WHO SHOULD BE LIABLE? EXAMINING THE CORPORATE LIABILITY REGIME FOR CYBERSECURITY RISKS

Angel R. Gardner, Esq.

WHO SHOULD BE LIABLE? EXAMINING THE CORPORATE LIABILITY REGIME FOR CYBERSECURITY RISKS

Angel R. Gardner, Esq.*

I. INTRODUCTION

The Internet of Things (IoT) has become ingrained in today's society, but there are many new threats and concerns related to these products. The IoT is a system of interrelated computing devices, mechanical and digital machines, objects, animals, and people that have the ability to transfer data over a network without human-to-human or human-to-computer interactions.[1] In other words, the IoT can be any type of physical object that is embedded with sensors, software, or other technologies for connecting and sharing data with other devices and systems over the Internet.[2] Examples of objects that are part of the IoT include: pacemakers, smartwatches, automatic pet feeders, smart home appliances, connected cars, etc. The introduction of new technology also poses new ways for criminals to commit new types of crimes. One of these crimes is known as hacking or computer and network intrusions. A computer or network intrusion is the unauthorized access of another person's system or device.[3] After a criminal actor has gained access to a victim's network, the bad actor can infect a system with malicious software or malware.[4] Cybercriminals are able to commit a wide variety of other crimes including data theft, ransomware attacks, or distributed denial of service (DDoS) attacks on a victim's network.[5]

Due to the increased connectivity that the IoT presents, hacking is no longer limited to computers. In 2015, Charlie Miller and Chris Valasek, two white-hat hackers,[6] hacked into a moving Jeep Cherokee as part of an experiment to expose a

---

* Angel R. Gardner, Esq., graduated from American University Washington College of Law in May 2023, and she is currently completing a dual degree at American University School of Public Affairs with an M.S. in Justice, Law and Criminology and a graduate certificate in Cyber Policy and Management (May 2024). Angel wrote this article during Spring 2023 as a requirement for her Tech, Law, and Security course. Through the class, she learned about privacy and technology and the lack of liability when a person's data is exposed. This gap prompted her to research how to apply existing laws to address this issue.

1. Alexander S. Gillis, *What Is the Internet of Things (IoT)?*, TECH TARGET, https://www.techtarget.com/iotagenda/definition/Internet-of-Things-IoT (last updated Mar. 2022). [https://perma.cc/TB83-LH6M]

2. Agnieska Mroczkowska & Karol Wrótniak, *IoT Applications: 7 Real-World Examples Across Industries*, DROIDS ON ROIDS (Nov. 16, 2023), https://www.thedroidsonroids.com/blog/iot-applications-examples-across-industries. [https://perma.cc/Y28J-AKLZ]

3. John Bandler & Antonia Merzon, Cybercrime Investigations: A Comprehensive Resource for Everyone 10 (CRC Press 2020).

4. *See* RODERICK S. GRAHAM & SHAWN K. SMITH, CYBERTRESPASS AND DIGITAL DEVIANCE 35-39 (Routledge 2019) (noting that viruses, worms, and Trojans are a few types of malware).

5. *Id.* at 39-40.

6. *See generally id.* at 35 (defining a white hat hacker as an individual who attempts to break into computer networks to identify vulnerabilities and patch them).

zero-day exploit.[7] Initially, they made minor adjustments, such as playing with the air conditioning and switching the radio stations.[8] Then, while the driver was going seventy miles on a busy highway, they cut the engine.[9] This experiment revealed the possibility of remotely taking over a vehicle because car companies like Chrysler are trying to turn modern automobiles into smartphones.[10] In 2019, there were at least 150 cybersecurity incidents related to automobiles.[11] The Global Automotive Cybersecurity Report revealed that this was a ninety-four percent increase in cybersecurity incidents since 2016.[12]

Beyond car hacking, cybercriminals can also gain unauthorized access into medical devices. Researchers have discovered over a dozen vulnerabilities in software used by medical devices and machinery that, if exploited, could cause critical equipment to crash.[13] This software flaw could affect patient monitors, anesthesia, ultrasound and x-ray machines, among other things.[14] Since 2011, hackers have been experimenting with various medical devices to determine what they can control.[15] At the Black Hat USA security conference, Jay Radcliffe demonstrated that he was able to hack his implantable insulin pump.[16] Other hackers demonstrated that pacemakers and other commonly used medical devices were also vulnerable to attack.[17] Currently, there are no adequate laws that protect consumers against these potential cyber intrusions. Additionally, there are no strong regulations requiring corporations to have advanced cybersecurity protections.

This paper argues that the current landscape of cybersecurity requires a strict liability regime for corporations who do not adequately protect consumers from external criminal activities or actors. Part II discusses traditional liability schemes and the current landscape for corporate liability as it relates to cybersecurity. Part III argues that large corporations should be held strictly liable for the software vulnerabilities of the entire product unless corporations exercise advanced cybersecurity protections. Part IV concludes by reiterating the importance of providing adequate protections from cyberattacks and highlighting the risks when corporations fail to protect consumers.

---

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

8. *Id.*

9. *Id.* (noting that Miller and Valasek did not inform the driver what they were going to do but informed him to remain calm).

10. *Id.*

11. Sebastian Blanco, *Car Hacking Danger is Likely Closer Than You Think*, CAR & DRIVE (Sept. 4, 2021), https://www.caranddriver.com/news/a37453835/car-hacking-danger-is-likely-closer-than-you-think/.

