University of Michigan Journal of Law Reform

Volume 50

2017

Products Liability and the Internet of (Insecure) Things: Should Manufacturers Be Liable for Damage Caused by Hacked Devices?

Alan Butler
Electronic Privacy Information Center

PRODUCTS LIABILITY AND THE INTERNET OF (INSECURE) THINGS: SHOULD MANUFACTURERS BE LIABLE FOR DAMAGE CAUSED BY HACKED DEVICES?

Alan Butler*

INTRODUCTION

On Tuesday, September 20, 2016, the website KrebsOnSecurity ("Krebs"), a blog run by a prominent cybersecurity reporter, was hit with one of the largest cyberattacks ever recorded.[1] Although Krebs's site was not taken down by the initial attack, it was forced offline for several days after his network security provider refused to continue protecting the site pro bono.[2] According to a report commissioned by Akamai, Krebs's former security provider, the average cost of a denial-of-service ("DoS") attack can be as high as $1.5 million.[3] The attack on Krebs's site was larger than most previous attacks by several orders of magnitude and was unique because it was carried out by an army of more than a million hacked consumer devices. A month later, Internet access was disrupted across the East Coast and in other areas of the U.S. after another similar DoS attack was launched against Dyn, a major Internet service provider.[4] At the peak of the Dyn attack, the network of hacked devices

* Senior Counsel, Electronic Privacy Information Center (EPIC); J.D., UCLA School of Law; B.A., *magna cum laude*, Washington University in St. Louis.

1. *See* Brian Krebs, *KrebsOnSecurity Hit With Record DDoS*, KREBSONSECURITY (Sept. 21, 2016), https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/.

2. Brian Krebs, *The Democratization of Censorship*, KREBSONSECURITY (Sept. 25, 2016), https://krebsonsecurity.com/2016/09/the-democratization-of-censorship/.

3. PONEMON INST., 2015 COST OF CYBER CRIME STUDY: GLOBAL 7 (2015), http://www.cnmeonline.com/myresources/hpe/docs/HPE_SIEM_Analyst_Report_-_2015_Cost_of_Cyber_Crime_Study_-_Global.pdf. DoS attacks are "coordinated attempts to overwhelm a given network resource (e.g., a Web server) with malicious traffic or requests for information to such an extent that legitimate traffic cannot get through." NAT'L RES. COUNCIL & NAT'L ACAD. OF ENG., TOWARD A SAFER AND MORE SECURE CYBERSPACE 201 (Seymour E. Goodman and Herbert S. Lin eds., 2007), https://www.nitrd.gov/fileupload/files/NRC_Toward_a_Safer_and_More_Secure_CyberspaceFull_report.pdf [hereinafter NRC REPORT]. These attacks are commonly carried out using "botnets," which are "collections of compromised computers that are remotely controlled by a malevolent party." *Id.* at 40.

4. Lily Hay Newman, *What We Know About Friday's Massive East Coast Internet Outage*, WIRED (Oct. 21, 2016, 1:04 PM), https://www.wired.com/2016/10/internet-outage-ddos-dns-dyn/.

was sending an estimated 1.2Tbps of traffic to the company's servers.[5]

Akamai estimates that, following a DoS attack, the technical support and damaged asset costs alone can be more than $100,000. That figure does not include revenue lost due to downtime or other business disruptions.[6] The mounting cost of these attacks is one of many reasons why cybersecurity is now a top priority for businesses, policymakers, and investors around the world.[7] But what the Krebs attack exemplified is that connected devices, commonly referred to as the Internet of Things ("IoT"), are increasingly being hacked and used to carry out devastating and costly cyberattacks. Use of these devices is becoming more widespread every year; reports estimate that by 2020, IoT devices will make up 24 billion out of the 34 billion devices connected to the Internet.[8]

Recent Internet security reports indicate that malicious software that can "take advantage of IoT architecture" has already been developed. Akamai predicted in mid-2016 that, "[i]n the near future, attacks may source from automated homes or vehicles."[9] As it turned out, Akamai's prediction came true within a few months. Once his site was back online, Krebs mused that, rather than being taken down by some "space-based weapon of mass disruption," his site was attacked "with the help of a botnet that has enslaved a large number of hacked so-called [IoT] devices—mainly routers, IP cameras and digital video recorders (DVRs) that are exposed to the

---

5. CHRISTIAAN BEEK ET AL., MCAFEE LABS, THREATS REPORT: APRIL 2017 16 (2017), https://www.mcafee.com/us/resources/reports/rp-quarterly-threats-mar-2017.pdf. According to subsequent analysis, this was the highest volume of traffic ever recorded in a DoS attack. *Id.* The Dyn attack was carried out by the "Mirai botnet," which, as of April 2017, had infected more than 2.5 million devices. *Id.* at 31.

6. PONEMON INST., *supra* note 3, at 1 fig.1.

7. *See* SHARED ASSESSMENTS, THE INTERNET OF THINGS (IOT): A NEW ERA OF THIRD-PARTY RISK (2017), http://sharedassessments.org/internet-things-iot-new-era-third-party-risk/; Bruce Schneier, *Your Wi-Fi Connected Thermostat Can Take Down the Whole Internet. We Need New Regulations*, WASH. POST (Nov. 3, 2016), https://www.washingtonpost.com/posteverything/wp/2016/11/03/your-wifi-connected-thermostat-can-take-down-the-whole-internet-we-need-new-regulations/ (describing how IoT vulnerabilities recently disrupted the operations of major websites including Twitter and Paypal). States have also begun to recognize the scope of the problem and to craft new legislative solutions that impose security standards on IoT manufacturers. *See* Jazmine Ulloa, *This California Lawmaker Wants to Crack Down on Toys and Electronics That Pick Up Conversations and Personal Information*, L.A. TIMES (Mar. 30, 2017), http://www.latimes.com/politics/essential/la-pol-ca-essential-politics-updates-california-state-bill-aims-to-prevent-1490914171-htmlstory.html.

