2010

Unleashing a Cure for the Botnet Zombie Plague: Cybertorts, Counterstrikes, and Privileges

T. Luis de Guzman

Follow this and additional works at: http://scholarship.law.edu/lawreview

Recommended Citation
Available at: http://scholarship.law.edu/lawreview/vol59/iss2/7
UNLEASHING A CURE FOR THE BOTNET ZOMBIE PLAGUE: CYBERTORTS, COUNTERSTRIKES, AND PRIVILEGES

T. Luis de Guzman

In an April 28, 2008, blog post, computer security researchers announced a startling breakthrough: they had finally discovered a way to battle the Kraken.1 The researchers had not, however, uncovered a way to slay the mythical sea monster.2 This Kraken was a botnet3—a network of some 400,000 personal computers that were infected without their owners’ knowledge4 by software that caused the computers to transmit thousands of unwanted e-mails.5 By commanding the infecting network to destroy itself, the researchers would have reduced the flow of unwanted e-mails to users all over the Internet.6


2. Id. The “Kraken” is a mythical being believed by Scandinavian sailors to be a many-armed sea monster, whose arms, “if they were to lay hold of the largest man-of-war . . . would pull it down to the bottom of the sea.” 23 ROBERT HAMILTON & WILLIAM JARDINE, THE NATURALIST’S LIBRARY: MAMMALIA VOL. 8, AMPHIBIOUS CARNIVORA 327–28 (1839).


5. Kraken Botnet Infiltration, supra note 1 (describing infected machines on the Kraken network as “SPAM [unwanted e-mail] delivering zombie[s]”).

6. Id. (claiming an ability “to provide an ‘update’ through the existing Kraken protocol that can simply remove the Kraken zombie [software]” and describing a process to reverse-engineer Kraken command-and-control protocol). The researchers uncovered the means by which the network’s creator could command and control thousands of infected computers—in effect, the researchers were able to impersonate a Kraken command-and-control node. Id. By their own estimate, the researchers reported that “within a single week [they] would have been able to take over anywhere from 4% to 14% of the infected population” of computers. Id. Had the researchers chosen to take control of the Kraken network, they could have instructed the infected computers to delete the Kraken software. Id; see also Owning Kraken Zombies, a Detailed Dissection, Posting of Cody Pierce to DVLabs Blog, http://dvlabs.tippingpoint.com/blog/2008/04/28/owning-kraken-zombies (Apr. 28, 2008, 19:13 UTC) [hereinafter Owning Kraken Zombies] (providing a detailed technical analysis of Kraken botnet command-and-control infrastructure).
However, they declined to strike that final blow because they feared legal liability.

This Comment seeks to both address the security researchers’ concerns regarding legal liability as it pertains to defeating botnets and also to supply the legal means to disrupt botnets by counterattacking individual botnet hosts. To do so, this Comment first seeks to examine what damage a botnet could do if used in a cyberattack on an Internet-connected computer system. Then, it asks whether that damage is a sufficient harm under current tort law to provide a recovery for its victims. After establishing the liability owed to victims, this Comment turns to the prospect of holding the individual botnet zombies liable for the attacks made by botnet masters, because the zombies allowed their computers to be used by botnet masters in those attacks.

This Comment notes that although a very small minority of jurisdictions might allow recovery under such a situation, the majority of jurisdictions would hold that the botnet master’s actions were a superseding cause that extinguished the zombie computer-owner’s liability. This Comment suggests that under a new characterization of an individual computer-owner’s duty of care to other users on a public network, zombie computer-owners could be held liable for making their computers available to botnet masters for Distributed Denial of Service (DDoS) attacks. Using negligence, rather than trespass, to determine liability for these attacks allows victims to both effectively shift costs onto zombies and avoid needlessly artificial pleading.

After establishing the possibility of holding zombie computer-owners liable, this Comment further advocates the recognition of a legal privilege to allow DDoS attack victims to make reasonable digital counterstrikes against individual botnet zombies in order to disrupt the botnet as a whole.

I. ANATOMY OF A BOTNET

Before discussing potential civil liability issues involving botnets, it is helpful to first have a basic understanding of the technologies involved. A botnet is a network of computers, usually programmed for some repetitive task, under a single control mechanism. Although some instances of distributed computing are composed of willing participants that perform useful work, the

7. Naraine, supra note 4 (“It’s a very tricky situation. What if that end-user system is performing a critical function? What if that target system is responsible for someone’s life support? . . . It really is a moral and a legal quandary.” (quoting interview with David Endler, Director of Security Research, TippingPoint Technologies, Inc.)).


9. See, e.g., Folding@home, http://folding.stanford.edu/ (last visited Feb. 12, 2010) (connecting Internet-connected computers and utilizing user-donated processor time to calculate protein folding); SETI@home, http://setiathome.berkeley.edu/ (last visited Feb. 12, 2010) (using processor time donated by users of Internet-connected computers to process and analyze radio-
term "botnet" is usually used to refer to networks of computers—zombies—that have been compromised in some way without their operators' knowledge.  

A botnet affords its master a number of advantages. First, because attacks are launched from the zombies, which are distributed over a wide variety of networks and geographical areas, a botnet makes it more difficult to trace attacks back to the master. Second, the botnet's size increases the potential volume of malicious traffic that a botnet master can generate.

Botnets can be used for a number of illicit purposes, including DDoS attacks and sending unsolicited e-mail (spam). Denial of Service (DoS) attacks are a crude but effective way to remotely disrupt an Internet server: essentially, a DoS overpowers the target host, rendering it unable to respond to any other traffic. With enough volume, an attacker can deny those server resources to telescope data). Unlike the networks described in this Comment, these networks are composed of computers whose users permit the use of their unused processor time. Malicious botnets may theoretically be used for similar computationally intensive distributed processing, but as of this writing, the author is unaware of any non-permissively propagated botnets that are primarily used for distributed processing.


11. SCHILLER ET AL., supra note 8, at 30–31 (discussing why it is difficult to track botnet masters).

12. Botnets of remarkable size have been reported. A recent list of the top eleven botnets in terms of spam activity estimates that these top eleven account for some 1,370,000 Internet-connected computers. Joe Stewart, Top Spam Botnets Exposed, SECUREWORKS, Apr. 8, 2008, http://www.secureworks.com/research/threats/topbotnets/. In Stewart's list, the Kraken botnet (identified by an alternate name, "Bobax") ranks second in spam activity. Id.; see also Kraken Botnet Infiltration, supra note 1 (listing alternate names for the Kraken botnet—including "Bobax"). A single botnet discovered in the Netherlands consisted of 1,500,000 individual computers. See Gregg Keizer, Dutch Botnet Bigger Than Expected, INFORMATIONWEEK, Oct. 21, 2005, http://www.informationweek.com/news/security/government/showArticle.jhtml?articleID=172303265.

13. See SCHILLER ET AL., supra note 8, at 46–49 (describing various types of botnet DDoS attacks); id. at 51–55 (describing botnet spamming); see also Choo, supra note 10, at 3 (describing use of botnets in DDoS and spam dissemination).

legitimate connections, effectively making the target host inaccessible while simultaneously taxing the target's processing power.\textsuperscript{15}

Faced with a DDoS attack, system administrators can attempt to mitigate damage and reduce their exposure, by modifying their networks.\textsuperscript{16} Some system administrators, however, have resorted to self-help, taking actions such as reflecting DoS packets back to their originating computer.\textsuperscript{17} More recently, software vendors have begun offering products promising "graduated countermeasures" against such cyberthreats.\textsuperscript{18} Finally, there are counterattacks

DDoS attacks have been used to harass network users by interfering with their ability to connect to the Internet. One such instance occurred throughout the months of April and May, 2007, when web servers in the Baltic state of Estonia came under severe, sustained DDoS attacks. See Mark Landler & John Markoff, \textit{After Computer Siege in Estonia, War Fears Turn to Cyberspace}, N.Y. TIMES, May 29, 2007, at A1. It was widely believed that the Estonian attacks were launched by Russian-controlled botnets in retaliation for the Estonian government's decision to remove a Soviet-era war memorial from a prominent position in Tallinn, the Estonian capital. \textit{Id.; see also 9th of May}, Posting of Mikko to F-Secure Blog, http://www.f-secure.com/weblog/archives/00001188.html (May 9, 2007, 12:59 GMT) (purporting to show an image of a Russian hacker website offering DDoS-attack instructions fashioned particularly for attacking Estonian websites). At least one ethnic Russian Estonian national was subsequently convicted and fined for one of the attacks. Mike Sachoff, \textit{Man Convicted in Estonia Cyber Attack}, WEBPRO NEWS (Jan. 24, 2008 4:48 PM), http://www.webpronews.com/topnews/2008/01/24/man-convicted-in-estonia-cyber-attack.

More recently, some botnet operators have used DDoS attacks as a means of extortion by "using a botnet to DDoS a computer or a company until a ransom is paid to make the DoS stop." SCHILLER ET AL., supra note 8, at 60.

