Act, H.R. 3388, 115th Cong. § 13(a)(1)(B), § 13(a)(1)(C)(7) (2017) [hereinafter SELF DRIVE Act].

2. Joe Queenan, *When Hackers Take Over Self-Driving Cars*, WALL STREET J. (Aug. 10, 2016), https://www.wsj.com/articles/when-hackers-take-over-self-driving-cars-1470845413.

interfering with your radio or heat settings.[3] Autonomous vehicles are predicted to "be at least as vulnerable to all the existing security threats that regularly disrupt our computer networks."[4] In fact, in 2015 a pair of hacker-activists ("hacktivists") seized control over an Internet-connected Jeep Cherokee that was going 70 mph.[5] The hacktivists demonstrated how they could control the vehicle's car radio and ventilation system, as well as the braking and transmission system, which led to the vehicle stalling on a highway.[6]

In the development and manufacture of self-driving cars, cybersecurity[7] research tends to be overlooked.[8] In addition to threats and vulnerabilities for traditional vehicles generally, harms unique to self-driving cars are emerging as technology advances to automated mobility.[9] Besides hackers having the possibility of seizing control of vehicles and demanding ransom, there are also "security threats to the wide-ranging networks that will connect with automated vehicles, from financial networks that process tolls and parking payments to roadway sensors, cameras and traffic signals to the electricity grid and our personal home networks."[10] Building technological systems without exploitable errors and vulnerabilities is practically impossible for complex network-connected systems; thus, an entire system could be compromised by a single mistake.[11] So, although self-driving vehicles represent a revolutionary improvement to transportation, this improvement also introduces risks

3. *Id.* Researchers at University of Michigan's autonomous vehicle center MCity have designed and "operate[] the world's first purpose-built proving ground for testing the performance and safety of connected and automated vehicles and technologies under controlled and realistic conditions." *Mcity Test Facility*, MCITY, https://mcity.umich.edu/our-work/mcity-test-facility/ (last visited Apr. 1, 2020).

4. André Weimerskirch & Derrick Dominic, *Assessing Risk: Identifying and Analyzing Cybersecurity Threats to Automated Vehicles* 1 (U. Mich. White Paper, 2018), https://mcity.umich.edu/wp-content/uploads/2017/12/Mcity-white-paper_cybersecurity.pdf (noting that this "could include data thieves who want to glean personal and finance information, spoofers who present incorrect information to a vehicle, and denial-of-service attacks that move from shutting down computers to shutting down cars.").

5. *Id.* at 6; *see also infra* Section II.E.

6. Weimerskirch & Dominic, *supra* note 4, at 6.

7. Cybersecurity is defined as "the art of protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information." *What is Cybersecurity?*, CISA, https://www.us-cert.gov/ncas/tips/ST04-001 (last updated Nov. 14, 2019).

8. Weimerskirch & Dominic, *supra* note 4, at 1.

9. *Id.* at 2.

10. *Id.*

11. *Id.* at 2, 7. For example, the idea of an automated vehicle, which is "within 15 minutes of your home and automatically turns on your furnace or air conditioner, opens the garage and unlocks your front door" is not threatening and acts as a convenience. However, "[a]ny hacker who can breach that vehicle system would be able to walk right in and burglarize your home." *Id.* at 2.

from hackers manipulating and gaining access to these highly automated systems.[12]

Congress has proposed, but failed to pass, legislation designed to promote passenger safety in self-driving vehicles. The Safely Ensuring Lives Future Deployment and Research in Vehicle Evolution Act ("SELF DRIVE Act"),[13] the first major bill to contain policies for regulating autonomous vehicles, stayed in the U.S. Senate for about two years and recently died in Congress.[14] The SELF DRIVE Act's primary goal was to establish a federal framework for regulation of autonomous vehicles.[15]

This Note first discusses the background and status of the SELF DRIVE Act, National Highway Traffic Safety Administration ("NHTSA"), self-driving vehicles, hacking, and Security by Design. Next, this Note identifies the legal problem surrounding an absence of federal legislation in vehicle cybersecurity. Finally, this Note analyzes the legal problem and proposes how the seven foundational principles of Security by Design can help form a minimum cybersecurity federal framework in self-driving cars.[16]

---

12. In 2015, some industry leaders, like Elon Musk, predicted that fully autonomous vehicles were two to three years away from being in wide use. *See, e.g.*, Fred Lambert, *Tesla CEO Elon Musk Drops His Prediction of Full Autonomous Driving from 3 Years to Just 2*, ELECTREK (Dec. 21, 2015), https://electrek.co/2015/12/21/tesla-ceo-elon-musk-drops-prediction-full-autonomous-driving-from-3-years-to-2/; Jeff McMahon, *Autonomous Vehicles Arrive in 3 Years, in 3 Stages*, FORBES (Sept. 28, 2015), https://www.forbes.com/sites/jeffmcmahon/2015/09/28/autonomous-vehicles-arrive-in-3-years-in-3-stages/#54c8e57116b4. However, autonomous vehicles appear to have stalled in the United States because of road hazards, media coverage about an autonomous vehicle striking and killing a woman on a street, a lack of investment, and state law obstacles. Jeff McMahon, *The 4 Reasons Autonomous Vehicles Seem Stalled in the U.S.*, FORBES (Jan. 27, 2020), https://www.forbes.com/sites/jeffmcmahon/2020/01/27/the-4-reasons-autonomous-vehicles-seem-to-have-stalled-in-the-us/#45ce9e0f2fe6; *see also* Daisuke Wakabayashi, *Self-Driving Uber Car Kills Pedestrian in Arizona, Where Robots Roam*, N.Y. TIMES (Mar. 19, 2018), https://www.nytimes.com/2018/03/19/technology/uber-driverless-fatality.html.

13. SELF DRIVE Act, *supra* note 1.

14. R. Nicholas Englund & Christopher Grigorian, *Congress Taking Another Look at Regulating Automated Driving Systems*, JD SUPRA (Sept. 10, 2019), https://www.jdsupra.com/legalnews/congress-taking-another-look-at-51054/; *Issues in Autonomous Vehicle Testing and Deployment*, CONG. RES. SERV. 14-18 (Nov. 27, 2019), https://fas.org/sgp/crs/misc/R45985.pdf; *H.R. 3388 (115th): SELF DRIVE Act*, GOVTRACK, https://www.govtrack.us/congress/bills/115/hr3388 (last updated Oct. 18, 2017); Colin McCormick, *What's in the SELF DRIVE Act?*, MEDIUM (Sept. 25, 2017), https://medium.com/@cfmccormick/whats-in-the-self-drive-act-6c090e8a2e9a.

15. Sean O'Kane, *The US is speeding toward its first national law for self-driving* cars, THE VERGE (Sept. 6, 2017, 4:41 PM), https://www.theverge.com/2017/9/6/16259170/self-drive-act-autonomous-cars-legislation.

16. I use the terms "self-driving" and "autonomous" synonymously. Additionally, this Note discusses current and developing technology in autonomous vehicles.

II. BACKGROUND

The purpose of the SELF DRIVE Act was to create a federal framework for regulation of autonomous vehicles in order to increase vehicle safety. To understand some of the reasoning behind the introduction of this legislation, Part II will briefly explain NHTSA's connection to automobile cybersecurity as well as the history of self-driving vehicles and their security vulnerabilities. Furthermore, since Congress failed to pass the SELF DRIVE Act, this Note will explain the seven principles of Security by Design prior to analyzing and proposing how federal legislation regarding autonomous vehicles could be improved.

A. The SELF DRIVE Act

The SELF DRIVE Act was introduced in the U.S. House by Representative Robert E. Latta on July 25, 2017.[17] On September 6, 2017, the SELF DRIVE Act unanimously passed in the House Committee on Energy and Commerce 54-0.[18] The SELF DRIVE Act was subsequently received by the Senate and referred to the Committee on Commerce, Science, and Transportation.[19] However, the Committee did not present the SELF DRIVE Act to the full Senate for a vote, prior to its expiration at the end of the 115th Congress.[20] The purpose of the SELF DRIVE Act "is to memorialize the Federal role in ensuring the safety of highly automated vehicles as it relates to design, construction, and performance, by encouraging the testing and deployment of such vehicles."[21] The SELF DRIVE Act also continues to give NHTSA power to be the agency responsible for regulation of safety within the design, construction, and performance of autonomous vehicles.[22]

Section Five of the SELF DRIVE Act, entitled "Cybersecurity of Automated Driving Systems," focused solely on a "cybersecurity plan."[23] The proposed bill stated: "[a] manufacturer may not sell, offer for sale, introduce or deliver for introduction into commerce, or import into the United States, any highly automated vehicle, vehicle that performs partial driving automation, or automated driving system unless

17. SELF DRIVE Act, *supra* note 1.

18. *Id.*

19. *Id.*

20. GOVTRACK, *supra* note 14. The 115th Congress was in session from 2017-2019. *Id.* The 116th Congress is in session from 2019-2021. *116th United States,* BALLOTPEDIA, https://ballotpedia.org/116th_United_States_Congress (last visited Jan. 15, 2020).

21. SELF DRIVE Act, *supra* note 1, at § 2.

22. Ashley Coker, *House committee urges Senate to advance self-driving vehicle legislation*, FREIGHTWAVES (Sept. 10, 2018), https://www.freightwaves.com/news/house-committee-urges-senate-to-advance-self-driving-vehicle-legislation.

23. SELF DRIVE Act, *supra* note 1, at § 5.

such manufacturer has developed a cybersecurity plan."[24] It further prescribes that a manufacturer's cybersecurity plan must include "[a] written cybersecurity policy with respect to the practices of the manufacturer for detecting and responding to cyber attacks, unauthorized intrusions, and false and spurious messages and malicious vehicle control commands."[25]

The cybersecurity policy must include "a process for identifying, assessing, and mitigating reasonably foreseeable vulnerabilities from cyber attacks or unauthorized intrusions, including false and spurious messages and malicious vehicle control commands" and a procedure "for taking preventative and corrective action to mitigate against vulnerabilities in a vehicle that [is highly automated or] performs partial driving automation, including incident response plans, intrusion detection and prevention systems that safeguard key controls . . . and procedures through testing or monitoring."[26] The other required elements of the cybersecurity plan are "[t]he identification of an officer or other individual of the manufacturer as the point of contact with responsibility to the management of cybersecurity," "[a] process for limiting access to automated driving systems," and "[a] process for employee training and supervision for implementation and maintenance of the policies and procedures required by [Section 5], including controls on employee access to automated driving systems."[27]

B. Who is NHTSA?

Congress and the U.S. federal government have attempted to actively monitor the deployment of self-driving vehicles in the United States.[28] Specifically, NHTSA, under the U.S. Department of Transportation, focuses on automobile cybersecurity.[29] NHTSA promotes cybersecurity by regulating wireless and wired vehicle entry points, which have potential vulnerabilities to a cyberattack.[30] Under the SELF DRIVE Act, Congress delegated NHTSA with the responsibility of writing safety, cybersecurity, and privacy policies for autonomous vehicles