8. John Greenough, *How the 'Internet of Things' Will Impact Consumers, Businesses, and Governments in 2016 and Beyond*, BUS. INSIDER (Jul. 18, 2016, 10:24 AM), http://www.businessinsider.com/how-the-internet-of-things-market-will-grow-2014-10.

9. Akamai Techs., *Q2 2016 Report*, 3 ST. OF THE INTERNET / SECURITY, no. 2, 2016, at 40, https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/akamai-q2-2016-state-of-the-internet-security-report.pdf.

Internet and protected with weak or hard-coded passwords."[10] Krebs issued his own ominous warning in that same post:

> The reality is that there are currently millions—if not tens of millions—of insecure or poorly secured IoT devices that are ripe for being enlisted in these attacks at any given time. And we're adding millions more each year.[11]

Given the tremendous costs incurred by victims of DoS and other network attacks, the central role that connected devices play in these attacks, and the large number of potential bystander victims, it is likely that there will be a steady rise in IoT-related litigation.[12] Products liability could provide a useful model to address injuries caused by insecure IoT devices.

While the application of products liability to insecure software is a frequently-discussed concept in academic literature, many commentators have been skeptical of the viability of such claims for several reasons.[13] First, the economic loss doctrine bars recovery for productivity loss, business disruption, and other common damages caused by software defects. Second, the application of design defects principles to software is difficult given the complexity of the devices and recent tort reform trends that have limited liability. Third, the intervening cause of damage from insecure software is typically a criminal or tortious act by a third party, so principles of causation might limit liability for manufacturers.

Even though discussions of liability for defective software go back more than forty years,[14] very few cases have addressed the issue

---

10. Krebs, *supra* note 2; s*ee also* Lorenzo Franceschi-Bicchierai, *How 1.5 Million Connected Cameras Were Hijacked to Make an Unprecedented Botnet*, VICE: MOTHERBOARD (Sept. 29, 2016, 12:03 PM), https://motherboard.vice.com/en_us/article/15-million-connected-cameras-ddos-botnet-brian-krebs.

11. Krebs, *supra* note 2.

12. We have already seen an uptick in data breach suits over the last five years as the frequency of such incidents has increased. *See* Robert D. Fram, Simon J. Frankel & Amanda C. Lynch, *Standing in Data Breach Cases: A Review of Recent Trends*, BLOOMBERG BNA (Nov. 9, 2015), http://www.bna.com/standing-data-breach-n57982063308/ (summarizing many data breach cases filed in the last ten years).

13. *See, e.g.*, Michael L. Rustad & Thomas H. Koenig, *The Tort of Negligent Enablement of Cybercrime*, 20 BERKELEY TECH. L. J. 1553, 1577 (2005) (noting that "it seems unlikely that the courts adopting the Restatement will be receptive to stretching product liability concepts to software, digital information, and other intangibles.").

14. *See* Frances E. Zollers et al., *Landings for Software: Liability for Defects in An Industry That Has Come of Age*, 21 SANTA CLARA COMPUTER & HIGH TECH. L.J. 745, 745 n.1, 756 n.57 (2005) (listing articles dating back to 1971 that have "speculated" about liability for various types of defective software); *see also* Michael D. Scott, *Tort Liability for Insecure Software*, 67 MD. L. REV. 425, 469 n.267 (2008) (summarizing calls to impose strict liability during the last twenty years); Michael Rustad, *The Commercial Law of Internet Security*, 10 HIGH TECH. L. J. 213,

outside the financial services context. However, the proliferation of IoT devices could be the catalyst for a new field of "connected devices" products liability law for several reasons. First, these attacks cause significant damage to property and are highly foreseeable given the widely acknowledged insecurity of IoT devices and numerous high-profile attacks. Second, IoT devices are often fully capable of being updated and secured remotely by the manufacturer; patching well-known security flaws could significantly reduce the risk of future attacks. And third, holding manufacturers liable for downstream harms caused by their insecure devices is well aligned with the purposes of products liability law—to minimize harm by encouraging manufacturers (as a least-cost-avoider) to invest in security measures.

I. PRINCIPLES UNDERLYING LIABILITY FOR PRODUCT DEFECTS

Products liability can be imposed on manufacturers and others involved in distributing commercial products that cause injuries. These claims can be pursued under theories of negligence, strict liability, or breach of warranty.[15] The core inquiry in products liability cases is whether the injuries were caused by a defect. Courts have long imposed liability on those "engaged in the business of selling or otherwise distributing . . . a defective product" where "harm to persons or property [is] caused by the defect."[16]

Products liability simultaneously serves two broad goals: (1) to compensate those injured by unsafe products and (2) to provide incentives for companies to take reasonable precautions in the design and manufacture of their products.[17] The basic policy rationale underlying all products liability law is that the manufacturer is in the best position to prevent harm from defects.[18] There are three

258 n.220 (1995) (listing prior commentators who have recommended extending strict products liability to defective software dating back more than thirty years).

15. Rustad & Koenig, *supra* note 13, at 1576.

16. RESTATEMENT (THIRD) OF TORTS: PROD. LIAB. § 1 (AM. LAW INST. 1998). There has been much dispute amongst courts, scholars, and legislators about the precise contours of products liability. This brief introduction is not meant to be a comprehensive overview of all products liability law. Instead, I will offer a quick summary of the basic tort law and economic principles underlying design defects.

