

SPAM—OY, WHAT A NUISANCE!

By Adam Mossoff[†]

ABSTRACT

This Article proposes that unsolicited commercial e-mail (“spam”) is indeed a nuisance, and that ISPs and other affected businesses should sue the persons responsible for swamping the Internet with billions of spam for creating a nuisance. Nuisance doctrine is superior to the currently favored “trespass to chattels” because it does not require courts to engage in unnecessary legal fictions or doctrinal somersaults in finding that spam has “dispossessed” a plaintiff from its computer network. The direct and consequential costs attributable to this e-mail scourge—such as loss of bandwidth usage, developing and maintaining filtering software, and hiring more staff—are simply not trespass harms. These costs reveal that the real problem is that spam is unreasonably and substantially interfering with an ISP’s commercial operations—a paradigmatic nuisance injury. As a common law cause of action, nuisance also avoids the over-protection problems inherent in anti-spam statutes, which have proven ineffective because legislators are rightly concerned about accidentally stifling legitimate commercial activity on the Internet. As ISPs and other businesses continue to sue spammers, they should utilize nuisance doctrine as part of their overall strategy to eliminate this omnipresent menace to the Internet because it precisely redresses the legal harm caused by spam.

TABLE OF CONTENTS

I. INTRODUCTION	626
-----------------------	-----

© 2004 Adam Mossoff

[†] Assistant Professor of Law, Michigan State University College of Law. J.D., University of Chicago; M.A., Columbia University; B.A., University of Michigan. The author would like to thank Scott Boone, Adam Candeub, Michael Carrier, Eric Claeys, Chris Cotropia, Shuba Ghosh, Llew Gibbons, Eric Goldman, Rob Heverly, Laura Heymann, Cory Hojka, Matt Jackson, Brian Kalt, Jay Kesan, Michael Landau, Lyrissa Lidsky, Michael Madison, Mark McKenna, Tom Nachbar, Jonathan Nash, Xuan-Thao Nguyen, David Post, Kathy Strandburg, Peter Yu, and the participants at the Tulane Law School Works-in-Progress Intellectual Property Colloquium and the MSU Intellectual Property & Communications Law and Policy Scholars Roundtable for their helpful comments. Nicholas Mathieu provided valuable research assistance, and Amy Mossoff, as always, was an excellent editor. The author also begs forgiveness from the MSU law college tech department for the spam and flames that may likely be sent his way after receipt of this Article by spammers and their industry groups.

II. A BRIEF HISTORY OF SPAM	631
III. THE LESS-THAN-SPECTACULAR ATTEMPTS AT KILLING SPAM	632
A. The Folly of Filters	632
B. Lackluster Legislation	634
C. Losing the Litigation: <i>Intel v. Hamidi</i>	640
IV. RETHINKING THE LITIGATION STRATEGY: SPAM AS NUISANCE.....	646
V. LITIGATING SPAM AS NUISANCE: COST-BENEFIT ANALYSES AND DEFENSES	654
VI. THE BROADER PERSPECTIVE: HOW TO PROTECT THE PROPERTY ENTITLEMENT AT ISSUE IN SPAM CASES	658
VII. CONCLUSION	665

Will the Minister explain how it is that an inedible tinned food can become an unsolicited email, bearing in mind that some of us wish to be protected from having an email?

—Lord Renton

House of Lords, May 6, 2003¹

I. INTRODUCTION

Aside from hopelessly out-of-touch English aristocrats and the dwindling number of American households without computers, few people are just waking up to the reality of spam. Anyone with an e-mail account knows firsthand that the crescendo of complaints about spam do not refer to Hormel's famous canned-ham product that fed U.S. troops as they marched across Europe in World War Two.² A new meaning has accrued to "spam" in a culture now saturated with the terms and acronyms of the digital revolution—from the innocuous-sounding "ISP" (Internet Service Provider) and "netizen" (an inhabitant of cyberspace) to the more menacing-sounding "flame" (an e-mail or web posting comprising abusive and insulting language). Thus, "spam" has re-entered the English lexicon as a term referring to the massive amount of unsolicited commercial e-mail

1. Will Sturgeon, *House of Lords Email Debate Reveals "Spam" Confusion*, May 7, 2003, at <http://www.silicon.com/management/government/0,39024677,10004059,00.htm> (last visited Apr. 21, 2004).

2. See *Spam in Time*, at <http://www.spam.com> (surveying the role of Hormel's Spam in twentieth-century America) (last visited Mar. 20, 2004).

(the formal and largely unused acronym is “UCE”) that is sent out each day across the Internet and into inboxes everywhere.³

Even if there were no term for it, the spam phenomenon would require a linguistic signifier to identify it. With each year, the deluge worsens. In 2001, e-mail accounts in the United States received more than 140 billion pieces of spam,⁴ a staggering and seemingly unbelievable number. More staggering still is that spam increased by 86 percent in 2002, numbering approximately 261 billion pieces.⁵ Studies predicted that it would further increase in 2003,⁶ although exact numbers have yet to be released.

The ever-growing tidal wave of spam is causing major headaches and consuming extensive resources at ISPs and in other businesses. It is now a primary factor driving the development of new versions of ISP software. Prior to the release of version 9.0 of its dial-up software in late July 2003, America Online (AOL) began marketing its software upgrade by touting the new spam-filtering capabilities. “Spam is the No. 1 concern,” declared AOL’s product manager, Roy Ben-Yoseph, who explained at that time that AOL blocked an average of 2.4 billion pieces of spam *each day*.⁷ Even Bill Gates has confessed, “Like almost everyone who uses e-mail, I receive a ton of spam every day.”⁸ He complained in the *Wall Street Journal* that “spam is worse than irritating. It is a drain on business productivity, an increasingly costly waste of time and resources that clogs corporate

3. See, e.g., AMERICAN HERITAGE DICTIONARY (4th ed. 2000) (defining “spam” as “[u]nsolicited e-mail, often of a commercial nature, sent indiscriminately to multiple mailing lists, individuals, or newsgroups; junk e-mail”), available at <http://dictionary.reference.com/search?q=spam> (last visited Oct. 8, 2003); see also *Prepared Statement of The Federal Trade Commission on “Unsolicited Commercial Email” Before the Senate Committee on Commerce, Science and Transportation*, at 1, available at <http://www.ftc.gov/os/2003/05/spamtestimony.pdf> (May 21, 2003) (defining “[u]nsolicited commercial email (‘UCE’ or ‘spam’) [as] any commercial electronic mail message that is sent—typically in bulk—to consumers without the consumers’ prior request or consent”). The anti-spam organization, The Spamhaus Project, includes “bulk” as an essential component of the definition of “spam.” See <http://www.spamhaus.org/definition.html> (noting that “[t]o be Spam, a message must be sent Unsolicited AND [in] Bulk”) (last visited Oct. 8, 2003).

4. Bob Sullivan, *Spam Wars: How Unwanted Email is Burying the Internet*, (Aug. 6, 2003), available at <http://www.spamsolutions.net/1059.asp> (citing a study by Jupiter Research).

5. *Id.*

6. See *Losing the War on Spam*, WIRE, Sept. 2003, at 50.

7. Jane Weaver, *AOL 9.0 Focuses on Spam, Security* (July 29, 2003), available at <http://msnbc.msn.com/id/3078624/>.

8. Bill Gates, *Why I Hate Spam*, WALL ST. J., June 23, 2003, <http://www.opinionjournal.com/editorial/feature.html?id=110003662>.

networks and distracts workers.”⁹ Surveys confirm what some might take as anecdotal grumbling by Bill Gates: spam will cost companies approximately \$20.5 billion in 2003, and predictions run as high as \$198 billion by 2007.¹⁰ In light of such numbers, the Federal Trade Commission (FTC) reported to Congress last spring that “the volume of unsolicited e-mail is increasing exponentially,” and that we are reaching the “tipping point” at which “spam is ‘killing the killer app.’”¹¹ The FTC concluded the obvious: finding “a solution to the spam problem is critically important.”¹²

As costs mount and exasperation rises, there is one word that is nearly universally used to describe spam: *nuisance*.¹³ At the same legislative debate in which Lord Renton inquired about the etymology of “spam,” Lord Mitchell complained, “Spam, whether it is nuisance advertising or hardcore pornography is literally choking the [I]nternet.”¹⁴ The title of a January 2003 article on the subject reads, “Study: Spam A Costly Nuisance.”¹⁵ A June 2003 survey released by BURST! Media, an Internet advertising company, found that 77.1 percent of respondents believe that spam is a nuisance and 54.1 percent of respondents believe that spam is a “major nuisance.”¹⁶ Dale Malik, a development leader for communications products in the BellSouth Internet Group, testified before the FTC that spam is considered a “major annoyance” by its customers today, although it was only an “occasional nuisance” in 2000.¹⁷ Steve Dougherty, director of

9. *Id.*

10. Sullivan, *Spam Wars*, *supra* note 4 (citing study of spam by Radicati Group).

11. *Prepared Statement of The Federal Trade Commission on “Unsolicited Commercial Email” Before the Senate Committee on Commerce, Science and Transportation*, *supra* note 3, at 2 (paraphrasing the conclusion of an FTC-sponsored conference on spam); *see also* Robert MacMillan, *Survey: Spam Driving Internet Users Away From E-mail*, WASH. POST, Mar. 17, 2004, <http://www.washingtonpost.com/wp-dyn/articles/A2279-2004Mar17.html> (reporting on a Pew survey that found that almost 30 percent of respondents have reduced their use of e-mail because of “mounting spam” and 63 percent were less trusting of e-mail as a “communications tool” because of spam).

12. *Prepared Statement of The Federal Trade Commission on “Unsolicited Commercial Email” Before the Senate Committee on Commerce, Science and Transportation*, *supra* note 3, at 2.

13. An unscientific survey by the author on October 8, 2003, consisting of a Google search of the string “spam + nuisance” produced 36,500 hits.