24. *Id.* at § 5(a).
25. *Id.* at § 5(a)(1).
26. *Id.* at § 5(a)(1)(A)-(B).
27. *Id.* at § 5(a)(2)-(4).
28. Mark Schaub & Atticus Zhao, *Cybersecurity: Achilles' Heel for Self-driving Cars?*, CHINA L. INSIGHT (Feb. 9, 2018), https://www.chinalawinsight.com/2018/02/articles/corporate/cybersecurity-achilles-heel-for-self-driving-cars/.
29. *Id.*
30. *Vehicle Cybersecurity*, NAT'L HIGHWAY TRAFFIC SAFETY ADMIN., https://www.nhtsa.gov/technology-innovation/vehicle-cybersecurity (last visited Jan. 31, 2019).

because NHTSA is America's "relevant expert safety agency."[31] However, NHTSA has a troubling "history when it comes to putting the interests of the American people first," and safety advocates have taken the NHTSA to court multiple times to force the agency to do the agency's job.[32] Some of the issues have included "forcing auto manufacturers to issue complete recalls and sufficient remedies and requiring companies to implement widely available safety technology, such as seat belts, air bags, electronic stability control, roof crush protection and automatic emergency brakes."[33] These issues indicate how a lack of leadership within the government and a focus on profits can disrupt progress.[34] For instance, "[r]oughly 41.6 million vehicles equipped with 56 million defective Takata air bags are under recall because these air bags can explode when deployed, causing serious injury or even death."[35]

C. History of Self-Driving Cars

The idea of self-driving cars has "gone from science fiction fantasy to road-bound reality."[36] These cars are the result of a slow and incremental development process spanning nearly a century. Inventor Francis Houdina, not the magician Harry Houdini, first drove through the streets without a person at the steering wheel in a radio-controlled car in 1925.[37] This radio-controlled car could "start its engine, shift gears, and sound its horn, 'as if a phantom hand were at the wheel.'"[38] At an exhibit at New York World's Fair in 1939, Norman Bel Geddes built an electric vehicle that was "guided by radio-controlled electromagnetic fields

31. Jason Levine, *Americans are right not to trust self-driving cars*, WASH. POST (Sept. 18, 2017), https://www.washingtonpost.com/opinions/americans-are-right-not-to-trust-self-driving-cars/2017/09/18/3490e066-9a3e-11e7-b569-3360011663b4_story.html?noredirect=on&utm_term=.66ed92707f0a.

32. *Id.*

33. *Id.*

34. *Id.*

35. *Takata Recall Spotlight,* NAT'L HIGHWAY TRAFFIC SAFETY ADMIN., https://www.nhtsa.gov/equipment/takata-recall-spotlight (last visited Jan. 31, 2019); *see also* Levine, *supra* note 31. The Takata recall has affected many automaker companies including Honda and Ford. *Takata Airbag Recall: Everything You Need to Know*, CONSUMER REPORTS, https://www.consumerreports.org/car-recalls-defects/takata-airbag-recall-everything-you-need-to-know/ (last updated Mar. 29, 2019).

36. Luke Dormhel & Stephen Edelstein, *Sit back, relax, and enjoy a ride through the history of self-driving cars*, DIGITAL TRENDS (Oct. 28, 2019, 6:09 PM), https://www.digitaltrends.com/cars/history-of-self-driving-cars-milestones/.

37. *Id.*; *see also* Jenn U, *The Road to Driverless Cars: 1925-2025*, ENGINEERING.COM (July 15, 2016), https://www.engineering.com/PLMERP/ArticleID/12665/The-Road-to-Driverless-Cars-1925—2025.aspx.

38. Dormehl & Edelstein, *supra* note 36.

generated with magnetized metal spikes embedded in the roadway."[39] In 1950s through the 1960s, General Motors created and showcased vehicles, where "[t]he car's front end was embedded with sensors called pick-up coils that could detect the current flowing through a wire embedded in the road. The current could be manipulated to tell the vehicle to move the steering wheel left or right."[40]

John McCarthy, a founding father of artificial intelligence, wrote an essay in 1969 that proposed creating an "automatic chauffeur," which would permit the user to enter information through a keyboard allowing the car to be capable of getting a user to their destination, stopping at a restroom or restaurant, and changing speeds.[41] Even though this vehicle was not built yet, McCarthy created a framework for future researches to embark towards.[42] As technological innovation continued, self-driving vehicles continued to advance in their "ability to detect and react to their environment."[43] In 1977, Japan-based Tsukuba Mechanical first implemented McCarthy's vision by "using a camera system that relayed data to a computer to process images of the road" but with a maximum speed of only 20 miles per hour ("mph").[44] A German engineer, Ernst Dickmanns, later refined the technology by using cameras in front of and behind a Sedan to detect objects on the road while increasing the maximum speed to 56 mph.[45]

Research into camera-enabled automation continued as computers became more capable and sophisticated. In 1992, Carnegie Mellon University (CMU) researcher Dean Pomerlau wrote a thesis "describing how neural networks could allow a self-driving vehicle to take in raw images from the road and output steering controls in real time."[46] By 1995, Pomerlau and his co-researcher, Todd Jochem, drove their self-driving system on the road.[47] Pomerleau's and Jochem's autonomous minivan, for which steering was automated but drivers manually

39. Bonnie Gringer, *History of the Autonomous Car*, TITLEMAX, https://www.titlemax.com/resources/history-of-the-autonomous-car/ (last visited Jan. 31, 2019).

40. *Id.*; *see also* Bradley Walker, *The timeline of automation*, HERE 360 (Oct. 5, 2017), https://360.here.com/the-timeline-of-automation.

41. JOHN MCCARTHY, COMPUTER CONTROLLED CARS 1-2 (Mar. 29, 1996), http://jmc.stanford.edu/commentary/progress/cars.pdf. Dormehl & Edelstein, *supra* note 36.

42. *Id. See also* Cade Metz, *John McCarthy – Father of AI and Lisp – Dies at 84*, WIRED (Oct. 24, 2011), https://www.wired.com/2011/10/john-mccarthy-father-of-ai-and-lisp-dies-at-84/.

43. Gringer, *supra* note 39.

44. *Id.*; *see also* Walker, *supra* note 40.

45. Gringer, *supra* note 39.

46. *See generally* DEAN A. POMERLEAU, NEURAL NETWORK PERCEPTION FOR MOBILE ROBOT GUIDANCE (Carnegie Mellon U., 1992), https://apps.dtic.mil/dtic/tr/fulltext/u2/a249972.pdf. Dormehl & Edelstein, *supra* note 36.

47. Dormehl & Edelstein, *supra* note 36.

controlled the vehicle's speed and braking, travelled "2,797 miles coast-to-coast from Pittsburg, Pennsylvania to San Diego, California."[48]

Then, Google began developing its secret self-driving vehicle project designated "Waymo" in 2009.[49] After a few years, Google announced that the autonomous cars in this project had "collectivity driven 300,000 miles under computer control without one single accident."[50] By 2013, several well-known automotive companies had begun working on self-driving vehicle technologies.[51] In 2018, Nvidia announced Xavier, which is "the world's first processor designed for autonomous driving."[52] Nvidia also announced the company's partnership with Volkswagen to connect artificial intelligence to hardware that is production ready.[53] Not only could this lead to stronger performance of self-driving vehicles, but it could also lead to the development of features like digital assistants.[54] Currently, Tesla notes that all of the vehicles produced in their factory have the hardware that is essential for full autonomous capability at a safety level significantly greater than that of human drivers.[55]

In June 2019, more than 1,400 autonomous vehicles were in testing by about eighty companies in thirty-six states plus Washington, D.C. across the nation.[56] Due to safety features, many vehicles currently on the road are deemed to be semi-autonomous.[57] These safety features include assisted parking and braking systems. However, only a few

48. *Id.*; *see also* Steve Crowe, *Back to the Future: Autonomous Driving in 1995*, ROBOTICS BUS. REV. (Apr. 3, 2015), https://www.roboticsbusinessreview.com/slideshow/back_to_the_future_autonomous_driving_in_1995/.

49. *See* WAYMO, https://waymo.com (last visited Apr. 3, 2020); *see also* Dormehl & Edelstein, *supra* note 36.

50. Rebecca J. Rosen, *Google's Self-Driving Cars: 300,000 Miles Logged, Not a Single Accident Under Computer Control*, ATLANTIC (Aug. 9, 2012), https://www.theatlantic.com/technology/archive/2012/08/googles-self-driving-cars-300-000-miles-logged-not-a-single-accident-under-computer-control/260926/.

51. Examples include General Motors, Ford, Mercedes Benz, and BMW. *See* Dormehl & Edelstein, *supra* note 36.

52. *Nvidia Drive AGX*, NVIDIA, https://www.nvidia.com/en-us/self-driving-cars/drive-platform/hardware/ (last visited Apr. 3, 2020); *see also* Gary Hicok, *Making the Grade: NVIDIA Xavier Achieves Another Milestone for Safe Self-Driving*, NVIDIA BLOG (Nov. 13, 2018), https://blogs.nvidia.com/blog/2018/11/13/xavier-milestone-safe-self-driving/.

53. *Volkswagen and NVIDIA to Infuse AI into Future Vehicle Lineup*, NVIDIA NEWSROOM (Jan. 7, 2018), https://nvidianews.nvidia.com/news/volkswagen-and-nvidia-to-infuse-ai-into-future-vehicle-lineup.

54. Dormehl & Edelstein, *supra* note 36.

55. *See Autopilot*, TESLA, https://www.tesla.com/autopilot?redirect=no (last visited Jan. 27, 2019).

56. *What's Happening with Automated* Vehicles, SENATE RPC (July 31, 2019), https://www.rpc.senate.gov/policy-papers/whats-happening-with-automated-vehicles.

57. Gringer, *supra* note 39.

vehicles "have the capability to drive, steer, brake, and park themselves."[58] Both auto manufacturers and technology companies are investing in autonomous vehicles, even though the technology is far from perfect, for the purpose of eliminating human error and reducing crashes.[59] Other benefits include efficient fuel consumption, time efficiency, monitoring of traffic, space savers, and safer streets.[60]

D. Hacking in General

The term "hacker" tends to carry a negative connotation, describing digital thieves and harmful viruses scattered in cyberspace.[61] Computer hackers, however, were originally seen as "technology enthusiasts who wanted nothing more than to optimize, customize and tinker."[62] However, once viruses and cybercrime began, "white hat hackers" and "black hat hackers" were not always distinguished.[63]

The term "hack" originated in 1961 when club members of Massachusetts Institute of Technology's Tech Model Railroad Club hacked the club's high-tech train sets for the purpose of modifying their functions.[64] This group then went from modifying toy trains to computers, aiming to broaden the utility of computers.[65] Then, once the general public had

---

58. *Id.*

59. *See* Keith Noonan, *What Does the Future Hold for Self-Driving Cars?*, THE MOTLEY FOOL, https://www.fool.com/investing/what-does-the-future-hold-for-self-driving-cars.aspx (last updated Oct. 18, 2019).

60. *See 5 benefits of autonomous cars*, GEMALTO (July 21, 2017), https://www.gemalto.com/review/Pages/5-benefits-of-autonomous-cars.aspx.

61. Tripwire Guest Authors, *The Evolution of Hacking*, TRIPWIRE (Aug. 17, 2016), https://www.tripwire.com/state-of-security/security-data-protection/cyber-security/the-evolution-of-hacking/; *see also Are All Hackers Bad?*, MCAFEE (Sept. 2, 2014), https://www.mcafee.com/blogs/consumer/identity-protection/are-all-hackers-bad/; *see also* Ben Yagoda, *A Short History of "Hack"*, THE NEW YORKER (Mar. 6, 2014), https://www.newyorker.com/tech/annals-of-technology/a-short-history-of-hack.