U.S. courts have found that sending spam in quantities that place unreasonable burdens on e-mail networks constitutes a type of DDoS attack. See CompuServe, Inc. v. Cyber Promotions, Inc., 962 F. Supp. 1015, 1022 (S.D. Ohio 1997); see also infra notes 51–74 and accompanying text (discussing the case brought against spammers under a trespass to chattels theory). The logic in \textit{CompuServe} has been applied in a number of subsequent e-mail spam cases. \textit{See, e.g., White Buffalo Ventures, LLC v. Univ. of Texas at Austin, 420 F.3d 366, 377 (5th Cir. 2005); Verizon Online Svcs., Inc. v. Ralsky, 203 F. Supp. 2d 601, 604 (E.D. Va. 2002); Am. Online, Inc. v. LCGM, Inc., 46 F. Supp. 2d 444, 451–52 (E.D. Va. 1998); Am. Online, Inc. v. IMS, 24 F. Supp. 2d 548, 550 (E.D. Va. 1998).}

\textsuperscript{16} See RFC 4987, supra note 14, at 6–11 (outlining the common defenses to DoS attacks).


that are designed to disrupt or destroy botnets by attacking their command and control protocols. However, such counterstrikes interfere with the functioning of a zombie computer, which may trigger unforeseen consequences if these measures cause the zombie computer to stop working.

II. THE TRADITIONAL LEGAL “LANDSCAPE” FOR CYBERATTACKS

The Internet, botnets, and DoS attacks are all relatively recent phenomena, but the legal doctrines that govern civil liability on the Internet are anything but recent. Generally, familiar common-law principles of liability continue to apply, albeit under changed circumstances.

A. Trespass to Chattels

The extension of common-law torts to cyberspace has resulted in the remarkable revitalization of the tort of trespass to chattels. Once thought moribund, this tort has returned as the primary cause of action after a DoS Attack.

1. At Common Law: Conversion’s Little Brother

At common law, the tort of trespass to chattels protects possessory interests in personal property. The Second Restatement of Torts sets forth the tort’s


19. See, e.g., Kraken Botnet Infiltration, supra note I (claiming an ability “to provide an ‘update’ through the existing Kraken protocol that can simply remove the Kraken zombie [software]”).

20. See id. (discussing counterstrikes and their possible effects). The researchers who reverse-engineered the Kraken botnet’s communication protocol expressed concern about the possible consequences of an active counterstrike using vital network-connected computers: “What happens if we accidentally crash the target system? What if that target system is responsible for someone’s life support?” Id.


22. See Omega World Travel, Inc. v. Mummagraphics, Inc., 469 F.3d 348, 358–59 (4th Cir. 2006) (noting that plaintiff’s claims rely in part on the common-law tort of conversion, which has not been recognized in Oklahoma); Intel Corp. v. Hamdi, 71 P.3d 296, 302–08 (Cal. 2003) (discussing the evolution of trespass to chattels—which requires proof of actual harm—and its application to actions based in computer use).

23. See Thrifty-Tel, Inc. v. Bezenek, 54 Cal. Rptr. 2d 468, 473 (Ct. App. 1996) (noting that trespass to chattels had not been used often in California but can be applied to conduct involving computer technology).

24. See id. (noting that the primary function at common law was to protect an owner from being dispossessed of his property); W. PAGE KEETON ET AL., PROSSER AND KEETON ON THE LAW OF TORTS § 14 (5th ed. 1984). “[i]t is a trespass to damage goods or destroy them, to make an unpermitted use of them, or to move them from one place to another.” Id.
three elements: intent,\textsuperscript{25} interference with the chattel,\textsuperscript{26} and actual harm.\textsuperscript{27} In an oft-quoted\textsuperscript{28} passage, Dean William Lloyd Prosser, editor of \textit{Prosser on Torts}, dismissed the tort's relative importance, noting that "[t]respass to chattels survives today . . . largely as a little brother of conversion."\textsuperscript{29}

2. Resurrection as a Cause of Action for Network Torts

Following the publication of the fifth edition of Prosser's treatise,\textsuperscript{30} the tort of trespass to chattels began to crawl out from under the shadow of its bigger brother, conversion, and come into its own as a cause of action in cases involving interferences with computers and computer networks.

In \textit{Thrifty-Tel, Inc. v. Bezenek}, the California Court of Appeals applied trespass to chattels to an early computer-hacking case.\textsuperscript{31} The plaintiff, Thrifty-

\begin{itemize}
\item \textsuperscript{25} \textit{Restatement (Second) of Torts} § 217 (1965); see also \textit{Keeton et al., supra} note 24, at § 14 (noting that trespass to chattels is "exclusively a wrong of intentional interference").
\item \textsuperscript{26} \textit{Restatement (Second) of Torts} § 217(b) (noting that "using or intermeddling with a chattel in the possession of another" constitutes trespass to chattel).
\item \textsuperscript{27} \textit{Restatement (Second) of Torts} § 218. Section 218 reads:
- One who commits a trespass to a chattel is subject to liability to the possessor of the chattel if, but only if,
  - (a) he dispossesses the other of the chattel, or
  - (b) the chattel is impaired as to its condition, quality, or value, or
  - (c) the possessor is deprived of the use of the chattel for a substantial time, or
  - (d) bodily harm is caused to the possessor, or harm is caused to some person or thing in which the possessor has a legally protected interest.
\item \textsuperscript{28} \textit{Id.; see also Keeton et al., supra} note 24, at § 14 (noting the "necessity of some actual damage to the chattel before the action can be maintained").
\item \textsuperscript{29} \textit{See, e.g., CompuServe, Inc. v. Cyber Promotions, Inc.,} 962 F. Supp. 1015, 1020 (S.D. Ohio 1997); \textit{Intel Corp. v. Hamidi,} 71 P.3d 296, 302 (Cal. 2003); \textit{Thrifty-Tel,} 54 Cal. Rptr. 2d at 473.
\item \textsuperscript{30} \textit{Keeton et al., supra} note 24, at § 14. Prosser notes that with the emergence of conversion as a cause of action for total dispossession of a chattel, trespass to chattels faded as a cause of action. \textit{Id.} Trespass to chattels's "chief importance now is that there may be recovery where trespass would lie at common law, for interferences with the possession of chattels which are not sufficiently important to be classed as conversion, and so to compel the defendant to pay the full value of the thing interfered." \textit{Id.}
\end{itemize}
Tel, was a long-distance telephone carrier. The defendants’ two teenage sons managed to obtain a code that enabled them to use Thrifty-Tel’s long-distance services without paying for them. The boys subsequently began to use their computer and modem to dial Thrifty-Tel’s network repeatedly, randomly trying combinations of numbers in an effort to find other authorization codes. The automated dialing overwhelmed Thrifty-Tel’s telephone lines.

Thrifty-Tel brought an action for conversion, not only of the six-digit authorization codes that the teenagers had used to make long-distance telephone calls, but also for the “tie-up” of its telephone system. The court declined to decide whether the use of the six-digit authorization codes constituted conversion. The court held that “the evidence supports the verdict on a trespass theory.” Noting that trespass to chattels includes the unauthorized use of personal property, the court held that repeated,
computer-scripted calls were an "intermeddling" with Thrifty-Tel's telephone network. The defendants' repeated dialing was "sufficiently tangible" to support a finding of trespass to chattels.

a. The Spam Cases: Protecting an Interest in the Functioning of Computer Networks

Thrifty-Tel involved the traditional telephone network, but its logic can be applied to DoS attacks on the Internet. The first set of Internet trespass-to-chattels cases was brought against spammers, whose unsolicited e-mails began to flood Internet users' mailboxes in the 1990s, taxing the resources of Internet Service Providers (ISPs). The Internet-spam cases are one step removed from the repeated direct dialing in Thrifty-Tel. Nevertheless, in determining whether such actions constitute an actionable trespass to chattels, courts have looked to the effect on the functionality of the plaintiff's computer equipment.

i. CompuServe: Spam as Trespass to Chattels

CompuServe, Inc. v. Cyber Promotions, Inc. was an early Internet-spam case, and has been the foundation for a number of subsequent cases involving...
claims against spammers under a trespass-to-chattels theory. In *CompuServe*, the defendant, Cyber Promotions, Inc., sent a “substantial volume” of spam to CompuServe’s subscribers, and CompuServe sought an injunction to prevent Cyber Promotions from sending any more e-mails to its subscribers.

Relying on the definition and commentary laid out in the *Second Restatement of Torts*, the court first addressed the element of “intermeddling.” Based on the logic in *Thrifty-Tel*, the court held that e-mail messages were enough of an intermeddling to support a trespass-to-chattels claim. The court went on to hold that the “possession” element was clearly met. Finally, the court found that there was sufficient intent, noting that although e-mails can reach a destination by varying paths, the defendants “affirmatively directed” their e-mails to CompuServe’s computers.