12. *Id.*

13. Sean Lyngass, *Researchers Uncover Software Flaws Leaving Medical Devices Vulnerable to Hackers*, CNN (Nov. 9, 2021, 7:04 AM), https://www.cnn.com/2021/11/09/tech/medical-devices-vulnerable-to-hackers/index.html. [https://perma.cc/Y7MC-4ES4]

14. *Id.*

15. Peter Jaret, *Exposing Vulnerabilities: How Hackers Could Target Your Medical Devices*, ASS'N AM. MED. COLL. (Nov. 12, 2018), https://www.aamc.org/news-insights/exposing-vulnerabilities-how-hackers-could-target-your-medical-devices.

16. *Id.* (explaining that Radcliffe could deliver lethal doses of insulin to patients through this vulnerability).

17. *Id.* (describing how the FDA recalled an implantable pacemaker because of hacking concerns).

II. CURRENT LANDSCAPE FOR TORT LIABILITY

Under civil lawsuits, an individual may bring a tort claim against another individual or company/entity when the other person causes the claimant to suffer a loss or harm. Generally, individuals will argue whether there should be a negligence standard or a strict liability standard for the harm caused to a claimant.

A. Negligence

In order to establish negligence, a plaintiff needs to prove the existence of four elements. First, a person must owe a duty of care—this is an obligation recognized by law that requires the actor to conform to a certain standard or conduct for the protection of others against unreasonable risk of harm.[18] Second, the individual must breach their duty to use reasonable care.[19] Third, the injury must be reasonably connected between the conduct and the resulting injury.[20] Finally, the plaintiff must have actual damage or loss resulting from the breach.[21]

B. Strict Liability—Products Liability

Strict liability is a higher standard than negligence and a viable tort option for plaintiffs. Strict liability means imposing liability without fault.[22] Liability without fault means that due care is not a defense in strict liability cases. Generally, the origin of strict liability is traced to the ruling in *MacPherson v. Buick Motor Company*.[23] In *MacPherson*, the court ruled that an automobile manufacturer has a duty of vigilance because it must know danger is probable if an automobile is defectively made.[24] The vast majority of states adopted the MacPherson rule throughout the early-to-mid twentieth century.[25] Nearly twenty years later, Justice Traynor's majority opinion in *Greenman v. Yuba Power Products, Inc.* became the standard for applying strict liability.[26] The substance of Justice Traynor's opinion were incorporated into the Restatement (Second) of Torts, and by 1986, forty-five states followed the Restatement and adopted the doctrine of strict liability.[27] The Second Restatement of Torts provides:

> (1) One who sells any product in a defective condition unreasonably dangerous to the user or consumer or to his property is subject to liability for physical harm thereby caused to the ultimate user or consumer, or to his property, if

18. Smith v. United States, 873 F.3d 1348, 1351 (11th Cir. 2017).
19. *Id.*
20. *Id.*
21. *Id.*
22. Caporale v. C.W. Blakeslee & Sons, Inc., 175 A.2d 561, 564 (Conn. 1961).
23. Justin (Gus) Hurwitz, *Cyberensuring Security*, 49 CONN. L. REV. 1495, 1524 (2017) (the case was the first to remove the privity requirement needed to bring a suit in tort law).
24. Thomas Rickettson, *Blinded by the Lease: Strict Products Liability in the Age of Amazon*, 125 PENN. ST. L. REV. 321, 327 (2020) (citing MacPherson v. Buick Motor Co., 111 N.E. 1050, 1053 (N.Y. 1916)).
25. *Id.* at 328.
26. *Id.*
27. *Id.* at 329-30 (the five states that follow consumer protection laws in terms of warranty are Delaware, Massachusetts, Michigan, North Carolina, and Virginia).

> (a) the seller is engaged in the business of selling such a product, and
> (b) it is expected to and does reach the user or consumer without substantial change in the condition in which it is sold.
> (2) The rule stated in Subsection (1) applies although
> (a) the seller has exercised all possible care in the preparation and sale of his product, and
> (b) the user or consumer has not bought the product from or entered into any contractual relation with the seller.[28]

Strict liability cases are usually under state law, and a majority of states have adopted the Second Restatement. Generally, under the products liability doctrine, "[a] manufacturer is strictly liable in tort when an article he places on the market, knowing that it is to be used without inspection for defects, proves to have a defect that causes injury to a human being."[29] There are three types of products liability claims a plaintiff can make—a manufacturing defect, a design defect, or an information defect.[30] For a successful products liability claim, the plaintiff must prove, "(1) a product was in a defective condition unreasonably dangerous for its intended use; (2) the defect existed at the time the product left the defendant's control; and (3) the defect proximately caused the plaintiff's injury."[31] Additionally, Justice Traynor articulated four policy rationales behind imposing strict products liability: (1) deterrence, (2) reliance, (3) insurance, and (4) administrative costs.[32] First, strict liability provides an incentive to parties with superior knowledge and ability to prevent or minimize product accidents. This also deters these parties from producing defective materials.[33] Second, in the era of mass production, consumers rely on manufacturers whose processes are generally unknown to the consumer.[34] Third, strict liability works as a form of insurance because it spreads the risks of injuries to the manufacturer instead of the injured party, who is probably unprepared to assume the risk.[35] Lastly, a party injured by a defective product is rarely equipped to provide evidence of a lack of due care. In the absence of strict liability, litigation would be costly and time-consuming.[36] Imposing strict liability thus reduces administrative costs associated with litigation.[37]