62. Tripwire Guest Authors, *supra* note 61.

63. *Id.* A "white hat hacker" is a hacker who carries out ethical hacking, which means a hacker who utilizes their computer and technological skills to determine vulnerabilities within an information system. *See White Hat vs. Black Hat Hackers and the Need for Ethical Hacking*, CLEARPATH IT SOLUTIONS, https://www.clearpathit.com/white-hat-vs-black-hat-hackers-and-the-need-for-ethical-hacking (last visited Apr. 3, 2020). Whereas a "black hat hacker" uses their knowledge with malicious intent to break into information systems while bypassing privacy and security protocols. *See What is the Difference Between Black, White and Grey Hat Hackers?*, NORTON SECURITY, https://us.norton.com/internetsecurity-emerging-threats-what-is-the-difference-between-black-white-and-grey-hat-hackers.html (last visited Apr. 3, 2020).

64. Tripwire Guest Authors, *supra* note 61; *see also* ERIC S. RAYMOND, THE CATHEDRAL & THE BAZAAR 4 (rev. ed. 2001).

65. Tripwire Guest Authors, *supra* note 61. Later in the 1970s, a new set of hackers called Phreakers arose and began modifying the telephone network to place long distance calls for free. *Id.*; *see also Definition of phreaker*, MERRIAM-WEBSTER, https://www.merriam-webster.com/dictionary/phreaker (last visited Apr. 3, 2020).

access to personal computers for their own purposes, there was a vast change and increase in the hacking community.[66] During this decade, a different classification of hacker developed that was motivated by personal gain.[67] Rather than hackers "using their technological know-how for improving computers, they used it for criminal activities, including pirating software, creating viruses and breaking into systems to steal sensitive information."[68] Congress responded in 1986 with the Federal Computer Fraud and Abuse Act, the first legislation directed against cyber criminals.[69] In 1990, many hackers were arrested and convicted for activities such as "stealing propriety software from big name corporations, duping radio stations to win luxury cars, launching the first computer worm, and leading the first digital bank heist."[70] These activities continued in the 2000s with newer and more harmful types of hacks, which targeted government entities and well-established businesses.[71]

---

66. Tripwire Guest Authors, *supra* note 61; *see also* Kim Ann Zimmermann, *History of Computers: A Brief Timeline*, LIVE SCIENCE (Sept. 7, 2017), https://www.livescience.com/20718-computer-history.html.

67. Tripwire Guest Authors, *supra* note 61.

68. *Id.* For example, in 1984, the global credit information corporation, which is now named Experian, was hacked leading to 90 million records being stolen. Ernie Hayden, *Data Breach Protection Requires New Barriers*, SEARCHSECURITY, https://searchsecurity.techtarget.com/feature/Data-breach-protection-requires-new-barriers (last visited Apr. 3, 2020). Additionally, there was a group of computer hackers, known as "The 414s," who gained unauthorized access to computer systems at the Los Alamos National Laboratory in New Mexico, several Milwaukee-area schools, and a major international bank system in Los Angeles. Timothy Winslow, *I Hacked Into a Nuclear Facility in the '80s. You're Welcome*, CNN BUS. (May 3, 2016), https://www.cnn.com/2015/03/11/tech/computer-hacker-essay-414s/index.html; *see also* Jake Kirchner, *Hackers Steal Legislators' Attention*, COMPUTERWORLD (Sept. 12, 1983), https://www.computerworld.com/article/2523544/hackers-steal-legislators—attention.html.

69. 18 U.S.C. § 1030 (1986).

70. Tripwire Guest Authors, *supra* note 61. Prior to becoming the CEO for his security consulting company, Kevin Mitnick was one of the most famous hackers. He hacked into the computers and networks of over forty major corporations. *About Kevin Mitnick*, MITNICK SECURITY, https://www.mitnicksecurity.com/about-kevin-mitnick-mitnick-security (last visited Apr. 5, 2020). Kevin Poulsen also became a famous hacker for gaining unauthorized access to a Los Angeles radio station and manipulating the phone lines to win a Porsche. *How Kevin Poulsen Became One of the World's Best Cybersecurity Hackers*, APPKNOX, https://www.appknox.com/blog/kevin-poulsen-worlds-best-cybersecurity-hackers (last visited Apr. 5, 2020). *See also The Morris Worm: 30 Years Since First Major Attack on the Internet*, FBI (Nov. 2, 2018), https://www.fbi.gov/news/stories/morris-worm-30-years-since-first-major-attack-on-internet-110218 (discussing how Robert Morris spread the Internet's first worm virus and infected numerous universities and research centers). In the mid-1990s, Vladimir Levin manipulated Citibank's computers and distributed about ten million dollars to him and his accomplices located in different countries. *See generally Notable Hacks*, PBS FRONTLINE, https://www.pbs.org/wgbh/pages/frontline/shows/hackers/whoare/notable.html (last visited Apr. 5, 2020) (describing other notable hacks from 1988-2000).

71. *See* PBS FRONTLINE, *supra* note 70 (explaining how a sixteen-year-old computer hacker pled guilty to fifty-six charges for distributing denial of service attacks against companies like Yahoo, eBay, CNN, and Amazon, leading to damages estimated at $1.7 billion).

For instance, a fifteen-year-old boy breached the systems of the Department of Defense and International Space Station.[72]

Hackers continue to increase the sophistication and complexity of their activities.[73] Recent hacking activities include "releasing highly classified documents, exposing government secrets and leading vigilante digital crusades in the name of defending the public from being harmed, exploited, or withheld information."[74] Therefore, government entities and enterprises are attempting to improve cybersecurity and modify their systems in reaction to various types of hackers.[75] However, hackers, good and bad, also continue to evolve and have managed to stay one step ahead.[76]

E. Security Vulnerabilities in Self-Driving Cars

Hacking a vehicle is an attempt "to gain unauthorized access to vehicle systems for the purpose of retrieving driver data or manipulating

72. Catherine Wilson, *15-Year-Old Admits Hacking NASA Computers*, ABC NEWS (Jan. 7, 2006), https://abcnews.go.com/Technology/story?id=119423&page=1 (explaining how the hacker caused a shutdown of NASA computers for twenty-one days and "invaded a Pentagon weapons computer system to intercept 3,300 e-mails, steal passwords and cruise around like an employee.").

73. *See* Adam Bradley, *Hackers Are Raising Their Game. Their Targets Need To Do The Same*, FORBES (Feb. 6, 2019), https://www.forbes.com/sites/adambradley1/2019/02/06/hackers-are-raising-their-game-their-targets-need-to-do-the-same/#489f9f1e22a2 (describing how hackers are "going to great lengths to craft hand-delivered, highly-targeted ransomware attacks").

74. Tripwire Guest Authors, *supra* note 61. For instance, on September 12, 2019, a hacker accessed 218 million records of customers who installed iOS and Android versions of Zynga games. *See generally* Megan Leonhardt, *The 5 Biggest Data Hacks of 2019*, CNBC MAKE IT (Dec. 17, 2019), https://www.cnbc.com/2019/12/17/the-5-biggest-data-hacks-of-2019.html (summarizing how hackers have accessed about 8 billion records in 2019 allowing hackers to gain access to personal, financial, and medical information). More recently, in 2020, more than "10.6 million guests who have stayed at the MGM Resorts have had their personal information posted on a hacking forum. The data dump exposed includes names, home addresses, phone numbers, emails, and dates of birth of former hotel guests." *See also* Steve Turner, *2020 Data Breaches: The Worst So Far*, IDENTITYFORCE, https://www.identityforce.com/blog/2020-data-breaches (last visited Apr. 5, 2020). Additionally, in January 2020, "[t]he FBI announced that nation state hackers had breached the networks of two U.S. municipalities in 2019, exfiltrating user information and establishing backdoor access for future compromise." *Significant Cyber Incidents*, CSIS, https://www.csis.org/programs/technology-policy-program/significant-cyber-incidents (last visited Apr. 5, 2020).

75. Tripwire Guest Authors, *supra* note 61. *See generally* FED. TRADE COMMISSION, START WITH SECURITY (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (consisting of ten lessons that companies and the government can learn from the Federal Trade Commission's data security settlements).

76. *Id.*; *see also SecureData: Leading the Cybersecurity Evolution*, SECUREDATA, https://www.secdata.com/securedata-leading-the-cybersecurity-evolution/ (last visited Apr. 5, 2020).

vehicle functionality."[77] A modern vehicle "has 50 to 150 electronic control units (ECUs)," which are like tiny computers, with each vehicle having "as much as 100 million lines of code."[78] There are as many as fifteen bugs for every 1,000 lines and such bugs can create vulnerabilities that can be exploited by hackers.[79]

Self-driving vehicles "will produce data related to in-vehicle, environmental, and driver/passenger information."[80] This data will contain "historical data, such as vehicle fluid levels, speed and acceleration, GPS positioning and, in the event of an accident, a snapshot of data prior to the crash as well as alerts for first responders."[81] Driver and passenger data will also include data about driving styles, seat preferences, and usage of infotainment systems.[82]

Hackers have the ability to infiltrate into systems to access unauthorized information, steak bank details, manipulate government websites and numerous other monstrous acts.[83] However, hacking has recently reached new levels; hackers can now target vehicles and use these vehicles like weapons.[84] As more autonomous cars are produced, "hackers could target fleets of cars" where these "fleets [are] comprised of 100s of cars with each car individually having over a 100 million lines of code and all collectively connected and exchanging data."[85] Therefore, significant vulnerability and risk exists in autonomous vehicles, which leaves cybersecurity as a central challenge.[86]

A pertinent example occurred in 2015.[87] Automobile manufacturer Chrysler announced a recall of 1.4 million vehicles when a pair of hackers, Charlie Miller and Chris Valasek, demonstrated their ability to remotely hijack the digital systems of a Jeep through the Internet.[88] The two reported their research of the hack to Chrysler for the company to

77. *Vehicle Cybersecurity*, U.S. DEP'T OF TRANSP., https://www.safercar.gov/Vehicle-Shoppers/Safety-Technology/cybersecurity (last visited Jan. 31, 2019).

78. Lucas Mearian, *Your car will eventually live-stream video of your driving to the cloud*, COMPUTERWORLD (Apr. 28, 2017, 10:40 AM), https://www.computerworld.com/article/3193209/car-tech/your-car-will-eventually-live-stream-video-of-your-driving-to-the-cloud.html; *see also* Schaub & Zhao, *supra* note 28.

79. Mearian, *supra* note 78.

80. *Id.*

81. *Id.*

82. *Id.*

83. Schaub & Zhao, *supra* note 28.

84. *Id.*

85. *Id.*

86. *Id.*

87. *Id.*; *see also* Andy Greenberg, *The Jeep Hackers are Back to Prove Car Hacking Can Get Much Worse*, WIRED (Aug. 1, 2016, 3:30 PM), https://www.wired.com/2016/08/jeep-hackers-return-high-speed-steering-acceleration-hacks/.