17. Nathan Alexander Sales, *Regulating Cyber-Security*, 107 NW. U. L. REV. 1503, 1533 (2013).

18. Zollers et al., *supra* note 14, at 768 (discussing the rationale adopted in Greenman v. Yuba Power Products, Inc., 377 P.2d 897 (Cal. 1963)); *see also* DAN B. DOBBS, THE LAW OF TORTS § 353, at 975–76 (2000); WILLIAM M. LANDES & RICHARD A. POSNER, THE ECONOMIC STRUCTURE OF TORT LAW 4–5 (1987).

discrete categories of product defect that give rise to liability in different circumstances: manufacturing defects, design defects, and defective or inadequate warnings.[19] Software defects have typically been seen as design defects, though in some cases harm could be caused by a "random failing or imperfection" in a software product, and thus be deemed a manufacturing defect.[20]

The downside of relying on a design defect theory is that there are significant disagreements over the necessary standard for proving that a product was defectively designed.[21] The *Third Restatement* adopts a "risk-utility" test, similar to the famous Learned Hand formula (B < PL), to determine whether the "foreseeable risks of harm posed by the product could have been reduced or avoided by the adoption of a reasonable alternative design."[22] This test typically boils down to "[a] 'micro-balance' of pros and cons of a manufacturer's failure to adopt some particular design feature that would have prevented plaintiff's harm."[23]

The alternative to the risk-utility test is the "consumer expectations" test, adopted by some courts, which seeks to answer whether the product "failed to perform as safely as an ordinary consumer would expect when used in an intended or reasonably foreseeable manner."[24] While adoption of the risk-utility standard involves importing a negligence concept into a "strict liability" regime, the consumer expectations test can be just as problematic when applied to products that pose obvious risks or involve "relatively complex design."[25] Unlike design defects, the liability for manufacturing defects is truly strict, and the *Third Restatement* makes clear that the no-fault liability serves several important goals: (1) creating safety incentives, (2) discouraging consumption of risky products, (3) reducing transaction costs in litigation, and (4) fairness in assigning liability to the party best equipped to spread the loss.[26]

Traditionally, the defectiveness of a physical good has been measured at the time of sale, and courts have not imposed a strict duty

---

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

20. Sales, *supra* note 17, at 1533; *see* Stephen R. Brenneman, *Computer Malfunctions—What Damages May Be Recovered in a Tort Product Liability Action*, 2 Santa Clara Computer & High Tech. L.J. 271, 279 (1986); Scott, *supra* note 14, at 468–70.

21. *See, e.g.*, Tincher v. Omega Flex, Inc., 104 A.3d 328 (Pa. 2014) (attempting to resolve the common law test for design defects in Pennsylvania based on conflicting interpretations in the *Second Restatement*, the *Third Restatement*, and prior case law).

22. RESTATEMENT (THIRD) OF TORTS: PROD. LIAB. § 2 (AM. LAW INST. 1998); Scott, *supra* note 14, at 467.

23. DAVID G. OWEN, PRODUCT LIABILITY LAW 315 (2d ed. 2008).

24. *Tincher*, 104 A.3d at 368.

25. *Tincher*, 104 A.3d at 388.

26. RESTATEMENT (THIRD) OF TORTS: PROD. LIAB. § 2 cmt. a (AM. LAW INST. 1998).

to insure harms caused by conditions that arise after the sale is completed.[27] However, both the *Third Restatement* and more than half of the states have adopted an affirmative post-sale duty to warn.[28] The post-sale duty to warn, like the *Third Restatement*'s design defect test, is premised on a risk-utility analysis. The risk of harm must be "sufficiently great to justify the burden of providing a warning."[29] There must also be a way to identify "those to whom a warning might be provided" and some mechanism for the warning to be "effectively communicated."[30] The seller's decision regarding a post-sale warning is ultimately judged based on their knowledge (or imputed knowledge) and whether a "reasonable person" in their position would provide a warning.[31] Courts are more likely to impose a post-sale duty to warn where the manufacturer maintains a post-sale relationship and contact with the user who needs to be warned.[32]

Ultimately, the problem of insecure devices and networks is precisely the kind of issue that strict products liability was designed to solve.[33] Liability for cyberattacks would be "predictably ineffective if directly applied to a class of bad actors," and the manufacturers of insecure devices are in a much better position to "mitigat[e] the damage they cause."[34] It is especially appropriate "in cases where liability can encourage a party to internalize some significant negative externality associated with its activities."[35] The National Academy of Sciences emphasized in its comprehensive review of cybersecurity threats that, as IoT devices proliferate, it is even more important for "information technology systems and networks [to be] adequately protected."[36] The Academy warned that the risks created by insecure devices will not only contribute to widespread harm, but will also cause other businesses and customers to "deem it unacceptably risky to increase their reliance on [these] insecure

27. DAVID G. OWEN & MARY J. DAVIS, OWEN & DAVIS ON PRODUCTS LIABILITY § 1:15 (4th ed. 2014).

28. RESTATEMENT (THIRD) OF TORTS: PROD. LIAB. § 10 (AM. LAW INST. 1998); Jill Wieber Lens, *Warning: A Post-Sale Duty to Warn Targets Small Manufacturers*, 2014 UTAH L. REV. 1013, 1014, 1020 n.24.

29. RESTATEMENT (THIRD) OF TORTS: PROD. LIAB. § 10(b)(4) (AM. LAW INST. 1998)

30. *Id.* §§ 10(b)(2)–(3).

31. *Id.* § 10(b)(1).

32. Lens, *supra* note 28, at 1027.

33. *See* Zollers et al., *supra* note 14; *see also* Doug Lichtman & Eric P. Posner, *Holding Internet Service Providers Accountable*, 14 SUP. CT. ECON. REV. 221, 233–40 (2006) (outlining justifications for imposing "indirect" liability on internet service providers).

34. Lichtman & Posner, *supra* note 33, at 223.

35. *Id.*

36. NRC REPORT, *supra* note 3, at 41.

technologies."[37] It is ultimately a question of how, not why, liability should attach for insecure devices that contribute to cyberattacks.[38]

II. THE ECONOMIC LOSS DOCTRINE

One potential limit to products liability is the economic loss doctrine, which has traditionally barred recovery for certain financial harms. Prior articles about potential liability for defective software have noted that some of the most common types of damage caused by software defects—such as loss of use of the software and consequential damages to business—would not be recoverable under the economic loss doctrine. But recent developments in the law and literature support the conclusion that the types of damage caused by insecure IoT devices would not be excluded under the rule.