III. FAILED TORT CLAIMS AGAINST CORPORATIONS FOR VULNERABLE IOT DEVICES

Several plaintiffs have attempted to bring lawsuits against corporations emerging from the lack of security in the computer systems of IoT devices. However,

28. RESTATEMENT (SECOND) OF TORTS § 402A.
29. Arriaga v. CitiCapital Com. Corp., 85 Cal. Rptr. 3d 143, 148 (2008).
30. Alan Butler, *Products Liability and the Internet of (Insecure) Things: Should Manufacturers Be Liable for Damage Caused By Hacked Devices?*, 50 UNIV. MICH. J. L. REFORM 913, 916-17 (2017).
31. *E.g.* Duxbury v. Spex Feeds, Inc., 681 N.W.2d 380, 393 (Minn. Ct. App. 2004) (Many states adopt these three elements in strict liability claims).
32. Rickettson, *supra* note 24, at 330.
33. *Id.*
34. *Id.*
35. *Id.* at 331.
36. *Id.*
37. *Id.*

these lawsuits have been largely unsuccessful due to courts determining that the plaintiffs have not met their burden to bring the suit.

In *Cahen v. Toyota Motor Corp.*, the plaintiffs brought a class action against Ford Motor Company, General Motors LLC, Toyota Motor Corporation, and Toyota Motor Sales, U.S.A., Inc. "alleging that defendants . . . equipped their [cars] with . . . technology . . . susceptible to [hacking] by third parties."[38] The defendants' cars used dozens of electronic control units ("ECUs"); these were "small computers that [controlled the] vehicle operations."[39] The parties explained that "The ECUs communicate through a controller area network, or 'CAN bus,' by sending . . . digital messages called 'CAN packets.'"[40] Further, "'[T]here is no ECU source or authentication, nor any encryption, built into CAN packets,' [so] anyone with physical access to a vehicle could utilize the CAN bus to send malicious CAN packets to the ECUs."[41] Additionally the plaintiffs noted, "[the] vehicles are equipped with wireless Bluetooth and cell phone integration capabilities . . . [and] when activated by the user . . . [the vehicles could become] susceptible to remote hacking via wirelessly transmitted CAN packets."[42]

The plaintiffs argued that the defendants knew that their vehicles could be hacked and cited various research studies dating back to 2011.[43] However, the plaintiffs did not allege that their vehicles have been hacked but that an alleged hacking is an "imminent eventuality."[44] Further, plaintiffs alleged that "despite the defendants' knowledge of the significant security vulnerabilities, they market the vehicles as safe."[45] The plaintiffs brought class action suits in California,[46] Oregon,[47] and Washington[48] under various state statutes.[49] The plaintiffs sought an injunction that would enjoin the respondents from continuing to market their vehicles as safe

38. Cahen v. Toyota Motor Corp., 147 F. Supp. 3d 955, 958 (N.D. Cal. 2015).

39. *Id.*

40. *Id.*

41. *Id.*

42. *Id.* at 958-59.

43. *Id.* at 959.

44. *Id.* (suggesting that any expert would say that an attack is unpreventable and therefore simply a matter of when an attack will occur).

45. *Id.*

46. The plaintiffs alleged "(1) violation of California's Unfair Competition Law, (2) violation of California's Consumers Legal Remedies Act, (3) violation of California's False Advertising Law, (4) breach of California's Implied Warranty of Merchantability, (5) breach of contract at California common law, (6) fraud by concealment at California common law, (7) violation of California's Song-Beverly Consumer Warranty Act, and (8) invasion of privacy under the California Constitution" (*Cahen*, 147 F. Supp. 3d at 960) (citations omitted).

47. The plaintiffs alleged "(1) violation of Oregon's Unlawful Trade Practices Act, (2) breach of Oregon's Implied Warranty of Merchantability, and (3) fraudulent concealment at Oregon common law" (*Cahen*, 147 F. Supp. 3d at 960) (citations omitted).

48. "The plaintiffs alleged "(1) violation of Washington's Consumer Protection Act, (2) breach of Washington's Implied Warranty of Merchantability, (3) breach of contract at Washington common law, and (4) fraudulent concealment at Washington common law" (*Cahen*, 147 F. Supp. 3d at 960) (citations omitted).

49. *Cahen*, 147 F. Supp. 3d at 960.

and establish a recall program and provide free repairs.[50] The respondents filed a motion to dismiss the claim under the Federal Rules of Civil Procedure.[51]

In order to bring a case, a plaintiff must have standing, and in this case, the respondents alleged that the plaintiffs did not assert an "injury in fact that is actual or imminent, not conjectural or hypothetical."[52] The respondents argued that the plaintiffs could not assert an injury in fact based on the risk of future harm.[53] The court agreed with the respondents stating that "while it is possible that a potential hacker would in fact attempt to gain control of a vehicle, 'allegations of possible future injury are not sufficient.'"[54]

