Florida State University Law Review

Volume 47 | Issue 3 Article 1

Spring 2020

More Is Different: Tort Liability of Compromised Systems in Internet Denial of Service Attacks

Robert A. Heverly

MORE IS DIFFERENT: TORT LIABILITY OF COMPROMISED SYSTEMS IN INTERNET DENIAL OF SERVICE ATTACKS

ROBERT A. HEVERLY*

"We attack not only to hurt someone, to defeat him, but perhaps also simply to become conscious of our own strength."

Friedrich Nietzsche

---

* Robert A. Heverly is an Associate Professor of Law at Albany Law School. This article began as one making a different argument while I was a Fellow at the Information Society Project at Yale Law School. I cannot begin to name the colleagues and mentors who read, responded to and critiqued the article over time, or who listened to presentations at a variety of workshops and presentations, but they were many and varied, and each contributed something useful to the article. I am deeply appreciative of the community of scholars that inhabits this space. Errors that remain after this lengthy development process are mine alone.

I. INTRODUCTION

Imagine a world in which stores, people, and information could be made to disappear at the whim of a distant and unknown magician. One moment they would be there, the next they would be gone. Now imagine further that the magician, to accomplish this dastardly feat, uses all of us to achieve her goal. The hidden resources will likely return, but anyone who needs them then, at that moment, will not be able to reach them. The magician might do this because she can, to prove she can, because she disagrees with whomever or whatever she has hidden, because someone has paid her, or because she hopes to extract payment from the people or owners of the resources she has hidden. The magician could not have done it without all of us. In these circumstances, to whom are we, those used by the magician, liable in damages suffered due to the interruptions?

The situation is not as fanciful as it at first might appear. There is a method of attacking internet websites that mirrors the above scenario very closely.[1] When an internet Denial of Service attack (DoS) takes place, the attacker uses computers and networking systems belonging to others to stop web users from accessing or utilizing networked resources.[2] When a user attempts to read a web page, they receive a message that the page either can't be found or is not responding.[3] This result is brought about by an attacker who has either compromised computers belonging to others or who utilized the functioning of the network itself to overwhelm the target web server.[4]

Denial of Service attacks were first identified as a significant potential problem around the turn of the century.[5] From February 7-9, 2000, the productive activity of a number of well-known commercial Internet sites—sites that had become essentially household names in relation to Internet commerce—ground to a halt.[6] At the same time, the sites' Internet connections were buzzing along at speeds higher than ever, receiving large numbers of "requests" for information from computers across the Internet.[7] Unfortunately, the commercial sites were not receiving valid requests for information; instead, they

---

1. *See generally* MOLLY SAUTER, THE COMING SWARM: DDOS ACTIONS, HACKTIVISM, AND CIVIL DISOBEDIENCE ON THE INTERNET, 10 (2014).

2. *See generally* A.B. Tickle et al., *Background*, *in* AN INVESTIGATION INTO THE DETECTION AND MITIGATION OF DENIAL OF SERVICE (DoS) ATTACKS: CRITICAL INFORMATION INFRASTRUCTURE PROTECTION 9, 10-11 (S.V. Raghavan & E. Dawson eds., 2011).

3. *See generally* SHUI YU, DISTRIBUTED DENIAL OF SERVICE ATTACK AND DEFENSE 2-5 (2014).

4. *Id.*

5. *Id.* at 2.

6. Some of the sites attacked included Yahoo!, Amazon, and CNN. YU, *supra* note 3, at 2.

7. *Id.*

wattacks.[8] The useless packets clogged up the veins of the Internet's transportation system.[9] In some cases, they caused the sites' servers to crash, sometimes with concomitant injury to hardware or software setups.[10]

The total loss from the February 2000 attacks was estimated to be above the two-million-dollar mark.[11] Other attacks have resulted in valid users being unable to obtain information, purchase items, or otherwise interact with the sites.[12] In one case, a sustained DoS attack caused an Internet Service Provider in the United Kingdom to close.[13] While the attack persisted, none of its subscribers could access the Internet.[14] Without the revenues generated by being able to provide Internet access to its subscribers, the company was forced to shut down.[15] Since then, the number of attacks has grown in terms of quantity, sophistication, and strength.[16] In addition, attacks have shifted in nature from those initiated by independent or groups of hackers becoming conscious of their own strength to organized criminal syndicates using networks of compromised systems to extort money from businesses who depend on Internet communications for their livelihoods or to spread their messages far and wide.[17]

Denial of Service attacks provide us with a unique opportunity to consider the role of negligence liability in the modern technological age. A DoS attack is launched by an attacker using technological resources, specifically computing and network power,[18] owned and

---

8. *Id.*

9. *Id.* at 1-2.

10. *Id.* at 2.

11. WIRED NEWS REPORT, *Prison Urged for Mafiaboy* (June 20, 2001); https://www.wired.com/2001/06/prison-urged-for-mafiaboy/ (last visited June 4, 2020).

12. Matt Richtel & Sara Robinson, *Several Web Sites Attacked Following Assault on Yahoo*, N.Y. TIMES, Section A, Page 1 (Feb. 9, 2000), https://www.nytimes.com/2000/02/09/business/several-web-sites-attacked-following-assault-on-yahoo.html (last visited June 4, 2020).

13. Graeme Wearden, *DoS Attack shuts down ISP Cloud Nine*, WIRED (Jan. 23, 2002) https://www.zdnet.com/article/dos-attack-shuts-down-isp-cloud-nine/ (last visited June 21, 2002); *See also*, Kevin P. Kalinich and Kristina McGrath, *Identifying and Evaluating the Business Impact of Network Risks and Liabilities*, 33 WTR BRIEF 18, 21 (2004) ("In extreme cases, lack of network exposures insurance can be fatal to an entity. When a small ISP called Cloud Nine Communications crashed to earth, it blamed hackers for overwhelming its network with bogus traffic and told customers it was forced to sell the company after finding insurance would not cover the cost of bringing its servers back online").

14. *Id.*

15. *Id.*

16. *See* Danny MacPherson, Craig Labovitz, & Mike Hollyman, *Worldwide Infrastructure Security Report: Volume IV* 9 (2008).

17. *See* SAUTER, *supra* note 1, at 39-41.

18. This concept of the amount of computing and networking power forms a central part of my claims in this article and is further defined later in the article. *See infra* Section III. I sometimes refer to this concept via the short-hand "power."

operated by others.[19] It is the liability of those "others"—the utilized system owners—that makes the questions raised particularly interesting, as well as particularly complex. Liability is an easier question if we can identify the attacker: this person or persons is or are most likely subject to a liability under a number of tort and statutory theories.[20] Most likely, however, we cannot identify the attackers, and if we can, they are out of our jurisdictional reach and unlikely to be brought within it.[21] Even if the attackers are found and served, they are unlikely to have the funds necessary to satisfy those injured by their actions. To find compensation for a DoS attack's victim, we must turn to the unwitting participants in the attacks in search of recoverable damages.

It is this need to focus on the negligence of internet users that makes the DoS scenario so complex. As we will see, defendants will have more and varied potential identities, more and varied motivations, engage in more and varied acts, and have more and varied levels of expertise and experience than is true for the majority of even complex negligence cases. DoS cases, given this context, involve *more*, and in this context, *more is different*.[22]

A DoS attack involves numerous computer and networked systems often spread across a wide geographic, perhaps even worldwide, range.[23] An attack involves actors—compromised computer system owners—who are unknown and cannot be easily identified, as well as those that are known or identifiable but that do not know each other and have no significant connection with each other.[24] The compromised systems used in the attacks vary in processing power, networking power, hard drive storage, random access memory, and installed operating systems.[25] Their owners span the gamut from large scale international corporations and organizations with rooms dedicated to computers and servers, to individuals holding three-year old mobile

19. *See* Ethan Zuckerman et al., *Distributed Denial of Service Attacks Against Independent Media and Human Rights Sites*, BERKMAN KLEIN CTR. FOR INTERNET & SOC'Y HARV. U. 1, 16-18 (Dec. 20, 2010), https://cyber.harvard.edu/sites/cyber.harvard.edu/files/2010_DDoS_Attacks_Human_Rights_and_Media.pdf.

20. *See, e.g.*, Massre v. Bibiyan, No. 12 Civ. 6615(KPF), 2014 WL 2722849, at *4 (S.D.N.Y. June 16, 2014) (upholding Magistrate Judge's recommendation of damages against defendant for denial of service attack).

21. *See* Joshua McLaurin, *Making Cyberspace Safe for Democracy: The Challenge Posed by Denial-of-Service Attacks*, 30 YALE L. & POL'Y REV. 211, 216-17 (2011).

22. Philip W. Anderson, *More is Different*, 177 SCI. 393 (1972).

23. *See* Stephen E. Henderson & Matthew E. Yarbrough, *Suing the Insecure?: A Duty of Care in Cyberspace*, 32 N.M. L. REV. 11, 13 (2002).

24. *See* Zuckerman et al., *supra* note 19, at 17.

25. *Id.*

phones in their hands.[26] They do not necessarily share a common goal or plan and are not engaged in any kind of joint activity.[27] There is very little to bind them together other than their connection to the internet and their use by the attacker.[28] The complexity that arises from the heterogeneity of the pool potential of defendants goes beyond these technological elements, however, as the owners themselves vary not only in structure and ownership regimes, but in sophistication and understanding of even the basics of the technologies that we all use.[29] Some are older individuals with their first computer, perhaps given to them by a son or daughter. Others are college students, sophisticated in use but not always inclined to understand the fundamentals of the underlying operations, while still others are companies with server farms through which they earn profits on previously unheard of scales of magnitude. The heterogeneity of the potential defendants is limited only by the heterogeneity of internet participants themselves, and this grouping is hardly limited in any realistic manner.

Because the third-party owners of systems utilized in DoS attacks vary greatly in their sophistication and potential for causing injury, I argue that system owners as an overall broad category of defendants should neither be *per se* liable for injuries suffered by internet resources that are the victims of DoS attacks using, nor should they be *per se* immune. Adapting the well-established notion of "communities of interest" from other areas of law, including election law, I argue that the tort mechanisms best suited to reaching this conclusion include duty[30] and proximate cause, but there is a complicated array of negligence doctrines relevant in this context.[31]

Using the communities of interest concept,[32] I argue that those who control only small amounts of computing and networking and power make up one community of interest and should have a duty to act to

---

26. *See* Kim Zetter, *Hacker Lexicon: What are DoS and DDoS Attacks?*, WIRED (Jan. 16, 2016), https://www.wired.com/2016/01/hacker-lexicon-what-are-dos-and-ddos-attacks/.

27. *Id.*

28. *Id.*

29. *Id.*

30. "An actor whose negligence is a factual cause of physical harm is subject to liability for any such harm within the scope of liability, unless the court determines that the ordinary duty of reasonable care is inapplicable." RESTATEMENT (THIRD) OF TORTS: PHYSICAL & EMOTIONAL HARM § 6 (AM. LAW. INST. 2010).

31. *See infra* Section II.

32. *See generally* Stephen J. Malone, *Recognizing Communities of Interest in a Legislative Apportionment Plan*, 83 VA. L. REV. 461 (1997) (discussing communities of interest in the election law setting); Michael McClosky, *Local Communities and the Management of Public Forests*, 25 ECOLOGY L.Q. 624, 627 (1999) (discussing communities of interest in the environmental law setting and noting: "As a consequence of this push toward expediency and community partnerships, a conflict is created between communities of place and communities of interest. The push toward localism exalts the interests of given communities of place (those in and around the public forests) over more extended communities of interest.")).

prevent DoS attacks launched using those systems only where their resources played a significant role in the damage caused by the attack. This will occur only where the target of the attack is also small, limiting the exposure of the small community of interest members in terms of damages for such attacks. In contrast, I argue that those who control large amounts of computing and networking power make up a second community of interest and should have such a duty imposed upon them. This reflects their larger capacity to cause damage and their commercial or financial motives for being connected to and providing services on or through the internet. The middle group, those who are neither small nor large, make up a third community of interest, and provide courts with an opportunity to use methods other than duty to end litigation early or continue it on where warranted.

My primary goal here is to provide courts with a path through the descriptive and normative thickets that present themselves in the DoS attack scenario. Lawyers, potential parties, insurers, and legislators are also likely to find the analysis instructive, to the extent they remain interested in these same issues. I begin in earnest in the next section by outlining the technologies and methods used by the attackers, including the systems that have either been compromised or are utilized in unintended ways to launch DoS attacks. Section II then analyzes the difficulties that would confront a DoS victim plaintiff from a doctrinal standpoint, describing the flexibilities that flow from those complexities for courts confronted with DoS cases. Section III proposes a clear path forward based on an appropriate normative framework built from concerns of fairness, judicial decision-making, and appropriate, internet-focused policy. Section IV concludes with a broadening of the scope of the conclusions given the increasing complexity and thin interconnectedness of individuals and entities in the modern technological world.

While questions of standard of care may also be well placed to play an important role in DoS litigation, leaving some determinations to the fact finder may unnecessarily embroil unsophisticated, low-intensity internet users in litigation that places a significant burden on them in regard to their contribution to the injury suffered. In contrast, the specter of liability should encourage larger contributors to such attacks to maintain a higher standard of care, one that might help prevent such attacks in the first place. In addition, by failing to provide a complete legal remedy for victim websites, the proposed framework aims to encourage the continued development of robust and active responses by the sites targeted by such attacks, providing the Internet with a stronger and more concerted effort to overcome the attacks both from the resource side and the victim side. It also addresses potentially significant doctrinal issues of fairness and of the judiciary's ability to

realistically address the far-flung disparities—both in nature and in location—in potential DoS defendants.

II. DENIAL OF SERVICE ATTACKS: THE MECHANICS

Denial of Service attacks can be divided into five categories of "players"[33]: the initiators of the attacks (the attackers);[34] the networks or computers that have been compromised and used in the attacks (the compromised systems);[35] the makers and distributors of the software that is compromised by the attackers and that allows them to

33. This terminology is not necessarily uniform in the literature. *But see,* John D. Howard & Pascal Meunier, *Using a 'Common Language' for Computer Security Incident Information in* COMPUTER SECURITY HANDBOOK 3.2, 3.19 (Seymour Bosworth & M. E. Kabay eds., 4th ed. 2002). Sometimes parties are identified by the type of technology that they own or use, or the commercial function that they play. *See, e.g.,* Kalinich and McGrath, *supra* note 13. For example, articles may discuss "Internet Service Providers" (ISPs) as being potentially subject to liability based simply on their status as ISPs. *See, e.g.,* Jennifer A. Chandler, *Security in Cyberspace: Combatting Distributed Denial of Service Attacks,* 1 U.O.L.T.J. 231 (2004). This is a perfectly reasonable approach, but I do not adopt it here. As we shall see, more important for my analysis than the commercial service that a party is providing is the extent of their role in a particular DoS attack. For that reason, I shy away from discussing types of services or owners, and rather, discuss those involved as "players" in the attack, focusing on how they are involved in particular DoS attacks.

34. "Attackers" is used here in place of the more common "hacker" because of the latter's loss of precise meaning over time. What was originally a term coined to define those who were interested not necessarily in injuring computer systems and networks, but only in investigating them, has morphed into a phrase used to describe anyone who does anything that could potentially be seen as unauthorized. Yet the historical understanding continues to confuse its use, and so an alternative term is adopted here.