88. *Id.*

fix the vehicle's errors, but they offered a serious lesson to the auto industry: the hack could have been, and in the future could be, much worse.[89]

Miller and Valasek compromised the Jeep through a vulnerability in the vehicle's Internet-connected entertainment system called Uconnect.[90] Uconnect was flawed because the system permitted anyone with the vehicle's IP address to obtain access throughout the United States.[91] The two researchers were "then able to send commands to the engine and wheels through the car's internal Controller Area Network (CAN)."[92] Control of the steering column, electronic brakes, parking assistance, and adaptive cruise control are all handled by the ECUs.[93] Other hackers and security researchers have also demonstrated their capability to remotely hack self-driving vehicles by taking control of essential car functions, like braking and acceleration.[94]

F. Security by Design

Ann Cavoukian, creator of Global Privacy and Security by Design, is a well-known leader in the privacy field.[95] Cavoukian served as the Information & Privacy Commissioner in Ontario, Canada.[96] While in this position, she founded Privacy by Design[97], which is "a framework that seeks to proactively embed privacy into the design specifications of information technologies, networked infrastructure and business practices, thereby achieving the strongest protection possible."[98] Privacy by

89. *Id.* Since Miller and Valasek disclosed their research to Chrysler, "the dangerous attacks can no longer be accomplished remotely and require physical access to the targeted vehicle. However, just imagine if it hadn't been white hat hackers who had uncovered the original flaws, that the security vulnerability had never been patched, and that malicious attackers were not able to crash cars and cause automobile accidents remotely?" Graham Cluley, *Car Hacking at Speed – Where Vulnerabilities Turn from Critical to Fatal*, WELIVESECURITY (Aug. 2, 2016), https://www.welivesecurity.com/2016/08/02/car-hacking-speed-vulnerabilities-turn-critical-fatal/.

90. Fahmida Y. Rashid, *Hacker History: The Time Charlie and Chris Hacked a Jeep Cherokee*, DECIPHER (May 25, 2018), https://duo.com/decipher/hacker-history-time-charlie-chris-hacked-jeep-cherokee.

91. *Id.*

92. A "CAN bus carries information between the vehicle's various electronic control units (ECU) to the central controller." *Id.*

93. *Id.*

94. Schaub & Zhao, *supra* note 28.

95. *About Us*, GPS BY DESIGN CTR., https://gpsbydesigncentre.com/about-us/ (last visited Jan. 31, 2019).

96. *Id.*

97. Ann Cavoukian, *Privacy by Design: The 7 Foundational Principles*, INTERNET ARCHITECTURE BOARD, https://iab.org/wp-content/IAB-uploads/2011/03/fred_carter.pdf (last visited Jan. 31, 2019) [hereinafter Cavoukian, *Privacy*].

98. GPS BY DESIGN CTR., *supra* note 95.

Design became recognized as an international standard in 2010.[99] Cavoukian subsequently helped define "Security by Design," which is "a set of foundational . . . principles that are modelled upon and support the 7 foundational principles of *Privacy by Design*."[100] The seven foundation principles include: (1) Proactive not Reactive; Preventative not Remedial; (2) Default Setting; (3) Embedded into Design; (4) Positive-Sum; (5) End-to-End Security; (6) Visibility and Transparency; and (7) Respect for the User.[101]

1. Proactive not Reactive; Preventative not Remedial

Historically, companies have responded to cybersecurity threats and harms through a reactive process.[102] According to Cavoukian and Dixon, with the ever-increasing frequency and sophistication of cybersecurity attacks, companies should construct "a security-minded culture" by being proactive and preventative when doing business.[103] Under this principle, a change is necessary in the "state of mind" of the enterprise.[104] This change begins with leadership of the company and then continues throughout the enterprise.[105] Rather than responding to imminent threats with just tactical actions, this will involve taking a strategic assessment.[106] Enterprises "need to take the strategic, proactive viewpoint, rather than the reactive, tactical one, defining what . . . security posture should be for an enterprise, and build upon that foundation."[107]

---

99. *Id.* The General Data Protection Regulation (GDPR), a European Union regulation, requires companies to implement Privacy by Design to be accountable for data privacy during the data collection and processing lifecycle. *See* Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), art. 25, 2016 O.J. (L 119) 78. *See also Privacy by Design GDPR*, PRIVACY TRUST, https://www.privacytrust.com/gdpr/privacy-by-design-gdpr.html (last visited Jan. 17, 2020).

100. Ann Cavoukian & Mark Dixon, *Privacy and Security by Design: An Enterprise Architecture Approach*, INFO. & PRIVACY COMMISSIONER OF ONTARIO 3 (2013), https://www.ipc.on.ca/wp-content/uploads/Resources/pbd-privacy-and-security-by-design-oracle.pdf.

101. *Id.* at 6.

102. *Id.* at 10. "Reactive business strategies are those that respond to some unanticipated event only after it occurs, while proactive strategies are designed to anticipate possible challenges." Scott Thompson, *Difference Between a Protective & Reactive Business Strategy*, HOUSTON CHRON., https://smallbusiness.chron.com/difference-between-proactive-reactive-business-strategy-62157.html (last updated Jan. 25, 2019).

103. Cavoukian & Dixon, *supra* note 100, at 10.

104. *Id.*

105. *Id.*

106. *Id.*

107. *Id.* Thompson, *supra* note 102 ("Proactive strategies are superior because they allow the company using th[is] strategy the freedom to make its own decisions rather than responding out of necessity to a situation that already may be out of control. Companies that use

2. Default Setting

Default setting, also known as "Secure by Default," is a principle "that covers policies for implementing security controls and specific methods for installing and configuring software."[108] The aim of this concept is to ensure configuration of information systems to be strongly secure by default, rather than improving security once the software is in the user's hands.[109] This "means that the initial setup or installation of a system contains a minimal set of software configured to the most secure settings as possible."[110] Default setting requires that users only have access to systems, programs, and data that are necessary to perform a particular task.[111]

Examples of these limiting policies to help with data minimization involve Least Privilege, Need-To-Know, Least Trust, Mandatory Access Control, and Segregation of Duties.[112] Least Privilege and Need-To-Know helps entities limit access to the minimum resources and information that are necessary for an individual to perform its function.[113] Least Trust is when an information system is designed in a way to limit "the number of components that require trust, and . . . the extent to which each component is trusted."[114] Mandatory Access Control means entities can "restrict[] access to objects based on the sensitivity of the information contained in the objects and the formal authorization (i.e., clearance, formal access approvals and need-to-know) of subjects to access

proactive strategies have a better chance of seizing and retaining the initiative in the competition with other companies.").

108. *Id.* at 11. *See also* Steven Kenny, *The Importance of Secure by Default*, AXIS COMM. (Feb. 25, 2019), https://www.axis.com/blog/secure-insights/the-importance-of-secure-by-default/. *See, e.g.*, Larry Anderson, *Secure By Default: New Standard for Surveillance Products In the United Kingdom*, SECURITYINFORMED, https://www.securityinformed.com/insights/secure-by-default-surveillance-product-standard-united-kingdom-co-227-ga-co-289-ga-co-1151-ga-co-3425-ga-co-13220-ga-sb.1562585086.html (last visited Apr. 5, 2020) (showing how companies like Hanwha Techwin use Secure by Default as a cybersecurity measure within cameras and recording devices).

109. Cavoukian & Dixon, *supra* note 100, at 11.

110. *Id.*

111. *Id.*; *see also* Nate Lord, *What is the Principle of Least Privilege (POLP)? A Best Practice for Information Security and Compliance*, DIGITAL GUARDIAN (Sept. 12, 2018), https://digitalguardian.com/blog/what-principle-least-privilege-polp-best-practice-information-security-and-compliance.

112. Cavoukian & Dixon, *supra* note 100, at 11-12.

113. *Id.* at 11. *See also* Bianca Soare, *What is the Principle of Least Privilege?*, HEIMDAL SECURITY, https://heimdalsecurity.com/blog/what-is-the-principle-of-least-privilege/ (last updated Nov. 14, 2019). Least Privilege and Need-To-Know are nearly synonymous, but Need-To-Know applies to people, whereas Least Privilege applies to processes. Cavoukian & Dixon, *supra* note 100, at 11.

114. Cavoukian & Dixon, *supra* note 100, at 11.

information of such sensitivity."[115] Segregation of Duties is when an entity separates specific areas of responsibilities and tasks with the goal of limiting fraud and unintentional mistakes.[116]

3. Embedded into Design

According to Cavoukian and Dixon, embedding security into the design of a system constructs a secure system.[117] Security can be embedded into the design of a system through both the software and hardware of a system.[118] Software Security Assurance is defined as "[t]he process of ensuring that software is designed to operate at a level of security that is consistent with the potential harm that could result from the loss, inaccuracy, alteration, unavailability, or misuse of the data and resources that it uses, controls, and protects."[119] The Software Security Assurance process seeks to reduce the risk of security vulnerabilities entering the information system lifecycle during the definition, development, deployment and maintenance progression.[120] Embedding security within the design of secure systems on the hardware side involves the "Trusted Platform Module (TPM)."[121] TPMs "provide hardware support for key management. They are computer chips (microcontrollers) with a finite storage capacity to store key material and certificates in a secure manner on the motherboard of computing devices and are based on open standards."[122] TPMs add an additional layer of security within the cryptographic and authentication services of an information system by protecting they key from being manipulated or stolen by software based threats, such as malware.[123] To successfully protect users of a service involving software and hardware, every standard and process must be embedded with security.[124]

115. *Id.* at 12.

116. *Id.* For example, an employee that accepts cash and check payments should be separated from the task of making bank deposits as well as reconciling bank statements. *Id. See also Segregation of Duties*, ACCOUNTINGTOOLS (Apr. 10, 2018), https://www.accountingtools.com/articles/segregation-of-duties.html.

117. Cavoukian & Dixon, *supra* note 100, at 12.

118. *Id.*

119. *Id.*

120. *Id.* at 13.

121. *Id.* at 14. The Trusting Computing Group, which is an international industry standards group, developed TPM "as a technology used to shift the baseline of trust within a system from the software to the hardware." *Id.*

122. *Id.* at 14. "Embedding key material and certificates into the hardware of a system allows data to be signed or hashed without the encryption key ever leaving the TPM." *Id.*

123. Cavoukian & Dixon, *supra* note 100, at 14.

124. *Id.* at 13.

4. Positive-Sum

Security by Design attempts to attain a positive-sum result, meaning a business can implement both privacy and security.[125] This principle is to avoid depriving privacy in exchange for security.[126] Other competing objectives with security causing conflict include the following: Easy Access versus Secure Access; Convenience versus Security; and Simple to Implement versus Secure to Use.[127] An example of these conflicts includes business executives wanting to simplify processes for a consumer to participate and purchase a product over the Internet.[128] This is similar to allowing a new consumer to log in to a separate account with his or her Facebook credentials, making it easy for a consumer to make the first connection. Yet, using Facebook credentials may not be dependable enough to make a transaction securely over the Internet because hackers could gain unauthorized access to a consumer's Facebook account, allowing them to easily access the separate account.[129]

5. End-to-End Security

Enterprise security has the objective of ensuring "confidentiality, integrity, and availability of all information for all stakeholders in the enterprise."[130] Cavoukian and Dixon assert that throughout the entire enterprise, not just a part of the enterprise, security must be addressed and compensated for any possible vulnerabilities to avoid hacking of a

125. *Id.* at 14; *see also* Andy Green, *Privacy by Design Cheat Sheet*, VARONIS, https://www.varonis.com/blog/privacy-design-cheat-sheet/ (last updated Mar. 29, 2020). *See also* Christoph Bier et al., *How Is Positive-Sum Privacy* Feasible, *in* FUTURE SECURITY: 7TH SECURITY RESEARCH CONFERENCE, FUTURE SECURITY 2012, BONN, GERMANY, SEPTEMBER 2012, PROCEEDINGS 266-267 (Nils Aschenbruck et al. eds., 2012) (comparing Zero-Sum, Positive-Sum, and Win-Win).