The defendants argued that a cause of action in trespass to chattels should not lie “[u]nless an alleged trespasser actually takes physical custody of the property or physically damages it.” Again relying on *Thrifty-Tel*, the court held that physical dispossession was not necessary to maintain a trespass-to-chattels claim. The court found that physical harm to the chattel was unnecessary, reasoning that damage to the “quality, condition, or value” of a chattel would be enough to sustain an action. In finding for CompuServe, the court focused on the way that Cyber Promotions’s spam denied CompuServe’s subscribers access to its computers. The court acknowledged the “tremendous burden” that processing spam had placed on CompuServe’s
equipment, and held that the value of CompuServe’s computer equipment had been impaired, as it was made unavailable to CompuServe’s subscribers.

ii. Hamidi: Limiting Consequential Damages

By adapting the reasoning in Thrifty-Tel to e-mail, CompuServe allowed civil recovery for victims of spam. The extent to which a plaintiff might recover from a spammer was, however, still unclear. Was recovery limited only to acts that placed such a “tremendous burden” on computer systems as to damage their “quality, condition or value”? Or, could a plaintiff also recover for the consequential damage done to such intangible interests as “business reputation and goodwill” by a spammer’s use of a plaintiff’s computer systems?

In Intel Corp. v. Hamidi, the California Supreme Court concluded that trespass to chattels “does not encompass, and should not be extended to encompass, an electronic communication that neither damages the recipient computer system nor impairs its functioning.” In Hamidi, the defendant, a former Intel employee, sent six mass e-mails to some 35,000 of Intel’s current employees. These e-mails were extremely critical of Intel’s personnel practices, and urged Intel employees to consider moving to other companies. However, there was no evidence that these e-mails either damaged any Intel computers or slowed their functioning. Because Intel could not point to any damage to its computers or networks, the court held that Intel was not entitled to summary judgment.

59. Id. (noting that excessive amounts of spam “demand[ed] disk space and drain[ed] the processing power of [CompuServe’s] computer equipment”).
60. Id. In addition to the “tremendous burden” that Cyber Promotions’ spam had placed on CompuServe’s computer equipment, the CompuServe court noted a number of other consequential harms—the cost of dealing with an increasing number of subscriber complaints about spam and the termination of subscriber “accounts specifically because of the unwanted receipt of bulk e-mail messages.” Id. at 1022–23. In finding for CompuServe, the court held that these losses, “insofar as they harm [CompuServe’s] business reputation and goodwill with its customers,” would themselves be actionable trespasses. Id. at 1023. But see Intel Corp. v. Hamidi, 71 P.3d 296, 311 (Cal. 2003).
62. Id. at 1022 (citing RESTATEMENT (SECOND) OF TORTS § 218(b)).
63. Id. at 1023.
64. Hamidi, 71 P.3d at 300.
65. Id. at 301.
66. Id.
67. Id.
68. Id. at 311.
iii. Beyond Spam: eBay and Unreasonable Server Load

Although CompuServe’s tort action was based on the burden that spam placed on the ISP’s servers, its reasoning was not limited only to cases involving spammers. In eBay, Inc. v. Bidder’s Edge, Inc., the same DoS logic of CompuServe was extended to cover repeated scripted access to a website. In eBay, the well-known online auction site sought a preliminary injunction to prevent Bidder’s Edge (BE), an aggregator of auction information, from using automated “robots” that repeatedly downloaded auction information from eBay’s servers up to 100,000 times a day. The robots’ continuous downloads placed a considerable load on eBay’s servers. Although eBay initially permitted BE to use its robots to search for a limited number of items, BE began to increase the frequency of its robots’ downloads.

Despite several communications from eBay requesting that they cease posting eBay auction listings, BE continued to do so, programming its robots to search eBay’s database continuously. Even when eBay attempted to block BE’s robots from accessing its site, BE attempted to evade these measures.

The court, ruling on eBay’s motion for preliminary injunctive relief, found that although eBay allowed the public to access its servers, BE’s robots “exceeded the scope of any such consent” and therefore BE’s actions constituted an actionable trespass. The court then turned to the question of damages, and found that BE’s repeated robotic searches consumed server

---

71. Id. at 1060–63.
72. Id. BE’s information requests accounted for somewhere between 1.11% and 1.53% of eBay’s total daily requests for information and between 0.70% and 1.10% of all the data transferred by eBay’s servers. Id. These figures seem low until one realizes that they account for traffic generated by a single entity at a time when eBay claimed to have some seven million registered users. Id. at 1060. Put another way, if we assume that each of eBay’s seven million users accounted for an equal share of eBay’s total traffic, a single entity like BE might account for .0000143% of total traffic. Instead, BE was consuming nearly seven thousand times its notional proportional share of eBay’s traffic.
73. Id. at 1062. eBay initially permitted BE’s robots to gather information only on auctions for Beanie Babies and Furbies. Id.
74. Id.
75. Id. at 1062–63.
76. Id. eBay attempted to filter access by IP address; information requests originating from addresses believed to be BE’s were ignored. Id. BE attempted to evade detection by redirecting its robot traffic through a rotating series of remote proxy servers. Id. BE’s use of proxies made it difficult to trace the robot activity to its originating IP address. Id. at 1061.
77. Id. at 1070 (finding that the use of automatic web-crawling robots on a publicly accessible site, where automated access is prohibited, exceeds the scope of consent and may be an actionable trespass to chattels).
resources—“necessarily compromising eBay’s ability to use that capacity for its own purposes.” 78

B. Negligence

Just as courts have extended an ancient cause of action—trespass to chattels—to new circumstances, the common law of negligence can be extended to govern the liability of individual zombies for botnet attacks. Unlike the intentional misconduct of eBay and CompuServe, 79 the owners of zombie computers are not committing intentional torts. They are, however, negligent in carelessly permitting their computers to cause harm to other computers. 80 Nonetheless, the common law does allow for recovery based on an actor’s negligence coupled with a third party’s malfeasance—which results in liability for both actors. 81

1. Palsgraf: Two Views of the Unexpected Plaintiff

The case of Palsgraf v. Long Island Railroad Co. serves as an excellent example of the two basic analytical frameworks used by courts in dealing with the problem of the unanticipated plaintiff. 82 The plaintiff, Mrs. Palsgraf, was standing on a train platform as a train pulled into the station and two men

---

78. Id. at 1071 (quoting CompuServe, Inc. v. Cyber Promotions, Inc., 962 F. Supp. 1015, 1022 (S.D. Ohio 1997)). The court held that the unreasonable consumption of server resources was an actionable trespass, even without a showing of actual damage to the server hardware itself. Id.

79. Id. at 1070–71; CompuServe, 962 F. Supp. at 1021.

80. If the owner of a zombie computer is not aware that his computer is being used to carry out a trespass to chattels, he cannot be said to have the intent to commit the trespass. Thus, in order to find the zombie liable, it is necessary to look to whether the zombie’s actions could be in any way negligent. See Stephen E. Henderson & Matthew Yarborough, Suing the Insecure? A Duty of Care in Cyberspace, 32 N.M. L. REV. 11, 14 (2002) (posing that zombies may be negligent because they are “knowingly insecure in the face of a well-known threat”).

81. KEETON ET AL., supra note 24, at § 14 (explaining that, at common law, trespass to chattels may lie both for “direct and forcible” interferences as well as “on the case,” but dismissed the distinction as “artificial”). Actions “on the case” (sometimes merely “case”) at common law were distinct from trespass; trespass required that the plaintiff plead a direct interference “vi et armis” (“by or with force and arms”), while actions on the case did not. See BLACK’S LAW DICTIONARY 1703–04 (9th ed. 2009); OLIVER WENDELL HOLMES, JR., THE COMMON LAW 77–106 (1881); Charles O. Gregory, Trespass to Negligence to Absolute Liability, 37 VA. L. REV. 359, 361–70 (1951) (describing the history of writs of trespass, case, and negligence). Because the harm to botnet victims is not a result of a direct act of the zombie, a revival of “case” as a form of action might allow courts to impose liability on botnet zombies. The resurrection of trespass to chattels in the cybertort context discussed above shows us that mere antiquity has not prevented these ancient writs from being reincarnated in surprising new contexts. See supra Part II.A.2. However, as argued more fully below, modern negligence doctrine provides us with a better, more readily adaptable tool to deal with unreasonable uses of computer networks. See infra Part IV.A.

rushed forward to board it. As a railroad employee on the moving train helped one of the men climb aboard, he dislodged an unmarked package that contained fireworks. After the package fell onto the tracks, it exploded and the resulting concussion knocked a set of luggage scales onto Mrs. Palsgraf, injuring her.