In *Flynn v. FCA US LLC*, plaintiffs brought a class action lawsuit against FCA US LLC, formerly known as Chrysler.[55] The plaintiffs brought the lawsuit after the 2015 article in *Wired* magazine revealed a controlled hack of a Jeep Cherokee exposing a vulnerability in the Jeep's "uConnect" infotainment system.[56] The plaintiffs "asserted claims under federal and state warranty and consumer-fraud laws" alleging that the vehicles were vulnerable to cyberattacks.[57] The plaintiffs alleged four causes of action against the defendants.[58] After several motions to dismiss, the judge dismissed the first three injury theories.[59] Only the plaintiffs' theory of overpayment remained, but the judge "held that the plaintiffs failed to adequately support their claimed overpayment injury."[60] On appeal, the Seventh Circuit upheld the decision of the lower court.[61] Again, the court highlighted that the plaintiffs failed to establish that they had standing to bring the case.[62]

In *Ross v. St. Jude Medical, Inc.*, the plaintiff brought a class action lawsuit against St. Jude Medical, Inc. and several other defendants.[63] The plaintiffs alleged that the remote monitoring of Implantable Medical Devices ("IMD") introduced significant security risks because devices that communicate wirelessly through

50. *Id.*

51. *Id.* (articulating that "dismissal under Rule 12(b)(6) is appropriate only where the complaint lacks a cognizable theory or sufficient facts to support a cognizable legal theory.").

52. *Id.* at 965 (quotations omitted).

53. *Id.* at 966 (claiming the future injury was based only on potential hacking by a third party).

54. *Id.* at 967 (emphasis removed).

55. Flynn v. FCA US LLC, 39 F.4th 946, 949 (7th Cir. 2022).

56. *Id.* (indicating that the hackers were able to access the vehicle's computer systems and take over many of the Jeep's functions).

57. *Id.*

58. *Id.* at 950. The plaintiffs alleged: "(1) increased risk of physical harm; (2) increased risk of fear and anxiety; (3) decreased market value of the plaintiffs' vehicles; and (4) 'overpayment'—that is, the plaintiffs paid more for the vehicles than they would have if they had known about the hacking vulnerability."

59. *Id.* at 950-51.

60. *Id.* at 951 (referring to the single controlled-environment *Wired* hack, the judge found that the plaintiffs failed to show any financial harm).

61. *Id.* at 954.

62. *Id.* at 952 (highlighting that the plaintiff must have "(1) suffered an injury in fact, (2) that is fairly traceable to the challenged conduct of the defendant, and (3) that is likely to be redressed by a favorable judicial decision[.]").

63. Ross v. St. Jude Med., Inc., No. 2:16-cv-06465, 2016 WL 4527336 (C.D. Cal. Aug. 26, 2016).

radiofrequencies could allow for unauthorized access to these devices.[64] The plaintiffs articulated that this ability to gain unauthorized access could result in a "major privacy breach" and allowed for far easier attacks on these systems.[65] For example, a bad actor who chooses to attack these devices would be able to "monitor and modify the [device] without . . . being close to the victim."[66] The named plaintiff in this case, Ross, explained how he discontinued using the transmitter because of the security issues associated with the software.[67] The plaintiffs alleged (1) breach of express warranty, (2) fraudulent concealment, (3) negligence, and (4) unjust enrichment.[68] However, the parties never litigated these claims because the plaintiffs voluntarily dismissed the case.[69]

IV. 2023 NATIONAL CYBERSECURITY PLAN & IMPLEMENTATION PLAN ON SOFTWARE LIABILITY

In March 2023, President Biden released the National Cybersecurity Strategy which outlines the current trends in the digital space and the potential threats stemming from cyberspace.[70] To combat these emerging threats, the White House proposed five pillars to enhance collaboration to prevent and protect against the threat actors.[71] An important shift in the Administration's goal is Strategic Objective 3.3 which "shift[s] liability for insecure software products and services."[72] The Strategy highlights how "vendors ignore best practices for secure development, ship products with insecure default configurations or known vulnerabilities, and integrate third-party software of unvetted or unknown [origin]."[73] Further, software companies are able to disclaim liability using contracts, "reducing their incentive to follow "secure-by-design principles . . . ."[74] The Strategy recognizes the importance of innovation and highlights the importance of holding companies liable when they fail

64. *Id.* at ¶ 17. The complaint lists pacemakers, defibrillators, neurostimulators, and infusion pumps as common IMDs. *Id.* at ¶ 8.

65. *Id.* at ¶ 17 (explaining that these devices store sensitive information including vital signals, diagnosed conditions, therapies, and a variety of personal data unique to each user).

66. *Id.* (lamenting that these attacks pose a risk to the safety of the patient and in certain cases have fatal consequences).

67. *Id.* at ¶ 34.

68. *Id.* at ¶¶ 47-86.

69. Ross v. St. Jude Med., Inc., No. CV 16-6465-DMG, 2016 U.S. Dist. LEXIS 179406, at *1 (C.D. Cal. Dec. 28, 2016).

70. U.S. WHITE HOUSE, NATIONAL CYBERSECURITY STRATEGY, at 1-4 (Mar. 2023) [hereinafter NAT'L CYBERSEC. STRATEGY], https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf [https://perma.cc/6XTQ-RFZM] (highlighting how China, North Korea, Russia, Iran, and other autocratic States are using advanced cyber capabilities to pursue objectives that run counter to U.S. interests and broadly accepted international norms).