35. The systems involved in DoS attacks have the two components required to initiate such an attack: *computer power* (also referred to as "processing power") and *transmission power.* Both transmission facilities and compromised systems may be made up of systems that have either or both kinds of power. The distinction between the two results not from the type of power that each possesses, but rather from the way in which Internet protocols lead to the expectation that certain communications traffic will be passed on from one system to another. Internet protocols are packet based, and as such, each communication is broken into packets, or pieces, then transmitted and received, and then reassembled at the receiving end. Systems along the way are expected to pass such traffic along. When this occurs, the Internet is functioning as it should. Transmission facilities are those facilities that are simply passing along what appears to be legitimate communications traffic. No control of transmission facilities is necessary to initiate a DoS attack, and in fact at times the Internet's protocols themselves may be used to amplify an attack. Control of at least some compromised systems, on the other hand, is necessary, as these are the engines that are used to initiate the attacks themselves.

"zombify"[36] the compromised systems; and, the networks and computer owners who pass the attack traffic on in the regular course of business (transmission facilities).[37]

For purposes of analyzing DoS liability, it is not likely to be determinative whether the owner or operator of a compromised system is an Internet Service Provider (ISP), a business, or an individual. The form of ownership, the name of the business or person, or even the type of business is largely irrelevant to an inquiry into liability. The question is not, "Is this an Internet Service Provider?" but rather "Was a particular system compromised such that its transmission or processing power was used by an attacker?" We must be particularly cautious in asserting that liability may exist in one circumstance or another based on the nature of the entity involved. It is much more likely that *any* entity, regardless of form, may be liable where their facilities or systems are compromised, while any other entity may be held blameless where the opposite is true.

The target of a DoS attack can be any Internet site or service. So long as the target is connected to the Internet, a DoS attack is possible.[38] Thus, commercial, governmental, non-profit, individual, and other sites connected to the Internet are vulnerable. Damages from such attacks might be easy to identify, such as lost profits, or more difficult to quantify, such as the loss of loyalty of a regular patron to the site or a loss of a reputation of quickness and reliability. In any case, there is likely to be damage from such an attack.

In contrast with the broad range of possible targets, the class of DoS attackers is narrower. A DoS attacker is any person who initiates an attack against a target site, using the compromised systems of computer owners and ISPs, and utilizing as well the general transmission protocols of the Internet.[39] Denial of service attackers may fit into the mold of those who are popularly considered "hackers," but most recently they have been associated with criminal syndicates seeking to extort money from Internet-based businesses.[40] They are not known, nor do they generally wish to become known.[41] They go to great pains to hide their identities and their activities.[42] Because the Internet was

---

36. To zombify: "To transform into a zombie." *Zombify*, OXFORD ENGLISH DICTIONARY (3d ed. 2005).

37. Diane E. Levine & Gary C. Kessler, *Denial-of-Service Attacks, in* COMPUTER SECURITY HANDBOOK 11.1, 11.2.1 (Seymour Bosworth & M. E. Kabay eds., 4th ed. 2002).

38. *Id.*

39. *Id.*

40. W.J. Caelli, S.V. Raghavan, S.M. Bhaskar, & J. Georgiades, *Policy and Law: Denial of Service Threat, in* AN INVESTIGATION INTO THE DETECTION AND MITIGATION OF DENIAL OF SERVICE (DoS) ATTACKS 34 (S.V. Raghavan & E. Sawson eds. 2011).

41. Levine & Kessler, *supra* note 37, at 11.1, 11.2.1.

42. *Id.*

designed for ease of communication and not for security or identity tracking, and because attackers are armed with extensive knowledge of network protocols and the networked environment, attackers are often able to hide their identities from target sites and from law enforcement or security experts who attempt to determine a particular attack's origin.[43]

In the context of DoS attacks, the initiators are possibly even more difficult to locate than with other types of network attacks, such as viruses and system intrusions.[44] DoS attacks are generally distributed, originating from a variety of compromised systems controlled by the attacker.[45] The identity of the communication packets that are being sent to and causing the service denial are identifiable by the target site.[46] But many times, the compromised systems either improperly log the traffic going to, going through, or originating within them.[47] Even if logging were properly done by the compromised sites—an unlikely eventuality given that properly administering their facilities to begin with would most likely preclude their use in a DoS attack—DoS attackers often successfully fake IP and other identifying information such that examining the logs would be a dead-end.[48]

If we could locate DoS attackers, they are likely to be either individuals, loose groups of confederates, or criminal syndicates, and are either unlikely to have the kind of resources that would be needed to ma*f*ke the target sites whole or those resources would be practically impossible to gain control over.[49] Given the nature of DoS attackers, we can reach one important conclusion about them: they are not likely to be a significant part of any regime of liability established in relation to DoS attacks. They are instead absent, invisible, unreachable, or not worth reaching. DoS target sites must thus search for other responsible parties from whom to recoup their losses.

Which brings us to the subjects of this article: the compromised systems. Compromised systems can be nearly any computer or transmission facility connected to the Internet.[50] They may have become

---

43. MICHAEL CALCE & CRAIG SILVERMAN, MAFIABOY: A PORTRAIT OF THE HACKER AS A YOUNG MAN 115 (2008) (Mafiaboy was located primarily because he bragged about the attacks in a chat room).

44. *See*, Hal Burch & Bill Cheswick, Tracing Anonymous Packets to Their Approximate Source, 2000 LISA XIV (Dec. 3-8, 2000) (describing various methodologies for attempting to locate the source of a DoS attack).

45. Levine & Kessler, *supra* note 37, at 11.1, 11.2.1.

46. *Id.*

47. *Id.* at 11.1, 11.3, 11.5.

48. *Id.*

49. This does not mean that attempts should not be made to locate such attackers for purposes of punishment or to deter others, but rather that attackers are often "judgment proof," lacking sufficient resources to pay the damages caused by their activities. *Id.*

50. *Id.*

compromised when the operator or administrator failed to run required updates to software, known as patches, and known security vulnerabilities have been taken advantage of by an attacker.[51] They might become compromised when a user clicks on an e-mail attachment sent by a friend—or apparently by a friend—that installs a stealth or hidden application on the user's computer, and this application is controlled by the attacker.[52] They can also be compromised by an attacker who has found a vulnerability, either in a particular application or a group of applications, that is as yet unknown within computer security circles.[53]

The owner of a compromised system might or might not be the direct user of that system. It might be an individual who owns a desktop computer connected to the Internet via a cable modem.[54] It might also be a large public university that maintains a series of computer classrooms or computer workstations for student or staff use.[55] It might be an Internet Service Provider that owns computers designed to store World Wide Web pages for users, and that also connects individual computer users' computers to the Internet (via dial-up or broadband service).[56] Regardless of the form of ownership, for a system to be useful to a DoS attacker, it must possess processing power, and it must have some way of accessing transmission power.[57]

Keep in mind that both processing power and transmission power may be provided by the same entity. A large university may have a "direct" connection to the Internet, while owning a number of computers used by staff and students (and possibly the general public). It is crucial for our purposes here, as we shall see, to accurately identify exactly what systems have been compromised, and who owns or controls them. It is not particularly important to identify the organizational role of the owning entity. If the university's computer stations have been compromised, then the fact that the university also provides the Internet connection to those computers may or

51. *Id.* at 11.1, 11.9-11.10.

52. *Id.* at 11.1, 11.2.

53. *Id.* at 11.1, 11.21-11.22.

54. *Id.* at 11.1, 11.19-11.20. Broadband or "always on" computers owned by individuals are regularly targeted by attackers, as individuals tend to be less skilled in preventing such attacks and also tend to less regularly patch software applications on their computers.

55. *Id.* at 11.1, 11.22.

56. *Id.*

57. *Id.* The exchange of floppy disks among computer users was at one time the main method of transmission; transmission power in these cases was the carrying of an infected floppy disk from one computer to another. As the Internet has taken hold, transmission power has come to mean the ability to send information over a network. A computer that cannot access the Internet is not only unlikely to be compromised to begin with, but once compromised, poses almost no threat to any other system that is connected to the Internet.

may not be relevant, but this fact raises issues separate from those raised by ownership of the compromised systems themselves.

A. DoS Attack Mechanics

Denial of Service of (DoS) attacks are any activities, intentional or unintentional, that result in a loss of network service: "either a host or a server system is rendered inoperable or a network is rendered inaccessible."[58] These attacks can be either deliberate or accidental.[59] We will focus primarily on intentional or malicious DoS attacks in the form of distributed denial of service (DDoS) attacks, but unintentional actions that cause loss of service may also be subject to a similar analysis.

Denial of service attacks are initiated in a wide variety of ways, and the categorization of an attack as a DoS attack means little more than that network connectivity or service was lost or hampered. This can occur by the use of computer viruses, by incorrect settings on e-mail,[60] or by improperly administered or secured software or hardware.[61] Without intending to downplay the significance of other types of intended or unintended DoS attacks, our focus here will be on DDoS attacks. The reasoning behind this choice is that it presents more directly the issues with which we wish to deal: the liability of ISPs and computer owners when their systems (or systems connected by them to the Internet) are compromised by DDoS attackers and used in subsequent attacks on systems or sites owned by innocent third parties.

Distributed denial of service attacks are generally launched by attackers using tools developed for that purpose.[62] The attackers search out vulnerable systems and "plant" the tools on them, generally establishing one system (or fewer than all) as a DDoS "master."[63] The

58. Levine & Kessler, *supra* note 37, at 11.1, 11.5.

59. *See*, Alexander Khalimonenko, Oleg Kupreev & Kirill Ilganaev, DDoS attacks in Q4 2017, DDoS Reports (Kapersky, Feb. 6, 2018), https://securelist.com/ddos-attacks-in-q4-2017/83729/ (last visited, June 4, 2020) ("Junk traffic has become so widespread that server failure from too many requests might not be attack-related, but the accidental result of botnet side activities.").

60. This situation generally arises when e-mail is set by a user to "auto respond," usually when he or she is away for a period of time and does not want those who send messages to feel they are being ignored. Problems arise when auto-respond is incorrectly configured, and large masses of messages are sent, decreasing bandwidth and using system resources. *Id.* at 11.4, 11.7.

61. *Id.*

62. *See* Robert Anderson et al., *Advanced Network Defense Research: Proceedings of a Workshop*, CR-159-NSA NAT'L DEF. RES. INST. 1, 13 (2000); *see also Hearing on the Role of Technical Standards in Today's Society and in the Future Before the Subcomm. On Tech. of the H. Comm. on Sci.*, 106th Cong. (2000) (statement of Martin C. Libicki, Senior Policy Analyst, RAND); Michael Ettridge & Vernon Richardson, *Assessing Risk in E-Commerce*, 22 INT'L CONF. INFO. SYS. 275 (2001).

63. Anderson, *supra*, note 62.

attackers keep track of the systems they "own,"[64] and subsequently command them to send packets of data directed to the targets' systems in an attempt to stop incoming and outgoing traffic to the site or resources, or to cause it to "crash" and stop operating.[65] The purpose is to deny service in all of these cases, and because of the decentralized nature of the attack, it is difficult and many times impossible to track the identity or location of the attacker.[66] It is also difficult to defend against DDoS attacks. To understand why, we must look at least briefly at the nature of the attack itself, as well as its launch through the attacker's distributed network structure.[67]

DoS attacks in general, and DDoS attacks specifically, can be initiated using a variety of approaches. One is the SYN flooding[68] technique, in which the attacker sends part one of a three-part network communication to an Internet server, which then responds with part two and waits for part three.[69] The DDoS attacker never completes the communication.[70] This leaves the receiving computer waiting, at least for a period of time, for the remaining portion of the communication.[71] When it is not received, the receiving server, in this case the target of the attack, resets.[72] It is the period of time, however, between receipt of the original request and the receiving server's resetting that has the capacity to slow, halt, or crash the system.[73]

As servers generally have an upper limit to the number of connections that can be established, when that number is taken up by failed or bad requests, valid requests cannot get through, and the server is

---

64. Keeping track can occur by different methods, but usually involves some type of "report" or "connection" by the tools back to the attacker. Systems that are "owned" may "report in" to the attacker via TCP/IP protocols, or may utilize IRC (Internet Relay Chat) protocols, in which case the attacker will not only know which systems he or she owns, but also when those systems are available for attacks. *See* Levine & Kessler, *supra* note 37, at 11.1.

65. *See* NAT'L RESEARCH COUNCIL, COMPUT. SCI. & TELECOM. BD., CYBERSECURITY TODAY AND TOMORROW: PAY NOW OR PAY LATER 3 (National Academy Press 2002).

66. *See*, Burch & Cheswick, *supra* note 44.

67. *See* Kevin J. Houle & George M. Weaver, *Trends in Denial of Service Attack Technology*, 1 CERT COORDINATION CENTER 1, 2-3 (2001).

68. The name, as with much of the terminology derives from the technical terms used to describe various Internet processes. In this case, the attacker is taking advantage of a three-part exchange between communicating TCP/IP hosts. The first part involves sending a segment of data that includes a synchronization (syn) flag; the other host then responds with an acknowledgment flag, and the server waits and "allocates resources for the about-to-be-established" connection, awaiting the third segment that completes the initial communication sequence. After a specified period without receiving this third segment, the server resets. *See* Levine & Kessler, *supra* note 37.

69. *Id.*

70. *Id.*

71. *Id.*

72. *Id.*

73. *Id.*

unreachable.[74] A few of these incomplete requests will not likely cause a problem for the server; in fact, the Transport Control Protocol/Internet Protocol (TCP/IP)[75] is designed to handle such difficulties.[76] The problem arises when the number of incomplete requests escalates and most or all available Internet connections are taken up by incomplete, invalid "attacker" communications.[77]

Attackers are not easy to locate. If one attacker is initiating a SYN flooding attack as a non-distributed DoS attack, all the failed requests may originate from one IP address (though not likely the attacker's home address).[78] This may allow the target site to filter out requests from that IP address and thus save the resources the attacker hopes to drain.[79] If, however, the attack is emanating from many or even hundreds of IP addresses, as it would in a distributed attack, this filtering method is not an effective way to fight the attack.[80]

Similar stories hold true for other DDoS techniques. For example, in an e-mail bombing attack, the attacker floods the target's e-mail system with hundreds, thousands, or even tens of thousands of messages.[81] The system fills up and the mailbox becomes unreachable or the system crashes.[82] Again, the messages may be sent from either one location or distributed.

Not all attacks, even in this day and age, are internet focused, however (though those that are not purely internet based often include an internet component). A 2016 Texas case recounts the following:

> "In July 2012, ERR experienced what is known as a 'denial of service attack' where false web advertisements generated so many

74. *Id.*

75. TCP/IP is the backbone of the Internet in terms of its operation. It is the basic standard through which all over applications and uses of the Internet take place. Lydia Parziale, David Britt, Chuck Davis, Jason Forrester, Wei Liu, Carolyn Matthews & Nicolas Rosselot, TCP/IP Tutorial and Technical Overview, 1 (IBM Redbooks, 2006)

76. *See* Levine & Kessler, *supra,* note 37.

77. *Id.*

78. *Id.*

79. *Id.*

80. *See, e.g.*, Steve Gibson, *DDoS Attack Mitigation*, SECURITY NOW! (Feb. 23, 2016), http://www.grc.com/sn/sn-548.htm.