Writing for the majority, Justice Benjamin Cardozo did not find the railroad company liable to Mrs. Palsgraf. He noted that “[n]egligence is not actionable unless it involves the invasion of a legally protected interest, the violation of a right,” and stressed that rights are created by legal duties to particular persons. In characterizing Mrs. Palsgraf’s suit as an attempt to act as the “vicarious beneficiary of a breach of duty to another,” Justice Cardozo implied that although the railroad might have owed a duty of care to the two men clambering onto the train, they owed no such duty to Mrs. Palsgraf.

According to Justice Cardozo, negligence “is . . . a term of relation,” and a finding of liability in negligence must necessarily arise from a breach of a duty owed to the particular plaintiff himself because “[p]roof of negligence in the air, so to speak, will not do.”

In his dissent, Justice William Shankland Andrews, rejected the majority’s duty-based conception of negligence, and instead advanced a more pervasive conception of negligence:

83. Palsgraf, 162 N.E. at 99.
84. Id.
85. Id. Subsequent investigations seem to indicate that the cause of the falling scales was the fleeing crowd, rather than any explosive concussion.
86. Palsgraf, 162 N.E. at 99.
87. Id.
88. Id. at 99–100.
89. Id. at 100. In characterizing Mrs. Palsgraf’s suit as an attempt to act as the “vicarious beneficiary of a breach of duty to another,” Justice Cardozo employed the language of contractual privity and standing to bolster his conception of proximate cause as a duty owed to a particular plaintiff.
90. Id. at 99.
91. Id. at 101.
92. Id. at 99 (internal citation omitted) (holding that a “victim does not sue derivatively, or by right of subrogation,” but rather for “breach of a duty owing to [the victim] himself”).
93. Id. at 102 (Andrews, J., dissenting) (rejecting the proposition that negligence involves a breach of a duty of care to a particular plaintiff as “too narrow a conception”).
Every one owes to the world at large the duty of refraining from those acts that may unreasonably threaten the safety of others. Such an act occurs. Not only is he wronged to whom harm might reasonably be expected to result, but also he who is in fact injured, even if he be outside what would generally be thought the danger zone.  

Instead of looking to a right/duty relationship that would give rise to a remedy, Justice Andrews focused on the action of the individual actor—whether an actor’s action “[u]nreasonably jeopardized the safety of any one who might be affected by it.” The difference between Justice Cardozo’s majority opinion—conceiving proximate cause as an inquiry about correlative rights and duties—and Justice Andrews’s dissent—focusing instead on the reasonableness of holding the actor liable—still remains; it particularly persists in cases involving the negligence liability of defendants for the intentional acts of third parties.

2. “Parked Car” Cases

One such example involves parked, unlocked cars. In each case, the defendant parks his car on the street, leaving the doors unlocked and the keys in the ignition. Along comes a thief, who steals the car; and as the thief is driving the car, he injures the plaintiff. In each case, the plaintiff brought an action for negligence against the owner of the stolen car.

---

94. Id. at 103.
95. Id. at 104.
96. Compare Hampton by Hampton v. Federal Exp. Corp., 917 F.2d 1119, 1120, 1124–25 (8th Cir. 1990) (recognizing under the Palsgraf majority, that because defendant had no knowledge of the plaintiff and could not reasonably foresee any injury, he could not be held liable), and Petition of Kinsman Transit Co., 338 F.2d 708, 711, 721–22 & n.5 (2d Cir. 1964) (following the majority in Palsgraf and finding that the ship owner and the wharfinger had a duty of care to “all within the reach of the ship’s known destructive power”), with Alvarado v. Sersch, 662 N.W.2d 350, 352–53 (Wis. 2003) (noting that the minority view in Palsgraf has long been followed in Wisconsin), and Gritzner v. Michael R., 661 N.W.2d 906, 910, 912 (Wis. 2000) (adhering to the minority view in Palsgraf and finding no duty of care).
97. See generally KEETON ET AL., supra note 24, at § 44 (providing background for this fact scenario).
99. See, e.g., Hartman, 139 F.2d at 14; Richards, 271 P.2d at 24; Mellish, 183 A.2d at 753; Nutt, 203 N.E.2d at 120; Liney, 218 A.2d at 337; McClenahan, 806 S.W.2d at 769.
100. See, e.g., Hartman, 139 F.2d at 14; Richards, 271 P.2d at 25; Mellish, 183 A.2d at 753; Nutt, 203 N.E.2d at 120; Liney, 218 A.2d at 337; McClenahan, 806 S.W.2d at 769.
a. Majority View: No Duty Owed to the Unexpected Plaintiff

On the facts above, a majority of jurisdictions would find no liability for the car owner. Some courts have relied on the inability of the defendant to foresee the (in)competence of a thief to control a car, while other courts have relied on the absence of a duty to control third persons. The question in these cases, however, is whether the defendant owed a duty to the plaintiff to prevent the theft of his car. Under either theory, the act of a third-party thief could serve to cut the chain of liability to the defendant—because the thief’s actions were unforeseeable, because there was no duty to control the actions of the thief, or because the thief’s actions were an “intervening efficient cause” that disrupted an “unbroken sequence” between the defendant’s negligence and the plaintiff’s harm.

b. Minority View: Liability for a Defendant-Created Hazard

A substantial and “growing” minority of jurisdictions would find the defendant liable for the hazard he created in permitting his car to be stolen. In Mellish v. Cooney, the defendant had parked his car on the street, after dark, with the keys in the ignition. The Connecticut trial court found the defendant liable because he “should have foreseen the distinct possibility that a thief might steal the car and cause damage to innocent persons.” The court reasoned that the owner of a dangerous object “capable . . . of doing injury” should be liable for the injuries suffered by third persons if the owner negligently leaves the dangerous object “unguarded and exposed.” Likewise, in Ross v. Hartman, the United States Court of Appeals for the District of Columbia Circuit held that, depending on the circumstances, leaving a car unlocked might be enough to support a finding of negligence in the event of harm to a third person. Additionally, in Maloney v. Kaplan, the New York Court of Appeals held that if the defendant is negligent in leaving his car unsecured, and as a result an injury is suffered that would not have occurred

101. See Richards, 271 P.2d at 29; Nutt, 203 N.E.2d at 121; Liney, 218 A.2d at 337.
102. See Richards, 271 P.2d at 25 (finding that “[e]ven if [the defendant] should have foreseen the theft, she had no reason to believe that the thief would be an incompetent driver”); Nutt, 203 N.E.2d at 121 (holding it to be “beyond the realm of reason to attach liability to an owner for acts of a nonpermissive user, a thief”); Liney, 218 A.2d at 337 (reasoning that defendant could not be “on notice that the thief would be an incompetent or careless driver”).
103. Richards, 217 P.2d at 27 (noting that, absent some special relationship, “there is no duty to control the conduct of at third person so as to prevent him from causing harm to another”).
104. See Richards, 271 P.2d at 27–29; Liney, 218 A.2d at 337.
105. See McClenahan, 806 S.W.2d at 774.
107. Id. at 754.
108. Id. at 753.
but for the fact that the car was unsecured, then the defendant is liable.\textsuperscript{110} Thus, the question for the trier of fact is whether the alleged negligence of the defendant created the hazard that made it possible for a third party to harm the plaintiff.

C. Privileges to Interfere with Chattels

If the common-law doctrines of trespass and negligence can determine liability in cyberspace, common-law privileges can likewise be extended to shield actors from liability for those cybertorts. Victims of botnet DDoS attacks can attempt to strike back against individual zombies in an effort to disrupt the botnet, limiting the damage caused by that attack. However, any counterstrike by the DDoS victim would necessarily entail actions that could otherwise be found tortious.\textsuperscript{111} In order to avoid liability for a counterstrike against a zombie, a DDoS victim would have to operate within a recognized privilege.