14. *Supra* note 1.

15. Margie Semilof, *Study: Spam A Costly Nuisance*, at http://searchwin2000.techtarget.com/originalContent/0,289142,sid1_gci871979,00.html (Jan. 3, 2003).

16. *See* BURST! Online Insights (July 2003), at http://www.burstmedia.com/release/advertisers/online_insights/july_2003.pdf (last visited Oct. 7, 2003).

17. Dale Malik, Testimony at the FTC Spam Forum (May 1, 2003). Malik’s Power-Point presentation from which these quotes are taken is available at <http://www.ftc.gov/bcp/workshops/spam/Presentations/malik.pdf> (last visited Oct. 7, 2003).

vendor systems management at Earthlink, a prominent ISP, has complained that spam is a “growing nuisance.”¹⁸

This Article proposes that spam should be treated under the law in precisely the same way it is characterized in our common speech—as a nuisance. Nuisance law represents a largely unexplored option for redressing the harms caused by spam; the viability of suing spammers for nuisance has not been examined in the academic literature,¹⁹ nor has a nuisance claim been adjudicated to a final judgment in a published court opinion.²⁰ This Article fills the lacuna in the literature by explaining how the substantial interference with the use of networks and business operations caused by spam is a paradigmatic example of a nuisance-type injury and how the elements of a traditional private nuisance claim would apply more easily to spammers than the trespass doctrine that plaintiff ISPs and other businesses have asserted to date.

This proposal is not intended to be exclusive of other responses to the spam problem, although it has definite policy advantages over the federal anti-spam legislation enacted in December 2003, the use of anti-spam filtering software, and the current litigation strategy pursued by ISPs and

18. Michelle Delio, *Spam-Cramming Foils Vacationers*, WIRED, July 5, 2002, <http://www.wired.com/news/technology/0,1282,53669,00.html>.

19. See, e.g., Anne E. Hawley, Note, *Taking Spam Out of Your Cyberspace Diet: Common Law Applied to Bulk Unsolicited Advertising via Electronic Mail*, 66 UMKC L. REV. 381 (1997) (proposing only trespass to chattels and tortious interference claims to deal with spam). *But cf.* Dan L. Burk, *The Trouble With Trespass*, 4 J. SMALL & EMERGING BUS. L. 27, 53 (2000) (suggesting that a new action for electronic nuisance be adopted to address spam). Burk is often cited for the general proposition that nuisance actions should be used against spam. See, e.g., Michael A. Fisher, *The Right to Spam? Regulating Electronic Junk Mail*, 23 COLUM.-VLA J.L. & ARTS 363, 389 (2000) (citing Burk for the proposition that “electronic nuisance” should be used in spam cases and discussing it in general terms for several paragraphs). Burk, however, does not analyze the issue of spam as nuisance, nor is this the thesis of his article. Rather, Burk critiques the doctrine of trespass of chattels as used in Internet cases. Burk, *supra*, at 27-53. In the penultimate paragraph of his critique, he mentions that his criticism of trespass of chattels “suggests” that nuisance may be a viable alternative. *Id.* at 53. His discussion of this point consists of only several sentences in which he briefly summarizes an economic analysis of nuisance as involving a cost-benefit assessment of the parties’ respective activities, and suggests a few ways this assessment would be applied to spammers. *Id.* While Burk deserves credit for being the first to suggest that nuisance may work against spammers, this Article presents a thorough treatment of the subject.

20. Although the extant court reporters do not reveal any evidence of a successful nuisance claim against a spammer, a Texas trial court ordered an injunction and payment of damages against a spammer in an unpublished opinion in 1997. This case is discussed at the end of Part IV.

other commercial firms.²¹ The response to spam should be multifaceted and wide-ranging in scope. Nonetheless, there are numerous advantages to suing spammers for nuisance. First and foremost, this approach redresses the harms caused by spam to ISPs and business networks without resorting to the legal fiction inherent in charging spammers with committing a “trespass.” Applying trespass doctrine to spam has been assailed as improperly requiring courts to construct fanciful legal fictions in which spam is somehow “dispossessing” a plaintiff of its computer network. The use of nuisance doctrine avoids these scholarly criticisms. Second, nuisance doctrine better focuses courts’ attention on the property entitlement at issue in spam cases. The problem is not that spam violates an ISP’s or business’s right to exclude people from its network; rather, it is the spammer’s misuse of the invitation to send e-mail through a network, resulting in substantial and unreasonable interference with the commercial use of this network. Third, the successful use of a nuisance action preempts the escalating technological arms race, in which programmers feverishly create filtering software and spammers deviously breach the anti-spam filters. This ongoing cycle is partly to blame for the substantial costs that spam imposes on ISPs and businesses.

From a broader perspective, suing spammers for nuisance would achieve efficiencies through the private ordering of the common law system. The parties experiencing the substantial financial harms caused by spam should be the ones to hold spammers accountable, not the individual end-users who experience legally *de minimus* frustration or inconvenience. A successful and coherent cause of action would also reduce the sense of immediacy among end-users and ISPs to expend valuable resources lobbying elected officials, who ultimately enact ineffectual legislation due to very real concerns about over-protection. The common law provides a cause of action that ISPs and other businesses can use to force spammers to take into account—to “internalize,” to use the economist’s turn of phrase—the millions of dollars in damages that spammers cause to these firms.

This Article explains these points in five parts. Part II presents a brief history of spam, explaining how both lawyers and Monty Python contributed to today’s spam phenomenon. Part III surveys the current tripartite response to spam by ISPs and businesses—technological innovation, special legislation, and litigation—and explains why these counterattacks have been less than spectacular at eliminating, or even reducing, spam. Part IV explains how the harms caused by spam are paradigmatic exam-

21. *See infra* Part III.

ples of nuisance-type injuries, and why spam is an injury to a commercial firm's utilization of its "land." Part V discusses how nuisance doctrine addresses the concerns expressed by courts and professors about the use of property rules to protect entitlements on the Internet. Finally, Part VI discusses the general doctrinal advantages to pleading nuisance against spam and notes some of the benefits in relying on the private ordering of the common law to protect new forms of property entitlements.

II. A BRIEF HISTORY OF SPAM

The provenance of "spam" is far more humble than its infamous status today. The term's current use was coined in the early 1990s, when participants on Usenet discussion groups referred to annoying and distracting cross-postings as "spam."²² The eponymous source was a famous comedy sketch from a 1970 episode of Monty Python's *Flying Circus*, which consisted of a waitress listing the contents of a menu for a customer, and each item contained Spam as an ingredient. As the waitress (it was actually Terry Jones in drag) spoke, a group of Vikings in the background was singing, "Spam, Spam, Spam, Spam! Lovely Spam! Wonderful Spam!" Eventually, the Spam-loving Vikings made it impossible to hear what the waitress was saying due to their incessant singing of "Spam, Spam, Spam, Spam!"²³ Thus, Usenet denizens labeled any mass Usenet posting that drowned out their discussions with repetitive nonsense as "spam."

As luck would have it, the first *commercial* Usenet spam was sent out by lawyers. On April 12, 1994, two immigration lawyers posted an advertisement for their services to 6,000 Usenet discussion groups in less than 90 minutes.²⁴ Their postings were entirely commercial: the lawyers sought to create business for themselves, not to engage Usenet users in discussion. Prior to this fateful date, the ethos of the Usenet—and of the Internet generally—was decidedly non-commercial. The lawyers received a blis-

22. See *The Jargon Files*, at <http://www.houghi.org/jargon/spam.php> (defining spam, in part, as "[t]o cause a newsgroup to be flooded with irrelevant or inappropriate messages" and "[t]o bombard a newsgroup with multiple copies of a message").

23. See *SPAM and the Internet*, at http://www.spam.com/ci/ci_in.htm (last visited Apr. 21, 2004) (discussing the birth of the term "spam" on the Internet); Neil Swidey, *Spambusters*, BOSTON GLOBE, Oct. 5, 2003, <http://boston.com/business/technology/articles/2003/10/05/spambusters/> (same).

24. K.K. Campbell, *A Net Conspiracy So Immense. . .*, at http://www.eff.org/Legal/Cases/Canter_Siegel/c-and-s_summary.article (interviewing one of the attorneys involved in this incident and recounting the event) (last visited Mar. 23, 2004); Ray Everett-Church, *The Spam That Started It All*, WIRED, Apr. 13, 1999, <http://www.wired.com/news/politics/0,1283,19098,00.html>.

tering avalanche of flames. The lawyers' ISP was also "bombed into oblivion by world-wide complaints."²⁵ In response, the ISP promptly closed the lawyers' account.²⁶ Yet the gates were opened. Despite the scathing complaints, the lawyers claimed to have made \$100,000 from this first, fateful commercial spamming.²⁷

Soon businesses, along with charlatans and pornographers, caught on to the enormous commercial opportunities in the low-cost, mass-communication medium of the Internet. By the end of the 1990s, the Internet was increasingly commercialized, a process that continues today despite the dot-com bust at the turn of the century.²⁸ Also, as e-mail replaced the Usenet as the principal means of communication over the Internet, the meaning of "spam" shifted from referring to mass bulletin board postings to mass e-mail. The lawyers' posting in 1994 of only 6,000 advertisements in 90 minutes would be considered insignificant by today's standards, when a single spammer can brag about sending from 50 to 250 million e-mails in a single day.²⁹

III. THE LESS-THAN-SPECTACULAR ATTEMPTS AT KILLING SPAM

ISPs and businesses have not taken the spam onslaught lying down. They have engaged the enemy on three interrelated fronts: technological innovation, legislation, and litigation. Thus far, the results of their efforts have been decidedly mixed, as evidenced by the rising flood of spam with each passing year.