The economic loss rule has long been a source of confusion and disagreement among courts and tort scholars.[39] In an effort to address these disagreements, the American Law Institute has begun work on a proposed *Restatement (Third) of Torts: Liability for Economic Harm*.[40] The first principle outlined in the proposed restatement is that "[a]n actor has no general duty to avoid the unintentional infliction of economic loss on another."[41] As the comments to the first section make clear, this is meant to establish a more limited principle than the economic loss rule that has been adopted by a minority of courts.[42] The minority view has been that "there is generally no liability in tort for causing pure economic loss to another."[43] Rather than bar all liability for pure economic loss, the comments to the proposed restatement make clear that while the

37. *Id.* at 42.

38. *See* Bruce Schneier, *Liability and Security*, CRYPTO-GRAM NEWSL. (Apr. 15, 2002), http://www.schneier.com/crypto-gram-0204.html#6. There is already broad support for the proposition that some liability should attach to such activities. *See* Shuba Ghosh & Vikram Mangalmurti, *Curing Cybersecurity Breaches Through Strict Products Liability* in SECURING PRIVACY IN THE INTERNET AGE 187, 192 (Anupam Chander et al. eds., 2008); BRENT ROWE ET AL., INST. FOR HOMELAND SEC. SOLUTIONS, THE ROLE OF INTERNET SERVICE PROVIDERS IN CYBER SECURITY (2011) https://pdfs.semanticscholar.org/ca45/575aee631a162e3c0d62d955fbb86bd33df9.pdf; Lichtman & Posner, *supra* note 33, at 21; Rustad & Koenig, *supra* note 13 (outlining a proposal for how to impose liability under a new tort theory); Sales, *supra* note 17, at 1538–39; Scott, *supra* note 14, at 467–68.

39. *See generally* Vincent R. Johnson, *The Boundary-line Function of the Economic Loss Rule*, 66 WASH. & LEE L. REV. 523 (2009); David W. Opderbeck, *Cybersecurity, Data Breaches, and the Economic Loss Doctrine in the Payment Card Industry*, 75 MD. L. REV. 935 (2016).

40. RESTATEMENT OF THE LAW (THIRD) TORTS: LIAB. FOR ECON. HARM (AM. LAW INST., Tentative Draft No. 1, 2012) [hereinafter ECONOMIC HARM RESTATEMENT DRAFT NO. 1].

41. *Id.* § 1(a).

42. *Id.* § 1 cmt. b.

43. *Id.*

"duties of care with respect to economic loss are not general in character," they will be recognized in specific circumstances.[44] There is no presumption against the existence of these duties, but merely an acknowledgement that such duties "require justification on more particular grounds than duties to avoid causing physical harm."[45]

The restatement defines "economic loss" as "pecuniary damage not arising from injury to the plaintiff's person or from physical harm to the plaintiff's property."[46] The rationale offered for this distinction is twofold. First, "[e]conomic losses proliferate" and are not self-limiting or predictable in the same way as physical injuries and thus create a risk of indeterminate liability.[47] Second, "[r]isks of economic loss tend to be especially well-suited to allocation by contract."[48] But the restatement also cautions that in some cases the plaintiff "is in a poor position to allocate the risk of economic loss by contract" and that a "court should not labor under a presumption against liability when the rationales for restricting it are absent."[49] Economic losses can also be more narrowly defined as those stemming from a "condition that may disappoint the purchaser's expectations as to [a product's] efficacy or fitness for the purposes intended."[50] Early cases involving malfunctioning computer hardware and software were dismissed on that basis.[51]

The economic loss rule has long been viewed as an impediment to products liability claims arising from defective software.[52] This was likely true for the type of software defect claims that early commentators envisioned, since the damage they predicted included inoperable systems, business interruption, or other harms associated with loss of use of the software itself. Unlike defective business software or other products previously considered, the security vulnerabilities that plague IoT devices threaten damage to private

---

44. *Id.*

45. *Id.*

46. *Id.* § 2.

47. *Id.* § 1 cmt. c(1).

48. *Id.* § 1 cmt. c(2).

49. *Id.* § 1 cmt. e.

50. W. PAGE KEETON ET. AL., PROSSER AND KEETON ON THE LAW OF TORTS § 95, at 678 (5th ed. 1984).

51. Zollers et al., *supra* note 14, at 757.

52. *See* Ghosh & Mangalmurti, *supra* note 38, at 192 (describing the "difficulty" in imposing tort liability in cyberspace due to "the reluctance of tort law to embrace the notion of economic harms as a form of personal harm"); Jeffrey D. Neuburger & Maureen E. Garde, *Information Security Vulnerabilities: Should We Litigate or Mitigate?*, 21 ANDREWS COMPUTER & INTERNET LITIG. REP. 13, at *5 (2004); Opderbeck, *supra* note 39, at 938 (describing the debate over the economic loss doctrine including those who view the doctrine as an impediment); Rustad & Koenig, *supra* note 13, at 1580; Sales, *supra* note 17, at 1535; Scott, supra note 14.

property and create unique risks to innocent bystanders that should support recovery.

Applying the proposed restatement principles to the problem of injuries caused by insecure IoT devices will be somewhat complex, but the restatement principles appear to favor recovery for the types of damages likely to be caused by cyberattacks. The comments to the proposed restatement clarify that "property damage" means "damage to tangible property," but also acknowledges that even "relatively minor damage to person or property" can give rise to liability for related monetary losses.[53] A recent report on the financial impact of DoS attacks estimated that the per-hour cost of an attack is $40,000 and that the average attack costs as much as $500,000.[54] The report found that more than fifty percent of the companies surveyed "had to replace hardware or software" as a result of the attack, fifty percent "had a virus or malware installed/activated on their network," thirty-three percent suffered "consumer data theft," and nineteen percent suffered "intellectual property loss."[55]