1. Defense of Chattels

The Second Restatement of Torts recognizes a privilege to interfere with the chattels of another in order to defend one's own chattels.\textsuperscript{112} The privilege essentially has two elements: (1) that the actor reasonably believes the action necessary to protect his interest in the possession of his chattel; and (2) that the harm he inflicts protecting his property be "not unreasonable" in light of the harm threatened.\textsuperscript{113}

The court in CompuServe noted that "sufficient legal protection of the possessor's interest in the mere inviolability of his chattel is afforded by his privilege to use reasonable force to protect his possession against even harmless interference."\textsuperscript{114}

\begin{enumerate}
\item \textsuperscript{110} Maloney v. Kaplan, 135 N.E. 838, 839 (N.Y. 1922); cf. Stagl v. Delta Airlines, Inc., 52 F.3d 463, 473–74 (1st Cir. 1995) (applying New York law and holding that "when the intervening act is a natural and foreseeable consequence of a circumstance created by the defendant, liability will subsist") (quoting Kush v. City of Buffalo, 449 N.E.2d 725, 729 (N.Y. 1983)).
\item \textsuperscript{111} See CompuServe, Inc. v. Cyber Promotions, Inc., 962 F. Supp. 1015, 1017 (S.D. Ohio 1997). A counterstrike may be tortious as a trespass to chattels as understood by the cybertrespass cases, or as cybernuisance, or even under the negligence theory advocated in this Comment.
\item \textsuperscript{112} RESTATEMENT (SECOND) OF TORTS § 260(1) (1965). The Restatement reads: one is privileged to commit an act which would otherwise be a trespass to a chattel or a conversion if the act is, or is reasonably believed to be, necessary to protect the actor's land or chattels or his possession of them, and the harm inflicted is not unreasonable as compared with the harm threatened.
\item \textsuperscript{113} Id.
\item \textsuperscript{114} CompuServe, 962 F. Supp. at 1023 (quoting RESTATEMENT (SECOND) OF TORTS, § 218 cmt. e (1965)).
\end{enumerate}
a. Bad Dogs and Reasonable Men

Whether an action is "not unreasonable" in light of the harm threatened is, necessarily, a question of fact. However, a line of cases involving trespassing dogs can at least trace the broad outlines of the privilege. In Hull v. Scruggs, the Mississippi Supreme Court held that the defendant was acting reasonably when he shot a trespassing dog. The dog had habitually entered the defendant's farm, disturbed his turkeys, and was in the habit of sucking on their eggs. The court held that the defendant, having attempted to pursue other means, was reasonable in shooting and killing the dog, in light of the continuing nature of the violation of the defendant's property interests.

Similarly, in McChesney v. Wilson, a trespassing dog was shot after he "almost daily . . . kill[ed] and destroy[ed] the defendant's domestic fowl[s]." In this case as well, the killing of the dog was found to be reasonable, in light of the frequent and ongoing violations of the defendant's property interests.

2. Abatement of Nuisance

The Second Restatement of Torts also recognizes a privilege "to commit an act which would otherwise be a trespass to the chattel of another" in order to abate a nuisance. Here again, the privilege is limited to "reasonable means of abating the nuisance." An early example of an actor asserting such a privilege may be found in the old English case of Slater v. Swann. In Slater, the plaintiff had left his cart and horse in front of the defendant's door, preventing the defendant from


117. Id. at 543. Evidently, egg-sucking dogs were common enough in Mississippi that the court felt obliged to take judicial notice of them, declaring: "It is a fact of common knowledge that when a dog has once acquired the habit of egg-sucking there is no available way by which he may be broken of it, and that there is no calculable limit to his appetite in the indulgence of the habitual propensity." Id.

118. Id. at 544.

119. Id. In finding for the defendant, the court focused on the dog's "habitual depredation" of the defendant's turkeys. Id. The offending dog "sucked all the eggs which were laid by the turkeys and guineas . . . and . . . his presence there was of sufficient frequency or continuity . . . that none of the eggs were left until after the dog was killed." Id. at 543. Note that the dog had effectively denied the defendant of the benefit of the eggs laid by defendant's fowl; it is also worth noting that the court stressed the interference with the chattels over the trespass to the defendant's farm. Id. at 543-44.

120. McChesney, 93 N.W. at 627-28.

121. Id. (focusing on the dog's attack on the farmer's poultry—his personal property—and not on the dog's mere entry upon the farmer's real property).

122. RESTATEMENT (SECOND) OF TORTS §264 (1965).

123. Id.

receiving any deliveries.125 The defendant “therefore . . . whipt the horse to remove the cart,” but did “so violently beat the horse, that the plaintiff was deprived of the use of his cart and horse for several days.”126 The trial court left to the jury the question of whether the defendant beat the horse “immoderately.”127 Thus, the court found that although the defendant was privileged to remove the cart from his door, the scope of that privilege was a question of fact for the jury.128

Likewise, in Hubbard v. Preston, another “naughty dog” case, the Michigan Supreme Court held that a landowner was not liable for shooting the plaintiff’s dog, which often gathered with several other dogs near the defendant’s house at night, “seriously annoy[ing]” his family.129 The court held that because the defendant “had a right to protect his family from such [a] nuisance,” it was proper for a jury to decide whether his actions were reasonable.130

In Maryland Telephone & Telegraph Co. v. Ruth, the defendant was found not liable to the plaintiff for cutting down a utility pole that the plaintiff had erected.131 The pole obstructed the defendant’s alley and had been erected without his permission.132 To regain use of the alley, the defendant removed the pole.133 The court held that the pole’s interference with the defendant’s use of the alley constituted a nuisance and that the defendant was authorized to abate that nuisance.134 Because the defendant committed “no breach of the peace,” and because he did not harm any third persons or their property, the defendant was found to have acted reasonably.135

125. Id.
126. Id. at 906–07.
127. Id. at 907 (distinguishing the defendant’s actions from an unjustified trespass vi et armis and requiring a finding of damages to support a cause of action).
128. Id. Here, the scope of the privilege is defined by the violence of the horse-whipping.
129. Hubbard v. Preston, 51 N.W. 209, 210 (Mich. 1892). The trespassing dog was one of a “large number of dogs about [the defendant’s] premises, barking, quarreling, and fighting there.” Id.
130. Id.
132. Id. at 359–60.
133. Id. The defendant was extraordinarily careful in removing the pole, by both having the wires cut by an expert “so that they would not hurt any one,” and removing the pole “by [using] competent men in a careful manner.” Id.
134. Id. at 360.
135. Id.
III. TRESPASS’S OUTER LIMITS

A. Trespass to Chattels and Botnet DDoS Attacks

Once dismissed as merely the “little brother of conversion,” trespass to chattels is no longer the ninety-pound weakling of property torts. Rather, it has emerged as the preferred common-law cause of action against disruptive network behavior.

Each extension of the tort into cyberspace has involved its application to new types of DoS attacks. Courts have been remarkably consistent in interpreting the “intermeddling” requirement of trespass to chattels to mean “denial of service.” It may not be too far of a stretch to assert that, in Internet cases, for an action for trespass to chattels to lie, there must be at least some showing of denial of service.

It may be impossible to factually distinguish eBay from a typical zombie botnet DDoS scenario. In both cases, a central coordinating actor makes use of a series of remote, Internet-connected hosts to flood a target server with unwanted traffic. Given the similarity between the two cases, it is almost certain that a trespass-to-chattels claim will lie against a botnet master conducting such an attack.

However, unlike eBay, in which Bidder’s Edge (BE) received at least temporary permission from eBay to operate its web-crawling robots on eBay’s network, most malicious botnet masters prefer to stay hidden. When eBay began complaining of BE’s constant downloads, BE began shifting its search-robot operations to a system of rotating proxy servers to make it more difficult to trace the activity to the originating host. However, because eBay

136. KEETON ET AL., supra note 24, at § 14.
137. See supra Part II.A.
138. See supra Part II.A.2.a.i–iii.
140. See supra note 58–60 and accompanying text.
141. See eBay, 100 F. Supp. 2d at 1062–63; supra notes 13–15 & 72 and accompanying text.
142. Cf. eBay, 100 F. Supp. 2d at 1069–72.
143. Id. at 1062.
144. See, e.g., BRUCE SCHNEIER, THE STORM WORM, reprinted in SCHNEIER ON SECURITY 256–59 (2008). The decentralized structure of peer-to-peer botnets, such as Storm, makes it extremely difficult to identify the botnet master. In such a botnet, certain zombies also act as redundant command-and-control relays; therefore, the inability to identify any single command-and-control node means that, to disrupt such a botnet, a counter-striker would necessarily have to act against individual zombie computers. See id.
145. eBay, 100 F. Supp. 2d at 1061–63.
remained in contact with BE, eBay could at least identify BE’s robots as the probing force without necessarily having to resort to complicated traceback methods.\textsuperscript{146}

In the case of a zombie botnet, however, the only contact an affected network may have with the botnet is the flood of traffic originating from the botnet zombies.\textsuperscript{147} Under those circumstances, it would be extremely difficult to track the botnet’s master and make him a party to an action for trespass to chattels.\textsuperscript{148}

\textbf{B. Criticisms of the Trespass-to-Chattels Theory for Denial of Service: Is Cybernuisance the Answer?}

Several commentators have suggested that common-law nuisance, rather than trespass to chattels, provides a better analytical framework for spam and DoS attacks.\textsuperscript{149}

Professor Dan Burk, the principal proponent of cybernuisance, attacks the “incongruity between common law trespass to chattels and the problem of spam” by focusing on the courts’ willingness to read strict-liability real-property trespass rules into trespass-to-chattels claims for spam.\textsuperscript{150} He notes that the “particulate trespass” cases used to support the holding in \textit{Thrifty-Tel} involved trespass to \textit{land}, rather than trespass to \textit{chattels}.\textsuperscript{151} This elision of real-property and personal-property trespass doctrines, he argues, “collap[es] the separate doctrines of trespass to land and trespass to chattels back into their single common law progenitor,” creating a hybrid cause of action “unknown to modern jurisprudence.”\textsuperscript{152}