71. *Id.* at 4 (the five pillars are: (1) Defend Critical Infrastructure, (2) Disrupt and Dismantle Threat Actors, (3) Shape Market Forces to Drive Security and Resilience, (4) Invest in a Resilient Future, and (5) Forge International Partnerships to Pursue Shared Goals).

72. *Id.* at 20.

73. *Id.*

74. *Id.*

to meet the duty of care owed to consumers, businesses, or critical infrastructure providers.[75]

While the strategy outlines specific objectives, it does not yet provide tangible solutions to meet these objectives. However, in July 2023, the Biden Administration released the National Cybersecurity Strategy Implementation Plan to outline a roadmap for meeting the goals set out in the Strategy.[76] Pillar Three specifically addresses the Administration's goal to shape market forces in order to drive security and resilience. First, the Implementation Plan seeks to improve IoT cybersecurity by implementing the Federal Acquisition Regulation requirements per the Internet of Things (IoT) Cybersecurity Improvement Act of 2020.[77] Additionally, the Implementation Plan requires the Office of the National Cyber Director to host a legal symposium to explore different approaches to a software liability framework.[78] The Administration highlights its intention to include an adaptable safe harbor provision to shield companies from liability if they securely develop and maintain their software products and services.[79] While the Implementation Plan is a necessary first step in addressing the mounting cybersecurity concerns, it fails to outline tangible steps to encourage companies to secure their software.

V. THE GOVERNMENT SHOULD IMPOSE STRICT LIABILITY IMPOSED ON CORPORATIONS FOR CYBERSECURITY RISKS TO SHIFT THE BURDEN AWAY FROM CONSUMERS

Insecure devices pose a significant threat to internet security, and currently, the consumer bears the brunt of liability. However, consumers are not the best equipped to handle these insecure networks. As early as 2007, researchers have known the security risks posed by the Internet infrastructure.[80] The researchers suggested "the need for embedded systems [to introduce] 'remote upgrade[s]' . . . to adjust to rapid changes in technologies and capabilities."[81] Three categories of product defects give rise to liability: (1) manufacturing defects, (2) design defects, and (3) defective or inadequate warnings.[82]

---

75. *Id.* at 20-21 (providing that responsibility must be placed on the stakeholders who are most capable of taking action to prevent bad outcomes rather than punish end-users who bear the consequence of insecure software).

76. U.S. WHITE HOUSE, NATIONAL CYBERSECURITY STRATEGY IMPLEMENTATION (July 2023) [hereinafter NAT'L CYBERSEC. IMPLEMENTATION], https://www.whitehouse.gov/wp-content/uploads/2023/07/National-Cybersecurity-Strategy-Implementation-Plan-WH.gov_.pdf. [https://perma.cc/UQ9Y-V6X2]

77. *Id.* at 29; *see also* H.R. 1668, 116th Cong. (2019) (requiring the National Institute of Standards and Technology "NIST" and the Office of Budget Management "OBM" to take specific actions to increase cybersecurity for IoT devices).

78. NAT'L CYBERSEC. IMPLEMENTATION, *supra* note 76, at 30 (incorporating different areas of regulatory law and including input from computer scientists to determine how software liability may be similar or different to other regimes).

79. *Id.*

80. Butler, *supra* note 30, at 925 (highlighting how the Internet is notoriously vulnerable to accidents and attacks by hackers, criminals, terrorists, and even state actors).

81. *Id.* at 925-26.

82. Butler, *supra* note 30, at 916-17 (articulating that typically, software defects are seen as design defects).

Courts should impose strict liability on companies that fail to adequately protect consumers from cybersecurity risk because the potential harm amounts to unreasonably dangerous conduct under the Second Restatement. First, while researchers have only conducted car hacks in controlled environments, they pose serious security and safety risks to consumers.[83] Additionally, insecure medical devices pose serious concerns that could lead to fatal outcomes.[84] Both of these outcomes could be detrimental not only to individuals but to national security. For example, bad actors could attempt to target high-ranking U.S. leaders in assassination attempts by hacking either vehicles or medical devices.[85] Additionally, cybercriminals have already shown that they are willing to attack hospitals and innocent people for various reasons, including financial motivation.[86] Attackers use ransomware attacks for financially motivated crimes and once they exploit the initial victim, such as a company, the attackers can implement double extortion by targeting the individuals whose information was leaked in the initial attack.[87] These attacks can have fatal consequences for consumers and the failure to protect consumers from these attacks should fall to the companies. A plaintiff should be able to claim recourse for a design defect when companies take too long to update the software or fail to look for existing vulnerabilities in their products.

Further, imposing strict liability satisfies policy rationales. First, strict liability for cybersecurity would increase deterrence.[88] Consumers are unable to prevent or minimize accidents to the same degree as corporations because consumers do not build the software.[89] Imposing strict liability would put the onus on companies to ensure that consumer data is adequately protected. Moreover, a large company is generally better equipped to assume the risk of unsecure software compared to the consumers who use the products.[90] For these reasons, courts should impose strict liability onto corporations instead of consumers.

---

83. *See* Greenberg, *supra* note 7 (detailing how two prominent hackers were able to remotely access a Jeep and cut the engine of the vehicle while it was going 70 mph on a freeway).

84. Ross v. St. Jude Med., Inc., No. 2:16-cv-06465, 2016 WL 4527336, at ¶ 17 (C.D. Cal. Aug. 26, 2016) (alleging that medical devices could be remotely accessed by unauthorized parties).