81. *See* T. Bass, A. Freyre, *E-Mail Bombs and Countermeasures: Cyber Attacks on Availability and Brand Integrity*, 12 IEEE NETWORK MAGAZINE, no. 2, Mar./Apr. 1998, at 10-17; *see also* Cristina Houle & Ruchika Pandey, *A Layered Approached to Defending Against List-Linking Email Bombs*, *in* 2018 APWG SYMP. ON ELEC. CRIME RES (ECRIME) (IEEE Network 2018); Levine & Kessler, *supra* note 37, at 11.2.4.2.

82. *See id.*

> telephone calls that the business number was useless. The company was also inundated with 'spam" emails."[83]

While there is a tendency in computer literature to treat a wide variety of activities as DoS attacks,[84] the general DoS category into which most DDoS attacks fall is resource denial or starvation.[85] In these cases, the attempt is made, using SYN flooding or other techniques, to deprive the system of the resources it needs to respond to valid requests.[86] In addition to e-mail bombing and SYN flooding, other types of attacks include buffer overflows,[87] bandwidth consumption attacks,[88] and the "catch-all" category of resource starvation.[89]

All of these attacks can lead to serious consequences for the sites that are their targets.[90] While there are responses that the target sites can initiate when they are subjected to DoS attacks, and the number

---

83. Roberts v. State, No. 05-15-00379-CR, 2016 WL 327290, at *1 (Ct. App. Tex. Jan. 27, 2016).

84. For example, we might treat activities that involve "intrusion" into a system and destruction of files as a DoS attack, as the destroyed files are no longer available. While this seems to be a somewhat imprecise use of the terminology, we need not work it out here, as generally DDoS attacks are generally aimed at denying access to resources, as opposed to defacing or actually destroying information or systems. *See* Levine & Kessler, *supra* note 37. This need not remain so, however, and caution is urged in reviewing and categorizing Internet attacks.

85. *See* Steve Gibson, *DDoS Attack Mitigation*, SECURITY NOW! (Feb. 23, 2016), http://www.grc.com/sn/sn-548.htm.

86. *Id.*

87. Buffer overflows work by exploiting programming design errors. The buffer holds information that is related to program operations. When information is sent that is larger than the buffer, it should simply reject it. Instead, because of errors in design or implementation, sometimes buffer overflows can crash an application, and allow part of the code of the offending information access to the computer system, so that arbitrary or injurious instructions can be executed on the computer. Where buffer overflow attacks are used to assist or aid attacks designed to denigrate service, they can be a part of a larger DDoS attack. *See*, Levine & Kessler, *supra* note 37, at 11.2.4.3.

88. Bandwidth consumption attacks are similar in general to Syn flood attacks. intent is to send "worthless" packets to the target server, eat up the bandwidth resource, which even when large is still limited, and either crash or make the server unreachable. Two general categories of bandwidth consumption attacks are "smurf" attacks, where the attacker "spoofs" the originating IP address of the target in an information request to a third "stooge" site, which then sends a response to the target. Depending on the structure of the stooge site, it will likely "amplify" the request, flooding the target with useless and unwanted packets of information. By initiating requests to more than one stooge site, the result can again be distributed, though without the need for the pre-arranged distributed infrastructure. *See* Levine & Kessler, *supra* note 37, at 11.2.4.4.

89. Resource starvation as the catch-all includes all those resource or service denying attacks that have not yet been thought up yet, as well as some that have. Some involve confusing the target's system and taking up processing power, which again can halt the system. Others simply confuse protocols by sending incorrect information and can also halt the system. Nearly all of these types of attacks can be initiated using DDoS methods and infrastructure. *See* Levine & Kessler, *supra* note 37, at 11.2.4.7.

90. *See generally* YU, *supra* note 3, at 2-5 (2014); *see also supra* notes 2-10 and accompanying text.

of options is increasing as sites targeted in such attacks encourage the development of alternatives, or where an attack is initiated through a distributed network of compromised systems, the only thing *guaranteed* to end the attack is time.[91]

B. DoS: Parties and Participants

Attackers place controlling software on compromised systems and use them as vehicles to attack target sites, building networks of "bots" which they can later use to attack others.[92] Attackers require two kinds of power to accomplish their goals: computing power and transmission power.[93] Attackers may or may not gain the power they need by compromising systems, and they may or may not rely on properly functioning networked systems to accomplish their goals alongside compromised systems. Once systems are compromised,[94] they are used by attackers to disable or otherwise injure target sites. In other words, an attacker uses compromised systems to attack downstream target sites. While this puts at least three players into the game (plus one additional in the form of the Internet Service Providers (ISPs) who connect all the players together), for reasons that will soon become quite clear, we are concerned here primarily with the potential downstream liability that might result from a compromised site unwittingly providing some of the resources necessary for such an attack to take place.

There is no need for this loose grouping of system owners and operators to be in any specific geographic proximity to the attacker, the victim, or even each other. A network of compromised systems known as ZeroAccess was estimated to have included more than 1.9 *million* computers as of February 2015, with the computers spread throughout the world.[95] A DDoS attack in September 2016 utilized more than 145,000 systems, many of them processor and network enabled devices such as webcams and Digital Video Recorders.[96] Understanding the

91. *See* Gibson, *supra* note 85.

92. *See generally* Levine & Kessler, *supra* note 37.

93. *Id.*

94. Keep in mind that to be "compromised" a system need not be "infected" or otherwise infiltrated. Reflected Distributed Denial of Service Attacks, for example, send messages to servers but "spoof" the origination IP address. The servers then send traffic to the spoofed IP address, flooding it. *See* A.B. Tickle et al., *Background, in* An Investigation into the Detection and Mitigation of Denial of Service (DoS) Attacks: Critical Information Infrastructure Protection 9, 10-11 (S.V. Raghavan & E. Dawson eds., 2011).

95. Karl Thomas, *Nine bad botnets and the damage they did*, WELIVESECURITY (Feb. 25, 2015), http://www.welivesecurity.com/2015/02/25/nine-bad-botnets-damage/.

96. *Major DDoS Attacks Involving IoT Devices*, E.U. AGENCY FOR CYBERSECURITY (Nov. 3, 2016), https://www.enisa.europa.eu/publications/info-notes/major-ddos-attacks-involving-iot-devices#:~:text=On%2020%20September%202016%2C%20%22KrebsOnSecurity,
website's%20digital%20security%20service%20provider.&text=Akamai's%20analysis%

extent of the networks of devices used to launch DoS attacks is critical to developing an appropriate legal response to such attacks. With individual networks, of which there are many, bringing nearly two million systems under their control, the "more" of DoS attacks comes into sharp focus.[97] Recognizing the distribution, variability in ownership and control, and nature of such systems forces us to consider the more to be different. And that difference will drive the approach to the legal regime surrounding these attacks.

III. NEGLIGENCE AND DENIAL OF SERVICE ATTACKS

A. The Big Picture

At first glance, it may appear relatively uncontroversial to conclude that owners of compromised systems used in DoS attacks would—and should—be liable in tort for injuries suffered by sites targeted using their systems. A number of articles and commentators have concluded exactly this, though with varying amounts of reticence.[98] Additional articles have also looked at addressing the injuries that flow from DoS attacks, but often from the point of view of criminal law, international law, or seeking to hold the attackers themselves liable for those injuries.[99]

Recent developments in tort law may make determinations about the likelihood of compromised system owners being held liable under these circumstances complicated, though some of these complications dissipate upon further inspection. Some of these complications arise

---

20indicated%20the%20use,botnet%20of%20compromised%20IoT%20devices.; *Snapshot: Turning Back DDoS Attacks*, DEP'T. OF HOMELAND SEC. (Feb. 16, 2017), https://www.dhs.gov/science-and-technology/news/2017/02/16/snapshot-turning-back-ddos-attacks; *see also* Tasneem Nashrulla & Sheera Frenkel, *Massive Cyber Attacks Bring Down Websites Across the US*, BUZZFEED NEWS (last updated Oct. 21, 2016, 4:53 PM), http://www.buzzfeednews.com/article/tasneemnashrulla/denial-of-service-attack-dyn#.wiKl7BjpvQ.

97. John Leyden, *How FBI, police busted massive botnet*, THE REGISTER (Mar. 3, 2010) https://www.theregister.com/2010/03/03/mariposa_botnet_bust_analysis/ (last visited, June 4, 2020) (noting that the botnet in question was made up of more than twelve million zombie computers).

98. *See* Henderson & Yarbough, *supra* note 23; Lilian Edwards, *Dawn of the Death of Distributed Denial of Service: How to Kill Zombies*, 24 CARDOZO ARTS & ENT. L.J. 23, 46 (2006); Margaret Jane Radin, *Distributed Denial of Service Attacks: Who Pays? (Part I)*, 6 CYBERSPACE LAWYER, no. 9, 2001 [hereinafter Radin, *Part I*]; Margaret Jane Radin, *Distributed Denial of Service Attacks: Who Pays? (Part II)*, 6 CYBERSPACE LAWYER, no 10, 2002 [hereinafter Radin, *Part II*].

99. *See, e.g.*, Neal K. Katyal, *Criminal Law in Cyberspace*, 149 U. PENN. L.R. 1003); Joshua McLaurin, *Making Cyberspace Safe for Democracy: The Challenge Posed by Denial of Service Attacks*, 30 YALE L. & POL'Y REV. 211, 248-250 (2011); Oona A. Hathaway et al., *The Law of Cyber-Attack*, 100 CAL. L. REV. 817 (2012); Graham Cluley, *World of Warcraft's Suspected DoS attacker has been arrested*, SEC. BOULEVARD (Sept. 24, 2019) https://securityboulevard.com/2019/09/world-of-warcrafts-suspected-ddos-attacker-has-been-arrested/.

from the nature of the Restatement of Torts, which was revised in 2010 following a somewhat prolonged process and came to fruition with disagreement over its formulations not fully resolved.[100] In addition, distinctions between affirmative duties and the perceived more general duty to act reasonably when one's acts were not fully resolved by the Restatement.[101] Add to this that a number of courts have explicitly rejected the Third Restatement's approach to duty, the picture becomes cloudier still.[102]

We must add to this that a number of well-established tort doctrines, along with at least one federal statute, further complicate the analysis given the unique circumstances of the DoS attack scenario. Specifically, the pure economic loss doctrine, factual and proximate cause, several states' provision for joint and several liability in tort cases, and the more recent development of enterprise liability in some states combine to make discerning tort doctrine applicable to DoS attacks muddled, at best, and entirely unpredictable, at worst. The role of Communications Decency Act § 230,[103] which immunizes online service providers for content uploaded by third parties, is also relevant here.

It is with these questions in mind that we will move ahead and make our way among the doctrinal and policy equations that will ultimately support the conclusion here: that some owners of compromised systems should be subject to liability to downstream DoS attack victim sites, and others should not. The full reasons for that distinction, and the articulation of where the distinction lies, is our next task.

---

100. *See generally,* William Rapp, *Torts 2.0: The Restatement 3RD and the Architecture of Participation in American Tort Law*, 37 WILLIAM MITCHELL L. REV. 1582 (2011).

101. *See* John C.P. Goldberg & Benjamin C. Zipursky, *The Restatement (Third) and the Place of Duty in Negligence Law*, 54 VAND. L. REV. 657 (2001).

102. *See, e.g.,* Riedel v. ICI Americas, Inc., 968 A.2d 17, 20 (Md. 2009) ("At this time, we decline to adopt any sections of the Restatement (Third) of Torts. The drafters of the Restatement (Third) of Torts redefined the concept of duty in a way that is inconsistent with this Court's precedents and traditions.") (Riedel was overruled by the Maryland Supreme Court in Ramsey v. Georgia Southern Univ. Advanced Dev. Ctr., 189 A.3d 1255, 1260 (Md. 2018), but the Ramsey court continued to rely on the Restatement (Second) of Torts for its guidance, noting, "The wife's theory of recovery against the asbestos product manufacturers is simple: under § 388 of the Restatement (Second) of Torts (the "Restatement"), which this State has embraced . . . ."). *See also* Quiroz v. ALCOA Inc., 416 P.3d 824, 836-38 (Ariz. 2018) (noting differences between the Third Restatement's approach to duty and Arizona's, with the Third Restatement focused on risk creation while Arizona's duty determination is limited by conceptions of foreseeability).

103. 47 U.S.C. § 230 (2012).

B. Disputes and Uncertainties: A Framework for DoS Liability

1. Negligence Law, Duty and DoS Attacks

Negligence liability has traditionally been predicted upon a four (or perhaps five) part analysis. A defendant will be found liable for injury caused by her negligence when she breached a duty of care owed to the plaintiff and thereby caused damages to the plaintiff.

The elements have been articulated as:

1) Plaintiff owed a duty to the defendant; and
2) Plaintiff breached the standard of care; and
3) The breach was the factual cause and
4) The proximate or legal cause of
5) A cognizable injury suffered by the plaintiff.[104]

This formulation was learned by law students and repeated by courts almost without question throughout much of the twentieth century. With the publication of the long-awaited draft of the Third Restatement of Torts, however, this calculus was altered in an attempt to clarify the roles of the fact finder and the judge in negligence actions.[105] Specifically, the draft Third Restatement appeared to assume that a duty exists in any case in which a person has acted and caused injury, ostensibly moving duty out of a position as an explicit element in the *prima facie* negligence case.[106] While the Restatement noted that there would be certain cases where a court might appropriately find a lack of duty in a specific case,[107] the normal or default position would be in favor of a duty existing where the plaintiff acted and the defendant was injured.[108]

The reaction from the legal academy was strong. John C.P. Goldberg and Benjamin Zipursky wrote an article pushing back against the draft Restatement's position,[109] making a strong case that duty played

---

104. *See generally,* DAN B. DOBBS, THE LAW OF TORTS 269 (2000); *see also* David G. Owen, *The Five Elements of Negligence*, 35 HOFSTRA L. REV. 1671 (2007).

105. RESTATEMENT (THIRD) OF TORTS § 3 (AM. LAW INST. 2001). The court in a negligence action takes up the issue of whether a duty existed as a matter of law. *Id.* Additional questions relating to the applicable standard of care and whether the injury was proximately caused by the defendant's actions are questions for the finder of fact unless they can be decided as a matter of law (because no reasonable person could find them otherwise). *Id.*

106. *See* Goldberg & Zipursky, *supra* note 101, at 660.

107. RESTATEMENT (THIRD) OF TORTS: LIABILITY FOR PHYSICAL AND EMOTIONAL HARM, §6 (AM. LAW INST. 2010) ("An actor whose negligence is a factual cause of physical harm is subject to liability for any such harm within the scope of liability, unless the court determines that the ordinary duty of reasonable care is inapplicable.")