Focusing on the dispossession element of trespass to chattels, he notes that the owners of the computer equipment in \textit{Thrifty-Tel} and \textit{CompuServe} were not

\begin{itemize}
\item \textsuperscript{146} \textit{Id.}
\item \textsuperscript{147} \textit{See supra} notes 14–19 and accompanying text.
\item \textsuperscript{148} \textit{See supra} notes 13–19 and accompanying text. The problems here are as much jurisdictional as technical; however, questions of Internet jurisdiction are outside the scope of this Comment.
\item \textsuperscript{150} Burk, \textit{supra} note 149, at 33.
\item \textsuperscript{151} \textit{See Thrifty-Tel, Inc. v. Bezenek}, 54 Cal. Rptr. 2d 468, 473 n.6 (Ct. App. 1996) (discussing particulate trespass cases and holding that “the electronic signals generated by [defendant’s] activities were sufficiently tangible to support a trespass cause of action”); Burk, \textit{supra} note 149, at 33–34 (discussing “‘particulate trespass’ cases relied upon in \textit{Thrifty-Tel}”).
\item \textsuperscript{152} Burk, \textit{supra} note 149, at 33.
\end{itemize}
dispossessed of their equipment. Because courts finding for plaintiffs in cyber trespass-to-chattels cases have found that the plaintiffs' computers had been interfered with by the collision of offending electrons, Burk contends that courts following the rules in Thrifty-Tel and CompuServe have begun to protect a previously unrecognized interest in the inviolability of personal property. The imposition of such an exclusionary property rule, however, would allow network users to maintain their connections with a wider network while simultaneously entitling them to compel outside network users to negotiate for licenses to access their internal systems. The pervasive "propertization" of Internet connectivity, argues Burk, would "tend to exacerbate rather than solve any problem of external costs," imposing significant transaction costs on Internet users.

153. Id. at 34 (noting that trespass to chattels requires dispossession or other interference, and the computers in Thrifty-Tel and CompuServe handled the flow of electrons as designed).

154. Id. at 33–34. Burk's observation flows from the very massless and insubstantial nature of the electrons themselves, although he professes to "resist the temptation to delve into a philosophical discourse about the comparative tangibility of electrons." Id. at 33. The CompuServe court, however, denied that it was dispensing with the physical contact element finding that the plaintiff was entitled to a remedy because it had exhausted available self-help to protect the "inviolability" of its servers from spam. CompuServe, Inc. v. Cyber Promotions, Inc., 962 F. Supp. 1015, 1023 (S.D. Ohio 1997) (quoting RESTATEMENT (SECOND) OF TORTS § 218, cmt. e).

155. Burk, supra note 149, at 47–49. In other words, imposing the exclusionary property rule would allow network users to maximize their benefit from Internet connectivity while simultaneously minimizing the aggregate benefit of network connectivity to all users.

156. Id. at 51. But see Richard A. Epstein, Cybertrespass, 70 U. CHI. L. REV. 73, 84–85 (2003). Epstein rejects Burk's premise that the application of real property rules will necessarily result in unmanageable "anti-commons" situations, and dismisses Burk's argument as "wrong in all its analogies." Id. at 85. Instead, Epstein contends that "strong property rights for non-network elements function as well in cyberspace as they do anywhere else." Id. at 84. Rather than the balancing test of nuisance, Epstein contends that "[t]he missing pieces in the puzzle are the rules on consent," or, in other words, the ability to contract. Id. at 85. Taking the eBay case as one example, Epstein praises the "level of particularization and standardization" of the carefully drafted license between eBay and BE which, he argues, is "a great improvement over a rule that allows one person to take the property of another until the system crashes or slows down." Id. at 83–84. Unfortunately, Epstein neither outlines a mechanism by which these fine allocations of rights may be negotiated among users, nor does he consider the social and network costs involved in administering such a complex system. The Hamidi court feared such a system would result in "a substantial reduction in the freedom of electronic communication, as the owner of each computer through which an electronic message passes could impose its own limitations on message content or source." Intel Corp. v. Hamidi, 71 P.3d 296, 310 (Cal. 2003) (citing an amicus brief by Professor Mark Lemley, who had argued that under Epstein's rule "each of the hundreds of millions of [Internet] users must get permission in advance from anyone with whom they want to communicate and anyone who owns a server through which their message may travel").
C. Attaching Liability to Botnet Zombies: Negligence

1. Scope of Zombie Liability for Botnet DDoS Attacks

Given the technological and jurisdictional problems associated with both finding botnet masters and holding them liable for DDoS attacks, a DDoS-attack victim’s focus necessarily turns to the possible liability of the individual zombie hosts of a botnet. Determining whether a zombie is liable in negligence to the victim of a DDoS attack involves defining the scope of a zombie’s possible liability. In the conventional language of courts and commentators, the question is whether a zombie’s failure to secure his computer was the proximate cause of the injuries suffered by the DDoS victim.

2. Proximate Cause Problem

All botnet DDoS attacks involve at least three parties: the botnet master, who initiates the attack; the zombie computer, from whose equipment the attack actually emanates; and the ultimate target of the attack. A target seeking to find the zombie liable immediately encounters a problem: if the zombie-computer owner is unaware that his computer is infected, the attack was caused by the independent, intentional act of a third party—the botnet master. This presents a question of whether the DDoS attack by the botnet master was the reasonably foreseeable consequence of the zombie’s failure to prevent his own infection. In other words, is a zombie’s failure to secure his own computer the proximate cause of the damage suffered by the victim?

3. Majority Rule: Botnet Masters as Intervening Causes

In the majority of jurisdictions, the answer will be no. Following Justice Cardozo’s reasoning in Palsgraf, a DDoS victim’s negligence claim will only succeed if a zombie had a duty to prevent interference with a DDoS victim’s

---

157. See SCHILLER ET AL., supra note 8, at 3–4 (describing the players and process involved in a DDoS attack).

158. See Henderson & Yarborough, supra note 80, at 14.

159. See id. at 17–18.

160. Cf. Richards v. Stanley, 271 P.2d 23, 26–27 (Cal. 1954) (holding that the owner of an automobile has no duty to a person injured by the acts of a third party using that automobile unless the owner is put on notice of the third party’s incompetence); Liney v. Chestnut Motors, Inc., 218 A.2d 336, 337–38 (Pa. 1996) (stating that a defendant is not liable for a plaintiff’s injury if the cause of that injury is merely remotely connected to the defendant’s actions); see also Hamidi, 71 P.3d at 300–01, 304, 306, 308 (reviewing precedent concerning computer-related tort law, with emphasis on the intent of the actors and no mention of Internet providers being liable to the injured subscribers). But see Henderson & Yarborough, supra note 80, at 14 (dismissing the element of causation in negligence as “unlikely to be unusually contentious” when applied to botnet zombies). The very nature of negligence law in the United States, however, makes it likely that proximate cause, a sub-element of causation, will be at least reasonably contentious. See supra Part III.C.1–2.
computer system. Absent such a specific duty, the majority of jurisdictions would find that a victim had no correlative right to recovery. Other jurisdictions will look at the events, from the defendant’s alleged negligence to the harm caused to the plaintiff, and will hold that the act of a third party necessarily breaks that sequence.

The majority of jurisdictions would also absolve zombies of liability for the harm actually caused by botnet masters because zombies have no duty to control the actions of third persons, nor would they need to worry about the intentional actions of a third person that might gain control of their computer. In each case, the denial of liability is founded on a lack of a duty giving rise to a correlative right to a remedy.

4. Minority Rule: Zombies Liable for Zombie-Created Hazards

The minority position—the modern trend—is moving away from the rigidity of the majority’s right/duty rule for proximate cause, and looks instead to the risks that an actor creates at the time of his allegedly negligent conduct; thus, the ultimate question is not whether an intervening cause cut off the actor’s liability. Rather, there are two questions to be answered: first, did the actor’s negligence enable the third party to cause the harm for which the plaintiff is seeking recovery; and second, if the actor’s negligence did enable the third party to cause harm, was it reasonably foreseeable that the third party would cause that harm.

---


163. See Ross v. Nutt, 203 N.E.2d 118, 120 (S.D. Ohio 1964) (finding that the thief’s actions were an intervening cause cutting off defendant’s liability); see also RESTATEMENT (SECOND) OF TORTS § 440 cmt. b (“[I]f in looking back from the harm and tracing the sequence of events by which it was produced, it is found that a superseding cause has operated, there is no need of determining whether the actor’s antecedent conduct was or was not a substantial factor in bringing about the harm.”); id. § 442(d) (noting that “the fact that the operation of the intervening force is due to a third person’s act or his failure to act” is a factor in considering “whether an intervening force is a superseding cause of harm”).

164. See, e.g., Richards, 271 P.2d at 27 (noting that “in the absence of a special relationship between the parties, there is no duty to control the conduct of a third person so as to prevent him from causing harm to another”).