A. The Folly of Filters

The technological response to spam has been purely defensive, akin to the efforts of medieval kings to protect themselves by building massive walls around their towns and castles in order to keep out brigands and invading armies. In the digital domain, ISPs and businesses are increasingly investing money, time, and capital in software that filters spam from other e-mail arriving into the network. If successful, the filter shunts spam away

25. Campbell, *supra* note 24.

26. *Id.*

27. Swidey, *supra* note 23.

28. See generally *The Net's Good Fortunes*, WIRED 57 (Mar. 2004) (noting that growth in online retail sales, among other commercial activities, are only lagging about one to two years behind predictions made in the late nineties).

29. See *World's Top 10 Spammers*, at http://www.msnbc.com/news/wld/tech/brill/Top10Spammers_dw.htm (citing spamhaus.org, an anti-spam organization) (last visited Apr. 17, 2004).

from customer or employee inboxes and into separate storage directories where it is deleted en masse; thus ensuring that the slings and arrows never reach their intended targets.³⁰ Filtering is one of the key components in AOL version 9.0, and it is the sole service sold by the Internet-companies Brightmail and SpamGuard, which are used by Microsoft's Hotmail and Yahoo! Mail, respectively.³¹

The problem with relying on filtering services and related technological fixes is that it creates a technological arms race between the parties. As the ISPs and "tech support" departments steadily work at blocking spam, increasingly mischievous spammers steadily work at circumventing these efforts.³² Spammers have every incentive to scale the technological ramparts created by ISPs and companies: substantial profit margins await the spammer who successfully sends out millions of spam a day.³³ Accordingly, the cycle repeats with increasing frequency: ISPs and businesses spend money, programmers write code, and spammers circumvent. Lather, rinse, repeat—ad nauseum.³⁴ Of course, the costs associated with this vicious cycle are part and parcel of the total economic harms imposed on ISPs and businesses by spam.³⁵

30. As early as 1997, the U.S. government recommended filtering as "the only practical solution today for removing spam messages, and it is less than perfect." *I-005c: Email Spamming Countermeasures*, U.S. Dep't of Energy Computer Incident Advisory Capability (Nov. 25, 1997), available at <http://ciac.llnl.gov/ciac/bulletins/i-005c.shtml> (last visited Mar. 23, 2004).

31. Mark Glassman, *Fortifying the In Box as Spammers Lay Siege*, N.Y. TIMES, July 31, 2003, at G8.

32. Mike Bruner, *In The Trenches of the "Spam War"* (Aug. 7, 2003), at <http://msnbc.msn.com/id/3078650/>.

33. A notorious spammer, Eddy Marin, once told the Miami Herald that he makes "over 80 percent profit," and that he once generated revenue of \$750,000 in the first quarter of a year. *World's Top 10 Spammers*, *supra* note 29. Other spammers report that they make \$10 for a single lead for a mortgage lender, and thus it takes only 40–50 responses from one day's mailing of 10 million emails to make \$400–500 in a single day. Sullivan, *supra* note 4; See also Bob Sullivan, *Who Profits From Spam? Surprise*, at <http://msnbc.msn.com/id/3078642/> (Aug. 8, 2003).

34. As early as July 2002, AOL representatives were characterizing their efforts at filtering spam as "a cat-and-mouse game" between AOL and the spammers. Delio, *supra* note 18 (quoting AOL spokesman, Nicholas Graham).

35. These costs are detailed in Part IV. A secondary problem is false positives, i.e., a filter blocks a legitimate email because it mistakes it for spam. Brightmail claims that it incurs only one false positive for every 1 million pieces of spam that it filters. Glassman, *Fortifying the In Box as Spammers Lay Siege*, *supra* note 31. For people who rely on email for business communications, such as lawyers, the loss of a significant or timely email could prove disastrous.

This technological arms race has also resulted in the same escalation of hostilities as that which now dominates the debate between the recording and movie industries and the peer-to-peer (P2P) file swappers (with equally little hope of peaceful resolution).³⁶ Representatives from the computer industry and spamming groups almost broke out into fistfuffs in front of FTC commissioners during an FTC-sponsored Spam Forum in the spring of 2003, and one marketing company used the conference as an opportunity to serve an anti-spam proponent with a subpoena.³⁷ In an article in the January 2004 issue of *Wired*, entitled “101 Ways to Save the Internet,” the number one proposal was that people should be permitted to “unleash vigilante justice on spammers” through denial-of-service attacks on a spammer’s ISP.³⁸ The search for a solely technological solution has quickly become part of the problem.

B. Lackluster Legislation

In 2003, an intensive lobbying effort for federal anti-spam legislation began to bear fruit. In the first half of the year, nine anti-spam bills were introduced in Congress, all of which proposed various civil and criminal penalties for spammers.³⁹ The two most prominent bills—the Controlling the Assault of Non-Solicited Pornography and Marketing Act⁴⁰ (“CAN-

36. Denial of service attacks on websites, nuisance mass mailings of catalogs to people’s homes, and even death threats are becoming commonplace in the battles between pro- and anti-spam forces. Brunker, *supra* note 32. In the first ever recognized case of “spam rage,” a California resident is facing criminal charges for “threatening to torture and kill employees of the company he blames for bombarding his computer with Web ads promising to enlarge his penis.” *Man Arrested Over “Spam Rage”*, WIRED, Nov. 21, 2003, <http://www.wired.com/news/culture/0,1284,61339,00.html>. The hostilities between the movie and recording industries and P2P file swappers are well known today. See David Pogue, *The Difference Between Movies and Music*, N.Y. TIMES, Oct. 2, 2003, <http://www.nytimes.com/2003/10/02/technology/circuits/02POGUE-EMAIL.html> (assuming his readers’ knowledge of the “escalating battle between music companies and their customers” in an essay addressing the movie industry); see also Peter K. Yu, *The Escalating Copyright Wars*, 32 HOFSTRA L. REV. (forthcoming 2003) (discussing the seemingly unending and escalating hostilities in the war between copyright-holders and P2P file swappers).

37. Sullivan, *supra* note 4.

38. Paul Boutin, *101 Ways to Save the Internet*, WIRED, Jan. 2004, at 132.

39. See <http://www.spamlaws.com/federal/list108.html> (describing and linking to the nine bills proposed in the 108th Congress); Mike Brunker, *Congress Targeting Outlaw Spammers*, at <http://www.msnbc.com/news/948022.asp> (Aug. 12, 2003). Senator Charles Schumer proposed a “do not email” list similar to the “do not call” list put into effect on October 1, 2003, but support for Schumer’s plan within the computer and Internet industry waned over the summer months. *Id.*

40. S. 877, 108th Cong. (2003).

SPAM Act”) in the Senate and the Restrict and Eliminate the Delivery of Unsolicited Commercial Electronic Mail or Spam Act⁴¹ (“REDUCE Spam Act”) in the House—were buoyed by the three-day FTC Spam Forum⁴² in April–May 2003 and by numerous news articles on spam throughout the summer. As a result, these bills appeared to garner the requisite momentum for the 108th Congress to overcome the federal government’s institutional inertia. In late 2003, Congress took a break from debating pending budget bills to enact the CAN-SPAM Act,⁴³ which President George W. Bush signed into law on December 16, 2003.⁴⁴

The CAN-SPAM Act of 2003⁴⁵ was the result of substantial back-and-forth lobbying efforts and bill amendments. The final version provides for up to \$2 million in fines and prison terms for fraudulent header information, such as false reply addresses or misleading subject lines.⁴⁶ In some cases involving substantial violations, the fines may be trebled up to \$6 million.⁴⁷ Other relevant provisions of the CAN-SPAM Act require all spam to offer an “opt-out” option for recipients⁴⁸ and to contain some kind of notice in the subject line if the spam contains pornographic material.⁴⁹ It also authorizes the FTC to investigate the implementation of a “do not

41. H.R. 1933, 108th Cong. (2003).

42. See FTC Spam Forum, April 30 – May 2, 2003, at <http://www.ftc.gov/bcp/workshops/spam/> (last visited Apr. 1, 2004).

43. See Grant Gross, *Senate Amends, Approves Spam Bill*, PC WORLD, Nov. 25, 2003, <http://www.pcworld.com/news/article/0,aid,113667,00.asp> (last visited Dec. 2, 2003); David McGuire, *House Passes Anti-Spam Bill*, WASH. POST, Nov. 22, 2003, <http://www.washingtonpost.com/wp-dyn/articles/A5892-2003Nov22.html> (last visited Apr. 1, 2004); David Firestone & Saul Hansell, *Senate Votes to Crack Down on Some Spam*, N.Y. TIMES, Oct. 23, 2003, at C1, available at <http://www.nytimes.com/2003/10/23/technology/23MAIL.html> (noting that the Senate voted 97-0 in favor of the bill).

44. See Jennifer S. Lee, *President Signs Law Aiming to Limit Spam*, N.Y. TIMES, Dec. 16, 2003, <http://www.nytimes.com/2003/12/16/politics/16CND-SPAM.html> (last visited Apr. 1, 2004).

45. Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003, Pub. L. No. 108-187, 117 Stat. 2699 (Dec. 16, 2003).

46. § 5(a)(1)-(2), 117 Stat. at 2706-07 (prohibiting fraudulent header information); § 7(f)(3)(B), 117 Stat. at 2713 (defining statutory damages).

47. § 7(f)(3)(C), 117 Stat. at 2713.

48. § 5(a)(3)-(4), 117 Stat. at 2707-08 (mandating a mechanism for recipients to request not to receive spam and prohibiting a spammer sending any additional emails after such a request is received).