108. *Id.*

109. Goldberg & Zipursky, *supra* note 101, at 667-74.

an important role in every-day negligence cases and urging judges to continue to consider it in all negligence cases. The final Restatement, which was published in 2010, addresses this argument but, to a large degree, decides against it, noting that where "a defendant who, by his own positive act, has carelessly caused physical damage to the plaintiff or his property is *always* held to owe a duty of care to the victim."[110] This discrepancy—between the requirement to consider duty as an explicit element of every negligence action and the contrary position that a general duty is owed to act reasonably to avoid harming others—may complicate matters here. This is true even though there is a distinction in the Restatement, the literature, and the judicial decisions between a defendant's actions that cause harm and the duty to take affirmative action to prevent harm to others not caused by the defendant's own negligence. A duty almost always exists in the former cases.[111] While it may be useful and consistent to consider the duty question at that point in all negligence cases, it is likely to come out in favor of the existence of a duty, with the standard of care and the issue of proximate causation serving as limiting factors on the extent of liability that arises from that duty.[112]

As for the latter—the "affirmative duty" cases—however, these are more limited in scope. The Restatement itself sets out a number of sections in which a defendant will have a duty to act to protect others, and disclaims a duty to act in other cases.[113] These circumstances imposing such a duty to act include situations in which statutes impose such duties directly,[114] where the defendant has a relationship either with the plaintiff[115] or with a third party or co-defendant,[116] or where the defendant has undertaken to assist[117] or has otherwise engaged in

110. RESTATEMENT (THIRD) OF TORTS: LIABILITY FOR PHYSICAL AND EMOTIONAL HARM, § 6, cmt. f (AM. LAW INST. 2010) (quoting Jane Stapleton, *Duty of Care Factors: A Selection from the Judicial Menus*, *in* THE LAW OF OBLIGATIONS: ESSAYS IN CELEBRATION OF JOHN FLEMING 61, 72 (Peter Cane & Jane Stapleton eds., 1998)) (emphasis in original).

111. *See* RESTATEMENT (THIRD) OF TORTS: LIABILITY FOR PHYSICAL AND EMOTIONAL HARM, § 7 ("(a) An actor ordinarily has a duty to exercise reasonable care when the actor's conduct creates a risk of physical harm."); *see also* Quiroz v. ALCOA Inc., 416 P.3d 824, 836 (Ariz. 2018) (criticizing the apparent distinction, or in the view of court lack of distinction, between action and inaction in the Third Restatement).

112. *See generally* Palsgraf v. Long Island R.R. Co., 248 N.Y. 339, 349 ("Where there is the unreasonable act, and some right that may be affected there is negligence whether damage does or does not result.") (Andrews, J., dissenting).

113. *See* RESTATEMENT (THIRD) OF TORTS: LIABILITY FOR PHYSICAL AND EMOTIONAL HARM § 7, cmt. l (AM. LAW INST. 2010).

114. RESTATEMENT (THIRD) OF TORTS: LIABILITY FOR PHYSICAL AND EMOTIONAL HARM, § 38 (AM. LAW INST. 2012).

115. *Id.* § 40.

116. *Id.* § 41.

117. *Id.* § 42.

conduct that has given rise to such a duty.[118] The chapter on affirmative duties begins, however, with the following: "An actor whose conduct has not created a risk of physical or emotional harm to another has no duty of care to the other unless a court determines that one of the affirmative duties provided in §§ 38-44 is applicable."[119]

Traditionally, decisions as to whether to impose a new duty have not followed a strict categorization scheme, nor have they been limited to situations in which a defendant failed to act. However, these decisions have included those situations where the defendant has acted and, through that action, is alleged to have harmed another. In these circumstances, courts have followed from the application of a multifactor analysis, the use of which contrasts with the Restatement's position that duties are appropriately found to exist in such cases.[120] While the terminology used has changed from case-to-case, when considering duties to protect others not just from one's own negligence but from the risk of harm posed by others or other circumstances not directly of the defendant's making, courts have considered factors such as the foreseeability of harm to the plaintiff, the degree of certainty that the plaintiff suffered injury, the closeness of the connection between the defendant's conduct and the injury suffered, the moral blame attached to the defendant's conduct, the policy of preventing future harm, the extent of the burden to the defendant and consequences to the community of imposing a duty to exercise care with resulting liability for breach, and the availability, cost, and prevalence of insurance for the risk involved.[121]

These factors have allowed courts to decide cases as a matter of law (as duty is a matter for the court to decide), and to consider not only the specific facts of the case, but also the policy, fairness, and process concerns that are often raised when courts are presented with novel fact situations. One recent analysis in a line of cases that raises some of the issues we will confront in the DoS scenario is illustrative. In *Kubert v. Best*, the New Jersey Appellate Division held that "the sender of a text message can potentially be liable if an accident is

118. *Id.* § 39.

119. *Id.* § 37.

120. Rowland v. Christian, 443 P.2d 561 (Cal. 1968).

121. *Id.* at 564. Some of these factors, especially those related to foreseeability, are also present in other negligence elements, such as in determining the standard of care and considering questions of proximate cause, and this overlap was part of what drove the effort to more precisely define and restrict the use of "no-duty" findings in negligence cases, limiting this outcome to specific circumstances rather than allowing it to be used across the spectrum of negligence disputes. *See* Dilan A. Esper & Gregory C. Keating, *Abusing "Duty"*, 79 S. CAL. L. REV. 265, 315-16 (2006).

caused by texting, but only if the sender knew or had special reason to know that the recipient would view the text while driving and thus be distracted."[122]

The appellate court discussed the New Jersey Supreme Court's principles for determining whether a duty exists in a particular case:

> [w]hether a person owes a duty of reasonable care toward another turns on whether the imposition of such a duty satisfies an abiding sense of basic fairness under all of the circumstances in light of considerations of public policy. That inquiry involves identifying, weighing, and balancing several factors—the relationship of the parties, the nature of the attendant risk, the opportunity and ability to exercise care, and the public interest in the proposed solution . . . . The analysis is both very fact-specific and principled; it must lead to solutions that properly and fairly resolve the specific case and generate intelligible and sensible rules to govern future conduct.[123]

Thus, attempting to discern whether courts would impose a duty of care on computer system owners when those systems are used by attackers to launch DoS attacks against victim sites presents us with quite a dilemma. If we follow the Restatement position, we would need to decide first whether the owners of such systems have taken an action or are being asked to take an action. Have they acted by connecting a system that is or can be compromised for use in DoS attacks to the Internet, or are we asking whether they should be required to act by securing any computer before it is connected to the Internet? While one can be negligent for both acts and omissions,[124] and thus the act/omission classification is not determinative for our purposes, it does seem to drive the Restatement's inquiry relating to duty. If we pursue a more traditional common law approach, we need not ask this question, but instead can look to the factors to determine whether liability is appropriately imposed. The choice of approach may be half the battle.

Robert Rabin has provided us, however, with a categorization of cases decided primarily under common law reasoning that is helpful here. Referring to what he terms "enabling torts," Professor Rabin identifies a number of cases in which courts have held defendants

---

122. Kubert v. Best, 75 A.3d 1214, 1219 (N.J. 2013).

123. *Id.* at 1223 (alteration in original) (citations omitted) (quoting Estate of Desir ex. rel. Estiverne v. Vertus, 69 A.3d 1247, 1257 (N.J. 2013), which quotes Hopkins v. Fox & Lazo Realtors, 625 A.2d 1110, 1116 (N.J. 1993)); *see also* Gallatin v. Gargiulo, No. 10401 of 2015, C.A. (Ct. Common Pleas, Lawrence Cty., Pa. (2016) (adopting the reasoning in *Kubert*).

124. *See* Luis E. Chiesa, *Actmissions*, 116 W. VA. L. REV. 583, 584 (2013) (discussing the act/omissions distinction and its slipperiness: "there are many cases in which actors cause harm by engaging in conduct that can be reasonably described as either an act or an omission. Think of a doctor who flips a switch that discontinues life support to a patient. If the patient dies as a result, did the doctor kill the patient (an act) or did he let the patient die (an omission)?").

liable even when unconnected third-parties have actively caused harm to plaintiffs.[125] The kinds of cases in which this has occurred involve the defendant in some way providing assistance to or enabling the third-party bad actor in their actions.[126] For example, where a defendant left the key to his car in the car's ignition and the car was stolen and, while stolen, was used to harm another, is the defendant liable to the person who was injured?[127] Some courts have said yes, while others have said no.[128]

The disparity comes from two quarters: one is the focus on the intervention of a bad actor in tort cases, a factor that was often used by courts at common law to cut off liability of an earlier actor under the doctrine of superseding-intervening cause.[129] The other is a contrasting and more modern recognition that criminal acts are sometimes foreseeable, and where specific circumstances reflect that foreseeability, it is not justifiable to cut off liability of the party who enabled the tortfeasor (by, for example, leaving his keys in the car) on duty grounds.[130] Thinking of the DoS scenario in terms of enabling torts will assist us in sorting out some of the more challenging aspects of the issues we confront here, and we will return to that concept soon. It is not that compromised system owners are directly causing injury to the target sites, but rather that they are furnishing the attacker with the tools necessary to launch the attack. The compromised system owners'

---

125. Robert L. Rabin, *Enabling Torts*, 49 DEPAUL L. REV. 435 (1999).

126. *Id.*

127. *Id.* at 440-43

128. *See* Hosking v. San Pedro Marine, Inc., 159 Cal. Rptr. 369, 372 (Cal. Ct. App. 1979) (collecting and summarizing cases as follows: "California courts have found 'special circumstances' in these cases: Richardson v. Ham, 44 Cal.2d 772, 285 P.2d 269 (unattended and unlocked 26 ton bulldozer); Murray v. Wright, 166 Cal.App.2d 589, 333 P.2d 111 (car dealer commonly left keys in cars on the lot); Hergenrether v. East, 61 Cal.2d 440, 39 Cal.Rptr. 4, 393 P.2d 164 (partly loaded 2-ton truck in area where persons disrespect law and populated by drunks, defendant intended to leave it for a long period of time); and Enders v. Apcoa, Inc., 55 Cal.App.3d 897, 127 Cal.Rptr. 751 (known that parking lot attendant left keys in cars in lot and there were past thefts). California courts have not found 'special circumstances' in these cases: England v. Mapes Produce Co., 238 Cal.App.2d 120, 47 Cal.Rptr. 506 (1966) (where the farm camp operator always left keys in ignition of trucks in unattended lot around Mexican laborers who were not good drivers); Holder v. Reber, 146 Cal.App.2d 557, 304 P.2d 204 (where appellant frankly admitted no 'special circumstances'); and Brooker v. El Encino Co., 216 Cal.App.2d 598, 31 Cal.Rptr. 24 (leaving keys in car in unattended lot)." (footnotes omitted)).

129. One well-known case in this area held specifically that the liability of a gas transportation company for damages that resulted when a man threw a match on a gasoline leak would be dependent on whether the man did so intentionally or negligently. If he did so intentionally, he would be viewed as a superseding-intervening cause that cuts off the liability of the transportation company. If instead he threw the match negligently, the transportation company's liability would not be cut off. Watson v. Kentucky & Indiana Bridge & R.R. Co., 126 S.W. 146 (Ky. 1910).

130. Rabin, *supra* note 125, at 440-43

actions are thus judged not based on the attack itself, but the ways in which they acted toward their own resources that allowed them to play a part in the attack.

While the duty issue has been raised in earlier scholarship relating to DoS attacks, the critical distinction between owing a duty where a defendant's own actions have created the risk of physical harm and where the physical harm arises from another's actions has meant that this element has at times been under-analyzed. Henderson and Yarbrough, relying on language in the draft Restatement that was removed from the final version, argued that finding a lack of duty should be a rare occurrence.[131] Focusing on individual users, Edwards engages in the more traditional duty analysis, concluding that as to home users, there are difficulties in both foreseeability and policy in holding such users have a duty to third-party victim websites in these circumstances.[132] In an early and rather prescient piece in 2001, Margaret Radin concluded that negligence liability for third-party actions of the kind that attackers undertake in DoS cases posed potential difficulties for plaintiffs.[133]

Part of the difficulty of addressing these questions stems from the inherent need to use analogy and metaphor to reach conclusions when confronted with novel facts. We have not had been confronted in the past with a situation in which one person could use resources provided by another person to attack and cause injury to a third person. When this is true, we adopt metaphors to try and come to grips with the similarities and differences between our various approaches to legal regimes.[134] Henderson and Yarbrough use a number of metaphors in their analysis. The first is of an automobile with a known flaw that is driven by its driver without fixing the flaw and despite this knowledge.[135] The second is a car with a flaw that can be brought about when a third person kicks the car, and where the possibility of this happening is again well known and again ignored.[136] The final metaphor is that of a gun, used against a plaintiff, who then sues the gun's manufacturer and distributor.[137] At the time of their article, gun

131. Henderson & Yarbrough, *supra* note 23, at 16.

132. Edwards, *supra* note 141, at 48-49. This conclusion is similar to the one reached here in regard to individual or unsophisticated users, but Edwards did not take up the question of more sophisticated users and how the arguments she makes fit in that regard.

133. Radin, *Part I supra* note 68, at 2 (noting that courts have been reluctant to impose liability on a defendant where to do so would expose the defendant "to an unknown and potentially large amount of risk, inappropriate in light of its role.")

134. For a thorough discussion of issues along these lines, *see* STEVEN L. WINTER, A CLEARING IN THE FOREST: LAW, LIFE, AND MIND 43-68 (2003).

135. Henderson & Yarbrough, *supra* note 23, at 16.

136. *Id.*

137. *Id.* at 16-17.

manufacturer liability was not well established in such cases, and while the authors predicted it was likely to become more so, that has not been the case.[138]

In each of these metaphorical situations, however, the article itself is either dangerous—a gun—or is faulty and *operated by* the defendant (and for the defendant's purposes). If we use the example of a compromised computer, its owner may very well have no idea that his computer is compromised. If the attacker never activates the botnet, the computer will never harm anyone. But even if the attacker does activate the botnet, the owner is unlikely to ever be aware that this has occurred. It is not like driving a faulty car. Such an act is easy to view as the car's owner acting, and in so acting we require her to act reasonably. Instead, the DoS scenario appears closer to a car parked on the side of the road by its driver with the key in the ignition. Early cases found no liability under these circumstances. It was not until cases arose with special circumstances—reasons for the owner to know that someone is likely to steal the car where it is parked—that a duty was imposed.

Even the modified car analogy, with the driver no longer present, is not sufficiently analogous to our current situation, and attempts to make it so become quickly fascicle. For the analogy to be accurate, the attacker would have to be hiding under the car and using it to throw rocks at others, even at great distances, while the owner left it idling in her garage or in her driveway. In addition, the owner would not have any evidence that the attacker was there, and in most cases, the attacker's activities would not have had any negative effect on the operation of efficiency of the car. If the owner went for a drive while the attacker was using the bathroom, the car would be perfectly safe and no one would be injured by the modifications the attacker made to the car. Only with the attacker taking action does the car cause harm. The attacker is enabled by the owner's negligence, but the injury itself follows only when the attacker takes specific steps to cause it.

Bringing the analogy back to the DoS scenario, even after being compromised, the computer system works perfectly well for its owner, causing no injury until the attacker acts. The owner can continue to use it for its intended purpose, and no injury to anyone will follow.[139] It is only after the attacker initiates the attack that the compromised system participates in causing the damages suffered by the target site.

---

138. *Id.*

139. This contrasts to some of the early analogies, such as a car with a wheel that might be broken by a kick and which is driven *by the owner* after it is kicked. The owner in such a scenario is taking steps that directly cause the subsequent injury. In our scenario, the owner takes one step–somehow allowing her computer to be compromised–but no injury follows from that, even if the owner continues to use the computer, unless and until the attacker initiates the attack.

Without this critical step on the part of the attacker, no injury will follow from the compromised system owner's alleged negligence.