126. Cavoukian & Dixon, *supra* note 100, at 14.

127. *Id. See, e.g.*, Lívia Maranhão, *7 Tips to Apply the 7 Principles of Privacy-by-Design*, MEDIUM (Nov. 8, 2019), https://medium.com/inlocotech/7-tips-to-apply-the-7-principles-of-privacy-by-design-c0d1d88c73dd (indicating how consumers should have the option to deny companies access to their personal information while still being able to use a product or service).

128. Cavoukian & Dixon, *supra* note 100, at 14.

129. *See id.*

130. *Id.* at 15.

system that may lead to a data breach.[131] End-to-end security is a proficient strategy to protect activities and assets within the enterprise.[132]

Information security has two key areas, which are "Database Security (DBSec)" and "Identity and Access Management (IAM)."[133] Confidentiality, integrity and availability of a database are required by information security to protect the system.[134] DBSec is when the confidentiality, integrity, and availability of a system can be protected.[135] A substantial impact transpires for the security of the database when there is a loss of confidentiality, integrity, and/or availability.[136] Additionally, information security also requires that information, systems, and applications only be accessed by the appropriate personnel.[137] IAM has been defined as "the security discipline that enables the right individuals to access the right resources at the right times for the right reasons."[138] When a business develops sufficient IAM capabilities, the business can lessen their identity management costs and become more active to support innovative business initiatives.[139]

---

131. *Id.* "End-to-end encryption is a secure line of communication that blocks third-party users from accessed transferred data. When the data is being transferred online, only the sender and recipient can decrypt it with a key." Meredit Galante, *What Is End-to-End Encryption and Why You Really Need It*, SQUARE, https://squareup.com/us/en/townsquare/end-to-end-encryption (last visited Apr. 5, 2020).

132. Cavoukian & Dixon, *supra* note 100, at 15; *See also Security Architecture*, BRIDEWELL CONSULTING, https://www.bridewellconsulting.com/security-architecture (last visited Apr. 5, 2020).

133. Cavoukian & Dixon, *supra* note 100, at 16. DBSec and IAM are core areas that "protect[] the information itself and secur[e] access to that information." *Id. See, e.g.*, *Identity Services*, HERJAVEC GROUP, https://www.herjavecgroup.com/services/identity-services/ (last visited Apr. 5, 2020); *Data Security*, IMPERVA, https://www.imperva.com/products/data-security/ (last visited Apr. 5, 2020).

134. Cavoukian & Dixon, *supra* note 100, at 16.

135. *Id. See also Confidentiality, Integrity and Availability*, MDN WEB DOCS, https://developer.mozilla.org/en-US/docs/Web/Security/Information_Security_Basics/Confidentiality,_Integrity,_and_Availability (last visited Apr. 5, 2020).

136. Cavoukian & Dixon, *supra* note 100, at 16. A loss of confidentiality occurs when there is an unauthorized access to a database server; a loss of integrity is present when there is an unauthorized modification to available data; and a loss of availability occurs when there is a lack of access to services of the database. *Id.*

137. *Id.*

138. *Id.*

139. *Id.* For instance, employers can get a declaration when offboarding employees that they have returned any proprietary information that belongs to the employer as well as terminating a former employee's access to any information systems. Solutions like these examples can help mitigate damage, as seen in *United States v. Levandowski*, where Levandowski was indicted for thirty-three counts involving "the theft and attempted theft of Waymo's trade secrets, largely centered around Light Detection and Ranging." *See* Christopher Burgess, *Former Google-Waymo Engineer Levandowski Charged With IP Theft*, SECURITY BOULEVARD (Aug. 28, 2019), https://securityboulevard.com/2019/08/former-google-waymo-engineer-

6. Visibility and Transparency

Visibility and transparency help reinforce customer and vendor confidence in an information system's security.[140] One factor when considering methods to provide visibility and transparency include adopting open standards.[141] Well-known and vetted systems include using extensively tested encryption standards, allowing for a high degree of confidence that the encrypted data will be secure and safe.[142] However, Cavoukian and Dixon state that novel encryption methods that have not been tested may lead to doubts about their security.[143] According to Cavoukian and Dixon, users will also develop more confidence in the production of the security of their systems when a well-known process[144] is tracked in the development of secure systems.[145]

Another method in developing a visible and transparent system is "external evaluation and validation."[146] Examples of security validation include following a U.S. government computer standard or an international standard involving certification.[147] Additionally, "[d]ocumenting and disclosing the constraint a security system may impose upon its users helps to ensure that a system is operating according to its stated promises and objectives."[148] Cavoukian and Dixon indicate how accountability on the part of an entity supports business processes, rather than weakens these processes.[149]

---

levandowski-charged-with-ip-theft/; *see also* Indictment, United States v. Levandowski, No. 19-00377 (N.D. Cal. filed Aug. 15, 2019).

140. Cavoukian & Dixon, *supra* note 100, at 16.

141. Cavoukian & Dixon, *supra* note 100, at 17. Open standards are "[w]ell-known and highly vetted security standards." *Id.*; *see, e.g.*, Peter Fry, *It's Time to Embrace Open Standards*, JAXENTER (Jan. 10, 2019), https://jaxenter.com/embrace-open-standards-benefits-154242.html.

142. Cavoukian & Dixon, *supra* note 100, at 17. *See also* STEVE QUIROLGICO ET AL., NIST SPECIAL PUBLICATION 800-163, VETTING THE SECURITY OF MOBILE APPLICATIONS 2-3 (Jan. 2015), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-163.pdf.

143. Cavoukian & Dixon, *supra* note 100, at 17.

144. *Id.* Possessing secure development processes and using secure coding standards are considered examples of well-known processes. *Id.*

145. Cavoukian & Dixon, *supra* note 100, at 17. *See generally* SAFECODE, FUNDAMENTAL PRACTICES FOR SECURE SOFTWARE DEVELOPMENT (3d ed. Mar. 2018), https://safecode.org/wp-content/uploads/2018/03/SAFECode_Fundamental_Practices_for_Secure_Software_Development_March_2018.pdf (focusing on best practices, technical, and implementation considerations regarding the development of a secure software development lifecycle program).

146. Cavoukian & Dixon, *supra* note 100, at 17.

147. *Id.*; *see, e.g.*, INT'L ORG. FOR STANDARDIZATION, https://www.iso.org/home.html (last visited Jan. 17, 2020).

148. Cavoukian & Dixon, *supra* note 100, at 17.

149. *Id. See generally* APTIV ET AL., SAFETY FIRST FOR AUTOMATED DRIVING (White Paper, 2019), https://www.aptiv.com/docs/default-source/white-papers/safety-first-for-

7. Respect for the User

When creating or modifying a security system, it is essential that cybersecurity "respect and protect the interests of all information owners, accommodating both individual and enterprise interests."[150] Even though cybersecurity is broader than privacy, privacy principles are nevertheless essential to separate the interests of individuals from those of enterprises.[151] Respecting the user is attained when companies minimize their collection and processing of consumer data by only using data for the purposes specified within a company's privacy policy and terms of use.[152]

III. IDENTIFICATION OF LEGAL PROBLEM

The federal government is attempting to establish its position in the future of self-driving cars.[153] Yet, the cybersecurity provisions of the SELF DRIVE Act are too vague. The inaction by the Senate has caused further delay in ensuring a much-needed federal framework for autonomous vehicles.[154] An essential cybersecurity framework for self-driving cars needs to pass from bill into law.

Autonomous cars "are generally treated as being the product of the car manufacturer[s] who in turn are normally considered responsible to ensure conformity with safety standards."[155] This approach "has worked well for non-connected, non-autonomous vehicles as manufacturers can ensure conformity of production and subject vehicles to fault-testing under real-world operating conditions."[156] Yet, autonomous vehicles will not only face familiar vulnerabilities, but also new threats that arise from

automated-driving-aptiv-white-paper.pdf (eleven automotive, supplier, and technology companies describing a framework for the development, testing, and validation of autonomous vehicles).

150. Cavoukian & Dixon, *supra* note 100, at 18.

151. *Id.* at 18; *see also* Maranhão, *supra* note 127 ("It is about caring for privacy and making it a priority.").

152. Cavoukian & Dixon, *supra* note 100, at 18. California has enacted a new law that creates new rights for consumers, allowing consumers the right to take back control over their personal information from giant corporations and small companies. *See* Cal. Civ. Code § 1798.100–1798.199 (2018).

153. Daniel A. Katz, *A Quick Analysis of the SELF DRIVE ACT*, TUFTS U. (Sept. 27, 2017), https://sites.tufts.edu/dankatz/2017/09/27/a-quick-analysis-of-the-self-drive-act/rive-act/.

154. Maggie Miller, *Advocates Rally on Capitol Hill for Self-Driving Car Legislation*, THE HILL (Dec. 3, 2019), https://thehill.com/policy/cybersecurity/472889-advocates-rally-on-capitol-hill-for-self-driving-car-legislation; Englund & Grigorian, *supra* note 14.

155. Schaub & Zhao, *supra* note 28.

156. *Id.*

increased automation.[157] In fact, a recent report from AAA's multi-year tracking study found that nearly three-quarters of surveyed U.S. drivers reported being too afraid to ride in a fully autonomous vehicle.[158] Nearly two-thirds of American respondents said they would feel less safe riding a bicycle or walking in the presence of autonomous vehicles rather than in the presence of traditional vehicles.[159]

The SELF DRIVE Act's requirements are essential but insufficient to support safety in self-driving vehicles.[160] As compared to a typical information technology environment, the SELF DRIVE Act does not adequately protect "the integrity and availability of human life and public safety on highways" because "[t]he operating environment, economics, components, adversaries, consequences, and time scales are very different" than protecting confidentiality of data in information centers.[161] Security vulnerabilities "may exist within a vehicle's wireless commercial functions, within a mobile device—such as a cellular phone or tablet connected to the vehicle via USB, Bluetooth, or Wi-Fi—or within a third-party device connected through a vehicle diagnostic port."[162] Therefore, hackers can exploit these vulnerabilities by gaining access to an autonomous vehicle's control network or data stored within the vehicle.[163] Due to the cyber threats to self-driving vehicles, the United States needs a nationwide policy that will promote uniformity in the safe manufacturing and deployment of autonomous vehicles.[164]

IV. ANALYSIS

Part IV starts by reviewing the current flaws of the SELF DRIVE Act. This analysis will discuss both the benefits and concerns of a federal framework from manufacturers' perspective as well as states' perspective. The last section of this analysis will explain soft law and some of the current best practices that NHTSA recommends.

---

157. *See* Nicole Casal Moore-Michigan, *Will Self-Driving Cars Threaten Your Security?*, FUTURITY (Jan. 4, 2018), https://www.futurity.org/self-driving-cars-cybersecurity-1646782/.