Most of these damages caused by DoS attacks could be fairly construed as "property damage" because they include destruction or interference with specific network devices, software, and other electronic property (including sensitive data). The destruction and/or theft of this property could not be characterized as a "purely economic loss." On the other hand, the type of business losses described in the Incapsula survey and the Akamai report, including "loss of customer trust" and "lost user productivity" would likely meet the definition of "economic loss" and not be recoverable absent damage to property.[56]

Given the rationale of the economic loss doctrine, it is especially appropriate to permit products liability claims brought by bystander victims who would not have any contractual remedies against the manufacturer. In fact, modern products liability law began with the recognition of claims brought by victims despite their lack of privity with the defective product's manufacturer.[57] The *Second Restatement* noted the "social pressure" that gave rise to products

---

53. ECONOMIC HARM RESTATEMENT DRAFT NO. 1, *supra* note 40, § 2 cmt. a.

54. TIM MATTHEWS, INCAPSULA, SURVEY: WHAT DDOS ATTACKS REALLY COST BUSINESSES, 5 (2014) (ebook) https://lp.incapsula.com/rs/incapsulainc/images/eBook%20-%20DDoS%20Impact%20Survey.pdf.

55. *Id.*

56. *Id.*; PONEMON INST., *supra* note 3, at 7.

57. *See generally* OWEN & DAVIS, *supra* note 27, §1:11; William L. Prosser, *The Assault Upon the Citadel*, 69 YALE L. J. 1099 (1960).

liability was "a consumers' pressure," but declined to express "approval [or] disapproval" for the extension to bystanders.[58] While the *Second Restatement* did not directly address the question of whether bystanders could bring products liability claims, subsequent cases have almost unanimously allowed recovery by foreseeable bystanders.[59]

III. PROXIMATE CAUSE AND FORESEEABILITY

The main difference between the injuries to foreseeable bystanders in prior products liability cases and the injuries suffered by victims of cyberattacks is the intervening actions of third party hackers.[60] Proof of proximate cause has previously been seen as an impediment to cybersecurity-related products liability claims.[61] Ultimately, the question of proximate cause in a cyberattack bystander case would likely turn on the foreseeability of the harm given the nature of the insecure product defect.[62] Foreseeability has been described as the "dominant test of proximate cause" and the "dark matter of tort."[63]

Proximate cause is the primary mechanism used by judges to limit the scope of liability for "remote" harms, but the concept has never been well defined.[64] Whether an intervening criminal event will break the causal chain depends upon "whether the type of intervention was a reasonably foreseeable consequence of the product defect."[65] The reasonable foresight doctrine of probable cause traces back to the famous *Palsgraf* case in which Judge Cardozo held that a railroad guard could not be liable for a remote harm caused to a bystander on the platform.[66] In *Palsgraf*, a railroad guard pushed a man who had just jumped aboard a departing train,

58. RESTATEMENT (SECOND) OF TORTS § 402A cmt. o (AM. LAW. INST. 1965).

59. OWEN & DAVIS, *supra* note 27, § 5.5, § 5.5 n.40 (reviewing bystander liability cases decided since the *Second Restatement*).

60. Rustad & Koenig, *supra* note 13, at 1602.

61. *See* Scott, *supra* note 14, at 450–53.

62. *See* Prosser, *supra* note 57, at 1143 ("A more difficult problem is that of what Professor Ehrenzweig has called 'typicality' of the injury. Put in more ordinary language, this means the foreseeability of the harm—the seller's reasonable anticipation of it as a normal consequence of the consumption or use of his product if it should turn out to be defective. It is the sort of issue that is likely to be buried under the name of 'proximate cause.'").

63. David G. Owen, *Figuring Foreseeability*, 44 WAKE FOREST L. REV. 1277, 1277 (2009); Meiring de Villiers, *Foreseeability Decoded*, 16 MINN. J.L. SCI. & TECH. 343, 344 (2015).

64. OWEN, *supra* note 63, at 1293; *see* Rustad & Koenig, *supra* note 13, at 1601. *See generally* JOSEPH A. PAGE, TORTS: PROXIMATE CAUSE (2003); Mark F. Grady, *Proximate Cause Decoded*, 50 UCLA L. REV. 293 (2002).

65. OWEN & DAVIS, *supra* note 27, § 1:16.

66. Palsgraf v. Long Island R.R. Co., 162 N.E. 99, 105 (N.Y. 1928).

causing him to drop a package that contained fireworks, which then exploded. This caused scales at the other end of the platform to fall and injure the plaintiff.[67] But unlike the guard in *Palsgraf*, companies that manufacture and distribute IoT products have ample notice that these devices might have significant security defects and that insecure devices are frequently used to carry out damaging cyberattacks.

Proximate cause and the foreseeability principle ultimately ensure that only a party who has a choice between alternative courses of action and chooses, "by some standard, incorrectly," can be held liable.[68] For example, the foreseeability test recently adopted in the *Third Restatement*, commonly referred to as the "risk standard," is based on "the idea that an actor should be held liable only for harm that was among the potential harms—the risks—that made the actor's conduct tortious."[69] Despite its precise formulation, the doctrine of foreseeability is broad enough to encompass considerations of "policy, practicality, and case-specific fairness."[70]

Professor Grady has explained the reasonable foresight test as, ultimately, addressing whether there is "a merely coincidental relationship" between the accident and the defendant's breach of duty.[71] In contrast, the direct consequences doctrine "examines concurrent causes to see whether the person responsible for the second cause has cut off the liability of the person responsible for the first cause."[72] One subset of direct consequences cases are those cases where a defendant "negligently create[s] tempting opportunities for judgment-proof people" to cause harm.[73] One example is the case of *Weirum v. RKO General, Inc.*, which involved a defendant radio DJ who ran a contest where he would travel around Los Angeles in a fast car and give prizes to the first listener to reach him.[74] The defendant was jointly liable when two teenage listeners, racing at high speeds, injured a plaintiff's family member.[75] *Weirum* is an example of what Professor Grady refers to as a "free radicals" case, where the court must determine whether "a reasonable person in the defendant's position, before the accident, must have been able