Considering the foundations laid above, how should courts answer the question of whether compromised system owners have a duty to those who are injured when a third party uses their systems to harm downstream persons? Because more in this case is also different, the answer is: it depends. The owners of compromised systems are not homogenous, and because the number of compromised systems is so large, we must dissect the pool of possible defendants and apply our standards to them separately, noting that even slight changes in one fact or another may alter our analysis. More compromised systems cannot simply be added together to yield a number of defendants. We must identify their characteristics, and at times their actions, before deciding whether a duty of care should attach.

How we conceive of DoS attacks, and the role that compromised systems and their owners play in those attacks, is thus critical to our conclusion as to whether a duty of care may be properly imposed here.[140] Where those resources are sufficient to inflict injury on particular internet resources, foreseeability may provide the best way forward in determining the appropriateness of liability. Where those resources are not, in and of themselves, sufficient to cause such injuries, finding a lack of duty based on the lack of computing and networking power may provide the most reasonable solution.

The Third Restatement, unfortunately, is not of significant help here. It is not clear under the Restatement whether compromised system owners are creating a risk by acting when they attach insecure computers to the Internet. If they have created that risk, a risk that will not materialize unless a third-party takes advantage of that opportunity, they are bound by the reasonable duty of care that always attaches when creating a risk. Alternatively, the Restatement may view plaintiffs as attempting to require computer owners to take affirmative actions to protect them from other, unaffiliated third-party bad actors by keeping their systems secure. If it's the former, the duty question is settled, and a duty is imposed. If it's the latter, we would need to identify which of the Restatement's exceptions to not having affirmative duties to act to protect others would apply.

None of the provisions of Chapter 7 of the Restatement, however, are clearly applicable. The compromised system owner has no relationship with the attacker or with the attacked site. The compromised system owner is unlikely to have taken actions that create reliance on his

140. A similar lesson is taught by a number of articles written as the internet itself was first being tested in the courts. *See, e.g.*, Dan Hunter, *Cyberspace as Place and the Tragedy of the Digital Anticommons*, 91 CALIF. L. REV. 439, 441-46 (2003); Mark A. Lemley, *Place and Cyberspace*, 91 CALIF. L. REV. 521, 521-23 (2003); *see also* Julie E. Cohen, *Cyberspace as/and Space*, 107 COLUM. L. REV. 210, 210-13 (2007).

security by the target site, and as of this writing no statutes create clear duties in this regard.[141] Other provisions within the Restatement might be useful, such as section 19, which provides: "The conduct of a defendant can lack reasonable care insofar as it foreseeably combines with or permits the improper conduct of the plaintiff or a third party."[142] The comments to this section indicate that a defendant may be found liable, when: "[f]or example, the defendant's conduct may make available to the third party the instrument eventually used by the third party in inflicting harm; . . . ."[143] The examples provided in the comments, however, all involve people who knew they were giving something to the third-party, such as the lending of a car, rather than someone who is unaware they are lending something or making any contribution to the harm.[144] The Restatement's § 19 also appears unlikely to clearly determine the matter on our facts. There are ways of interpreting the facts that are likely to bring them within the duty of care and ways that are unlikely to do so. This most likely means that under the Third Restatement, advocates will have significant room in which to make their arguments, and courts will have significant room to work with those arguments. We cannot assume that courts will find a duty, but we cannot assume they will not, either.

The same is true when we consider the multi-factor test. If we use the New Jersey formulation of the factors, we must consider:

- the relationship of the parties;
- the nature of the attendant risk;
- the opportunity and ability to exercise care; and
- the public interest in the proposed solution.[145]

There is no relationship between the parties—the third-party attacker and the compromised system owner—in our scenario. We can assume that they do not know each other, have not been in contact with each other, and are generally unaware of each other's actual identities. While the attacker knows that she has compromised a computer system, the owner may not even have this knowledge. As for the

141. Some statutes do impose general or specific cybersecurity obligations on system owners, but these again are patchwork quilt of regulatory and statutory requirements that only emphasize that "more is different" when it comes to DoS cases. *See generally*, Benjamin P. Edwards, *Cybersecurity Oversight Liability*, 35 GEO. ST. U.L. REV. 663 (2019); Judith H. Germano & Zachary K. Goldman, *After the Breach: Cybersecurity Liability Risk*, CTR. ON L. & SEC. (2014), https://www.lawandsecurity.org/wp-content/uploads/2014/06/CLS-After-the-Breach-Final.pdf.

142. RESTATEMENT (THIRD) OF TORTS: LIABILITY FOR PHYSICAL AND EMOTIONAL HARM, § 19 (AM. LAW INST. 2005).

143. *Id.* § 19 cmt. e.

144. *See* RESTATEMENT (THIRD) OF TORTS: LIABILITY FOR PHYSICAL AND EMOTIONAL HARM § 19 cmt. f (AM. LAW INST. 2005).

145. Goldberg v. Housing Auth., 186 A.2d 291 (N.J. 1962).

relationship between the compromised system owner and the downstream victim, there is again unlikely to be any notable relationship. They are both connected to the internet. The system owner may have visited the victim's website, but that visiting has no connection to the DoS attack or the subsequent harm that the victim suffers. Factor one takes into account Judge Cardozo's admonition that, "Proof of negligence in the air, so to speak, will not do,"[146] and here the parties are remote both in terms of their relationships (or lack thereof) and likely their geographical locations. Factor one is likely to favor a finding of no-duty.

The second factor is likely neutral between the victim and the compromised system owner. Owning computers systems of all types—cell phones, printers, laptop and desktop computers, cars, televisions, and other types of computer processing and network enabled devices—is almost essential to everyday life in many countries. Some European countries have gone so far as to find that internet access is a human right.[147] Some of these devices have relatively straight forward procedures for keeping them updated and to assist with avoiding the kinds of traps that attackers would use to compromise the systems.[148] Others cannot be easily updated, patched, or controlled, and indeed are not expected to be maintained by their owners.[149] It might be possible for courts to craft a duty depending on the kind of device—with owners of Windows and Apple computers being held to one standard and owners of internet connected thermostats and toasters being held to another.

The uncertainty in this element, however, may work in our favor, as we may be able to divide the potential defendants into groups depending on the computing and networking power of their computer systems (as I will argue in greater detail in Section III). A business with servers providing web hosting for consumers could be held to have a duty, while a non-technology-industry individual with a computer and a mobile phone would not. Such a calculation could be made based on the industry or specific expertise the individual has, but it could also be based on the amount and power of computing and networking power the individual has. Where an individual has significant computer or networking power at their disposal, the attendant risk of their carelessness in maintaining their systems rises; where the computing

146. Palsgraf v. Long Island R.R. Co., 162 N.E. 99, 99 (N.Y. 1928) (citing Pollock, Torts, 11th ed, p. 455).

147. *See, e.g.*, Colin Woodard, *Estonia, where being wired is a human right*, CHRISTIAN SCI. MONITOR (July 1, 2003), https://www.csmonitor.com/2003/0701/p07s01-woeu.html. The United Nations has also passed a non-binding resolution recognizing that internet access is a human right. *See also* G.A. Res. 32/L.20, The promotion, protection and enjoyment of human rights on the Internet (June 27, 2016).

148. Diane E. Levine & Gary C. Kessler, *Denial-of-Service Attacks, in* Computer Security Handbook (Seymour Bosworth & M. E. Kabay eds., 4th ed. 2002).

149. *Id.*

power is less significant, the attendant risk decreases. Increased risk militates in favor of finding a duty, while lower risk militates against finding a duty. With this distinction, we start to see how we can use power—computing and networking—to establish groups of computer system owners on whom duties of care are either imposed or not imposed, depending on their circumstances.

To the extent that the attendant risk element includes considerations of foreseeability of harm, this would further support dividing the risk as described. Those with larger systems are more likely to better understand the risks to others of their insecure systems—or we, as a society, will want to make sure they understand those risks—while those with less computing and networking power at their disposal are less likely to foresee the injuries that may occur by not updating their software or keeping their virus protection up-to-date.

The third factor, the opportunity and ability to exercise care, will likewise change from less sophisticated owners with less power in their hands and fewer opportunities to exercise such care, to more sophisticated owners who will have significant incentives across a host of regimes to encourage them to take greater care with their systems. Medical regulations, financial regulations, Federal Trade Commission guidance, and state laws and regulations are more likely to govern enterprises with large computing power, those "in the business," as it were, and are less likely to either apply to or influence the actions of users with less power in their systems. These incentives will increase both the opportunity for and the ability of those systems with more power to exercise care. This factor again favors recognizing a split in liability based on the power wielded by system owners.

The public interest is also served by adopting a rule that does not that apply to every computer system owner, but that focuses on those best placed to do the most damage to internet connected infrastructure when utilized by bad actors to launch DoS attacks. This structure will encourage those who can do the most to secure the resources used in such attacks to do so, while not burdening those who play an otherwise minor role in such attacks. This is not to say that such attacks must use computer systems with large computing and networking power. Attacks can be launched with botnets consisting solely of individually owned computers each connected by its own, relatively small internet connection, but in such a case it does not follow that this justifies holding any one of the individual users liable.

As we shall see as we continue, additional tort doctrines will strengthen this conclusion as to the public interest, concerns grounded in the potential unfairness of holding a single individual with low computing power jointly and severally liable for the entirety of damages suffered by a downstream victim. Additional questions will arise relating to the ability of the courts to handle cases in which millions of

individuals are potential defendants. There appears to be no limit to the actual number of potential defendants in such a case. As such, it makes sense to focus on those with greater resources used by the attacker.

Analysis under other multi-factor formulations, such as that used by the California courts, will not differ substantially from the above. The conclusion here begins to become clear. Where a defendant computer system owner has a suitable amount of computing and networking power, they are bound by a duty to take reasonable steps to secure their systems against use by third-parties to attack victim sites using DoS attacks. The "suitable amount" will vary from attack to attack, and while I hesitate to arbitrarily set a number—such as one who has provided 5%, 10%, or 20% of the computers for any attack—courts may wish to use the numbers when making individual determinations as to the duty in any particular case.

2. *The Problem (or not) of Purely Economic Loss*

Another wrinkle in the negligence travails of DoS victims is found in the pure economic loss doctrine. Damages are an element of the *prima facie* negligence case, and the damages must be of the right "kind" to be cognizable in negligence law. This has generally meant that a physical injury is required to sue in negligence, and though this category has grown to include emotional distress under certain circumstances,[150] it does not generally include purely economic loss. In other words, when accompanied by physical injury, economic loss is recoverable, but it is generally not recoverable when not accompanied by physical injury.[151]

Does a DoS attack cause physical loss? The initial answer to this question in looking at other areas of the law initially seemed to be no, but more recent developments indicate that it is likely that a court would find that the interruption of internet service and the concomitant effect of such an attack on the internet servers that serve the web pages to their viewers would be considered physical. This is the natural outcome of cases that follow the *eBay v. Bidder's Edge* decision, in which a cause of action for trespass to chattels was allowed by the district court.[152] The court reasoned that the actions taken by Bidder's Edge had the potential to significantly affect eBay's servers because if

150. *See* Julie A. Davies, *Direct Actions for Emotional Harm: Is Compromise Possible*, 67 WASH. L. REV. 1 (1992); John. J. Kircher, *The Four Faces of Tort Law: Liability for Emotional Harm*, 90 MARQ. L. REV. 789 (2007);

151. *See generally* Catherine M. Sharkey, *Can Data Breach Claims Survive the Economic Loss Rule?*, 66 DEPAUL L. REV. 339 (2017); Peter Benson, *The Problem with Pure Economic Loss*, 60 S.C. L. REV. 823 (2009); Catherine M. Sharkey, *In Search of the Cheapest Cost Avoider: Another View of the Economic Loss Rule*, 85 U. CIN. L. REV. 1017 (2018).

152. eBay, Inc. v. Bidder's Edge, Inc., 100 F. Supp. 2d 1058, 1071-72 (N.D. Cal. 2000).

the same actions were engaged in by additional actors the servers would not be able to handle the load.[153] Bidder's Edge's actions thus, according to the court, caused a physical injury to eBay's servers.[154]

While criticized for basing its holding on the hypothetical additional interlopers, courts approve of the basic proposition that where harm to a server can be shown, a physical injury has occurred.[155] In the DoS case, harm is the entirety of the attacker's purpose, and if the attack is in the least successful, the defendant will have little trouble establishing this element of negligence under these circumstances.

While some courts have backed away from strict adherence to this doctrine,[156] there is no need to push on what has been a limited schism in the otherwise long history of courts refusing to allow negligence actions in cases where the injuries are purely economic.

3. *Causation: Factual Causation and the Substantial Factor Test*

Another element of negligence law that pushes us toward a dual scheme of liability for compromised system owners is causation. In order to recover for negligence, the defendant's actions must be a cause—both factual and proximate—of the defendant's harm. Factual causation is often straightforward, showing only that there is a link between the defendant's actions and the injury suffered.[157] That is not the case here, however, because of the number of compromised systems used. The greater the number of systems involved in an attack, the lesser the chance that any one of them can be considered a cause of the resulting damage. The damage comes from the accumulation of power from many systems and networks, not the use of one of those many. No one alone is sufficient to wage the attack.

This raises problems for tort law's causation requirement. "But for" causation exists whenever one can say that "but for" these events or these actions, an injury would not have occurred.[158] To be a but for

---

153. *Id.*

154. *Id.*

155. *See* Intel Corp. v. Hamidi, 1 Cal. Rptr. 3d 32, 50 (Cal. Ct. App. 2003) (holding that where sending E-mail did not actually affect Intel's servers, there was no trespass to chattels); *see also* White Buffalo Ventures LLC v. Univ. of Tex. at Austin, 420 F.3d 366, 377 n.24 (5th Cir. 2005) (expressing skepticism that the injury claimed in a trespass to chattels claim can be found where it is merely speculative).

156. *See* People Exp. Airlines, Inc. v. Consol. Rail Corp., 495 A.2d 107 (N.J. 1985).

157. *See generally* Danielle Conway-Jones, *Factual Causation in Toxic Tort Litigation: A Philosophical View of Proof and Certainty in Uncertain Disciplines*, 35 U. RICH. L. REV. 875 (2002); *see also* David W. Robertson, *The Common Sense of Cause in Fact*, 75 TEXAS L. REV. 1765 (1997)

158. *See, e.g.*, Perkins v. Texas & New Orleans R. Co., 147 So.2d 646 (La. 1962) (court found no factual causation for accident between train and automobile based on train driver's negligence in traveling faster than company-imposed speed limit where evidence did not

cause, an action need not be the sole cause, but it must have been a part of the causal chain leading up to the to the injury.[159] Actions that are too remote in time or place from the injury may be factual causes, but may be cut off by the requirement that the action also be a proximate or legal cause of the injury.[160]

Where an alleged cause of injury, however, combines with other causes such that the alleged causes can no longer be distinguished, "but for" causation fails.[161] The most well-known cases where this occurs are cases involving fires.[162] In one famous case, two fires combined to destroy a house.[163] One was started negligently and the other was a fire of unknown origin.[164] When they combined, the defendant who negligently started the one fire argued that he should not be liable because the home would have been destroyed even if he had not started his fire.[165] In such a case, the court said, a defendant's acts will be found to meet the requirements of "but for" causation where the defendant's negligence was a substantial factor in bringing about the harm.[166] It need not be the only cause, and it need not be a cause without which the injury would not have occurred, but it must be something more than a minor part of the overall chain of causation.[167]

In addition, even if a court is unwilling to say as a matter of law that a compromised system with low computing and network power was not a cause-in-fact of the victim website's injuries, it should be willing to consider whether such a site should be liable using concept of proximate cause. Proximate cause asks a court to consider, using aspects of law such as policy, fairness, and foreseeability, whether liability should be imposed or whether the results were too remote or otherwise divorced from the defendant's actions to justify such a finding.[168] Proximate cause has been used to preclude liability when the

---

prove that, had the train stayed within the speed limit, the accident would not have occurred).