85. *See* Andrea Peterson, *Yes, Terrorists Could Have Hacked Dick Cheney's Heart*, WASH. POST (Oct. 21, 2013, 8:58 AM), https://www.washingtonpost.com/news/the-switch/wp/2013/10/21/yes-terrorists-could-have-hacked-dick-cheneys-heart/ [https://perma.cc/J2YV-EF25] (detailing that former Vice President Dick Cheney's doctor ordered he turn off the wireless functionality of his heart implant due to concerns of hacking for an assassination attempt).

86. Andrea Fox, *Half of Ransomware Attacks Have Disrupted Healthcare Delivery, JAMA Report Finds*, HEALTHCARE IT NEWS (Jan. 10, 2023, 11:06 AM), https://www.healthcareitnews.com/news/half-ransomware-attacks-have-disrupted-healthcare-delivery-jama-report-finds [https://perma.cc/UWW8-ZTLN] (discussing how ransomware attacks on hospitals have doubled from 2016 to 2021).

87. *Risk Briefing: Double Extortion Ransomware Explained*, STRATEGIC RISK (Sept. 4, 2023), https://www.strategic-risk-global.com/home/risk-briefing-double-extortion-ransomware-explained/1445492.article. [https://perma.cc/3K6W-4C6U]

88. Rickettson, *supra* note 24 at 330.

89. *Id.*

90. *Id.* at 331 (strict liability serves as a form of insurance).

VI. STRICT LIABILITY PROVIDES CONSUMERS WITH A PATHWAY TO LITIGATION & INCENTIVIZES CORPORATIONS TO MAINTAIN SECURE SOFTWARE

In the National Cybersecurity Strategy, President Joe Biden highlighted the importance of protecting the United States from threats in cyberspace. One such objective was to shift liability to corporations for having insecure software products and services.[91] The defense and aerospace industries generated roughly $741 billion in 2022,[92] the global automotive manufacturing market generated roughly $2.9 trillion in 2022,[93] and the implantable medical devices market size was valued at $98.45 billion in 2021.[94] In contrast, an individual person has limited options to prevent themselves from becoming the target of a cyberattack.[95] Corporations have more financial means to prevent or mitigate the damages from unauthorized intrusions into software. Currently, "vendors ignore best practices for secure development, ship products with insecure default configurations or known vulnerabilities, and integrate third-party software of unvetted or unknown [origin]."[96] Strict liability addresses issues arising from insecure devices and networks, and it encourages corporations to better protect consumers from software vulnerabilities.[97]

A negligence scheme asks for the bare minimum of protection, and companies could still attempt to escape liability for failure to protect their software. Plaintiffs have been trying for years to recover for a company's failure to safeguard against cyberattacks, but the courts have continuously dismissed these claims.[98] A negligence scheme requires the harm to be causally linked to the breach of a duty.[99] A defendant could easily overcome the negligence standard, whereas strict liability imposes liability regardless. Additionally, the negligence standard requires that a plaintiff suffer harm before bringing a suit. This is a problematic standard because it requires that the individual suffer from potentially fatal consequences before they are able to recover damages. In contrast, strict liability establishes several goals: "(1)

---

91. NAT'L CYBERSEC. STRATEGY, *supra* note 70, at 20.

92. *Global Aerospace and Defense: Annual Industry Performance and Outlook*, PwC (2023), https://www.pwc.com/us/en/industrial-products/publications/assets/pwc-aerospace-defense-annual-industry-performance-outlook-2023.pdf. [https://perma.cc/5WZT-BW8J]

93. Sarah Moore, *The Current State of the Global Automotive Manufacturing Market*, AZO MATERIALS (Nov. 24, 2022), https://www.azom.com/article.aspx?ArticleID=22236. [https://perma.cc/NVJ6-Y9R5]

94. *Implantable Medical Devices Global Market Report 2022: Sector to Reach $157.07 Billion by 2028 at a CAGR of 6.90%*, GLOBE NEWSWIRE (Feb. 23, 2023), https://www.globenewswire.com/en/news-release/2023/02/23/2614007/28124/en/Implantable-Medical-Devices-Global-Market-Report-2022-Sector-to-Reach-157-07-Billion-by-2028-at-a-CAGR-of-6-90.html. [https://perma.cc/XD2W-WCT6]

95. *See Protect Myself from Cyberattacks*, CISA (Feb. 21, 2023), https://www.cisa.gov/news-events/news/protect-myselfcyberattacks [https://perma.cc/9R6J-VCFK] (outlining that individuals can prevent cyberattacks by not clicking links in emails, not giving personal information over the phone or email, and not opening attachments).

96. NAT'L CYBERSEC. STRATEGY, *supra* note 70, at 20.

97. Butler, *supra* note 30, at 918 (articulating that manufacturers are better equipped to mitigate the damage that cyberattacks cause).

98. *See e.g., Cahen*, 147 F. Supp. 3d 955 (N.D. Cal. 2015); Flynn v. FCA US LLC, 39 F.4th 946 (7th Cir. 2022) (dismissing the plaintiffs' claims for failing to establish that they had standing to bring the case).