67. *Id.* at 99.
68. Owen, *supra* note 63, at 1280.
69. RESTATEMENT (THIRD) OF TORTS: LIAB. FOR PHYSICAL AND EMOTIONAL HARM § 29 cmt. d. (AM. LAW INST. 2010)
70. Owen, *supra* note 63, at 1293.
71. Grady, *supra* note 64, at 299.
72. *Id.*
73. *Id.* at 306 (Professor Grady categorizes these as EFR (Encourage Free Radicals) cases).
74. 539 P.2d 36 (Cal. 1975).
75. *Id.* at 38–40.

to foresee that his act or omission would likely encourage free radicals."[76]

As Professor Grady has explained, the core principle of the proximate cause test is that "[r]esponsible people should avoid creating opportunities for irresponsible people to do harm."[77] That is precisely what is not happening in the IoT marketplace—manufacturers who distribute IoT devices are failing to provide adequate security, and are therefore creating opportunities for hackers to use the devices to harm innocent bystanders. Ultimately, a judge's determination of whether to extend liability to vendors of insecure devices will turn on an evaluation of the desirability, fairness, and likely deterrent impact that such liability would have on manufacturers.[78]

The combination of the heavy losses suffered by victims of DoS and other attacks and the significant role that insecure IoT devices play in such attacks should justify an extension of products liability to protect bystander victims. It would be hard to argue that victims of network attacks are not "foreseeable bystanders" of these security defects when industry and incident reports cite with increasing urgency the significant risks created by these insecure devices.[79] These security flaws are known defects, and the risk of third party hacking caused by these defects has been well documented.

Mr. Krebs was not the first victim of a network attack carried out by a so-called "zombie army" of hacked IoT devices, and he will not be the last.[80] In fact, victims of IoT-based attacks would not be the first bystanders to recover for harms caused by defective software. As Professors Rustad and Koenig described in their seminal article on tort liability for cybercrime, courts have had no problem imposing liability where defective software causes physical injury or

76. Grady, *supra* note 64, at 308.

77. Grady, *supra* note 64, at 295.

78. *See* Owen, *supra* note 63, at 1293; Rustad & Koenig, *supra* note 13, at 1602 n.251 (discussing Judge Andrews's dissent in *Palsgraf*).

79. *See, e.g.*, FED. TRADE COMM'N, INTERNET OF THINGS: PRIVACY & SECURITY IN A CONNECTED WORLD 12 (2015), https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf; Akamai Techs., *supra* note 9; Dick O'Brien, *The Internet of Things: New Threats Emerge in a Connected World*, SYMANTEC OFFICIAL BLOG (Jan. 20, 2014), https://www.symantec.com/connect/blogs/internet-things-new-threats-emerge-connected-world.

80. *See* Lorenzo Franceschi-Bicchierai, *In the Future, Hackers Will Build Zombie Armies from Internet-Connected Toasters*, VICE: MOTHERBOARD (July 5, 2016, 8:30 AM), https://motherboard.vice.com/read/in-the-future-hackers-will-build-zombie-armies-from-internet-connected-toasters (describing an attack on a jewelry store website carried out using 25,000 hacked CCTV cameras and another attack several days later against three U.S. gaming companies using 1,000 internet-connected cameras).

death.[81] For example, a man in Alabama successfully sued General Motors after a defective computer chip caused his truck engine to stall in the middle of an intersection, which led to his car being hit by a tractor trailer, killing his grandson.[82] While DoS attacks may not cause the same type of bodily injuries, they are still proximate causes of severe property damage and should be considered reasonably foreseeable given the widespread recognition of the risks they pose.

IV. TOWARDS LIABILITY FOR DEFECTIVELY INSECURE DEVICES

Insecure devices pose a significant threat to internet security in general, to destruction of digital assets and network infrastructure in particular, and to the population as a whole. As early as 2007 the National Academy of Sciences recognized the scope of the problem. In the preface to their comprehensive report on cybersecurity, the Chair acknowledged that, given the important role of internet infrastructure in the global economy, it is:

> in the public interest to have a safe and secure cyberspace. Yet cyberspace in general, and the Internet in particular, are notoriously vulnerable to a frightening and expanding range of accidents and attacks by a spectrum of hackers, criminals, terrorists, and state actors who have been empowered by unprecedented access to more people and organizations than has ever been the case with any infrastructure in history. Most of the people and organizations that increasingly depend on cyberspace are unaware of how vulnerable and defenseless they are, and all too many users and operators are poorly trained and equipped. Many learn only after suffering attacks. These people, and the nation as a whole, are paying enormous costs for relying on such an insecure infrastructure.[83]

The report predicted that the cybersecurity risks created by the proliferation of "pervasive computing" (IoT) devices would require "security solutions and approaches to scale upward by many orders of magnitude."[84] The report specifically identified the need for embedded systems to enable "evolution of security" through "remote

81. Rustad & Koenig, *supra* note 13, at 1578.
82. Gen. Motors Corp. v. Johnston, 592 So. 2d 1054 (Ala. 1992).
83. NRC REPORT, *supra* note 3, at xi.
84. *Id.* at 197.

upgrade[s]" in order to adjust to rapid changes in technologies and capabilities.[85]

Insecure IoT devices pose a unique problem that products liability law is well positioned to address, but that will require adjusting the standard defect paradigm applied by courts. Many devices, like the ones used to attack the Krebs site, are vulnerable because they are configured to be administered with default credentials, and can easily be identified and accessed by malicious hackers.[86] These default settings are not difficult or costly to change, so a failure to take such precautions would likely be deemed a design defect. But other vulnerabilities, such as those caused by coding errors embedded in basic protocols common across different devices or services, can be more difficult to identify or fix.[87]

Some have argued that software vulnerabilities are more akin to manufacturing defects and could fit within that existing strict liability regime.[88] Fundamental flaws that are hard to detect might more appropriately be treated as manufacturing defects under a strict liability regime. It might be possible, for example, to argue that certain types of coding errors and oversights (such as "buffer overflow" vulnerabilities[89]) are akin to manufacturing defects. This may not be a perfect fit for many IoT security flaws, but certain types of vulnerabilities could be treated as random errors in the software production line akin to those likely to cause an exploding soda bottle.[90] Imposing strict liability in such cases would have the added benefit of encouraging manufacturers to insure against the loss and therefore spread the cost more evenly across the industry rather than forcing innocent bystanders to bear the risk.[91]

Given the nature of software vulnerabilities, it is likely that most insecure IoT products liability claims would be analyzed as design

---

85. *Id.* at 198.