49. § 5(d), 117 Stat. at 2709. The CAN-SPAM Act also directs the FTC to define and implement the required warning, see § 5(d)(3), 117 Stat. at 2710. On January 28, 2004, the FTC filed a notice of proposed rulemaking, seeking comment on a rule requiring the phrase “sexually-explicit-content” in the subject line of any pornographic spam, as required under the CAN-SPAM Act. 16 C.F.R. 316 (Jan. 28, 2004).

e-mail” list similar to the “do not call” list implemented in September 2003.⁵⁰ Finally, the Act permits the FTC and other regulatory agencies, state attorneys general, and ISPs to take spammers to court for violations, but precludes individual end-users from suing spammers.⁵¹

Despite its myriad prohibitions and sanctions, the CAN-SPAM Act has been heavily criticized for being ineffective. Zoe Lofgren and Mike Honda, House members from the high-tech Silicon Valley, voted against the CAN-SPAM Act because they believed that the bill was too weak. “We clearly recognize the need for anti-spam legislation,” stated Honda’s press secretary, “but what they passed will not significantly reduce the amount of spam.”⁵² Why not? The oft-cited reason is that the CAN-SPAM Act implicitly authorizes spam that does not violate its prohibitions; in other words, all non-fraudulent commercial spam that contains opt-out information and appropriate header information is immunized from legal attack under the Act.⁵³ Essentially, the CAN-SPAM Act offers legitimate business spammers a federal stamp of approval: if you meet our list of requirements, you can continue to spam with abandon.⁵⁴ A representative

50. § 9, 117 Stat. at 2716.

51. § 7, 117 Stat. 2711-15. The likely reason for this limitation on individual end-users suing under the CAN-SPAM Act was that state anti-spam legislation had already obeyed the law of unintended consequences: additional costs were imposed on companies and ISPs by individual end-users suing them under the very statutes intended to alleviate their burgeoning costs attributed to spam. *See* Federal Trade Commission Spam Forum, May 1, 2003 (day two), at 98-99, 101 (statements of Steve Smith, CEO of MindShare Design, and Laura Atkins, President of SpamCon Foundation), *available at* http://www.ftc.gov/bcp/workshops/spam/transcript_day2.pdf. Accordingly, the CAN-SPAM Act also preempts all state laws addressing the same issues. *See* § 8(b), 117 Stat. at 2716. As of the date of the enactment of the CAN-SPAM Act into law, thirty-six states had adopted various anti-spam laws, some of which were far stricter than it. *See* <http://www.spamlaws.com/state/summary.html> (summarizing the anti-spam statutes in the 38 states that have enacted such laws to date) (last visited Apr. 1, 2004).

52. Roy Mark, *Lawmakers: Spam Bill is a Turkey*, at <http://www.internetnews.com/bus-news/article.php/3113941> (Nov. 26, 2003) (last visited Dec. 11, 2003).

53. After the Senate and House reached a compromise on their competing versions of the CAN-SPAM Act on November 21, one expert on spam declared that “[t]his bill legalizes spam that isn’t fraudulent. There will be a lot more spam by legitimate marketers because they will be able to point to the federal law and say, ‘We are following all the rules.’” David Stout, *Congress Poised for Vote on Anti-Spam Bill*, N.Y. TIMES, Nov. 21, 2003, <http://www.nytimes.com/2003/11/21/politics/21CND-SPAM.html> (quoting David Sorkin, a law professor at the John Marshall Law School in Chicago).

54. *See* Jacquelyn Trussell, *Is The Can-Spam Act The Answer To The Growing Problem Of Spam?*, 16 LOY. CONSUMER L. REV. 175, 187 (2004) (“By regulating spam, the CAN-SPAM Act legitimizes certain types of spam. Many fear that a wave of legitimate spam will be unleashed from companies that previously feared being labeled as spammers.”).

from Internet Security Systems has likened the CAN-SPAM Act to “trying to write a law to ban viruses. It’s just about that effective. I expect the volume of traffic in your in-box to increase.”⁵⁵

The CAN-SPAM Act ultimately under-protects and does not solve the spam problem because of the concern that such legislation may over-protect and do more harm than good. One extreme example of this is China’s recent decision to classify some spam as “reactionary,”⁵⁶ which implies all of the attendant consequences for the hapless individual labeled as such by China’s authoritarian regime.⁵⁷ Another example of over-protection, albeit far less worrisome than China’s approach, was reflected in the REDUCE Spam Act, one of the primary bills competing with the CAN-SPAM Act for adoption by the 108th Congress.⁵⁸ The REDUCE Spam Act arguably failed to win support in Congress due to concerns that it may over-protect by punishing innocent commercial behavior. The REDUCE Spam Act, as originally proposed, mandated that *any* unsolicited business-related e-mail state in its subject header “ADV” (shorthand for “advertisement”).⁵⁹ The justification for this requirement was that it would

55. Grant Gross, *CAN-SPAM Law Won't, Critics Say*, PC WORLD, Oct. 27, 2003, <http://www.pcworld.com/news/article/0,aid,113137,00.asp> (quoting Pete Privateer, senior vice president for product strategy and marketing at security and anti-spam vendor, Internet Security Systems).

56. *China Vows to Curb Junk E-Mail*, at <http://www.siliconvalley.com/mls/siliconvalley/news/editorial/7855530.htm> (Feb. 2, 2004) (quoting the official Xinhua News Agency, which cited the China Police Daily).

57. China is known to torture and execute “criminals,” which includes people labeled as “reactionary.” See, e.g., Amnesty International, *Appeal Cases: Tenzin Deleg Rinpoche & Lobsang Dhondup*, Mar. 22, 2004, at <http://web.amnesty.org/library/Index/ENGASA170022004> (detailing denial of due process rights and torture of two individuals labeled as “reactionary and anti-government”); see also *Organs for Sale: China's Growing Trade and Ultimate Violation of Prisoner's Rights, Hearing Before the House Committee on International Relations* (June 27, 2001), available at http://www.house.gov/international_relations/107/73452.pdf (discussing China’s executing criminals after which family members are required to pay for the bullet used to kill the prisoner and China’s harvesting of organs from executed prisoners).

58. The REDUCE Spam Act was proposed by Representative Lofgren, one of the few members in the House who voted against the CAN-SPAM Act due to its perceived ineffectiveness. See *supra* note 52, and accompanying text; see also Roy Mark, *Spam Solutions Hard to Find*, at <http://dc.internet.com/news/article.php/2199191> (Apr. 30, 2003) (last visited Apr. 1, 2004).

59. Declan McCullagh, *A Modest Proposal To End Spam*, CNET News.com, at <http://news.com.com/2010-1071-998513.html> (Apr. 28, 2003). Notably, this was incorporated into the final version of the CAN-SPAM Act, but only by dint of requiring the FTC to deliver a report on the subject within eighteen months to the Senate Committee on Commerce, Science, and Transportation and the House of Representatives Committee on

make it easy for ISPs or end-users to set their filters to delete automatically any e-mail with “ADV” in its subject header.⁶⁰ In effect, unsolicited commercial e-mail would be banned—because everyone would filter out e-mails with “ADV” in their subject headers. The REDUCE Spam Act also levied heavy criminal and civil penalties on any person who failed to include “ADV” in the subject header of an unsolicited business e-mail.⁶¹

Although initially enticing in its promise of spam-free e-mail, the impact of the REDUCE Spam Act would have reached far beyond spammers, and threatened legitimate commercial activities. Anyone who sent an unsolicited e-mail for business purposes, such as a person sending resumes to potential employers, would have fallen within the Act’s ambit.⁶² Professor Eugene Volokh noted that the bill “would cover freelance writers pitching a story or photographers pitching a photo.”⁶³ Sanctioning such innocent uses of e-mail would only deter people from using the Internet for communication and business purposes. The commercial growth and opportunities of the Internet would be stymied,⁶⁴ while political, religious and other non-commercial persons would remain free to send out millions of e-mails a day.⁶⁵ The legislative medicine would have been worse for the Internet than the disease.

In response to such criticisms, the bill’s sponsor amended it to provide for an affirmative defense against liability for anyone who sends less than

Energy and Commission. *See* § 11, 117 Stat. at 2717. Again, the weakening of the provisions of the REDUCE Spam Act is evident.

60. Bill Gates supported this legislative requirement for this very reason. *See* Gates, *supra* note 8.

61. H.R. 1933 §§ 3(a), 6(b), 108th Cong. (1st Sess. 2003) (providing for imprisonment up to one year and a fine multiplied by as much as \$10 for *each* unsolicited email sent).

62. McCullagh, *supra* note 59; *see also* Joseph P. Kendrick, “Subject: ADV:” *Anti-Spam Laws Force Emerging Internet Business Advertisers to Wear the Scarlet “S”*, 7 J. SMALL & EMERGING BUS. L. 563, 573-75 (2003) (criticizing the “ADV” requirement given its negative impact on legitimate businesses).

63. McCullagh, *supra* note 59.

64. By midyear 2002, commercial firms discovered the real gold in the Internet: increased efficiency in business-to-business (B2B) transactions. Steve Butler, *The Internet Has Greatly Helped to Increase the Efficiency of Transactions*, at <http://www.gcis.ca/cdne-213-jul-15-2002.html> (July 15, 2002). Already numbering in the billions, total online retail sales also virtually doubled in just two years—from \$27.3 billion in 2000 to \$44.1 billion in 2002. eMarketer’s U.S. Online Holiday Shopping Report, at http://www.emarketer.com/products/report.php?holiday_us_02 (last visited Apr. 1, 2004). Fourth quarter (Christmas) online sales more than doubled from 1999 to 2001, despite a recession in 2001. *Id.*

65. Jacob Sullum, *Return Spam Laws to Sender*, WASH. TIMES, June 2, 2003, <http://www.washingtontimes.com/commentary/20030601-090114-4695r.htm>.