159. *See generally* Conway-Jones, *supra* note 157.

160. *Id.*

161. *See* Tory A. Wiegand, *Tort Law—The Wrongful Demise of But For Causation*, 41 W. NEW ENG. L. REV. 75 (2019).

162. *See, e.g.*, Anderson v. Minneapolis, St. P. & S. St. M. Ry. Co., 179 N.W. 45 (Minn. 1920).

163. *Id.*

164. *Id.*

165. *Id.*

166. *Id.*

167. *Id.*

168. *See* Palsgraf v. Long Island R.R. Co., 248 N.Y. 339, 349 (Andrews, J., dissenting) (1928) (The Andrews dissent in Palsgraf is a one of the preeminent articulations of the proximate cause standard in a case where the majority and dissent disagreed over the role of duty and proximate cause. Andrews noted, "It is all a question of expediency. There are no fixed rules to govern our judgment. There are simply matters of which we may take account. We have in a somewhat different connection spoken of "the stream of events." We have asked

end results of actions were not foreseeable or predictable to those involved.[169] It is not a test of what the defendant intended, but rather of what was a natural and sufficiently direct consequence of the defendant's actions.[170]

Proximate cause would give a court another avenue for releasing system owners who control lower amounts of computing and networking power from DoS lawsuits. Policy reasons why this makes sense are taken up below, as many of these are also related to the concept of duty (and of standards of care, which, as they serve primarily as factual inquiries, are not addressed in this argument). But the indirectness and incompleteness of a low-powered system's contribution to a DoS attack supports a finding that such a system owner should be found to not be a proximate cause of the victim website's ultimate harms. The amount of power being too small to cause significant harm should lead a court to conclude that such a use of power, even combined with additional small amounts, is not such a proximate cause.

These understandings again push us toward releasing low-power system owners from liability while keeping those who have more power at their disposals potentially liable. A larger amount of power is more likely to be found to be a substantial factor in the kinds of injuries victim websites are likely to sustain, while lower power systems are less likely to be able to inflict the same kind and amount of injury. As elsewhere in this analysis, more is different, not just more, and the law should recognize this and analyze these cases to take such factors into account.

---

whether that stream was deflected—whether it was forced into new and unexpected channels. This is rather rhetoric than law. There is in truth little to guide us other than common sense. There are some hints that may help us. The proximate cause, involved as it may be with many other causes, must be, at the least, something without which the event would not happen. The court must ask itself whether there was a natural and continuous sequence between cause and effect. Was the one a substantial factor in producing the other? Was there a direct connection between them, without too many intervening causes? Is the effect of cause on result not too attenuated? Is the cause likely, in the usual judgment of mankind, to produce the result? Or, by the exercise of prudent foresight, could the result be foreseen? Is the result too remote from the cause, and here we consider remoteness in time and space." *Id.* at 353 (internal citations omitted); *see also* Ryan v. New York Central R.R. Co., 35 N.Y. 210 (1866) ("It is a general principle that every person is liable for the consequences of his own acts. He is thus liable in damages for the proximate results of his own acts, but not for remote damages. It is not easy at all times to determine what are proximate and what are remote damages.")

169. *See* THE RESTATEMENT (THIRD) OF TORTS §29 (2010) ("'An actor's liability is limited to those harms that result from the risks that made the actor's conduct tortious.' Consider each of these cases and think about whether plaintiff's harm was within risk of defendant's conduct").

170. *Id.*

4. Additional Wrinkles

There are additional doctrinal wrinkles that support the argument for dividing compromised system owners in these circumstances. These involve the concepts of joint and several liability and enterprise liability. Many states still apply the doctrine of joint and several liability to tort defendants who contribute to the same injury.[171] Joint and several liability requires that any one defendant can be held liable for the entirety of the damages she contributed to, but then can seek contributions to that award from the other defendants.[172]

The unfairness of such a regime to those who might own only one or two computers or network enabled devices is apparent on its face. If all a victim website needs to do is identify one computer that participated as a zombie in the DoS attack, one entity or person may he held liable for the carelessness of millions of other actors (and potential defendants). Yet, a system owner that controls more power is in a position to better help itself identify other likely defendants and seek contribution through either hiring computer forensics experts or through its own expertise. Again, the doctrine pushes us toward recognizing the distinction between DoS zombies made up of those with little computing and networking power and those with more.

One final note is relevant to this part of the discussion: some states have also allowed plaintiffs to sue one or more participants in an industry on the theory that it is unfair to require the plaintiff to prove which caused the actual injury, but that all were engaged in pursuing common goals relating to their shared industry; a concept known as market share liability. In *Sindell v. Abbott Laboratories*,[173] the California Supreme Court applied a version of enterprise liability to manufacturers of the drug DES. Because those injured by DES could not generally prove which manufacturer's DES they took, but all manufacturers produced essentially the same drug, the California court held them liable to the extent of their participation in the marketplace.[174] Both enterprise liability, which has been imposed to put all the liability for an injury on any of the participants in a market where those participants were bound together by industry standards related to safety and preventing injuries,[175] and market share liability are not

171. *See generally* Nancy C. Marcus, *Phantom Parties and Other Practical Problems with the Attempted Abolition of Joint and Several Liability*, 60 ARK. L. REV. 437, 439 (2007); *see also* Richard W. Wright, *The Logic and Fairness of Joint and Several Liability*, 23 MEM. ST. U. L. REV. 45 (1992).

172. *Id.*

173. 607 P.2d 934 (Cal. 1980).

174. *Id.* at 937.

175. *See* Hall v. E.I Du Pont De Nemours & Co., Inc., 345 F. Supp. 353 (E.D.N.Y. 1972) (holding that where blasting cap manufacturers all agreed individually to safety standards and allowed an industry organization to play a lead role in safety guidelines, plaintiffs need

likely to be applicable to the situations arising in DoS attack cases. While there is some superficial appeal to applying the doctrines here, the users of computers, networks, and computing or network enabled devices do not share any industry thereby, and are not in any way likely to be pursuing common or joint interests. These concepts do not push us in one direction or the other in determining compromised system owner liability in DoS attack cases, nor do they provide fertile ground for courts searching for doctrinal foundations in this complicated, more is different, scenario.

5. Closing Thoughts on Tort Doctrine

Within the tort context, a number of concepts come into play. Duty, especially the concept of duty as viewed in the enabling tort context, causation, joint and several liability, and alternative theories of holding defendants liable (such as market share liability) are all potentially relevant in DoS cases. Leading up to this point, I have argued that the DoS scenario is likely to present us with daunting factual scenarios from a variety of perspectives: the sheer numbers of potential defendants, their wide geographic dispersion, and their nature (whether individual, small business, or large concern). The many and complicated tort doctrines, combined with the unique and difficult factual scenarios and the myriad approaches taken by differing jurisdictions, make predicting outcomes based on existing doctrine uncertain at best and a complete guess at worst. Finding a way through the labyrinth of tort doctrine to reach the correct conclusion, and the basis for choosing a particular path, are the tasks we turn to next.

IV. WHERE TO GO AND HOW TO GET THERE: COMMUNITIES OF INTEREST IN INTERNET SYSTEM OWNERS

The legal analysis above provides the necessary foundation for the discussion of how and why more is different matters and how law and legal institutions should react to the potential for widespread, disparate liability of system owners in DoS attacks. The solution I propose, given the plasticity of the doctrine and the challenging factual basis outlined above, is to focus on the amount of computing power brought to bear in a particular attack and each defendant's contribution to that power.

To reach a conclusion on the appropriateness of dividing computer and network owners by the amount of computing and networking power they control, we will look to concerns that are routinely

---

only prove that one of the industry participants sold the blasting caps in question—the defendants would then be able to try to prove which of them was actually liable or would be held jointly and severally liable for the injuries caused by the industry's negligence).

discussed by judges, lawyers, and legislatures in making the decision whether to make particular actors liable or not liable for injuries in which their actions played at least some part. In this context, the "communities of interest" concept provides a framework that can assist courts in initially determining whether a duty should be imposed on a particular grouping of users based on the computing and network power those users tend to have.

"Communities of interest" are a well-worn legal concept used across a host of legal contexts. They have perhaps been most used in the area of voting rights, where they have been asserted as a neutral principle in redistricting and racial gerrymandering cases.[176] They have also been used in cases involving selection of juries,[177] labor practices,[178] farm equipment dealership regulation,[179] and airport operations,[180] among others.[181] The community of interest terminology has also been used in cases referring to property interests[182] and in a case involving a class action lawsuit seeking access to a water source.[183] Early uses

176. "In February 2011, the House Committee on Privileges and Elections adopted a resolution establishing criteria to guide the redistricting process. Among those criteria were traditional redistricting factors such as compactness, contiguity of territory, and respect for communities of interest." Bethune-Hill v. Va. State Bd. of Elections, 137 S. Ct. 788, 795 (2017); *see* Stephen J. Malone, *Recognizing Communities of Interest in A Legislative Apportionment Plan*, 83 VA. L. REV. 461, 464-65 (1997).

177. United States v. Booker, 367 F. App'x 571, 575 (6th Cir. 2007) ("Booker has not shown that citizens engaged in full-time study or citizens over 70 years old represent distinct communities of interests, *cf. Taylor,* 419 U.S. at 531, 95 S.Ct. 692, nor shown that either group is substantially underrepresented on jury venires, nor shown that granting these dismissal requests breaches the prohibitions of the Jury Selection and Service Act.").

178. Staten Island Univ. Hosp. v. N.L.R.B., 24 F.3d 450, 455 (2d Cir. 1994) ("Unit determination, by contrast, requires only a substantial community of interests among a group of employees to support casting them as a unit. Substantial communities of interest may be found for units of varying scope, and the NLRB enjoys discretion to select from those possible arrangements in reaching its unit determination.").

179. Frieburg Farm Equip., Inc. v. Van Dale, Inc., 978 F.2d 395, 398 (7th Cir. 1992) (noting the Wisconsin Supreme Court's adoption of guideposts for determining communities of interest using "continuing financial interest" in business relationships and interdependence of relationships).

180. South Dakota v. Civil Aeronautics Bd., 740 F.2d 619, 620 (8th Cir. 1984) ("The Deregulation Act defines essential air transportation as a minimum of two daily round trips, five days a week. 49 U.S.C. § 1389(f). Other than this requirement, the Act expressly leaves to the Board the development of criteria for determining what service 'satisfies the needs of the community concerned for air transportation to one or more communities of interest and insures access to the nation's air transportation system.' *Id.*").

181. *See, e.g.*, Christopher S. Yoo, *The Role of Politics and Policy in Television Regulation*, 53 EMORY L.J. 255, 271-72 (2004) (discussing the role of geographic localism in comparison with communities of interest in television regulation).

182. *See* Allison v. Cody, 89 So. 238, 239 (1921) (referring to tenancies in common "or other communities of interest in properties").

183. *See* Manro v. City of Tulare, No. F043091, 2003 WL 23096997 (Cal. Ct. App. Dec. 31, 2003).

were often focused on courts of equity to combine lawsuits together to prevent multiple lawsuits on the same issues,[184] though this process was not without controversy.[185]

The notion of a community of interest is thus malleable to the circumstances, but we must focus less on the kinds of geographic or territorial concerns less likely to be relevant to internet related issues[186] and more on the similarities and dissimilarities shared by those drawn into a particular exchange or dispute.[187] Some past uses lend themselves more closely to our goal here than others. Because many of the other uses of the communities of interest concept have foundational territorial elements,[188] I leave those uses aside. For our purposes, a community of interest is a group of computer and network system owners who share not only a similar amount of computing and networking power but who also share similar purposes in connecting to and utilizing the internet itself. Such groups may be composed of categories such as "home users," home businesses, small businesses, large organizations, internet service providers, online retailers, internet content providers, and others (determined on a case by case basis).

Communities of interest for purposes of DoS liability should be based primarily on the computing and networking power controlled by the compromised system owner in question. Additional factors

---

184. *See* Comment, *The Jurisdiction of A Court of Equity to Prevent A Multiplicity of Suits*, 22 YALE L.J. 49, 53 (1912) ("There is some diversity of opinion among the writers as well as the courts as to the power of a Court of Equity to grant an injunction to enjoin numerous tort actions where there is merely a community of interest in the questions of law and fact involved in the controversy").

185. *See, e.g.*, Roanoke Guano Co. v. Saunders, 56 So. 198, 199 (Ala. 1911) (rejecting the view that the existence of a community of interest was enough, in and of itself, for a court of equity to grant a bill of peace, i.e., a request to consolidate numerous plaintiffs' actions into one case).

186. For a discussion of how metaphors around physical places influence the development of internet regulatory structures, *see* Hunter, *supra* note 140; *see also* Lemley, *supra* note 140.

187. *See, e.g.*, Critchfield Physical Therapy v. Taranto Grp., Inc., 263 P.3d 767, 776-77 (Kan. 2011) (in the class action setting, noting "Commonality requires a plaintiff to demonstrate that the proposed class members have suffered the same injury and their claims must depend on a common contention that is capable of class-wide resolution, meaning that determination of its validity will resolve an issue that is central to the validity of each of the claims with one answer. Wal–Mart Stores, Inc. v. Dukes, 564 U.S. ——, ——, 131 S.Ct. 2541, 2551, 180 L.Ed.2d 374 (2011)").

188. Nicholas O. Stephanopoulos, *Redistricting and the Territorial Community*, 160 U. PA. L. REV. 1379, 1385 (2012) ("A few points of clarification: First, by 'territorial community,' I mean (1) a geographically defined group of people who (2) share similar social, cultural, and economic interests and (3) believe they are part of the same coherent entity. Under this definition, territorial communities sometimes, but not always, mirror political subdivisions such as towns and counties. Territorial communities also are not quite the same thing as "communities of interest" (a common term in the redistricting case law), which are not necessarily geographically rooted and can form on the basis of any shared concern. Rather, territorial communities arise from the unique combinations of geography, interests, and identity that characterize particular places").

relevant to assigning defendants to appropriate communities for purposes of assigning liability include their purposes in being connected to the internet, their level of technical sophistication, and their past experiences in being connected to the internet. Each of these may nudge the defendant toward or away from a new community of interest when combined with the primary concern of power provided by their compromised systems.

The most relevant of these secondary concerns should be the defendant's purpose in connecting to the internet. A defendant who has a primarily commercial interest in using the internet may belong in a community made up of those who have a greater responsibility for protecting against DoS attacks than those who use the internet for primarily personal purposes, such as staying in touch with friends and family. In such a case, an internet based commercial defendant whose systems contributed to an attack may be placed in a community that owes a duty to prevent such attacks, whereas a defendant with similar power involved in the attack but who is a private individual may be placed in a community that does not owe such a duty. The defendant's purpose in utilizing the internet should not be the controlling factor—that should remain the networking and computing power hijacked by the attacker—but, along with other similar concerns, may provide additional guidance in appropriately categorizing defendants for purposes of lawsuits in such cases.