165. See, e.g., Richards, 271 P.2d at 26; Liney, 218 A.2d at 337–38.

166. See, e.g., Richards, 271 P.2d at 27; Liney, 218 A.2d at 338.

167. Compare Nutt, 203 N.E.2d at 120 (finding that the actions of a third party cut off the chain of causation even when the defendant may have also been liable), with Ross v. Hartman, 139 F.2d 14, 15–16 (D.C. Cir. 1943) (finding liability when actor creates the risk of harm), Mellish v. Cooney, 183 A.2d 753, 753–54 (Conn. Cir. Ct. 1962) (finding liability where the owner of an object capable of inflicting injury is careless, leaving a substantial risk of injury), and Maloney v. Kaplan, 135 N.E. 838, 839 (N.Y. 1922) (finding a duty in a driver to secure his vehicle to prevent anticipated third parties from using the vehicle to injure others).

168. See, e.g., Hartman, 139 F.2d at 15–16; Mellish, 183 A.2d at 754; Maloney, 135 N.E. at 839–40; see also Illinois Farmers Ins. Co. v. Tapemark Co., 273 N.W.2d 630, 634–35 (Minn.
Applying these concepts to zombie botnets, these questions become: first, did a zombie, in failing to secure his computer, enable the botnet master to use that same computer to launch a DDoS attack; and, if so, was it reasonably foreseeable to the zombie that a third party might take control of his computer and launch a DDoS attack? If the answer to both of these questions is yes, then the damage caused by the botnet master in a DDoS attack using the zombie computer is not outside the scope of the zombie’s liability.\(^1\)

For the answer to the second question—whether it was foreseeable to the zombie that his failure to take adequate precautions would enable a botnet master to take control of his computer—a victim seeking to establish the liability of a zombie would have to point to the state of network security generally; perhaps the most dramatic measure of the foreseeability of the breach of an otherwise unsecured computer is its “survival time.”\(^2\) Survival time is defined as the average time between a computer’s first connection to the Internet and its being compromised by a remote exploit.\(^3\) For users of the most dominant operating system in the market, Microsoft Windows, the survival-time statistics are grim: as of this writing, the survival time of an Internet-connected computer running the latest version of Microsoft’s operating system is quoted at “around 4 minutes.”\(^4\) Given this speed, an unprotected computer is likely to be compromised, and fairly quickly.

D. Striking Back against a Zombie DDoS Attack: Privileges

1. Actions against Bot Herders

Despite some misgivings among network administrators, it would appear that reasonable counterstrikes against botnet masters would be afforded a complete privilege. Indeed, the CompuServe court suggested that the use of “reasonable force” provided “sufficient legal protection” to a DDoS victim’s

\(^{169}\) The answer to the first question is easily ascertainable: any indication of repetitive, automated traffic, particularly traffic structured specifically to consume as many server resources as possible, would indicate a DDoS attack in progress. See SCHILLER ET AL., supra note 8, at 144–50.


\(^{171}\) See Hutcheson, supra note 170; see also SANS, supra note 170.

\(^{172}\) Hutcheson, supra note 170.
interest in the condition of his servers.\textsuperscript{173} Indeed, the same court explicitly recognized a “privilege to protect \ldots computer systems.”\textsuperscript{174}

2. Actions against Zombies

A privilege for self-help against individual zombie computers, however, is not as straightforward as self-help against botnet masters. However, it is a more defensible option if the victim can attach liability to the zombies.

Even if zombies are themselves not liable, a victim may conceivably invoke the privilege of private necessity, which privileges actions taken “to prevent serious harm to the actor, his land or chattels.”\textsuperscript{175} However, private necessity only affords a partial privilege, with the counterstriking party being possibly liable to the zombie for excessive harm to the zombie’s computer.\textsuperscript{176}

IV. UNLEASHING THE CURE: HOLDING ZOMBIES LIABLE FOR THE VULNERABILITY OF THEIR COMPUTERS

A. The Case for Negligence

Because of the conceptual difficulties of adapting trespass or nuisance to “intangible” property, the negligence doctrine might provide us with a more attractive framework for assigning liability. Unlike trespass to chattels or cybernuisance, negligence allows a botnet-attack victim to strike at zombies directly, while avoiding needlessly artificial pleading.\textsuperscript{177}

\textsuperscript{173} CompuServe, Inc. v. Cyber Promotions, Inc., 962 F. Supp. 1015, 1023 (S.D. Ohio 1997) (citing \textsc{Restatement (Second) of Torts} § 218, cmt. c).
\textsuperscript{174} Id. (recognizing plaintiff’s actions as “attempt[s] to exercise [legal] privilege to protect its [servers]”).
\textsuperscript{175} \textsc{Restatement (Second) of Torts} § 197 (1965); see also Smith, supra note 18, at 191–92.
\textsuperscript{176} Smith, supra note 18, at 191–93 (citing Vincent v. Lake Erie Transp. Co., 124 N.W.2d 221, 222 (Minn. 1910)). Because the general requirement is that self-help be “reasonable,” the partial privilege of private necessity may not be all that different from the theoretically “total” privileges of defense of property and nuisance abatement. \textsc{Compare \textsc{Restatement (Second) of Torts} § 218 (defense of property), with \textsc{Restatement (Second) of Torts} § 264 (privilege to interfere with chattels to abate private nuisance), and \textsc{Restatement (Second) of Torts} § 197 (private necessity). See also supra Part II.C (discussing privileges to tortious interferences with personal property). Even in defense of property or abatement of nuisance, liability may be incurred if an actor exceeds the scope of the privilege; once exceeded, the actor is liable to the extent of the excess. See Slater v. Swann, (1865) 93 Eng. Rep. 906, 907 (K.B.). Thus, should the parties in a given transaction litigate, the limited compensation due to one whose property interests are invaded under the doctrine of private necessity is functionally identical to the compensation owed to one who is harmed by another who exceeds a privilege to commit harm. Either doctrine allocates resources as among the two parties in exactly the same way.\textsuperscript{177} See infra note 184.
1. Negligence, Not Trespass

Both Thrifty-Tel and CompuServe found claims for trespass to chattels viable in DoS contexts. By permitting plaintiffs to claim trespass for the mere impact of massless electrons upon their servers, a heightened cybertrespass rule raises the specter of a digital "anti-commons," in which individual Internet users regulate access to their servers in ever more restrictive ways, driving up transaction costs for legitimate actors. Moreover, a cybertrespass regime would not allow botnet DDoS victims to bring actions against individual zombies unless the victim could show intent by the zombie to interfere with the functioning of the victim’s computer server.

2. Negligence, Not Nuisance

Cybernuisance is an attractive potential cause of action for network-based wrongs because situations involving spam and DDoS attacks typically involve an actor’s imposition of either a “tremendous burden” upon a victim’s servers or an unreasonable demand upon a victim’s services. These situations are more appropriately dealt with using a harms-benefits analysis. However, just as the court in Thrifty-Tel conflated trespasses to real property and personal property, cybernuisance proponents urge the imposition of real-property rules to personal property. But we need not go through such
mental contortions to arrive at a rule that governs the unreasonable use of personal property because a cause of action already governs the creation of unreasonable hazards—negligence.

Negligence can, without further extension, do double duty. It can free us of the artificial pleading required by trespass-to-chattels claims on the one hand, and allow us to impose liability upon botnet zombies on the other.

3. Forcing Zombies to Internalize the Costs of their (In)Action

Adopting negligence also has a number of important economic benefits. Cost-benefit analyses of computer security have tended to focus on costs and benefits to the actor taking the precaution, rather than any effects on the security or functioning of the network as a whole. Imposing a duty to prevent infections on zombie-computer owners, whether by applying the reasonable-foreseeability test or by establishing continuing control over the computer, would shift the costs from the innocent victims of botnet DDoS attacks to computer owners, whose unprotected computers actually caused the damage. Eventually, the distribution of these costs to zombies would create a powerful incentive for computer owners to avoid liability by increasing the security of their own computers and networks, which would increase the

---

185. See, e.g., Robert W. Hahn & Anne Layne-Farrar, The Law and Economics of Software Security, 30 HARV. J. L. & PUB. POL’Y 283, 310–11 (2006) ("[A] user will invest in preventative measures (spending X) when those investments reduce expected costs (losses plus administrative costs) by enough to offset the investment: pL + pC > X + qL + qC."). Under this model, for the additional cost of greater security to be economically rational, the potential damage to the user's own system, multiplied by the probability of that damage actually occurring must be greater than the cost of the additional precaution, itself multiplied by the lowered probability of loss. This is the same cost-benefit analysis employed by Judge Learned Hand in United States v. Carroll Towing Co., 159 F.2d 169, 173 (2d Cir. 1947). This standard model fails to account for the type of harm that results from a botnet attack, where the individual zombie suffers little harm, but is itself the means by which a third party can cause harm to a target computer system.