158. *AAA: American Trust in Autonomous Vehicles Slip*, AAA NEWSROOM (May 22, 2018), https://newsroom.aaa.com/2018/05/aaa-american-trust-autonomous-vehicles-slips/.

159. *See id.*

160. Grant Gross, *Self-driving car bill leaves cybersecurity rules open to interpretation*, THE PARALLAX (Sept. 18, 2017), https://the-parallax.com/2017/09/18/self-driving-car-bill-cybersecurity/.

161. *Id.* (quoting Beau Woods, founder and CEO of Stratigos Security).

162. U.S. DEP'T OF TRANSP., *supra* note 77.

163. *Id.*

164. *The only way the US can safely move forward with self-driving cars*, CNBC (June 5, 2018, 11:13 AM), https://www.cnbc.com/2018/06/05/us-needs-to-pass-self-driving-car-legislation-now.html.

A. Current Flaws of the SELF DRIVE Act

Although manufacturers and suppliers in the automobile industry have improved in protecting vehicles from cybersecurity threats, vehicle hacking remains a very real and gradually serious problem as self-driving cars begin connecting to one another.[165] The current version of the SELF DRIVE Act will not accomplish the goal of ensuring self-driving vehicles are safer.[166] The SELF DRIVE Act contains only two out of thirty-six pages that include information about cybersecurity.[167] Much of the bill "focus[es] on defining the [NHTSA's] role in setting safety standards for autonomous vehicles, while limiting state regulation and waiving some traditional safety regulations during research."[168] The SELF DRIVE Act would demand that self-driving cars manufacturers implement and comply with a procedure that detects and mitigates reasonably foreseeable vulnerabilities, but the SELF DRIVE Act does not define how this process would begin.[169] While the SELF DRIVE Act does require auto manufacturers "to have cybersecurity managers, training, and intrusion prevention and response systems in place, it doesn't detail how the companies should follow through on the requirements."[170]

When considering how to regulate a dynamic field, many considerations need to be considered. Cybersecurity is a concern for public safety, and autonomous vehicles that include complex software and are accessible via a network connection are susceptible to hackers.[171] Creating software without any bugs can be incredibly difficult, and bugs within the software may cause security vulnerabilities, leading to possible exploitation.[172] For instance, hackers can trick the vehicle's sensors into making certain decisions: "a road sign that looks like a stop sign to a human might be constructed [by a hacker] to look like a different sign to the car."[173] The SELF DRIVE Act could provide detail about how

165. JC Reindl, *Car hacking remains a very real threat as autos become ever more loaded with tech*, USA TODAY, https://www.usatoday.com/story/money/2018/01/14/car-hacking-remains-very-real-threat-autos-become-ever-more-loaded-tech/1032951001/ (last updated Jan. 15, 2018, 1:56 PM).

166. Catherine Chase et al., *Congress is trying to pass legislation to make self-driving cars safer. It doesn't go far enough*, CNBC (June 12, 2018, 1:20 PM), https://www.cnbc.com/2018/06/12/self-driving-car-legislation-in-congress-doesnt-go-far-enough.html.

167. *See* SELF DRIVE Act, *supra* note 1; Gross, *supra* note 160.

168. Gross, *supra* note 160.

169. *Id.*

170. *Id.*

171. Jason Kornwitz, *The cybersecurity risk of self-driving* cars, PHYS.ORG (Feb. 16, 2017), https://phys.org/news/2017-02-cybersecurity-self-driving-cars.html. "[A]ny computerized system that has an interface to the outside world is potentially hackable." *Id.*

172. *Id.*

173. The SELF DRIVE Act should account for these types of security vulnerabilities. *Id.*

auto manufacturers should ensure that their self-driving vehicles and components (e.g., sensors, operating systems and networks) go through continuous software updates and patches.[174] Also when considering a legal framework, it is critical to be aware of liability and damages. For instance, "what will happen if a security incident is triggered by an end user installing unsafe software on a mobile phone or device connected to a car? Should end users be liable for such resulting incident? Jointly liable?"[175] Yet, the SELF DRIVE Act does not answer these questions.

B. The Benefits for Manufacturers of a Federal Framework

Lobbying groups, like the Self Driving Coalition for Safer Streets, released a statement that praised the House for passing the SELF DRIVE Act.[176] This statement recognized that autonomous cars "offer an opportunity to significantly increase safety, improve transportation access for underserved communities, and transform how people, goods and services get from point A to B."[177] The SELF DRIVE Act also permits the auto industry to do substantial testing, while summarizing research about improving road safety.[178] The SELF DRIVE Act applies to all fifty states and would help state agencies focus on registering vehicles, enforcing traffic laws, and overseeing insurance and liability.[179] Due to the federal nature of the SELF DRIVE Act, states would be precluded from enacting state regulations and companies would not have to deal with a patchwork of state laws to comply with.[180] Furthermore, the SELF DRIVE Act promotes the development of self-driving cars through broad language that gives the auto industry the freedom to innovate and test more security solutions to ensure safety.[181]

---

174. Schaub & Zhao, *supra* note 28.

175. *Id.*

176. O'Kane, *supra* note 15. The Self Driving Coalition for Safer Streets includes companies like Google, Lyft, Uber, Ford, and Volvo. *Id.*

177. *Id.* (quoting *Self Driving Coalition for Safer Streets Statement on House Passage of the SELF DRIVE Act*, SELF-DRIVING COALITION (Sept. 6, 2017), https://www.selfdrivingcoalition.org/newsroom/press-releases/self-driving-coalition-statement-on-house-passage-of-the-self-drive-act).

178. *Id.*

179. *Id.*

180. Supporters of the SELF DRIVE Act contend that this bill would have "provide[d] a much-needed consistent federal framework to smooth out the disparate state laws." *The first national law dealing with autonomous vehicles could by the SELF DRIVE Act*, GOVTRACK INSIDER (Oct. 19, 2017), https://govtrackinsider.com/the-first-national-law-dealing-with-autonomous-vehicles-could-be-the-self-drive-act-96caa59b5299.

181. Ariel Darvish, *The SELF DRIVE Act: Cybersecurity and Cars on Autopilot*, FORDHAM J. OF CORP. & FIN. L. (Jan. 15, 2018), https://news.law.fordham.edu/jcfl/2018/01/15/the-self-drive-act-cybersecurity-and-cars-on-autopilot/.

As self-driving cars continue to become more powerful and connected, consumers must feel confident that auto manufacturers are safeguarding the integrity, confidentiality, and availability within these systems[182] Security protocols like authentication, encryption, and minimization of data collection assist in mitigating risks to a vehicle's system.[183] When it comes to safety and security, a nationwide framework would create liability, motivating auto manufacturers to be accountable for their actions.

C. State Concerns Raised by a Federal Framework

The SELF DRIVE Act, however, will not give the auto industry absolute permissibility to test whatever and whenever they want on public roads or highways.[184] Automakers argue autonomous vehicles will progress faster with less regulation.[185] Automakers also argue that "[t]he sooner fully autonomous vehicles reach the road, the sooner the 40,000 annual traffic deaths on U.S. roads will decline."[186] Other commentators have said narrower laws with specificity "tend to not be effective because a particular technical approach or countermeasure is going to be obsolete long before any law is changed."[187]

Even though the bill passed through the house unanimously, consumer and other advocacy groups have expressed apprehension about the legislation over safety concerns because of preemption.[188] If states are preempted, consumers may be left "at the mercy of manufacturers as they use . . . public highways as their private laboratories however they wish with no safety protections at all."[189] As Congress lacks consensus in the House and Senate on different bills regarding self-driving

182. Sean Slone, *Benefits and Challenges of the Autonomous and Connected Vehicle Future*, THE COUNCIL OF STATE GOV'TS (July 14, 2017, 1:56 PM), http://knowledgecenter.csg.org/kc/content/benefits-and-challenges-autonomous-and-connected-vehicle-future.

183. *Id.*

184. O'Kane, *supra* note 15.

185. Ashley Halsey III, *Senate Democrats fight push to pass driverless-car bill during lame duck Congress*, THE WASH. POST (Dec. 10, 2018), https://www.washingtonpost.com/local/trafficandcommuting/senate-democrats-fight-push-to-pass-driverless-car-bill-during-lame-duck-congress/2018/12/10/92cdc7a4-f7f6-11e8-8d64-4e79db33382f_story.html?utm_term=.dded76376c3f.

186. *Id.*

187. Gross, *supra* note 160 (quoting Stefan Savage from, Professor at the University of California, San Diego).

188. GOVTRACK INSIDER, *supra* note 180.

189. *Id.*

vehicles, the auto "industry is navigating inconsistent state laws," affecting the progress of improving cybersecurity.[190]

D. Soft Law and Best Practices under NHTSA

Congress has attempted to enact new laws, such as the SELF DRIVE Act, to create a federal framework for self-driving vehicles.[191] Since these efforts have been stalled, "soft law" has been filling the governance void to provide road rules.[192] "Soft law" is "a set of informal norms, multistakeholder arrangements, and non-binding guidance standards that provide an adaptable alternative to more traditional regulations or legislation."[193] In other words, "[w]hether generally applicable or only applicable to a particular party, guidance documents are not legally binding on the public."[194] "Hard law," on the other hand, comprises requirements under treaties and statutes.[195] Soft law has increased in part due to "the increasing gap between the rate of innovation and policymakers' ability to achieve legal and regulatory parity without strangling innovation in the cradle" and because "traditional legislative and regulatory hard law processes are somewhat broken."[196]

On October 24, 2016, NHTSA released its non-binding *Cybersecurity Best Practices for Modern Vehicle* ("NHTSA Best Practices").[197] The guidance is voluntary, and its purpose is to support the auto industry in improving vehicle cybersecurity with a risk-based, layered approach.[198] Parts of NHTSA's Best Practices included using a security by

190. Tamir Bechor, *Cybersecurity for Autonomous Vehicles Must Be a Top Concern for Automakers*, IEEE U. OF LAHORE (Jan. 23, 2019), https://site.ieee.org/sb-uol/cybersecurity-for-autonomous-vehicles-must-be-a-top-concern-for-automakers/.

191. Ryan Hagemann et al., *'Soft Law' Is Eating the World*, MERCATUS CTR. (Oct. 11, 2018), https://www.mercatus.org/bridge/commentary/soft-law-eating-world-driverless-car.

192. *Id.*

193. *Id.*

194. *Guidance Documents*, NAT'L HIGHWAY TRAFFIC SAFETY ADMIN., https://www.nhtsa.gov/laws-regulations/guidance-documents (last visited Jan. 31, 2019).

195. *Hard Law / Soft Law*, ECCHR, https://www.ecchr.eu/en/glossary/hard-law-soft-law/ (last visited Feb. 11, 2020); *see generally* Gregory C. Shaffer & Mark A. Pollack, *Hard vs. Soft Law: Alternatives, Complements, and Antagonists in International Governance*, 94 MINN. L. REV. 706 (2010).

196. *Id.*

197. NAT'L HIGHWAY TRAFFIC SAFETY ADMIN., CYBERSECURITY BEST PRACTICES FOR MODERN VEHICLES (2016); Moriah Daugherty, *NHTSA Releases Proposed Cybersecurity Guidance for the Automotive Industry and Solicits Public Comment*, COVINGTON & BURLING LLP (Oct. 28, 2016), https://www.insideprivacy.com/data-security/cybersecurity/nhtsa-releases-proposed-cybersecurity-guidance-for-the-automotive-industry-and-solicits-public-comment/.