99. Smith v. United States, 873 F.3d 1348, 1351 (11th Cir. 2017).

creat[es] safety incentives, (2) discourage[es] consumption of risky products, (3) reduc[es] transaction costs in litigation, and (4) . . . assign[s] liability to the party best equipped to spread the loss."[100] In the cybersecurity space, courts should recognize that these same goals are necessary to protect domestic interests both for national security and for consumer protection. The biggest challenge in litigation will be allowing plaintiffs to recover solely on the failure to maintain adequate cybersecurity protection in the absence of an attack. Imposing liability on companies will ensure that they keep their software up to date against potential bad actors.

VII. CORPORATIONS THAT EXERCISE ADVANCED CYBERSECURITY MEASURES SHOULD ENJOY A SAFE HARBOR PROVISION SO THEY CAN CONTINUE TO INNOVATE.

A major concern against using strict liability is that litigation, or fear of liability, will decrease innovation to keep creating new or better technology. To address this matter, Congress, when drafting the new legislation, should carve out an exception from liability for corporations that practice advanced cybersecurity measures and still experience a breach. The Biden Administration has already identified that there should be a safe harbor provision carve out for companies who securely develop and maintain their software products and services.[101] Many regulatory agencies already provide recommendations or best practices for cybersecurity. These existing frameworks can provide Congress with guidance on how to frame any new legislation regarding cybersecurity liability. Additionally, the legislation that congress proposes would need to define what advanced cybersecurity measures are to ensure that there is no ambiguity as to the exempt expectations. Some potential considerations that Congress can look to are the cybersecurity architecture that a company has, if the company contracts for cybersecurity, or have a protection system similar to the National Cybersecurity Protection System ("NCPS").

Regulatory agencies continuously attempt to guide the government, corporations, and individuals on how to protect themselves in cyberspace. For example, the Cybersecurity and Infrastructure Security Agency ("CISA") provided a whitepaper to technology providers and software developers aimed at encouraging them to take the lead in protecting consumers from cyber harms.[102] CISA, in collaboration with various domestic and international agencies suggests that companies adopt a "secure by design" and "secure by default" approach to cybersecurity.[103] The secure by design approach proposes that products are built to protect against malicious cyber actors.[104] The authoring organizations recognize that taking ownership over security outcomes may increase developmental costs, but

100. Butler, *supra* note 30, at 917.

101. NAT'L CYBERSEC. IMPLEMENTATION, *supra* note 76, at 30.

102. Bob Lord, Jack Cable, Lauren Zabierek, & Grant Dasher, *The Next Chapter of Secure by Design*, CISA BLOG (Oct. 17, 2023), https://www.cisa.gov/news-events/news/next-chapter-secure-design. [https://perma.cc/YZ3V-7FXK]

103. *Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Secure by Design Software*, CISA, 8 (Oct. 25, 2023), https://www.cisa.gov/news-events/alerts/2023/04/13/shifting-balance-cybersecurity-risk-security-design-and-default-procedures. [https://perma.cc/LF23-67H5]

104. *Id.*

reason that investing in secure by design practices while developing innovative products can substantially improve the security posture for the benefit of customers and reduce the likelihood of compromise.[105] The secure by default approach means that products are resilient against exploitation techniques out of the box without additional charges to the customer.[106] The authoring organizations propose three software product principles for software manufacturers to build software security in their design processes prior to the development, configuration, and shipment of their product.[107] The authoring organizations outline several recommendations that companies can implement to protect their products.[108] Companies should proactively build in secure by design and default principles during product development because of their substantial knowledge and are in the best position to protect their product from cyber risks.

There are several types of cybersecurity measures that a company could adopt to increase security on their networks. One potential consideration would be to determine what level of cybersecurity the company practices. Companies that exercise a Secure Access Service Edge ("SASE") may be exempt from liability for a cyberattack. In 2019, Gartner introduced SASE, a newer security framework that builds on Zero Trust.[109] SASE differs from Zero Trust by offering a "more comprehensive network and security services, including Zero Trust."[110] This is a potential indicator of companies exercising advanced cybersecurity measures because the model vets everyone who attempts to gain access to their servers and decrease the likelihood of an attack against the company and its consumers.

Alternatively, Congress may consider whether a company contracts with a cybersecurity company to protect its networks before an attack happens. Cybersecurity is a $156.24 billion market because of the rise of IoT technology and the growing threat of advanced cybercriminals.[111] Cybersecurity firms play an increasingly critical role to protect businesses from potential cyber threats by thwarting any potential threats that might disrupt a business's operations.[112] A company that takes proactive steps in preventing cyberattacks by employing a specific company or maintaining an advanced internal team to protect the network should be exempt from civil liability because they did everything in their power to prevent the attack. Therefore, it is not in the best interest of the government to punish companies that attempt to prevent or mitigate harm to their network.

---

105. *Id.*

106. *Id.* at 9.

107. *Id.* at 10. "(1) take ownership of customer security outcomes; (2) embrace radical transparency and accountability; and (3) build organizational structure and leadership to achieve these goals."

108. *Id.* at 15-27 (some recommendations include discourage the use of legacy systems, implement zero trust architecture, responsibly use open source software, publish software bills of material, provide regular reports to the board of directors, include details of a secure by design program in corporate financial reports).

109. Andrew Magnusson, *Zero Trust vs. SASE: Everything You Need to Know*, STRONG DM (Feb. 14, 2023), https://www.strongdm.com/blog/zero-trust-vssase. [https://perma.cc/4N7M-6QZF]

110. *Id.* (SASE uses identity and context-aware trust levels to determine whether to grant a person access whereas a Zero Trust model trusts no one).