1,000 unsolicited commercial e-mails.⁶⁶ By amending the bill in this way, though, the problem with such a stringent regulation or prohibition of spam was brought into sharp focus. If legislation strictly banned spam and harshly punished spammers, it would require repeated amendments to accommodate new legitimate Internet uses. Once a bill was enacted into law, however, this would become exceedingly difficult.⁶⁷ For example, Congress took almost one year to agree on the terms of the more watered-down CAN-SPAM Act. If past experience dictates, Congress would likely be slow to adopt an amendment to a more inflexible anti-spam statute, and such a delay might cause severe economic repercussions. As California Supreme Court Justice Janice Brown coolly observed, “[I]n the rapidly changing world of technology, in which even technologically savvy providers like America Online and CompuServe are one step behind spammers, the Legislature will likely remain three to four steps behind.”⁶⁸ Thus, as the Internet continues to evolve in ways unforeseen by legislative drafters (not to mention computer companies and technology pundits), legislation on Internet-related issues risks stifling the ever-expanding commercial applications of this new digital domain. This explains why the less-prohibitory CAN-SPAM Act ultimately was favored over the more-restrictive REDUCE Spam Act, because the 108th Congress did not want the ignoble distinction of having been the legislative body that killed the goose that laid the golden egg.

Thus far, the CAN-SPAM Act’s predicted ineffectiveness is being borne out. The CAN-SPAM Act went into effect on January 1, 2004. Businesses and ISPs noted that the spam deluge continued on that date, and has not abated over the first few months of 2004. “Since January 1, we have seen no change in volume. In fact, spam has continued to rise,” reported Susan Larson, vice president of a spam-management company, on February 18, 2004.⁶⁹ One California-based company, Postini Inc., reported that spam entering its network reached an all-time high in the first week of

66. See H.R. 1933, § 4(d)(2), 108th Cong. (1st Sess. 2003). The prominent tech commentator Declan McCullagh reported that Lofgren explicitly amended the REDUCE Spam Act due to the criticisms noted here. McCullagh, *supra* note 59.

67. This observation applies even to the watered-down version of anti-spam legislation, the CAN-SPAM Act. Before Bush signed the Act into law on December 16, 2003, some in Congress were already admitting that “it is quite possible that we will have to revisit this matter again.” *Bush Signs Anti-Spam Bill Into Law*, CNET News.com, at <http://www.msnbc.msn.com/id/3662680> (Dec. 16, 2003) (quoting Rep. John Dingell).

68. *Intel Corp. v. Hamidi*, 30 Cal. 4th 1342, 1374 (2003) (Brown, J., dissenting).

69. Lance Ulanoff, *Spam: A Reality Check*, PC MAG., Feb. 18, 2004, <http://www.pcmag.com/article2/0,4149,1529737,00.asp>.

2004, accounting for 84.9 percent of the processed e-mail.⁷⁰ By February 2004, Brightmail was reporting that 62 percent of all e-mail was spam, which was an increase from 58 percent in December 2003.⁷¹

It may be too early to judge the overall effectiveness of the CAN-SPAM Act, as the FTC has yet to adopt its regulations under the statute.⁷² Moreover, four major ISPs filed hundreds of lawsuits in March 2004 against spammers throughout the country, alleging violations of the new federal law.⁷³ But if the seemingly inexorable rise in the amount of spam in the first several months of 2004 means anything, it suggests that spammers believe that their activities are unaffected by the CAN-SPAM Act.

C. Losing the Litigation: *Intel v. Hamidi*

The third response to spam—litigation against spammers using the trespass to chattels doctrine—suffered a serious blow in the 2003 decision in which Justice Brown made her prophetic remark (in dissent) about the inherent lag between technological advances and legislative responses.⁷⁴ In *Intel Corp. v. Hamidi*,⁷⁵ the California Supreme Court overturned two lower court decisions and rejected Intel's claim that a disgruntled former employee, Kourosh Hamidi, committed "trespass to chattels" by sending unsolicited e-mails critical of the company to thousands of Intel employees.

The *Hamidi* decision deserves attention because it represents the apex of the development of the archaic doctrine of trespass to chattels as a litigation tool against spammers. The significance of *Hamidi* is two-fold. First, Intel cannot be faulted for its litigation strategy in this case because plaintiff ISPs and other businesses successfully had used trespass to chattels against spammers for many years prior to *Hamidi*.⁷⁶ Based on this fa-

70. Jonathan Krim, *Spam is Still Flowing into E-Mail Boxes*, WASH. POST, Jan. 6, 2004, at E1, available at <http://www.washingtonpost.com/wp-dyn/articles/A57315-2004Jan5.html>.

71. Saul Hansell, *Four Big Internet Providers File Suits to Stop Spammers*, N.Y. TIMES, Mar. 11, 2004, at A1, available at <http://www.nytimes.com/2004/03/11/technology/11spam.html>.

72. See MacMillan, *supra* note 11 (reporting that the FTC is still "developing regulations for implementing the law"). As a spokesperson for Sen. Ron Wyden, a co-sponsor of the CAN-SPAM Act, stated on March 17, 2004: "It's premature to judge the effectiveness of the Can-Spam Act 77 days after it becomes effective." *Id.*

73. Hansell, *supra* note 71 (reporting on the coordinated lawsuits filed by AOL, Earthlink, Yahoo, and Microsoft).

74. See *supra* note 68 and accompanying text.

75. 30 Cal. 4th 1342 (Cal. 2003).

76. See *Am. Online, Inc. v. LCGM, Inc.*, 46 F. Supp. 2d 444 (E.D. Va. 1998); *Am. Online, Inc. v. IMS*, 24 F. Supp. 2d 548 (E.D. Va. 1998); *Hotmail Corp. v. Van\$ Money*

avorable precedent, Intel prevailed before the trial court and on direct appeal.

Intel's initial success in the lower courts and its loss before the California Supreme Court also illustrates the second significant aspect about the *Hamidi* decision. Intel lost in the final round of appeals, because the California Supreme Court diverged from the anti-spam case law that had developed over the past seven years by requiring plaintiffs to prove that they have suffered *substantial interference* with their networks in order to recover against spammers. This reveals a fundamental doctrinal flaw in framing the harm caused by spam as a *trespass*. As all first-year law students learn in their property courses, trespass does not have a substantiality requirement, as it protects a property owner's absolute right to exclude. *Hamidi* thus reveals that the courts view the harm caused by spam as a *nuisance* injury, not a trespass. This was best exemplified in the *Hamidi* court's attempt to mollify concerns that the new substantial-interference requirement would not undermine "legal remedies of Internet service providers (ISP's) against senders of unsolicited commercial bulk e-mail (UCE), also known as 'spam.'"⁷⁷ Do not worry, the court intoned, as "unsolicited commercial bulk e-mail" is always substantial enough to justify a finding of trespass to chattels. Underlying the legal trespass analysis, such comments reveal the courts are in fact *conceptualizing* the property entitlement that is being infringed by spammers as one that is protected by nuisance doctrine—the right to use and enjoy one's property without substantial and unreasonable interference. This doctrinal confusion unsettles *ex ante* expectations and creates incoherency and indeterminacy in the developing case law governing the Internet.

As noted, Intel was justified by the extant case law in asserting trespass to chattels against *Hamidi*. The common law doctrine of trespass to chattels was reintroduced into modern jurisprudence in the 1996 California case, *Thrifty-Tel, Inc. v. Bezenek*,⁷⁸ which specifically addressed the issue of protecting computer networks from unauthorized access or use by third parties. In *Thrifty-Tel*, a young computer hacker was held liable for

Pie Inc., No. C-98 JW PVT ENE, C 98-20064 JW, 1998 WL 388389 (N.D. Cal. Apr. 16, 1998); *CompuServe Inc. v. Cyber Promotions, Inc.*, 962 F. Supp. 1015 (S.D. Ohio 1997). eBay also successfully used trespass to chattels to sue an Internet company that was searching eBay's auctions without authorization. *See eBay, Inc. v. Bidder's Edge, Inc.*, 100 F. Supp. 2d 1058 (N.D. Cal. 2000).

77. *Hamidi*, 30 Cal. 4th at 1348.

78. 46 Cal. App. 4th 1559 (1996). All of the Internet cases holding spammers or other offending persons liable for trespass to chattels have relied on *Thrifty-Tel*, *see supra* note 76. Notably, the *Hamidi* court barely acknowledges the existence of *Thrifty-Tel*.

accessing a local telephone company's network, although he hacked the computer network only a limited number of times over the span of about six to seven hours.⁷⁹ The evidence of damage, if it could even be called that, was limited and largely circumstantial: the defendant "overburdened the [plaintiff's] system, denying some subscribers access to phone lines" during the short period in which he queried the system looking for the codes to make unauthorized telephone calls.⁸⁰ The plaintiff "presented no evidence of actual losses,"⁸¹ relying instead on regulatory tariffs governing unauthorized use of a phone system to establish damages.⁸² The defendant in *Thrifty-Tel* was found liable for trespass to chattels solely because he gained unauthorized access to plaintiff's computer network. In reviving the trespass to chattels doctrine in the new digital world, *Thrifty-Tel* established that liability was predicated on only "an intentional interference with the possession of personal property [that] has proximately caused injury," regardless of how negligible this "injury" might be.⁸³

The cases following in the wake of *Thrifty-Tel* set equally low damage thresholds for finding defendants liable for trespass to chattels. Each successive court ruling found defendants liable on no more evidence than *some* interference with plaintiffs' computer networks, regardless of the actual losses asserted by plaintiffs.⁸⁴ In one illustrative case, CompuServe (an ISP) obtained a preliminary injunction against a spammer on the basis of trespass to chattels. CompuServe obtained the injunction solely on the basis of asserting that the spammer's use of disk space and processing power showed that "the value of that equipment to CompuServe is diminished even though it is not physically damaged by defendants' conduct."⁸⁵

79. *Thrifty-Tel*, 46 Cal. App. 4th at 1564.

80. *Id.*

81. *Id.* at 1564.

82. *Id.*

83. *Id.* at 1566.