186. Costs include the damage suffered during denial of service, plus other damages not usually actionable under trespass to chattels: lost productivity, lost sales, and other opportunity costs. Even if consequential damages are limited by a Hamidi-like rule, the imposition of liability on individual botnet zombies would allow botnet victims to shift at least their direct DoS costs—bandwidth, disk space, and so on—onto the zombies. Intel Corp. v. Hamidi, 71 P.3d 296, 300 (Cal. 2003) (denying recovery for consequential damages claimed to have been incurred as a result of the defendant's cyber actions).

187. BRUCE SCHNEIER, LIABILITY AND SECURITY (2004), reprinted in SCHNEIER ON SECURITY, supra note 144, at 152–54. Schneier envisions a role for the insurance industry as a clearinghouse for risk: "[O]nce the CEO starts buying security products based on his insurance premiums, the insurance industry will wield enormous power in the marketplace. . . . And since the insurance companies pay for the actual liability, they have a great incentive to be rational about risk analysis and the effectiveness of security products." Id. at 153.
security of the Internet as a whole: "[e]nforce liability, and everything else will flow from it. It has to." 188

B. Two Ways to Fight Zombies

1. In Majority Jurisdictions: Creating a Continuing Duty of Care to Other Network Users

A majority of jurisdictions present the botnet victim with the problem of establishing proximate cause. Although the DDoS makes use of the zombie computer, the attack is not directed by the zombie himself. A botnet victim must somehow distinguish his case from the parked car cases and establish some kind of correlative right/duty relationship that would give rise to a remedy. 189

A closer examination of the facts common to all parked car cases, however, reveals a few critical distinctions between those cases and DDoS botnet attacks. In parked car cases, the owner of the car left his car unattended, which allowed a third-party thief to enter and dispossess the owner of his car. 190 In each case, the owner of the car did not have possession or control of the car at the time that the thief caused harm to the plaintiff. 191

The presence of the botnet software on a zombie, however, is a minor, but continuing, interference with the zombie's property right. In most cases, the zombie computer continues to function while the zombie computer owner continues to use it. In other words, although the computer may be in the thrall

188. Id. at 154. Although Schneier's main concern is for the absolute security of the individual network host, he describes the same negative externality problem that permits botnet zombies to flourish:

[M]ost organizations don't spend a lot of money on network security. Why? Because the costs are significant: time expense, reduced functionality, frustrated end users. On the other hand, the costs of ignoring security and getting hacked are small: the possibility of bad press and angry customers, maybe some network downtime, none of which is permanent . . . . The result: a smart organization does what everyone else does, and no more.

Id. at 152.

He notes, approvingly, a judicial order that required the U.S. Department of the Interior to take its website offline until the department could guarantee the safety of its data. Id. at 153. Schneier concludes that once liabilities are enforced, parties will avoid liability under a least-cost avoider theory—upgrading individual computer security. Id. at 154.

189. See supra Part II.B.2.a.


191. Hartman, 139 F.2d at 14; Richards, 271 P.2d at 25; Mellish, 183 A.2d at 753; Maloney, 135 N.E. at 839; Nutt, 203 N.E.2d at 120; Liney, 218 A.2d at 337; McClenahan, 806 S.W.2d at 769.
of a botnet master, it is never wholly out of the control of its owner. A
networked computer, in other words, is less like a parked car, and more like
a car on the highway. Because the zombie owner is still in control and
possession of his computer, the argument for liability is stronger.

2. In Minority Jurisdictions: Towards a Duty to Avoid Harm to Other
Network Users

Fortunately for botnet victims, under the minority rule, a botnet DDoS
victim need only concern himself with the zombie’s duty of care found in
Justice Andrews’s dissent in Palsgraf. Under the theory endorsed in this
Comment, to establish zombie liability for a botnet DDoS attack, one must
show that a zombie: (1) failed to take reasonable precautions against infection;
(2) as a result of the failure to take adequate precautions, the zombie was
infected; (3) as a result of the infection, the zombie actually caused the harm of
the DDoS; and (4) it was reasonably foreseeable to the zombie that failure to
secure his computer would result in the harm. Given the size and prevalence
of botnets, and the speed at which computers may be compromised, it does not
seem unreasonable to assert that zombies may be found liable according to this
theory.

192. A parked car is not under its owner’s control. See, e.g., Richards, 271 P.2d at 27
(noting, in a parked car case, that the defendant “has relinquished control of his property to the
third person”).

193. The owners of cars operated on public highways are generally presumed to be in control
of their vehicle. Even when not directly in control of their vehicle, owners have generally been
found to owe a duty of reasonable care as to the maintenance of their vehicles, lest they become
hazards to other road users. See, e.g., Prosser v. Glass, 481 So.2d 365, 368 (Ala. 1985) (“The
operator of a motor vehicle on public highways has a duty to see that the automobile is in
reasonably good condition so as not to present a source of danger to others.”); Levitt v.
Hammonds, 628 N.E.2d 280, 283 (Ill. App. Ct. 1993) (finding that maintaining a vehicle’s brakes
is the responsibility of the operator, and may also be the responsibility of the owner); Shelmire v.
Linton, 343 So.2d 301, 305 (La. Ct. App. 1977) (“Any failure on [defendant’s] part to use
ordinary care to prevent mechanical malfunction is likewise negligent conduct.”); Naumenko v.
excuse himself from liability for operating a vehicle with defective brakes if “he offered not a
shred of excuse for driving the car in such a vitally defective condition”); Prevette v. Bullis, 183
S.E.2d 810, 811 (N.C. Ct. App. 1971) (“It is the duty of a motorist operating a motor vehicle on a
public highway to exercise reasonable care to see that it is in reasonably good condition and
properly equipped, so that it may not become a source of danger to its occupants or to other
travelers.”). Thus, because a zombie computer remains at least in part under the control of its
owner, then its owner has a continuing duty not to allow his property to harm that of another.
On the highway, the duty is breached by a failure to properly maintain one’s car; on the Internet, the
duty would be breached by a failure to maintain adequate control over one’s own computer.

dissenting).
C. Effects of a Duty to Prevent Infection: Creating a Privilege to Disrupt Botnets

Establishing liability for individual zombie hosts would also allow botnet DDoS victims to strike back aggressively and disrupt available botnets without fear of liability.\textsuperscript{195} It should be stressed, however, that the privilege proposed is limited to reasonable counterstrikes only, and the reasonableness of any counterstrike would depend on the facts in that particular situation.\textsuperscript{196} By extending immunity from tort liability to reasonable counterstrikes, we would encourage more efforts to disrupt and destroy existing botnets. Armed with the technical ability to destroy a botnet, researchers should not have to cower in fear at the ability of a zombie to impose tort liability for an action that, in the final analysis, increases the security and safety of the network as a whole.\textsuperscript{197}

V. CONCLUSION

A viable theory of liability, grounded in common-law negligence, affords botnet-attack victims two ways to fight back against their zombie aggressors: litigation and self-help. Imposing negligence liability would change user behavior, making botnet infections less likely. Recognizing a counterstrike privilege protects and rewards actors who develop ways to destroy existing botnets and protect network computing assets. The combination of the imposition of liability on botnet zombies and the creation of the counterstrike

\textsuperscript{195} See supra notes 1–7 and accompanying text.

\textsuperscript{196} Subjecting counterstrikes to a standard of reasonableness necessarily means that courts will have to examine whether a given counterstrike is reasonable in the particular circumstances under which it is launched. Nevertheless, I can suggest a number of situations where a counterstrike might be considered presumptively reasonable. A reasonable counterstrike should exploit a vulnerability on a zombie computer of which the zombie’s owner is, or reasonably should be, aware. Additionally, the counterstrike should only attack a vulnerability for which a fix has been issued—the zombie owner should have had at least a reasonable opportunity to become aware of the fix and to apply it. If counterstrikes exploiting well-known vulnerabilities are presumptively reasonable, and thus privileged, botnet victims would have an even more powerful incentive to attempt to disrupt the connections of zombie computers whose owners have failed to take even minimal steps to secure them. Cf. Henderson & Yarborough, supra note 80, at 21 (suggesting a standard of care for network-connected computers). For example, suppose there exists a well-known flaw in a computer operating system that allows a remote user to execute programs on the target system, without the owner of the target system being aware of any unusual activity. Suppose again that the developers of the operating system are aware of this flaw and have made available to the operating system’s users a means to correct that flaw. If a reasonable time has passed between the issuance of the fix, and if the reasonable user would have become aware that a fix was available, then it is equally reasonable for such a user to have applied the fix to his operating system, closing the well-known vulnerability. If a user had not applied the fix, and his computer had become a zombie node as a result of that omission, then it should be presumptively reasonable for a counterstriking botnet DDoS victim to make use of the same vulnerability to destroy the botnet, or disrupt its operations.

\textsuperscript{197} See supra note 7.
privilege creates powerful incentives to halt the spread and disrupt the growth of malicious botnets.