On the whole, courts would be well placed to find that those who have sufficient computing and networking power to be a substantial factor in causing the injuries a victim website suffers from a DoS attack have a duty to act with reasonable care in dealing with their systems and keeping them secure, while holding those less sophisticated owners to not have such a duty. This conclusion is supported by the notion that more is not just more in these situations—more computing power, more computers, more potential defendants—but that more here is different, and that difference allows not only for differing attacks and harm but also for differing analysis of the potential liability based on the number and diversity of potential defendants.

A. The Test of Power

The critical element of sorting potential defendants in DoS cases into communities of interest should rely on assessing the extent to which those defendants contributed to a particular attack. In other words, to utilize a notion of computing and networking power when deciding which tort doctrines should be applied and how they should direct the outcome of DoS cases, we must first understand what it means to have, and for attackers to utilize, computing and networking power. As noted when discussing the mechanics of DoS attacks,

attackers require two specific resources to launch their attacks: computer systems and network connections. Computer systems are used to create and initiate the sending of information. Network connections provide a way for the information to reach its intended target.

When a DoS attack takes place, large numbers of computers and many network connections are used to overwhelm the target site. Within a particular attack, we can measure the extent to which each compromised system contributed to an attack. A modern, up-to-date gaming computer with high end hardware—computer processor, random access memory, graphics card—and a high capacity internet connection will be more useful to an attacker, and do more damage to a target site, than an older, low-end system with a less powerful processor, less memory, and no separate graphics card connected to the internet by a dial-up-modem. The distinction becomes more pronounced if we compare a larger number of high-end systems over high capacity connections with a single, low-end system over a more limited connection.

To make "power" a useful metric in determining liability in any particular case, we must first determine the entire amount of power brought to bear against the target site. Thus, we must ask: How many packets of information were directed at the target site, what network connections delivered them to their destination, and how many computers and connections played a role in the attack? Once this factual and empirical question has been answered in a specific case, a particular defendant's role in the attack can be determined. Even without tracing each individual packet back to the specific defendant, a court could survey the computers that were identified as having participated in the attack and determine their capacity to contribute to the attack. Combining this with information concerning the network connection used by the computer in question, the court could determine the overall percentage participation of a particular system. By adding together the computing power of all of the compromised systems owned by a particular person or entity, and then making appropriate adjustments for the networking capacity of that owner's systems, a court could reach a reasonable basis for determining the role that these systems played in the injury suffered by the target site.

Note that we're not simply counting computer systems here and noting the percentage of computers owned by defendant that were used in the attack. Instead, we're both quantifying and qualifying the power that those computers have. Using the processing power, ram, and related hardware specifications, we can tell how often a particular system can send information over the network, bearing in mind the capacity of the network itself. This allows us to more appropriately gauge the potential for damage that can be caused by any system or

grouping of systems, and to choose appropriate tort doctrines to filter those contributions into "low (computing and networking) power" and "high (computing and networking) power."

This approach allows a court to consider whether to use duty or causation to dismiss a case against a particular compromised system owner, or whether to allow such a suit to continue. In so doing, courts can better further a host of public policy goals relevant to internet DoS attacks, while at the same time making efficient and effective use of judicial resources and treating the parties to a DoS lawsuit fairly. To prove this point, we turn now to questions of policy, judicial resources and fairness.

B. Networks and Network Operations: Another Big Picture

The internet was designed as a method for the efficient communication of information without regard to the information's content or substance.[189] By breaking transmissions into pieces and routing them across different paths according to network conditions, the internet's design provides increased efficiency and robustness for communications channels.[190] Not only are the "pipes" used more efficiently than in communication systems' previous designs, but they are also able to "route around" broken or busy nodes to keep communication flowing.[191] An "end to end" design, the internet's hardware and software protocols pass along traffic without distinguishing one type of content from another.[192] Whether content is beneficial or illegal, legitimate or stolen, video or text, it passes across the internet in the same way. There may be more of it (if it is video content, for example), and one file may take longer than another to make the journey, but so long as the internet's basic transportation and internet protocols are followed, both will make the trip from sender to receiver without difficulty. This is a feature of the design, not a bug.[193]

This design, however, can also be utilized to launch DoS attacks either using compromised systems or by harnessing the internet's

189. *See* Robert A. Heverly, *Breaking the Internet: International Efforts to Play the Middle Against the Ends—A Way Forward*, 42 GEO. J. INTL. L. 1083, 1088-1095 (2011).

190. *See* Kevin Werbach, *The Centripidal Network: How the Internet Holds Itself Together, and the Forces Tearing It Apart*, 42 U.C. DAVIS L. REV. 343 (2008).

191. Philip Elmer-Dewitt et al., *First Nation in Cyberspace*, TIME (Dec. 6, 1993), http://www.time.com/time/magazine/article/0,9171,979768,00.html (last visited June 4, 2020).

192. Mark A. Lemley & Lawrence Lessig, *The End of End-to-End: Preserving the architecture of the Internet in the Broadband Era*, 48 UCLA L. REV. 925 (2000); John Palfrey & Robert Rogoyski, *The Move to the Middle: The Enduring Threat of Harmful Speech to the End-to-End Principle*, 21 WASH. U.J.L. & POL'Y 31 (2006).

193. Mark Lemley et al., *Don't Break the Internet*, 64 STAN. L. REV. ONLINE 34 (2011).

basic functions and protocols and leveraging them to overwhelm a victim website. Attackers use not only systems connected to the internet that have been compromised, but also systems that are functioning normally, systems such as the DNS system or even basic functions of the internet's routers themselves.[194] The law's response to this utilization of internet connected resources will affect not only those directly involved in the attacks, but also those connected to the internet. A response that imposes too much liability risks creating disincentives for people to join or remain on the network, while a response that imposes too little liability risks creating incentives that diminish the overall response to DoS attacks across the entirety of the internet.

Consistent with the development of negligence from its early English roots, courts and legislators confronted with problems that affect broader structures such as the internet often take into account the effects their decisions will have on those larger structures when establishing whether liability should be imposed. Specifically, the policy choices made here must take into account the effect on the internet as a whole, and not just the effects on individual victims or websites involved in DoS attacks.

For the internet, the choices made in DoS attack cases have potentially important effects on its functioning. For example, if individuals are required to defend lawsuits brought by the likes of Amazon or Facebook, with the possibility of being held jointly and severally liable for all of the damages these internet behemoths suffered in a large-scale DoS attack, individuals may quickly become wary of utilizing the internet to the scales they have been utilizing it so far. They may trade smart phones for phones that stick to making telephone calls and take computers offline. They may also be unwilling to buy and use the highly efficient devices currently being developed and deployed in the Internet of Things. These outcomes undo the efficiency gains in tasks such as communication, economic transactions, and practical control of systems and products.

Where computers owned by an entity or person with relatively small amounts of computing and network power are used in an attack against a large and powerful (from a computing and networking standpoint) target site, owners should not be liable where their contribution to the attack was low enough that it did not make a substantial contribution to the overall injury suffered by the target. Absent such a rule, low power internet users may decide the risks of participation on

194. *See* YU, *supra* note 3, at 10.

the internet are too high. Encouraging people to disconnect from the network in large groups cannot be the end game of imposing liability on the internet.

Keep in mind that the spectrum of users may mean that a lower powered compromised site may be liable to one plaintiff and not another. Following this methodology, a small business with fifteen compromised computers[195] would be unlikely to make a substantial contribution to an attack against Google but may have sufficient power to play a substantial role in an attack against a similarly sized small business. There may be some users with so little power that they may never make a substantial contribution to an attack—home users, for example, with few computers connected to the internet through a home broadband provider.

It should be clear that this rule does not require us to insulate all internet users from liability. As we have seen, the most basic argument in favor of DoS liability of compromised systems proceeds as follows: where owners of compromised systems have failed to secure their systems against use by attackers, they have breached a duty of care and as such should be held liable for the harm that follows when their systems are used to cause such harm. This analysis takes account of none of the larger concerns that attach to internet related liability determinations. It over-simplifies the incentives structure in which it operates and ignores the substantial distinctions in purpose, method, sophistication, and effect that such determinations have on internet operations.

It thus becomes critical to acknowledge again that when it comes to potential DoS defendants, more is not just more, more is different. The "more" here changes not just the magnitude, but the nature of the attack and the nature of the resources used in the attack. In other words, the millions of computers used in a DoS attack are not duplicates of each other, owned by owners with similar interests, sharing core values and purposes in connecting their systems to the Internet. Some system owners run small businesses and use the Internet for ordering and basic advertising of brick and mortar stores, other system owners provide internet-based services such as e-mail, web design and hosting, and online shopping, while still others provide the basic services necessary for the internet itself to function. There is no shared interest among these varying communities other than that the internet is in some way relevant to their business interests. The level of that interest can and does vary significantly from entity to entity. In this context,

195. Number of computers here is used as a rough proxy for the computing and networking power utilized in an attack. The correct measure would need to not simply count the computers, but place a value on their combined processing speed, ram configuration and network bandwidth.

not all compromised system owners should be easily excused from lawsuits based on DoS attacks launched using their systems, but some compromised system owners should be dismissed.

By grouping compromised system owners into communities of interest, groupings made up of defendants who are similarly situated according to the amount of computing and networking power they control, their purpose in utilizing the internet, and other related concerns, courts will have a framework that allows them to appropriately determine which defendants in the myriad of possible defendants should be in a position to defend against a lawsuit from a website targeted by a DoS attack using those defendants' computing and networking resources. Combined with the additional concerns outlined below, courts can provide appropriate incentives to involved parties to take efficient precautions to prevent harm to others while not imposing potentially crippling liability on defendants inappropriately.

C. *Risk and Resources*

Famously, or perhaps infamously, Judge Learned Hand designed a formula to articulate the circumstances under which a negligence defendant should be required to take steps to prevent injuries to others.[196] It is stated as follows:

$$B < PL$$

In this formula, B equals the burden of taking a particular precaution, while P equals the probability a loss will occur without the precaution, and L equals the likely extent of the loss.[197] Where the burden of taking the precaution is less than the probable loss from failing to take it, Judge Hand suggests that the precaution should be taken.[198] In that case, courts should require that defendants meet a standard of care that would prevent the injury in question.[199]

Applied loosely—it has long been admitted that the Hand Formula is not subject to rigorous mathematical application[200]—the formula acknowledges that those who are in a position to affect others should, in appropriate circumstances, take appropriate precautions to prevent those injuries.[201] In the DoS case, the community of interest concept

196. United States v. Carroll Towing Co., 159 F.2d 169, 172 (2d Cir. 1947).

197. *Id.* at 173.

198. *Id.* at 174.

199. *Id.*

200. *See* U.S. Fid. & Guar. Co. v. Jadranska Slobodna Plovidba, 683 F.2d 1022, 1026 (7th Cir. 1982) ("Though mathematical in form, the Hand formula does not yield mathematically precise results in practice; that would require that B, P, and L all be quantified, which so far as we know has never been done in an actual lawsuit.").

201. *Id.* ("[T]he formula is a valuable aid to clear thinking about the factors that are relevant to a judgment of negligence and about the relationship among those factors.").

allows us to think through these issues at a deeper level. It may appear that low power compromised system owners, those in the community of interest with the least likelihood of being held liable under the analysis I propose, are still in a position to take on a relatively light burden of maintaining the proper and secure functioning of their systems, and thus under the Hand Formula should be required to do so, regardless of the other factors discussed here. In some cases, relatively simple steps may be all that are necessary: allowing a Microsoft Windows computer to automatically install updates to the operating system and word processing suite; allowing other programs, especially those prone to compromises such as Adobe's "Flash" application, to likewise update; and, installing and maintaining functioning antivirus and anti-malware programs.

Yet the appearance of a low burden here can be deceiving, and the difficulties with causation raise additional complications. In our situation, one with low computing and networking power is unlikely to be a sophisticated computer user. Home users, parents, teens, and brick and mortar businesses are unlikely to have access to dedicated technical support. They may not fully understand the settings needed to fully secure their systems, and they may over-rely on off-the-shelf solutions provided by their software providers, solutions that may be targets of hackers themselves because of the unsophisticated nature of their users. Even allowing for those who correctly secure their systems, zero-day attacks—attacks against computing infrastructure based on vulnerabilities that users and providers are not yet aware of—can subject a well secured individual or small system to compromise and infiltration. Thus, while the burden of asking individual or small computing and networking power holders to secure their systems at first blush appears small, on deeper reflection any the burden grows larger and at the same time seems likely to be ineffective.

There are additional aspects of computing and networking security that add uncertainty to the burden/probability of loss formula. There may be good reasons, for example, for individuals and small users not to quickly and unthinkingly update their systems as soon as an update is available. This is a reasonable approach because software vendors often integrate "upgrades" to software with their security patches. Microsoft, for example, often rolls out significant changes to the functioning and capabilities of its signature operating system, Microsoft Windows.[202] It is well-established that such changes can cause existing software on a system to stop functioning properly or at all.[203] Small

202. *See generally Overview of Windows as a Service*, https://docs.microsoft.com/en-us/windows/deployment/update/waas-overview?redirectedfrom=MSDN (last visited June 4, 2020).

203. *Id.*

users have learned this from experience, and often wait to watch what effects such changes on others before installing the upgrades on their own systems.[204] This is a rational approach to addressing the complexities that computing and networked systems bring to our lives, and it is one that the law should allow small users to continue to take.

When taking this tack, we must compare the dangers to other systems posed by small or solo networked or computerized systems. It would be difficult to launch a successful DoS attack against a target site of any significance with a single or even a few computerized or networked systems. More are needed. The required network of zombies could conceivably be made up entirely of individual systems, in which case the methodology advocated here would preclude any recovery by the targeted and injured site.

Yet in this context, where no one system could provide the basis for a successful attack, fairness and policy require focus on those individual systems, on their rational choices, and on the actual contribution they make to the attack. If the threat of liability looms too large, we risk chasing some of these entities from the net, increasing inefficiency in communication and isolating individuals and small entities from the wider world. But our analysis does not end with the community of interest made up of small power holders. The corollary holds true for those larger resources, ones with greater computing and networking power, and who have greater ties to the internet ecosystem. It is that larger power that provides the justification for a duty and the establishment of a standard of care that would assist in combatting DoS attacks from the compromised system side of the calculation.

In contrast to the risk/reward determination for individual and small users, as the amount of computing and networking power held increases, so does the basis for imposing a duty to keep downstream users safe from DoS attacks using those systems. This community of interest, the group of larger computing and networking power holders, most often seeks to use the internet for commerce, either in providing internet services or using the internet to sell goods or services (including information goods). The potential reward for this group's internet-based activities increases as computing and networking power increases. Therefore, the corollary imposition of a duty begins to make more sense. As the potential increases, the risk to others of DoS

204. *See* Ed Bott, *How to take control of Windows 10 updates and upgrades (even if you don't own a business)*, ZDNET (Jan. 17, 2018) https://www.zdnet.com/article/how-to-take-control-of-windows-10-updates-and-upgrades-even-if-you-dont-own-a-business/ (Last visited June 4, 2020).

attacks increases as well, and that risk reward correlation justifies imposition of potential liability on grounds of both fairness, and policy.