84. In one case litigated by AOL, the ISP evidenced that a spammer was responsible for sending more than 92 million emails, which consumed server capacity, caused technical costs, reduced the functioning of AOL's server for its clients, and generated more than 450,000 complaints by AOL customers, which indirectly damaged AOL's goodwill. *See Am. Online, Inc. v. LCGM, Inc.*, 46 F. Supp. 2d 444, 448-49 (E.D. Va. 1998). In another AOL case, the ISP submitted evidence that the spammer sent over 60 million emails, causing technical staff to be redirected to "defend" against his spam, generating more than 50,000 complaints from customers and again damaging AOL's goodwill. *See Am. Online, Inc. v. IMS*, 24 F. Supp. 2d 548, 549 (E.D. Va. 1998). In neither case did AOL offer evidence of substantial, direct monetary damages caused by the spam.

85. *CompuServe Inc. v. Cyber Promotions, Inc.*, 962 F. Supp. 1015, 1022 (S.D. Ohio 1997).

The lack of any requirement of actual damages is striking, but understandable because the cause of action is a type of trespass.

As the legal standard for a trespass action is interference with exclusive possession, the *extent* of harm resulting from this interference is not relevant in determining liability.⁸⁶ The *Hamidi* court correctly noted that trespass to chattels requires an injury proximately caused by the alleged tortfeasor's interference with the *possession* of the plaintiff's chattel,⁸⁷ but the court then concluded that it was relevant that Intel suffered only *indirect* and *consequential* harms from Hamidi's e-mails. In fact, Intel's injuries were quintessential examples of the harms suffered in previous trespass to chattels cases, such as the cost of redeploying tech support personnel to block e-mails and projected losses in employee productivity resulting from the time spent reading or deleting Hamidi's e-mails.⁸⁸ Still, the court held that it was dispositive that Intel's exclusive possession of its network—the central issue in any trespass claim—was not damaged or substantially interfered with in any way. As the court poignantly observed: “Reading an e-mail transmitted to equipment designed to receive it, in and of itself, does not affect the possessory interest in the equipment.”⁸⁹ But substantially interfering with a possessory interest is *irrelevant* in determining whether a trespass has occurred—the interference *as such* establishes liability because “any loss of possession by the plaintiff is regarded as necessarily a loss of something of value, even if only for a brief interval.”⁹⁰

By focusing on the extent of both the interference and the resulting harm, the *Hamidi* court required that Intel demonstrate *substantial interference* with the *use* of its property—in other words, Intel was required to prove that Hamidi was liable for *nuisance*, not trespass. But that is not the

86. WILLIAM PROSSER ET. AL., PROSSER AND KEETON ON TORTS § 14, at 87 (5th ed. 1984) (noting that “any loss of possession by the plaintiff is regarded as necessarily a loss of something of value, even if only for a brief interval—so that wherever there is found to be dispossession . . . the requirement of actual damages is satisfied”). Justice Brown also cogently describes how the majority opinion, by requiring a showing of substantial harm, contradicts—and emasculates in practice—the doctrine of trespass to chattels. *Hamidi*, 30 Cal. 4th at 1367-85 (Brown, J., dissenting).

87. *Hamidi*, 30 Cal. 4th at 1350-51.

88. *Id.* at 1349, 1352-53 (noting that Intel submitted *uncontroverted* evidence that employees requested that the company block emails from Hamidi and that Intel's technical support staff spent “time and effort” in attempting to do so). *See supra* note 84 (detailing similar evidence of harms caused to plaintiffs' networks in past trespass to chattels cases).

89. *Id.* at 1359 (quoting *Intel Corp. v. Hamidi*, 94 Cal. App. 4th 325 (2001) (Kolkey, J., dissenting)).

90. PROSSER § 14, *supra* note 86, at 87.

cause of action with which Intel obtained a judgment against Hamidi, nor is this required in pleading trespass to chattels. By entertaining claims for trespass to chattels against spammers for what is actually conceived of as a nuisance injury, courts are creating doctrinal confusion. Based on the trespass to chattels case law, Intel was justified in spending substantial resources in litigation against Hamidi. Also, given the divergence between the *Hamidi* and *Thrifty-Tel* decisions, as well as the other trespass to chattels cases decided between these two momentous cases, it is now unclear how much spam is actionable, and whether other jurisdictions will follow California.

This doctrinal confusion is the second reason for the significance of the *Hamidi* decision. The *Hamidi* court's choice to cherry-pick a pleading requirement from nuisance and graft it onto the trespass to chattels doctrine was driven by the substantial academic criticism of the past court decisions applying trespass to chattels in Internet cases.⁹¹ Commentators have maintained that trespass is "too broad a claim,"⁹² which, according to one oft-cited article relied on by the *Hamidi* court,⁹³ requires judges to employ "legal gymnastics" in adopting the "fiction of impinging electrons" as the *sole* criterion for liability in trespass to chattels cases.⁹⁴ If *any* "impinging electron" creates the fiction of "disposing" an ISP or business from its computer network, then how are courts to distinguish abhorrent spam from innocuous, albeit unauthorized, electronic signals? Trespass to chattels does not provide an answer to this question, but only because it is not the function of any trespass doctrine to this question.⁹⁵

As one dissenting judge on the California Court of Appeal sardonically explained the logic of extending trespass in this area:

Under Intel's theory, even lovers' quarrels could turn into trespass suits by reason of the receipt of unsolicited letter or calls from the jilted lover. Imagine what happens after the angry lover

91. See, e.g., John D. Saba, Jr., *Internet Property Rights: E-Trespass*, 33 ST. MARY'S L.J. 367 (2002); R. Clifton Merrell, Note, *Trespass to Chattels in the Age of the Internet*, 80 WASH. U. L.Q. 675 (2002); Mary Anne Bendotoff & Elizabeth R. Gosse, *Stay Off My Cyberproperty!: Trespass to Chattels on the Internet*, 6 INTELL. PROP. L. BULL. 12 (2001); Burk, *supra* note 19. For a more limited criticism of the courts' use of trespass to chattels only as a "cure-all" doctrine without imposing proper limitations on its application, see Edward W. Chang, *Bidding on Trespass: eBay, Inc. v. Bidder's Edge, Inc. and the Abuse of Trespass Theory in Cyberspace Law*, 29 AIPLA Q. J. 445 (2001).

92. Saba, Jr., *supra* note 91, at 402. This claim is further explored in Parts IV and V.

93. *Hamidi*, 30 Cal. 4th at 1358 (quoting Burk, *supra* note 19, at 35, 37).

94. Burk, *supra* note 19, at 40 (comparing this to similar problems in adjudicating intellectual property entitlements in digital media).

95. How nuisance doctrine escapes this problem is discussed *infra* Part V.

tells her fiancé not to call again and violently hangs up the phone. Fifteen minutes later the phone rings. Her fiancé wishing to make up? No, trespass to chattels.⁹⁶

By agreeing with this dissent and reversing the appellate court, the California Supreme Court demanded that a plaintiff pleading trespass to chattels show harms similar to “the burdens and costs caused ISP’s and their customers by the ever-rising deluge of commercial e-mail.”⁹⁷ Yet this takes the court out of trespass doctrine and into the traditional requirements of nuisance doctrine, in which *substantial interference* with the use of one’s property is a prerequisite for stating a claim.

Ironically, the *Hamidi* court chided Richard Epstein’s arguments in an amicus brief that trespass rules should be extended to the Internet based on a “metaphorical application of real property rules.”⁹⁸ The court contended that “such fictions promise more confusion than clarity in the law.”⁹⁹ The same charge of “confusion,” though, can be leveled at the *Hamidi* court for conflating requirements from two separate legal actions for protecting property rights—trespass and nuisance.¹⁰⁰ The distinction between trespass and nuisance is already marked with confusion.¹⁰¹ The courts should not muddle the law any more than it already is, leaving ISPs and businesses uncertain of their legal rights and remedies.¹⁰² This is particularly true in the context of the Internet, a fast-growing and somewhat unruly domain in dire need of legal guidance and the protection of the rights of its netizens.

In the last analysis, the *Hamidi* court simply balked in the face of the basic requirement of trespass doctrine that *any* uninvited encroachment of plaintiff’s property creates liability for the defendant. The logic of relying on trespass to redress harms caused by spam was leading the courts into a

96. *Intel Corp. v. Hamidi*, 94 Cal. App. 4th 325, 348 (2001) (Kolkey, J., dissenting), *rev’d*, *Intel Corp. v. Hamidi*, 30 Cal. 4th 1342 (2003).

97. *Hamidi*, 30 Cal. 4th at 1356.

98. *Id.* at 1360-61.

99. *Id.* at 1361.

100. *Cf.* *Johnson v. La. Dep’t of Educ.*, 330 F.3d 362, 365-71 (5th Cir. 2003) (Wiener, J., dissenting or specially concurring), *reh’g en banc granted*, 343 F.3d 732 (5th Cir. 2003), (criticizing the majority opinion for conflating two separate tests for determining a state’s waiver of its sovereign immunity).

101. PROSSER § 13, *supra* note 86, at 69.

102. *Cf.* THE FEDERALIST NO. 62, at 287-88 (James Madison) (Clinton Rossiter ed., 1961) (discussing the benefits of stability in public policy, and noting that the “internal effects of a mutable policy are still more calamitous. It poisons the blessings of liberty itself. . . . Law is defined to be a rule of action: but how can that be a rule, which is little known, and less fixed?”)

dizzying and unsettling realm of legal fiction in which ISPs and other businesses are “dispossessed” of their computer networks by a single, uninvited, infringing electron. Worse yet, trespass doctrine provided no means to limit the scope of this liability. Rather than face these uncomfortable facts, the *Hamidi* court chose the easy way out: affirming the use of trespass to chattels, but making a further mess of the law by requiring courts in California to now treat digital trespass as a *de facto* nuisance. Why not simply treat spam as a *de jure* nuisance?

IV. RETHINKING THE LITIGATION STRATEGY: SPAM AS NUISANCE

Notably, Intel originally pleaded both nuisance and trespass to chattels in its complaint against Hamidi. However, Intel voluntarily dismissed the nuisance claim before the trial court ordered summary judgment on its behalf.¹⁰³ Intel likely pleaded both nuisance and trespass because its counsel was acting properly as an advocate, claiming that the defendant breached two alternative legal entitlements.