86. *See* Zach Wikholm, "When Vulnerabilities Travel Downstream," FLASHPOINT BLOG (Oct. 7, 2016), https://www.flashpoint-intel.com/when-vulnerabilities-travel-downstream/.

87. *See* Bruce Schneier, *The Internet of Things is Wildly Insecure—And Often Unpatchable*, WIRED (Jan. 6, 2014, 6:30 AM), https://www.wired.com/2014/01/theres-no-good-way-to-patch-the-internet-of-things-and-thats-a-huge-problem.

88. *See* Scott, *supra* note 14, at 469–70 (detailing the debate over whether to impose strict liability on software vulnerabilities).

89. *See generally* Peter Bright, *How Security Flaws Work: The Buffer Overflow*, ARS TECHNICA (Aug. 25, 2015, 9:00 PM), http://arstechnica.com/security/2015/08/how-security-flaws-work-the-buffer-overflow/ (explaining "butter flow" vulnerabilities).

90. *See, e.g.*, Escola v. Coca Cola Bottling Co. of Fresno, 150 P.2d 436 (Cal. 1944) (holding bottling company liable for harm caused by an exploding bottle).

91. Emmett Vaughn & Therese Vaughn, Fundamentals of Risk and Insurance 126 (10th ed. 2007).

defect claims.[92] But the design defect paradigm still leaves much to be desired. Courts are largely split over the question of what standard to apply in design defect cases.[93] This uncertainty will make it more difficult to resolve insecure IoT products liability claims and could make outcomes more random or incentivize forum shopping by plaintiffs and defendants. Still, regardless of whether courts apply the traditional *Second Restatement* test, the risk-utility test, the consumer expectations test, or some mix of all three, many of these vulnerabilities are so egregious that they will meet any standard.

The consumer expectations test is likely the most difficult to apply to insecure software defect claims because the test is poorly suited to address defects in complex systems.[94] Consumers, especially those purchasing IoT devices, do not typically have an understanding of how their devices function, their role in the internet ecosystem, or the significance of any security vulnerabilities embedded in those systems. A purchaser of a DVR (or a webcam, or a "smart" refrigerator) likely does not have any expectations about how the software in that device will function. So long as the device carries out the tasks that that the user expects, the user is not likely to think about what software is embedded in the device or how the software was developed. If a device has been hacked and is simultaneously being used as part of a botnet to attack servers of a major news site or gaming company, the user may not even be aware of that fact.

The risk-utility test would provide a much better way to resolve design defect claims for insecure IoT devices. Under the risk-utility test, courts analyze whether the defect could have been avoided through adoption of a reasonable alternative design. Because most vulnerabilities are the result of unintentionally bad coding or poor design choices (like weak default passwords and failure to follow best practices), it would be straightforward to argue that an alternative software design could have enabled the same functionality without creating the vulnerability. But the design defect analysis would still be limited in time, focusing entirely on the pre-sale behavior of the manufacturer and not on their role in securing devices post-sale.

Software vulnerabilities present an evolving problem, distinct from most product defects that have been considered in the past.

---

92. *See* sources cited *supra* notes 14 and 52 (articles discussing the application of products liability principles to computer software).

93. *See supra* note 21 and accompanying text.

94. *See* Tincher v. Omega Flex, Inc., 104 A.3d 328, 388 (Pa. 2014).

Unlike a Ford Pinto design that creates a risk of a gas tank explosion even in a minor traffic accident,[95] an IoT device may not be vulnerable, even in retrospect, at the time that it is designed or sold. Security researchers and hackers are constantly discovering new vulnerabilities, and these discoveries require software vendors to update their software on a regular basis.[96] These post-sale updates likely make software vendors even more likely to be liable for downstream vulnerabilities than modern automobile manufacturers. In many cases, software companies have an even greater degree of control over the downstream use of their products,[97] and the manufacturers' ongoing post-sale involvement in monitoring and maintaining that software increases their responsibility to address defects down the line. Consider how often the average user of a smartphone, laptop, app, or connected device receives or initiates a software or firmware update compared to how infrequently most car owners take their vehicle in to process a manufacturer's recall.

Many manufacturers and vendors of IoT devices are also likely have sufficient contact with their users to trigger a post-sale duty to warn. Take, for example, a product like a "smart" home security system that the user can remotely access and that the vendor can remotely control.[98] The vendor not only knows who the user is, where they live, and how to contact them in the event of an emergency, the vendor also has direct control over the insecure device itself.[99] Such extensive post-sale contact with the user and control over the product would almost certainly justify imposing a post-sale

---

95. See Gary T. Schwartz, *The Myth of the Ford Pinto Case*, 43 RUTGERS L. REV. 1013, 1015–17 (1991).

96. *See* NRC REPORT, *supra* note 3, at 182 ("One key issue in the security of legacy systems is patch management."); Robert W. Hahn & Anne Layne-Farrar, *The Law and Economics of Software Security*, 30 HARV. J. L & PUB. POL'Y 283, 318 (2006) ("it has been widely recognized that computer security is as much a management problem as it is a technology problem.") (footnote omitted) (quoting LAWRENCE A. GORDON ET AL., 2005 CSI/FBI COMPUTER CRIME AND SECURITY SURVEY 14 (2005), http://www.firenetltd.it/materiale/FBI2005.pdf.); Dan J. Klinedinst, *Coordinating Vulnerabilities in IoT Devices*, SOFTWARE ENGINEERING INST.: CERT/CC BLOG (Jan. 27, 2016), https://insights.sei.cmu.edu/cert/2016/01/coordinating-vulnerabilities-in-iot-devices.html; *Why Security Updates Are Vital*, NORTON, https://us.norton.com/vital-security/article (last visited May 8, 2017).