198. Daugherty, *supra* note 197.

design approach.[199] However, cybersecurity in vehicles is too essential to be left to auto manufacturers to choose whether to adopt these voluntary measures.[200] NHTSA Best Practices include "Vehicle Development Process with Explicit Cybersecurity Guidance;" "Leadership Priority on Cybersecurity;" "Information Sharing;" "Vulnerability Reporting / Disclosure Policy;" "Vulnerability / Exploit / Incident Response Process;" "Self-Auditing;" and "Fundamental Vehicle Cybersecurity Protections."[201]

Although NHTSA should be applauded for taking this initiative, Congress should develop standards for cybersecurity that are mandatory and "based on sufficient public research and consultation with other federal agencies, and to require full reporting of cybersecurity considerations and vulnerabilities in the interim."[202] Some regulation is needed to fill the gap, yet nonbinding guidance as it exists in the self-driving vehicle field is "informal," has an "open-ended nature," and is "ripe for abuse."[203] Many also find it outrageous that autonomous vehicle regulations and policies are being guided in a slideshow-like presentation.[204] By permitting soft laws to operate, the democratic process is weakened when agencies, rather than elected officials, create non-binding guidelines.

Self-driving vehicles and technology are continuing to rapidly develop; thus, the auto industry is facing many complex problems.[205] Under these current guidelines, there is a lack of liability for damage that is caused by any defects in self-driving vehicles.[206] As of now, it is not clear who will be liable—a third party or infrastructure provider—if there is a hack and what the process will be to remedy damages.[207]

Even though automobile and technology companies admit that completely autonomous vehicles are still possibly decades away, it is important that the U.S. government focus on modifying a nationwide policy to promote and ensure the safe deployment of self-driving

199. *See id.*; *see also The Imperative of Security by Design: NHTSA Releases Cybersecurity Best Practices*, BUTZEL LONG (Oct. 26, 2016), https://www.butzel.com/resources-alerts-The-Imperative-of-Security-by-Design—NHTSA-Releases-Cybersecurity-Best-Practices.html.

200. *CR-CU comments to NHTSA on cybersecurity best practices for modern vehicles*, CONSUMER REP. (Nov. 28, 2016), https://advocacy.consumerreports.org/research/nhtsacybercomments/.

201. Daugherty, *supra* note 197.

202. CONSUMER REP., *supra* note 200.

203. Hagemann et al., *supra* note 191.

204. *Id.*

205. Schaub & Zhao, *supra* note 28.

206. *See generally* CYBERSECURITY BEST PRACTICES FOR MODERN VEHICLES, *supra* note 197.

207. Schaub & Zhao, *supra* note 28.

vehicles.[208] "While data breaches have failed to cause widespread public outcry, loss of life from a cybersecurity incident would shatter public confidence in autonomous vehicles, denying or delaying their benefits."[209] By developing minimum standards, Congress would be supporting our country in ensuring reliability within this innovative field to ensure security.[210]

V. PROPOSAL

The SELF DRIVE Act could be improved by recognizing that laws behind self-driving vehicles "should reflect the notion that hacks of autonomous vehicles are more dangerous than many other types of cyberattacks."[211] The auto industry must proactively and vigilantly address the potential dangers surrounding autonomous cars to ensure safety among drivers, passengers, and pedestrians. By using the seven foundational principles of Security by Design within the development of a cybersecurity plan for auto manufacturers, this proposal outlines a process for auto manufacturers to follow to identify and mitigate reasonably foreseeable vulnerabilities. The 116th Congress should reintroduce and amend the SELF DRIVE Act to strengthen the federal framework and create minimum requirements for cybersecurity in self-driving cars by incorporating the seven foundational principles of Security by Design.

The Security by Design Foundational Principles support enablement and protection of activities and assets for both people and companies.[212] These foundational principles can be applied in the context of the development and manufacture of self-driving vehicles. Such application will help protect both passengers and third parties such as pedestrians and drivers.

A. Proactive not Reactive; Preventative not Remedial

The goal of acting proactively is to start with the end in mind and by leveraging enterprise architecture methods when implementing security.[213] Rather than just focusing on technology, investment in cybersecurity can align with the business's goals.[214] The SELF DRIVE Act

208. Chase et al., *supra* note 166.

209. Gross, *supra* note 160 (quoting Beau Woods, founder and CEO of Stratigos Security).

210. *See* Chase et al., *supra* note 166.

211. Gross, *supra* note 160.

212. *See* Cavoukian & Dixon, *supra* note 100, at 9.

213. *Id.*

214. *See id.* at 19. For a list of the top cybersecurity companies, see Drew Robb, *Top Cybersecurity Companies*, ESECURITY PLANET (Jan. 3, 2020), https://www.esecurityplanet.com/products/top-cybersecurity-companies.html.

should require auto manufacturers of self-driving vehicles to focus on developing secure systems by identifying and addressing any potential issues early in the design process. A required cybersecurity plan should require auto manufacturers to be active while acting in a preventative manner. This means asking important questions and interacting with various stakeholders to identify vulnerabilities. Some critical questions include: "What would happen if our basic designs, our formulas, or our codes were compromised?"; and "What would happen if our networks were taken down or corrupted?"[215] As stakeholders answer these questions, companies should conduct a risk analysis by identifying potential risks and then assessing both their likelihood of occurrence and potential severity. Once these risks are identified and prioritized, companies should begin mitigating to reduce the risk. Under this element, companies should aim to prevent cybersecurity issues entirely; these are not issues a company wants to deal with once a security breach arises.

B. Default Setting

Having a default setting in cybersecurity does not mean that all auto manufacturers must be identical. Rather, the focus is on securing the consumer, which will enable trust in the brand of self-driving vehicles.[216] By requiring cybersecurity as a default setting in the cybersecurity policies, an auto manufacturing company should include policies about least privilege, need-to-know, least trust, mandatory access control and separation of duties.[217] For example, consider a consumer who uses a map device through the infotainment system. The default setting on this navigation device should only permit the driver to see the vehicle's geolocation, unless the driver chooses a potential option of letting certain people see their geolocation. Furthermore, cybersecurity policies must clearly define which vendors and employees have access to consumer data and such access should be as limited as reasonable. For example, a third-party vendor of infotainment content should not have automatic access to the user's heating, ventilation, and air conditioning system.

C. Embedded into Design

Embedded into Design means applying "Software Security Assurance practices" and using "hardware solutions such as Trusted Platform

215. Cavoukian & Dixon, *supra* note 100, at 10.

216. *Id.* at 11.

217. *Id.* at 11-12. *See Establish Access Rights Based on Least Privilege*, UNIFIED COMPLIANCE FRAMEWORK, https://www.unifiedcompliance.com/products/search-controls/control/1411/ (last visited Apr. 6, 2020).

Module."[218] The auto industry needs to address the full development of self-driving cars "from requirements and design to implementation, testing and deployment."[219] In other words, security must be engineered into each step of the self-driving vehicle's lifecycle, including the braking system, infotainment system, radar sensors, and the keyless entry.[220] On these different auto parts and systems, it is also important that the law demand auto manufacturers to analyze various threats as part of their cybersecurity plan. Self-driving vehicles store potentially sensitive data.[221] Therefore, when doing a comprehensive threat analysis, auto manufacturers should look at the system processes that handle the data and the potential consequences that would occur from the loss, misuse, or unauthorized access of the data.[222] Looking at misuse cases and data flows, techniques by auto manufacturers should be used to determine any threat level of potential security breaches in self-driving vehicles.[223] Once threats are identified, developers shall address potential threats by designing improved security measures within "the architecture of the

218. Cavoukian & Dixon, *supra* note 100, at 9. *See, e.g.*, GOOGLE CLOUD, GOOGLE SECURITY WHITEPAPER 8 (Jan. 2019), https://services.google.com/fh/files/misc/google_security_wp.pdf.

219. Cavoukian & Dixon, *supra* note 100, at 13. *See, e.g.*, APTIV, https://www.aptiv.com (last visited Apr. 6, 2020); *see also* Sam Daley, *Nice Ride: 10 Automotive Cybersecurity Companies Making Vehicles Safer and More Secure*, BUILT IN, https://builtin.com/cybersecurity/automotive-cyber-security (last updated Oct. 29, 2019) ("Aptiv develops software and computing platforms for self-driving vehicles. The company's cybersecurity tools protect everything from a car's infotainment system to its wiring.").

220. *See* Cavoukian & Dixon, *supra* note 100, at 13. Companies like Nvidia "employ[s] a rigorous security development lifecycle into [their] system design and hazards analysis processes, including threat models that cover the entire autonomous driving system—hardware, software, manufacturing, and IT infrastructure." *See* NVIDIA, SELF-DRIVING SAFETY REPORT 27 (2018), https://www.nvidia.com/content/dam/en-zz/Solutions/self-driving-cars/safety-report/auto-print-safety-report-pdf-v16.5%20(1).pdf.

221. *See infra* Section II.E.

222. *See* Cavoukian & Dixon, *supra* note 100, at 13. *See also* Adrienne Lafrance, *How Self-Driving Cars Will Threaten Privacy*, THE ATLANTIC (Mar. 21, 2016), https://www.theatlantic.com/technology/archive/2016/03/self-driving-cars-and-the-looming-privacy-apocalypse/474600/ (describing scenarios that show how self-driving vehicles will be able to collect vast data about a user); *The Privacy Implications of Autonomous Vehicles*, NORTON ROSE FULBRIGHT (July 17, 2017), https://www.dataprotectionreport.com/2017/07/the-privacy-implications-of-autonomous-vehicles/ (noting various privacy and security issues associated with autonomous vehicles).

223. *See* Cavoukian & Dixon, *supra* note 100, at 13. *See, e.g.*, Rilind Elezaj, *Autonomous Cars: Safety Opportunity or Cybersecurity Threat?*, MACHINE DESIGN (July 16, 2019), https://www.machinedesign.com/mechanical-motion-systems/article/21837958/autonomous-cars-safety-opportunity-or-cybersecurity-threat ("As with any other hacking scenario, hacking into an autonomous car would expose a great deal of [a user]—including [the user's] destination. With this information, someone could potentially track the user with an aim toward robbery or assault. If hackers can gain access to the controls of the vehicle, it could also be possible to redirect the vehicle to a more convenient location for either of those scenarios.").

system, not bolted on after the fact."[224] Construction of a security system within a vehicle's system is an essential component.[225]

Furthermore, "[e]xploitable flaws in the source code must be discovered through repeated code reviews and audits and fixed through recoding and/or redesigning of the system."[226] Manufacturers shall make sure secure coding standards are enforced and security modules should be manufactured for reuse.[227] Before deployment of self-driving vehicles, auto manufacturers must follow policies involving rigorous security assessments that "must be assured through structured testing and methods-based evaluation of the software-features being delivered."[228] Cases of misuse should be researched and tested with a live system, where employed "hackers" can attempt to disrupt systems of self-driving vehicles.[229] Although software is critical in autonomous vehicles, hardware must also be considered. Self-driving vehicles may not exactly use the "Trusted Platform Module," but shall include a hardware system that will protect key material from be modified or stolen by malware.[230]

D. Positive Sum

Positive-Sum ensures accommodation of all stakeholders and resolves conflicts to seek a win-win.[231] To achieve a "win-win" outcome for both privacy and security, rather than achieving solely privacy or security, some considerations can be taken to improve self-driving vehicles.[232] First, developers should make sure to "seek to understand the objectives of all constituents."[233] This means making sure all of the issues are out on the table and acknowledging that possible privacy and security conflicts might exist.[234] This may include privacy and security

224. *Id.*

225. *See id.*; *see also* Elezaj, *supra* note 223 ("Just like any other computer-enabled device . . . driverless cars are prone to cybercrimes.").