Why then did Intel voluntarily dismiss the nuisance claim? Although none of the court opinions indicate why the nuisance claim was dismissed, one can infer an answer from the definition of a “private nuisance.” The Restatement of Torts defines a “private nuisance [as] a nontrespassory invasion of another’s interest in the private use and enjoyment of land.”¹⁰⁴ To understand this definition, it is necessary to distinguish the different legal rights protected by the complementary actions of nuisance and trespass. A nuisance is a substantial and unreasonable interference with the use and enjoyment of land, and a trespass is an act that dispossesses the rightful owner from his land. Historically, courts described the difference between interference and dispossession in terms of “intangible” versus “tangible” invasions of land—the distinction between dust particles floating over land versus a person stepping onto it—but this method of differentiating nuisance and trespass has long since been abandoned in most jurisdictions.¹⁰⁵ Nonetheless, courts continue to distinguish nuisance from trespass inasmuch as nuisance-type disturbances constitute only “low-

103. *Hamidi*, 30 Cal. 4th at 1349-50.

104. RESTATEMENT (SECOND) OF TORTS § 821D (1979); *see also* Richard A. Epstein, *Nuisance Law: Corrective Justice and Its Utilitarian Constraints*, 8 J. LEGAL STUD. 49, 53 (1979) (“Nuisances are invasions of the plaintiff’s property that fall short of trespass but which still interfere in the use and enjoyment of land.”).

105. *See* *Borland v. Sanders Lead Co.*, 369 So. 2d 523, 529 (Ala. 1979) (noting that the “tangible” versus “intangible” distinction is no longer dispositive in determining whether an unlawful intrusion is a trespass or nuisance).

level invasions”¹⁰⁶ that fall short of directly taking physical possession of the land itself.¹⁰⁷ Accordingly, courts typically frame the now-dominant distinction as follows: “If the intrusion interferes with the right to exclusive possession of property, the law of trespass applies. If the intrusion is to the interest in use and enjoyment of property, the law of nuisance applies.”¹⁰⁸ Regardless of whether an owner is seeking to protect the right to use (nuisance) or the right to exclusive possession (trespass), the property that is at issue is real property—land.

If one considers only the abstract definition of nuisance and ignores how it applies in practice, these broad doctrinal statements suggest that pleading nuisance against spammers is a non-starter because spam does not interfere with land. Even the *Hamidi* court pointed out what it thought was obvious: the “plain fact is that computers, even those making up the Internet, are . . . personal property, not realty.”¹⁰⁹ Who could deny this plain fact? Computers are chattels. The networks created by computers exist only in the wires that connect the computers together. Wires, like computers, are chattels. E-mail consists of programming code and electronic signals transferred over wires between computers. The Internet is a world comprised solely of chattels. The question naturally arises: in a spam lawsuit, where is the land that the spammer is interfering with, hindering, or obstructing use and enjoyment of? It’s just chattels all the way down.¹¹⁰

106. RICHARD A. EPSTEIN, *TAKINGS* 230 (1985) (distinguishing the type of invasion to property required by nuisance versus trespass).

107. PROSSER § 13, *supra* note 86, at 70 (noting that “an intentional and nontrespassory interference with the use and enjoyment of another’s real property is actionable as a private nuisance,” and that “[a]ny physical entry upon the surface of the land is a trespass”).

108. *Borland*, 369 So. 2d at 529; *see also Carrigan v. Purkhiser*, 466 A.2d 1243, 1243-44 (D.C. App. 1983) (holding that trespass and nuisance are distinguished on the basis of whether a defendant interferes with *possession* or *use* of land); *Exxon Corp. v. Yarema*, 69 Md. App. 124, 148 (1986) (“Nuisance is not contingent upon whether the defendant physically impinged on plaintiff’s property, but whether the defendant substantially and unreasonably interfered with plaintiff’s use and enjoyment of its property.”).

109. *Hamidi*, 30 Cal. 4th at 1361.

110. I am referring here to the famous philosopher’s joke about an exchange between a philosophy professor and a student studying metaphysics. They are discussing the problem of infinite regress and how philosophers answer this with such conceptions as metaphysical “essences,” and the student tells his professor that the universe rests on the back of a giant turtle. The professor asks a logical question: what does the turtle stand on? The student answers: another giant turtle. And that turtle, asks the professor. Naturally, answers the student, another turtle. The professor asks again: and what does that turtle stand on? The student answers: you don’t understand, it’s just turtles all the way down. *See* Roger C. Cramton, *Demystifying Legal Scholarship*, 75 *GEO. L.J.* 1, 1-2 (1986) (identify-

But is it really? Computer networks do not float in the ether, nor does the e-mail that travels through them. Computers—whether mainframes, desktops or notebooks—are machines used by companies in their business operations. For Internet companies, such as an ISP, their computers *are* their business. Without their computers, AOL or CompuServe have no product to offer to their customers—no connection service to the Internet or storage capacity for hosting websites and databases. The same holds true for firms that sell software or computer consulting services, such as Intel, Microsoft and PeopleSoft. Without their computers and networks, these firms have no commercial function. Traditional brick-and-mortar (“old economy”) firms have also integrated computers into their production processes, and their computers are now as vital to their successful operation as are the robots working in their manufacturing plants or the copying machines used by their office employees. Computers are a necessary, omnipresent fact in the business operations of virtually all commercial firms today.

Simply put, it is not chattels all the way down. Computers and computer networks are chattels, but these chattels are integral and necessary tools for the productive use of real property by a commercial firm. In this sense, computers are analogous to the animals that constitute a farmer’s use of his property or the production-line machines that likewise constitute an industrial firm’s use of its property. Maintaining that the sole legal wrong committed by spammers is trespass to chattels is an exercise in over-abstraction, and certainly a legal fiction. For ISPs and other businesses, day-to-day operations are significantly hindered by spam, which constitutes a substantial and unreasonable interference with their use and enjoyment of their real property. When land is dedicated to commercial goals that are achieved only with computers, the interference with the use of these computers is *ipso facto* an interference with the use of the land.

It is unnecessary to engage in the same rationalistic and formalistic treatment of legal terminology that led to using trespass to chattels in spam cases in order to expose its folly. Moving beyond simple definitions and looking at both the commentary and the cases, it becomes clear that nuisance has always been applied to redress harms caused to chattels in the use of real property. The commentary in the Restatement of Torts, for instance, provides that “[t]he phrase ‘interest in the use and enjoyment of land’ is used in this Restatement in a *broad sense*. It comprehends . . . the

ing the source of this story in the work of William James, one of the originators of pragmatism).

interests that a person may have in the actual present use of land for residential, agricultural, *commercial*, *industrial* and other purposes.”¹¹¹

The traditional applications of nuisance universally confirm this broad reading of “use and enjoyment of land.” While some nuisance cases entail a tangible or physical invasion of land,¹¹² the typical nuisance cases are those in which ephemeral interferences substantially and unreasonably prevent a land-owner from using and enjoying chattels for personal or commercial purposes, regardless of whether those chattels are machines, products, animals, or crops. A quick review of modern nuisance cases reveals claims involving: cement dust interfering with the functioning of a lumber yard;¹¹³ smoke and spray paint from a shipyard interfering with an automobile company’s production of new cars;¹¹⁴ construction of a bank disrupting customer access to a store at a shopping mall;¹¹⁵ annoyance and discomfort affecting homeowners of a neighbor who kept “junk” cars in his front yard;¹¹⁶ emission of gas and airborne particles from a copper smelter interfering with a husband and wife’s use and enjoyment of their home;¹¹⁷ noxious odors, flies, and dust from a cattle feedlot interfering with the agricultural use of neighboring farmland;¹¹⁸ and pesticide blown by winds from a farm damaging a neighboring farm’s bean crop.¹¹⁹ The Oregon Supreme Court affirmed a nuisance verdict against a telephone company that negligently listed a homeowner’s telephone number as an

111. RESTATEMENT (SECOND) OF TORTS § 821D cmt. b (emphases added).

112. *See* *Canton v. Graniteville Fire Dist. No. 4*, 171 Vt. 551 (2000) (flooding of basement); *Holmberg v. Bergin*, 172 N.W.2d 739 (Minn. 1969) (encroaching tree); *Graham v. Lowden*, 15 A.2d 69 (Me. 1940) (erecting a building on plaintiff’s land).

113. *Jefferson Lumber & Concrete Prods., Inc. v. Jimco, Inc.*, 217 So. 2d 721 (La. Ct. App. 1969).

114. *Nissan Motor Corp. v. Md. Shipbuilding & Drydock Co.*, 544 F. Supp. 1104 (D. Md. 1982), *aff’d*, 742 F.2d 1449 (4th Cir. 1982). In this case, the district court ruled that Maryland Shipbuilding was not liable for nuisance only because “the utility of defendant’s conduct outweighs the gravity of the occasional harm which Nissan has sustained.” 544 F. Supp. at 1118. Of course, this meant that the smoke and spray paint was interfering with the use of Nissan’s property, but only that it was not deemed substantial after the requisite utility calculus.

115. *Great Atlantic & Pac. Tea Co., Inc. v. LaSalle Nat’l Bank*, 77 Ill. App. 3d 478 (1979) (reversing trial court’s dismissal of nuisance claim and remanding for trial).

116. *Foley v. Harris*, 223 Va. 20 (1982).

117. *Bradley v. Am. Smelting & Refining Co.*, 104 Wash. 2d 677 (1985) (certifying question from federal district court that plaintiffs could plead both trespass and nuisance claims).

118. *Scott v. Jordan*, 99 N.M. 567 (N.M. Ct. App. 1983).