111. *What Do Cybersecurity Firms Do?*, PACKETLABS (July 15, 2021), https://www.packetlabs.net/posts/ cybersecurity-firms/. [https://perma.cc/HMQ2-H9H5]

112. *Id.*

Lastly, Congress could create a system similar to NCPS for private companies to adapt and follow to maintain advanced cybersecurity in the private sector. CISA designed the NCPS to improve the cybersecurity posture of the Federal Civilian Executive Branch and other partners.[113] The NCPS delivers capabilities such as intrusion detection, analytics, information sharing, and intrusion prevention.[114] NCPS includes all hardware, software, supporting processes, training, and services to meet the agency's mission.[115] One of the key technologies of the NCPS is the EINSTEIN system.[116] The benefits of a similar program for the private sector is that it would implement similar tactics as the public sector to combat cyberattacks. However, the private sector does not have a single entity similar to CISA that could maintain this system. The public sector and the private sector differ in their needs, so it could pose a challenge to create one system to address all cybersecurity needs of private companies. The above recommendations are a few considerations that Congress could adopt when determining how to balance the interests of consumers and corporations.

While it is important to create an avenue for redress when a person is harmed, a genuine concern in this space is about whether liability would hinder innovation. Innovation is "the introduction of new things, ideas or ways of doing something."[117] Fear of litigation is a legitimate concern for companies who innovate, but if there were exceptions that outlined how companies should protect their consumers, then companies that do not practice these standards should be held liable. The United States can potentially look to other countries to determine fee mitigation options for companies that exercise some level of cybersecurity protection. In 2018, the European Union released the General Data Protection Regulation (GDPR), which provided the most stringent laws in the world in relation to data privacy, collection, and protection.[118] Under Article 83, failure to comply with the GDPR can result in a fine.[119] Additionally, Article 82 allows any person who "suffers material or non-material damage as a result of an infringement of this Regulation" the right to receive compensation.[120] Similarly, the Brazilian General Data Protection Law (LGPD)

113. *Securing Federal Networks: National Security Protection System*, CISA, https://www.cisa.gov/securing-federal-networks-national-cybersecurity-protection-system (last visited Apr. 28, 2023). [https://perma.cc/GJ8V-R3DR]

114. *National Cybersecurity Protection System*, CISA, https://www.cisa.gov/resources-tools/programs/national-cybersecurity-protection-system (last visited Apr. 28, 2023) (identifying the NCPS as an integrated system-of-systems). [https://perma.cc/C6CG-M2SV]

115. *Id.*

116. *Id.* (listing EINSTEINs capabilities as providing the Federal Government with an early warning system, improved situational awareness of intrusion threats to FCEB networks, near real-time identification of malicious cyber activity, and prevention of that malicious cyber activity).

117. *Innovation*, Oxford Dictionary, https://www.oxfordlearnersdictionaries.com/us/definition/english/innovation (last visited Apr. 29, 2023). [https://perma.cc/4Z6G-UABR]

118. Ramya Mohanakrishnan, *What Is GDPR and Why Is It Important?*, SPICEWORKS (Feb. 16, 2023), https://www.spiceworks.com/it-security/security-general/articles/what-is-gdpr/. [https://perma.cc/36DT-VSJF]

119. Commission Regulation 2016/679, art. 83, 2016 O.J. (L 119) 1 [hereinafter GDPR].

120. GDPR, art. 82; *see also* Mohanakrishnan, *supra* note 118 (Tier 1 fines are for less severe infractions and can be up to €10 million or 2% of the violating company's global annual revenue from the previous year and Tier 2 fines are up to €20 million or 4% of the violating company's global annual revenue from the previous year).

entered into force in 2020, and the penalties issued by the LGPD became enforceable in 2021.[121] Under Article 52 of the LGPD, the national authority may impose (1) a warning with a time period indicating when the party must implement adoptive corrective measures; (2) a simple fine of up to two percent of a private legal entity, group, or conglomerate's revenues in Brazil, for the prior financial year, excluding taxes, up to a total maximum of fifty million reais per infraction; or (3) a daily fine subject to the total amount referenced previously.[122] The GDPR and LGPD can guide Congress on different ways to sanction non-complying corporations.

VIII. CONCLUSION

Corporate responsibility for their cybersecurity is imperative to ensure that United States assets are protected, but it also would allow individuals an avenue for recourse when they are harmed by a company's failure to adequately protect the consumer's data. By holding companies responsible, it will ensure that cybersecurity standards keep pace with the evolving threats posed by insecure networks. Strict liability ensures that these goals are met and consumers are protected or able to seek recourse after an attack occurs. The private sector needs to take cybersecurity risks more seriously and ensure that consumers are protected from these threats. Additionally, companies are in the best position to protect against these types of threats, and they should be liable for harm when failing to protect consumers. Congress needs to act on these issues because the current method allows corporations to escape liability while maintaining poor software.

121. *Data Protection Laws of the World*, DLA PIPER (last modified Jan. 28, 2024), https://www.dlapiperdataprotection.com/index.html?t=law&c=BR. [https://perma.cc/GN3P-ULAJ]

122. Decreto No. 13,853, de 14 Augusto 2018, art. 52 (Braz.), https://iapp.org/media /pdf/resource_center/Brazilian_General_Data_Protection_Law.pdf. [https://perma.cc/YT6D-H5PW]