Initially, however, in what ways does this group, the community of interest of high-power holders, differ from the smaller power holders? For example, larger power holders would also be subject to the game changing updates imposed by software companies. An update to Microsoft Windows that breaks portions of an individual's system will break concomitantly more systems in a larger environment. Some of these may be mission critical, their failure bringing significantly more disruption to more people than a single such failure on a smaller computing and networking power holder's system. How, then, to justify refusing to impose a duty on small power holders but imposing one on the community of high-power holders?

The answer is in the risk/reward calculus. An entity that is caretaker to a large amount of computing and networking power is leveraging that power in search of rewards. Part of that search for rewards must be the duty to play a role in ensuring the integrity of the system by which the rewards themselves are sought (in other words, the internet). The high-power holding community of interest should thus be expected to hire expert technical help, to contract for what help they cannot secure themselves, and to negotiate with software and hardware providers to provide the opportunities necessary for the community members to secure their systems without breaking them.

Policy concerns support this path to duty—and past the other uncertainties in negligence liability questions raised above—where the group held liable is an active participant in seeking to gain financially from internet connectivity, it follows logically that additional burdens, including those flowing from imposition of a duty of care, may and should be imposed by the law. These additional burdens should not outweigh the dangers posed by the activities in which they are engaged. To hold otherwise would allow internet businesses to reap the benefit of their actions in financial terms while externalizing at least one potentially significant cost on other internet users. Even where a non-profit concern is involved, where larger amounts of computing and networking power are involved, the scale of the operation should be sufficient to justify the imposition of liability on what is obviously an internet directed operation, as opposed to those smaller scale or individual users who are focused instead on utilizing the internet to accomplish goals not directly related to its functioning.

It is also fair for the community of interest that includes compromised systems that utilize great amounts of computing and networking power to be asked by the law to shoulder some of the burden of defending against DoS attacks. Unlike smaller or individual computer and network users, for whom taking the steps required may be both ineffectual and a barrier to participating in internet exchanges at a

relatively small level, the grouping of large users should have both the resources and the technical expertise available to take any steps demanded by reasonableness in relation to securing their systems against use by outside forces in DoS attacks. Fairness allows this latter group to be required to do so where their interests go beyond individual online interactions to actually using the systems they've connected to the internet for active participation in commerce on a grander scale.

This shows us one more way in which more is different in the context of DoS attacks. I advocate for imposing a duty of care on high power holders in this scenario not simply because they have more computers, or even simply because they have more computing and networking power—though that is likely to be a primary element of reaching this conclusion—but because the more of their systems is different. It has different aims than smaller power holders, it has different abilities than smaller power holders, and so we assert a duty on the one while eschewing such an imposition on the other.

In between, of course, is the gray area, where the question of duty will be closer, and where the discussions surrounding the appropriate standard of care will become ever more complex. Courts in the middle cases, where power held is neither small nor large, where the aims of the relevant community are mixed between personal communication and engagement and solicitation of a greater engagement across the globe, should still use the community of interest paradigm to decide whether the imposition of a duty—or the finding of no duty in Third Restatement terms—is the most appropriate result. Where the power and shared interests in the middle community push toward either the larger or the smaller communities, courts can impose or not impose duties as the analysis shows will result in the best outcomes both for the particular parties and for the internet as a whole. This greater awareness of the entirety of the equation, of the pieces from beyond the individual dispute, is what the communities of interest paradigm provides in this context, and courts should take advantage of it appropriately to obtain the most appropriate results in such case.

Courts confronted with the community of interest formed by the middle group of users that pushes toward the larger side may also impose a duty so that the jury can more carefully investigate the manner of contribution of that particular community's members. Using jury instructions concerning proximate cause, as well as through its identification and articulation of the standard of care, the court can guide the jury to the relevant criteria for assigning or not assigning liability. Where the facts are sufficiently clear regarding the actual role played in the attack by the medium sized compromised systems owner, the court may decide that summary judgment is appropriate. Defending a lawsuit beyond a motion to dismiss may be the cost of being something

more than the small or individual computer or network user, but being able to escape such a lawsuit on a motion to dismiss may be the benefit of not quite making it into the big leagues. Such a framework again comports with fairness and policy concerns considered by courts in negligence cases, as it reflects well the risk-reward dynamic of this group of internet users as it does the larger group. It is a tailored approach to liability based on the community of interest into which the potential defendants fit.

There are more reasons, however, that the "high-power community" and the "small-power community" concept provides leverage for reaching appropriate outcomes in DoS cases. Next we turn to the effects that this liability scheme would have on the target sites and the incentives provided to or withdrawn from those target sites by the liability decisions within the scheme.

D. A Robust Defense

The argument regarding the identification of groups of like internet users with shared interests based on computing and networking power and dividing them into communities of interest based on the level of power a particular attack brought to bear also provides another benefit. Where a DoS victim cannot rely on being able to seek compensation from all compromised systems that were used in a particular attack, that victim must act proactively to defend itself from such attacks. By using active defenses against DoS attacks, many of which exist today, target sites can help to erect another fundamental layer of defense against DoS attacks, making them harder to launch successfully.

During the early growth of the internet as a public network, a now famous New Yorker cartoon opined that, "On the Internet, nobody knows you're a dog."[205] The cartoon acknowledged the ability of internet users to be relatively anonymous and to represent themselves as they wished to be represented. In other words, the internet makes all users equal. I take the position that in relation to DoS attacks, all those connected to the internet are not equal. What kind of users, then, would be motivated to actively defend themselves by the potential liability or lack thereof on the part of compromised system owners?

The answer is that many internet connected interests, both large and small, may be motivated to take steps to have the ability to mitigate ongoing DoS attacks against their resources. In each case the calculation will be made based on that target site's understanding of the risk of attack and knowledge that some or all of its damages will not be compensated by the law of negligence. This is a marginal

205. Paul Roberts, *On the Internet Nobody Knows You're a Dog*, DIGITALGUARDIAN (Sept. 28, 2015), https://digitalguardian.com/blog/internet-everyone-knows-you%E2%80%99re-dog.

but useful effect of the structure set out above. If an attacker gathers together one million compromised systems, all owned and controlled by those in the "small power" community of interest, the site targeted in the attack would have no recourse against the compromised systems' owners.

This is an unlikely scenario, however. It is more likely that an attacker will use compromised systems from a variety of communities of interest. Even in that case, all of the damages may still not be forthcoming. Uncertainties in addressing the standard of care, as well as questions concerning causation and whether the damages caused are cognizable in tort law will remain. This uncertainty will increase the likelihood that a site that views itself as likely to be a target of an attack will seek technological responses to such attacks. These include using a content delivery network to increase the site's bandwidth in the hopes its resources cannot be overwhelmed (and that it will thus stay live on the internet during the attack).

This effect on decision-making of the self-identified likely target sites is a reflection of the similar calculation on the other side. Where system owners with significant computing and networking power and similar interests are aware that their systems may be used in attacks, even though there is uncertainty as to whether they will ultimately be held liable for their role in the attack, they will likely act to combat such attacks. Even where the precautions they take are not certain to achieve their goals, they will at least be able to make a colorable claim of having met the reasonable person standard in their circumstances.

Thus, by leaving some indecision in the system, actors who act reasonably and rationally are likely to try to stop DoS attacks on both ends: at the compromised system and by active resistance and response at the target site. This doubling up of defenses creates additional barriers for the attacker, making such attacks more difficult, more expensive, and less effective. The uncertainty of the involved innocent parties is thus visited on the attacker.

Admittedly, this part of the framework in particular is likely to have effects only at the margins. The "nudge" to the potential target sites based on how the tort regime aligns potential liabilities within communities of interest is likely to be persuasive and lead to action on the part of compromised systems primarily when it aligns with other incentives. These concerns include the legal, regulatory, and contractual need to secure systems from the start against intrusions by third parties. Such intrusions are likely problematic under strictures such as HIPAA and SEC regulations, even where one of the outcomes is the use of the system in a DoS attack. A system that has been used in a DoS attack has been compromised, and it is the compromising of such systems that many of these requirements address. This, however, shows us more work that the communities of interest concept does: it

puts together in groups those entities that not only should be more attuned and responsive to the outside use of compromised systems, but those that likely are more attuned due to other, shared interests and concerns. As such, one more push at the margins is helpful in reaching our goal of asking system owners to act reasonably to prevent use of their systems in DoS attacks.

Similarly, the even lighter push for smaller and individual system owners travels the same analytical path. Those in the low power community are unlikely to handle patient health information or to be required to adhere to financial services industry or SEC regulations. As such, there is less of a push from a liability standpoint for those we've identified as both less likely to contribute significantly to large-scale DoS attacks and less likely to be able to efficiently take the steps necessary to effectively secure their systems from this kind of intrusion.

Again, within the complex and difficult arena involving liability in DoS attacks, it is the interest of the putative defendant, reflected in their purposes for connecting to the internet and their choices in regard to how much computing and networking power they maintain, that should drive the liability analysis. I hope by now I have firmly convinced you that the communities of interest analysis based on these factors provides a useful framework for undertaking this review. There are two more concerns, however, that we must take up, and each again is appropriately responsive to the touch of the community of interest analysis.

E. The Challenge of the DoS Pool for the Courts

The expansive nature of the potential DoS defendant pool is daunting. The potential geographic distribution, as well as the sheer number, of potential defendants is without any comparable analog in other tort situations. The doctrinal methods that courts have used to address situations in which many defendants contributed in some way to a plaintiff's injury are not well suited to the DoS case. In addition, some of these methods are directed toward problems not related to the heterogeneity of a defendant pool, such as questions of proof or factual causation in particular cases of injury. This counsels in favor of adopting the community of interest methodology to provide the courts with a suitable way forward in DoS cases, a way forward that acknowledges that in the DoS arena, more is different and accounts for those differences. The focus on computing and networking power, organized into communities of interest, with a requirement that defendants have systems with sufficient levels of power in

relation to the overall attack to justify holding them responsible at least in part for the attacks, provides a way forward in these cases.[206]

Without a methodology to organize potential defendants, courts may be presented with defendants of varying abilities, technical sophistication, knowledge, purposes, and technical equipment. Adding defendants to such a lawsuit could be a never-ending process. The initial defendants will simply use IP addresses to identify other potential compromised systems used in the attack and will then implead them. The new defendants will do likewise, and without any sort of organizing theme, the defendant class will grow unwieldy and difficult to manage. Third-party claims by one defendant against another, and by that defendant against others, could overwhelm the litigation system. Discovery in such an environment could likewise be extensive and never-ending, as new defendants are identified and brought into the litigation.

These are real concerns for courts and should not be dismissed lightly. While courts will not dismiss cases (or even individual defendants) based on complexity alone, where other policy and fairness concerns justify a framework that will release the least of those defendants, the courts are presented with new opportunities to examine these issues and provide some recompense to injured target sites, while not allowing those sites to entirely avoid their own responsibility to take action to defend themselves against DoS attacks.

By separating these groups out, leaving the low-power communities to the side, the battles over factual and proximate causation can be fought among similarly situated groups who have each contributed significant computing and networking power to the attack. This lessens the load on the court system, while still maintaining the goals of integrity of the negligence system and the robust defense of the internet from these attacks.

F. Fairness and Proportionality in Liability

So far, I have advocated for adoption of a framework that encourages courts to use the concept of duty to exempt system owners in the low-power community from liability. This is not the full argument, however, as I have also acknowledged that in certain circumstances many of the objections to low-power community member liability fall away. In this way, individual users might be liable for the damages suffered by a target site, but only where those individual (or other

206. This methodology has analogs to conversion doctrine, which requires that an interference with property must "so seriously interferes with the right of another to control it" before it will sustain a cause of action for conversion. RESTATEMENT (SECOND) OF TORTS § 222A (AM. LAW INST. 1965).

low-powered) users played an outsized role in an attack. Thus, an attack on a smaller entity launched using relatively few systems might be an appropriate scenario to impose a duty on the smaller compromised system. Larger target sites are unlikely to be seriously harmed by small scale attacks, while smaller target sites are likely to suffer lower damages than their larger counterparts. The liability in low-power attacks will thus be limited by the damages likely to be suffered by the system, and so are less likely to draw objections on the basis of fairness or policy.

From a fairness perspective this makes sense. Low-power users may be liable for low-power attacks that actually cause injury but will not be liable for their smaller contributions to larger attacks. The threat of crippling damages awards against smaller entities who may not have the technical and financial ability to make their systems compromise-proof could drive resources and users from the efficiencies provided by the internet. Likewise, a low-power community of interest member should not be able to fully externalize on other similarly situated entities the full damages that would flow where the low-power attack actually does damage. The community of interest framework allows us to thread the needle of these concerns and end up with a system that meets the requirements of both of these critical norms.

This conclusion leads us back to the underlying theme of my article: in the context of potential DoS liability, more is different. The potential liability of smaller, lower power interests must be contrasted with that of larger, higher power interests, but they are not opposite sides of the coin. In certain circumstances liability, or at least the need to defend a lawsuit past the filing stage, is likely to be appropriate. In other situations, liability is inappropriate. Using communities of interest to help match fairness concerns and provide proportionally appropriate results to litigants in DoS cases will thus be aided by the consideration of power to direct users into their appropriate communities.

V. CONCLUSIONS AND FURTHER THOUGHTS

The reasons attackers utilize compromised systems to attack target sites are often difficult to ascertain precisely. It may be out of a feeling of strength, a desire to exact retribution, to blackmail the target sites, or to inflict injury on a competitor, either industrial or governmental. The attacker plays a key role in the DoS attack, and we cannot forget that the third person in these situations is the one who actually initiates the series of actions that lead to the ultimate injury. Yet, because such attackers are hard to find, and are likely to be judgment proof or unreachable in other jurisdictions, the attacker does not hold the key to determining the full liability picture in these situations. Instead,

target sites seeking redress, and their subrogated insurance companies, are likely to seek compensation from the compromised sites that are used in the attack. These sites are easier to identify—the attacker often does not mask their internet addresses because they say little about the attacker or the attacker's identity or location—but, as I have shown, the compromised sites present us with a host of doctrinal and normative questions that leave their liability a question mark.

By organizing potential defendants into communities of interest—groupings of systems and their owners according to the amount of computing and networking power that they possess, along with related reasons for connecting to the internet—I have proposed a methodology to guide any court confronted with a DoS case. The analysis urges that a duty to take reasonable steps to prevent use of systems by attackers be imposed on the community consisting of high power systems with commercial interests, and fall along a spectrum until reaching low power systems, where such a duty should be imposed only when such systems are used in low-power attacks on smaller internet sites. Along the way courts will be forced to draw lines between duty and no duty circumstances, but will then have additional tort doctrines on which to fall back—proximate causation and purely economic damages doctrine, for example—to reach decisions that are equitable and that accommodate the many policy concerns raised by internet attacks of this kind.

The community of interest concept does not provide a discrete answer in every case, but it is not intended to. Instead it provides a path through the thorny and uncertain thicket of tort doctrine and policy. The uncertainty has its own place in the scheme of things, however, as it serves to provide incentives on the margins that allow parties to take efficiency and perceived risks into account in designing their responses to the threats of DoS attacks. This is true not only for compromised sites, but also for the target sites, which may need to shoulder some responsibility for providing an active defense against such attacks. In the end, only an internet wide effort led by those with the resources, motivation, and ability will make a dent in the continuing growth and exploitation of DoS attacks. This framework hopefully goes some way in placing law in a position to help achieve that goal.