226. Cavoukian & Dixon, *supra* note 100, at 13.

227. *See id.*

228. *Id.*

229. *Id.* For an example of a case of misuse that should be researched and tested with a live system, see Elezaj, *supra* note 223 ("As the technology evolves, driverless cars will be able to turn on any smart device in [a user's home], be it the TV, heater, garage door, or front gate, and everything programmable in the home. Hackers could use these features to gain access to [a user's] home.").

230. Cavoukian & Dixon, *supra* note 100, at 14.

231. *See id.* at 9.

232. *See id.* at 15.

233. *Id.* at 15.

234. *See id.* Some issues may include car manufacturers wanting to add additional features that may compromise both privacy and security, such as selling access to customer data. *See also* Stephanie Miles, *Digital Advertisers Look to Connected Cars to Push Industry Forward*, STREET FIGHT (Aug. 28, 2019), https://streetfightmag.com/2019/08/28/digital-advertisers-look-to-connected-cars-to-push-industry-forward/#.Xot7Ui-ZNQI ("With a connected

issues that relate to data from the infotainment system. Next, auto manufacturers should make sure to "evaluate potential conflicts" and ask questions like "[w]hy do they exist?" and "[a]re there ways to reframe expectations to minimize conflicts?"[235] Successful cybersecurity occurs when companies understand current methods, standards, and technology.[236] For instance, maybe the conflicts exist because of certain limitations or maybe there are ways that existing technology or other methods can be modified to minimize this conflict.[237] These conflicts may have to do with some type of error in coding the infotainment system or an error in detection for the radar systems. By evaluating new methods and technologies, conflicts like errors in coding, may be solved.[238] This includes finding if a code can be improved to remove conflicts within the detection of radar systems or using new technology for seat customization, while keeping an eye on emerging technologies to support companies in the future.[239] Overall, it is essential to "seek effective compromise" and "implement trade-offs at the lowest level possible."[240] Auto manufacturers will need to ensure continuous oversight; auto manufacturers cannot just end their security responsibilities when a signature is in place for the terms and service agreement. Auto manufacturers must forever ensure security and not take advantage of consumers' lack of knowledge about the importance of cybersecurity.

E. End-to-End Security

End-to-End Security's purpose is to support stakeholders by ensuring confidentiality, integrity and availability of all information.[241] Security should be considered throughout the cybersecurity plan and policies. Database Security can be achieved by a two-pronged approach.[242] Under the first prong, "Preventative Security Controls,"[243] auto manufacturers

system in place, automakers—and certain outside firms—can access data, download software, and communicate with IoT devices.").

235. Cavoukian & Dixon, *supra* note 100, at 15.

236. *See id.* For an example of standards, guidelines, and practices, see NIST, FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY (Apr. 16, 2018), https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

237. *See* Cavoukian & Dixon, *supra* note 100, at 15.

238. *See id.*

239. *See id.*

240. *Id.*

241. *See id.* at 9. *See also How to Protect Your Business With End-to-End Data Security*, FIS (Aug. 5, 2019), https://www.fisglobal.com/en/insights/merchant-solutions-worldpay/article/how-to-protect-your-business-with-end-to-end-data-security.

242. Cavoukian & Dixon, *supra* note 100, at 16.

243. *See id.*; *see, e.g.*, *Cybersecurity for Small Business*, FCC, https://www.fcc.gov/general/cybersecurity-small-business (last visited Apr. 6, 2020) (indicating how businesses can

must continuously prevent hacks from occurring in the database by "mak[ing] information unusable by the wrong people," "allow[ing] the right people to have access," "keep[ing] the wrong people out," "enforce[ing] Segregation of Duties policies," and preventing illegitimate changes in software language from entering the database.[244] Some "Preventative Security Controls" that auto manufacturers must include are encryption, masking, access control, strong authentication, label security, and data redaction.[245] For instance, geolocation data and financial data systems within the infotainment system should be limited in how it is delivered from the central database in the car to any requesting application. Under the second prong, "Detective Security Controls,"[246] auto manufacturers must identify when bad actions are happening, analyze the situation, and learn from experiences.[247] Functional capabilities of "Detective Security Controls" include auto manufacturers making sure to monitor, audit, report, and analyze.[248] For instance, if a hacker is attempting to break into the braking system, auto manufacturers must take preventative and remedial steps to fix a potential bug in the braking system.

Furthermore, under IAM, auto manufacturers need to identify governance and their administrative capabilities.[249] This includes making sure "[t]he right people do get access rights" and "[t]he wrong people don't get access rights."[250] Identity governance also ensures that auto manufacturers "[k]now who has access to what," "[q]uickly disable access rights when people leave," and "[e]nforce audit policy" to "[e]nsure compliance."[251] Technical capabilities of identity governance include "identity lifecycle management" and "password management."[252] Auto manufacturers must manage the entire lifecycle of identities and certain access rights for users. For instance, whether the driver is a parent or teenager, may make a huge difference to access restrictions on the Internet. Password management is also important to ensure security. Otherwise hackers could disrupt a user's system and have access to data stored within the autonomous vehicle.

---

protect their business, customers, and data by training employees in security principles and requiring employees to change passwords every three months).

244. Cavoukian & Dixon, *supra* note 100, at 32.

245. *Id.* at 32-33.

246. *Id.* at 16; *see also* Debbie Walkowski, *What Are Security Controls*, F5 NETWORKS (Aug. 22, 2019), https://www.f5.com/labs/articles/education/what-are-security-controls.

247. Cavoukian & Dixon, *supra* note 100, at 33.

248. *See id.* at 34.

249. *See id.* at 35.

250. *Id.* (emphasis omitted).

251. *Id.* (emphasis omitted).

252. *Id.* at 36; Walkowski, *supra* note 246.

Auto manufacturers must also have a "[u]nified repository of user identity information" and a "[d]efinitive source for who has access and what access they have."[253] An example in the auto industry is ensuring who has access to consumer information that is being transferred from their cars, whether it is banks having access to financial data or engineers having access to the system when a consumer experiences a glitch. Additionally, auto manufacturers should require access management and grant the right access through authentication and authorization.[254] For instance, authenticating and authorizing the driver of the car in question. Companies must also continuously "enforce [their] security policy," whether that is through the web, mobile, or cloud services.[255] In the auto industry, this would affect capabilities, like single sign-on systems, and companies must figure out the safest way to manage how long a session lasts, how to authenticate fingerprint access, and how to erase user behavior history and geolocation.

Furthermore, it shall be mandatory that security updates be part of an auto company's cybersecurity plan. The cybersecurity must also require "rigorous and independent third-party auditing in addition to companies' self-audits."[256] Since this field is ever-changing, the plan must "account for aftermarket devices designed to improve vehicle cybersecurity" and how the auto company will make these changes.[257]

F. Visibility and Transparency

Visibility and Transparency means to "[s]trengthen security through open standards, well-known processes and external validation."[258] Here, auto manufacturers would have to use systems that create a strong degree of confidence. Whether this is through encryption of data or having experienced customer service representatives, using developed and secure processes that have been evaluated and validated is critical. It is also essential to inform consumers with policies about the company's securities policies because consumers must know the benefits and limits of the vehicle and the data that is created and retrieved. Thus, auto manufacturers will be accountable for what they tell their consumers about security, otherwise a business would have legal liability for committing an unfair or deceptive practice against their

253. Cavoukian & Dixon, *supra* note 100, at 35 (emphasis omitted).

254. *See id.*

255. *Id.*; *see, e.g.*, *Apple Platform Security,* APPLE, https://support.apple.com/guide/security/introduction-seccd5016d31/web (last visited Apr. 6, 2020).

256. CONSUMER REP., *supra* note 200.

257. *Id.*

258. Cavoukian & Dixon, *supra* note 100, at 9.

customers. Stronger vehicle security is achieved when companies are transparent, allowing consumers to make informed choices while prompting market competition.[259]

G. Respect for the User

Respect for the User is to "[r]espect and protect the interests of all information owners. Security must accommodate both individual and enterprise interests."[260] Here, creating trust is the bottom line. For users to have an active role in managing their data, auto manufacturers must ensure they attain consent from the consumer about data being collected; must accurately update consumer personal information; permit users to have access to their information; and be compliant when any redress or communication is needed.[261] For instance, if there is a health app through the infotainment system where a consumer can enter their height and weight, companies must receive consent from the consumer about collecting this data and updating the data whenever a user makes a change to their information. Users must also be able to access this information at any time and may have it deleted or removed at their will. Respect for the user applies to personal data given directly by the user and to data that might not be as well-known that the user is giving, like their seat preferences or preferred car temperature.

VI. CONCLUSION

In conclusion, the SELF DRIVE Act and NHTSA Best Practices provide an adequate starting point for the regulation of cybersecurity and vehicle hacking in self-driving cars. However, a stronger and detailed minimum federal framework is necessary in this field to improve consumer safety and protect users' data. The complexity and importance of regulating the autonomous vehicle field is vital. Congress should pass a bill into law surrounding cybersecurity in autonomous vehicles to

259. *See* Comments to "*Cybersecurity Best Practices for Modern Vehicles"*, RAPID 7 (Nov. 28, 2016), https://www.rapid7.com/globalassets/_pdfs/rapid7-comments/rapid7-comments-to-nhtsa-cybersecurity-best-practices-for-modern-vehicles—-docket-id-nhtsa-2016-0104-112816.pdf.

260. Cavoukian & Dixon, *supra* note 100, at 9.

261. *See generally* Cavoukian, *Privacy*, *supra* note 97. One way auto manufacturers can respect their users is by following their company's privacy policy. For examples of privacy policies, *see, e.g.*, *Privacy Policy*, OPTIMIZELY, https://www.optimizely.com/privacy/ (last updated Jan. 1, 2020); *Microsoft Privacy Statement*, MICROSOFT, https://privacy.microsoft.com/en-us/privacystatement (last updated Feb. 20, 2020); *SAP Privacy Statement*, SAP, https://www.sap.com/corporate/en/legal/privacy.html (last updated Mar. 18, 2020); *Starbucks Privacy Statement*, STARBUCKS, https://www.starbucks.com/about-us/company-information/online-policies/privacy-policy (last revised Jan. 1, 2020); *Privacy Policy*, WAYMO (Feb. 20, 2018), https://waymo.com/privacy/.

support their safe deployment. This bill should incorporate the seven foundational principles of Security by Design into a national framework, encouraging auto manufacturers to be accountable and meet their responsibilities without picking and choosing when they can ensure exceptional cybersecurity standards. By enacting a binding and minimum federal framework, consumers can enjoy the benefits and automation of self-driving vehicles while auto manufacturers reduce the risks of physical harm and/or a data breach.