97. *But see* Klinedinst, *supra* note 96 ("Companies like Microsoft and Google have public ways to report vulnerabilities, standard methods of patching, bug bounty programs, and other practices. However, many of the companies that make consumer products do not yet have these practices in place.").

98. *See, e.g.*, *Frequently Asked Questions*, ALARM.COM, https://www.alarm.com/get_started/faq.aspx (last visited May 8, 2017).

99. Compare this to the automotive industry where there are several layers of removal between the average customer and the manufacturer (e.g. the car dealer processing the sale and the service station processing repairs).

duty to warn about defects. But these contacts could also justify additional post-sale duties than have not previously been imposed on vendors. On the other hand, many manufacturers of low-cost consumer electronic devices do not design their products with security in mind and might not retain sufficient contacts to effectively patch or mitigate vulnerabilities.[100] This is the result of a "fundamental market failure at work."[101]

Another important question that could be raised in products liability cases related to insecure IoT devices is whether manufacturers and vendors have a post-sale duty to patch insecure software. Unlike in traditional duty-to-warn cases, the victim of a cyberattack likely has no relationship to the manufacturer or the user who could be warned of the defect post-sale. The user may not know or care that their IoT device is insecure or that the device has been hacked, and use of the device in a botnet to attack some innocent bystander would not directly impact the user. Therefore, even if a manufacturer has a duty to warn the user, there is no guarantee that the user will take affirmative steps to remedy the problem (like changing the default password or updating the software). Instead, it would be more consistent with the underlying purposes of products liability law to hold manufacturers liable if they fail to patch significant vulnerabilities that they know or should have known could cause harm to others.[102]

Like the post-sale duty to warn under the *Third Restatement*, a post-sale duty to patch could be evaluated under a risk-utility analysis based on what a reasonable person in the manufacturer's position would have done.[103] Courts and commentators have recognized that the post-sale duty to warn imposes significant burdens on manufacturers, but nevertheless over half the states have adopted the *Third Restatement* approach.[104] Commentators and legislators

---

100. *See* Klinedinst, *supra* note 96. In this sense, where IoT vendors fall on the "spectrum" of post-sale contacts will be key in determining their post-sale duties. Some vendors have such extensive contacts with users and control of devices that it would be reasonable to impose new post-sale duties.

101. *Understanding the Role of Connected Devices in Recent Cyber Attacks: Joint Hearings Before Subcomm. on Commc'ns & Tech. and Subcomm. on Commerce, Mfg., & Trade of the H. Comm. on Energy & Commerce,* 114th Cong. 3 (2016) (statement of Bruce Schneier, Fellow, Berkman-Klein Center at Harvard University), http://docs.house.gov/meetings/IF/IF17/20161116/105418/HHRG-114-IF17-Wstate-SchneierB-20161116.pdf.

102. A more complex question would be whether a vendor's potential liability is extinguished once they have given adequate warning to the user. This would likely depend on the degree of direct control over the device and whether there was a reasonable and cost-effective way for the manufacturer to cure the defect directly via a patch. But the intervening act of a user who rejects such a patch could also break the chain of proximate cause.

103. *See supra* note 28, 31 and accompanying text.

104. *See* Lens, *supra* note 28, at 1020–21.

have already expressed concern over the potential impact that cybersecurity regulations might have on innovation and technological advances.[105] Still, the lack of clear legal standards and guiding best practices for patch management has long been recognized as a problem in securing critical infrastructure.[106] Without a post-sale duty to patch, it is not clear how a court could impose liability on a company for failing to secure embedded software that is still in use. Absent liability, innocent victims would have to bear the losses caused by these unsafe products and manufacturers would not be properly incentivized to take precautions; failing to impose liability for these defects would run contrary to the core purposes of products liability law.[107]

CONCLUSION

The proliferation of insecure IoT devices poses a significant risk to the Internet ecosystem in general, and to individual users and companies that rely on Internet services in particular. These insecure devices have already been used to carry out high-profile denial-of-service attacks on websites and service providers. Attacks impose significant costs on innocent bystanders and will likely give rise to litigation. A traditional products liability model could provide a means to adjudicate claims arising from injuries caused by insecure devices. The most significant hurdles to insecure IoT products liability claims would be (1) the application of the risk-utility defect test and (2) the reasonable foreseeability of the harm under a proximate cause analysis. Many of the risks posed by insecure devices could be mitigated by imposing a post-sale duty to patch vulnerable software, though legislators have so far been hesitant to impose such regulations on software vendors. Regardless of the mechanism, some manufacturers should bear that costs imposed by the deployment of insecure devices so that vendors take adequate precautions to prevent broad-scale harm to Internet users.

---

105. *See Understanding the Role of Connected Devices in Recent Cyber Attacks: Joint Hearings Before Subcomm. on Commc'ns & Tech. and Subcomm. on Commerce, Mfg., & Trade of the H. Comm. on Energy & Commerce*, 114th Cong. 1–2 (2016) (Statement of Greg P. Walden, Chairman, Subcomm. on Commc'ns & Tech. of the H. Comm. on Energy & Commerce), http://docs.house.gov/meetings/IF/IF17/20161116/105418/HHRG-114-IF17-MState-W000791-20161116.pdf.

106. *See* COMM. ON CRITICAL INFO. INFRASTRUCTURE & THE LAW, NAT'L RESEARCH COUNCIL, CRITICAL INFORMATION INFRASTRUCTURE PROTECTION AND THE LAW 50–51 (Stewart D. Personick & Cynthia A. Patterson eds., 2003).

107. *See supra* note 17 and accompanying text.