119. *Hall v. Phillips*, 231 Neb. 269 (1989) (reversing summary judgment for plaintiff only on grounds of outstanding factual issues concerning the unreasonableness of defendant’s actions).

after-hours florist, which resulted in severe emotional distress arising from “an invasion of plaintiff’s right to enjoy her property without unreasonable interference.”¹²⁰ In 1996, the Wisconsin Supreme Court, reversing an appellate court’s ruling to the contrary, affirmed a nuisance verdict against a defendant electrical company whose power lines produced stray electrical voltage that harmed a farmer’s dairy herd.¹²¹

How can it be that stray electrons interfering with the milk production of a farmer’s dairy herd are a nuisance, but electrons intentionally sent over wires in the form of e-mail that interfere with the operation of a company’s computer network are not? If injuries suffered to automobiles, lumber, crops, cattle, as well as general annoyance injuries caused by unsightly junk cars or excessive late-night telephone calls, are sufficient for a successful nuisance claim, then so are injuries suffered to computers and business operations by e-mail. To distinguish between computers and other chattels is inconsistent with long-standing commentary and case law on the “broad property interest” that is protected by the doctrine of private nuisance.

The injuries suffered by ISPs and businesses are classic examples of a nuisance injury, not a trespass injury. ISPs and businesses are not dispossessed of their networks; spammers are not literally coming into their offices to seize or even to hijack their networks. ISPs and business are suffering from *substantial and unreasonable interference* with the use of their computer networks, which is literally a substantial and unreasonable interference with their normal business operations.¹²²

The amount of spam is simply staggering. As noted earlier, spam now numbers in the hundreds of billions.¹²³ One notorious spammer claims he can send from 50 to 250 million e-mails in a single day.¹²⁴ Others are believed to send merely 30 to 40 million e-mails each day.¹²⁵ But this is only

120. *Macca v. Gen. Tel. Co. of N.W., Inc.*, 262 Or. 414, 418 (1972).

121. *Vogel v. Grant-Lafayette Elec. Coop.*, 548 N.W.2d (Wis. 1996). *See also* *Page County Appliance Ctr., Inc. v. Honeywell, Inc.*, 347 N.W. 2d 171 (Iowa 1984) (reversing on evidentiary issues a nuisance verdict against an electronics vendor whose computers were “leaking radiation” that interfered with television signals in nearby appliance store).

122. RESTATEMENT (SECOND) OF TORTS § 821F, cmt. g (noting that “[s]ignificant harm is necessary for a private nuisance”); *see also id.* § 822 (requiring some type of liability-forming conduct on the part of the defendant, such as intentional, unreasonable, or reckless conduct).

123. *See supra* notes 4-7, and accompanying text.

124. *See World’s Top 10 Spammers*, *supra* note 29 (speaking of Eddy Marin, a spammer based in Boca Raton, Florida).

125. Sullivan, *supra* note 33 (identifying Juan Garavaglia, a spammer known as “Super-Zonda”).

what a single person or company can do; there are hundreds, if not thousands, of spammers around the world who believe in their “God-given right to spam.”¹²⁶ The results of their activities are painfully clear. A representative from BellSouth Internet Group testified at the 2003 FTC Spam Forum that approximately 75 percent of its inbound e-mail traffic is spam, and that this accounted for 60 percent of all of BellSouth’s e-mail processing activities on its network.¹²⁷ BellSouth is probably suffering more than most ISPs, but only by a little. In mid-2003, Brightmail found that about 48 percent of all e-mail sent each day is spam.¹²⁸ By January 2004, Brightmail found that spam accounted for approximately 60 percent of the e-mail it handled.¹²⁹ Another study revealed that spam accounted for almost two-thirds of all business e-mail sent in December 2003, up from approximately 50 percent of all business e-mail traffic in May 2003.¹³⁰

The ISPs have responded by investing increasingly more resources to stop the onslaught—hiring more personnel, directing existing personnel to work on spam issues, and purchasing filtering software or services. The filter used by Hotmail must be upgraded every 10 minutes in order to incorporate the new data required to continue blocking the flood of spam.¹³¹ And yet spam continues to pour into ISP networks, resulting in high costs to manage it. In 2001, Verizon sued a notorious spammer for \$37 million for twice paralyzing the company’s network with a deluge of bulk e-mail.¹³² BellSouth’s costs in dealing with spam rose 500 to 700 percent from 2000 to 2002, and then doubled from 2002 to 2003.¹³³ These costs included lost productivity and expenses incurred in system overhead, buying and running anti-spam filtering software, hiring personnel, producing educational materials, and providing additional customer support.¹³⁴ With

126. *World’s Top 10 Spammers*, *supra* note 29 (quoting Mike Cunningham, one of the “top 10” spammers of 2003, who made this statement on a Usenet discussion group).

127. Malik, Presentation Slides of Testimony at the FTC Spam Forum, *supra* note 17. Except for the information cited in note 135, all of the data concerning BellSouth is taken from this source.

128. Glassman, *supra* note 31.

129. Krim, *supra* note 70.

130. *Bush Signs Anti-Spam Bill Into Law*, *supra* note 67 (referring to a study by e-mail security company, MessageLabs).

131. Glassman, *supra* note 31.

132. *World’s Top 10 Spammers*, *supra* note 29 (discussing the exploits of Alan Ralsky, who ultimately settled with Verizon in 2002, which included a promise by him to stop sending spam over Verizon’s network).

133. Malik, Presentation Slides of Testimony at the FTC Spam Forum, *supra* note 17.

134. Chris Lewis, Transcript of Testimony at FTC Spam Forum (Matter No. P024407), at 79, *available at* http://www.ftc.gov/bcp/workshops/spam/transcript_day2.pdf (May 1, 2003) (breaking spam costs down into costs associated with bandwidth us-

thousands of customers, BellSouth estimates that it spends from \$3 to \$5 per customer on spam, a cost it must absorb because the hyper-competitive nature of the ISP market means that it cannot raise prices without losing its customer base.¹³⁵ Smaller ISPs are in worse straits. A representative from Aristotle, Inc., a small Arkansas-based ISP with only 26,000 customers, testified at the 2003 FTC Spam Forum that 65 to 70 percent of the e-mail it receives is spam.¹³⁶ Aristotle estimated that overall costs directly attributable to spam were approximately \$5 per customer, almost the entire amount of a one-month subscription rate of \$6.¹³⁷ Thus, at 26,000 customers, Aristotle is suffering recurring annual damages of approximately \$130,000. A representative from NortelNetworks testified at the 2003 FTC Spam Forum that 80 percent of its bandwidth costs are attributable to spam, and that it operates entire servers dedicated solely to fighting spam.¹³⁸ Despite the dedicated filtering servers, somewhere between 5,000 and 10,000 spams get past its filters on a daily basis,¹³⁹ and that each one costs NortelNetworks approximately \$1 in lost productivity.¹⁴⁰ According to its testimony before the FTC, NortelNetworks is incurring spam-related damages *each day* of approximately \$5,000 to \$10,000,¹⁴¹ which amounts to annual damages of approximately \$1.8 to \$3.6 million. This is what it means in exact dollar terms when one columnist stated in the abstract that the “costs of spam are paid mostly by Internet service providers (ISPs), which are forced to invest in extra capacity and maintain filtering systems.”¹⁴²

age, additional equipment, hiring additional staff, and reputational effects); Dale Malik, Transcript of Testimony at FTC Spam Forum (Matter No. P024407), at 92, *available at* http://www.ftc.gov/bcp/workshops/spam/transcript_day2.pdf (May 1, 2003) (noting that of “software, hardware, and abuse desk,” most of the cost attributable to spam is software-related).

135. Malik, Transcript of Testimony at FTC Spam Forum, *supra* note 134, at 88-92.

136. Carl Shivers, Transcript of Testimony at FTC Spam Forum (Matter No. P024407), at 92, *available at* http://www.ftc.gov/bcp/workshops/spam/transcript_day2.pdf (May 1, 2003).

137. *Id.*

138. Lewis, *supra* note 134, at 79.

139. *Id.* at 81. Mr. Lewis further stated that “if our filters weren’t as good as they are, we would be talking a million [unsolicited commercial emails getting through the filters] per day.” *Id.* at 82.

140. *Id.* at 81 (stating that “every e-mail that gets past our filters costs us \$1 in lost productivity”).

141. *Id.* (confirming that spam costs NortelNetworks “approximately \$5,000 to \$10,000 a day”).

142. Sullum, *supra* note 65.

Such substantial harms meet a plaintiff's burden for establishing a nuisance claim, i.e., that a defendant's activities cause *substantial and unreasonable interference* with the plaintiff's use of its property. Spam causes direct damage to computers: network servers crash under the spam onslaught, which in one case caused \$37 million in damages.¹⁴³ Spam also causes numerous consequential damages: additional computer servers purchased to run the filters and store spam before it is deleted, reduced services to paying customers, lost productivity in wasted time of employees, lost productivity resulting from employees' inability to use the company network, and wasted resources spent on redirecting employees to address and prevent these harms. In some cases, these consequential damages run into the millions.¹⁴⁴ Establishing harm for purposes of nuisance would be simple: the documentation that underlies the ISPs' testimony before the 2003 FTC Spam Forum would easily serve as a basis for establishing this element of a nuisance claim. At the very least, such damages are likely far more than the damages incurred in the nuisance cases mentioned earlier to plaintiffs' cattle, crops and other chattels, not to mention the harms of interfering with peaceful sleep and pleasant-looking neighborhoods.¹⁴⁵

It bears noting that identifying spam as a nuisance is not merely an exercise in academic conjecture. At least one court has already ordered legal and equitable remedies against a spammer on the grounds that the spam constituted a nuisance (and a trespass). In *Parker v. C.N. Enterprises & Craig Nowak*,¹⁴⁶ a Texas trial court found that the defendant spammer had used plaintiffs' "flowers.com" domain name without authorization, resulting in plaintiffs being deluged with returned ("bounced," in Internet parlance) e-mails. The ISP hosting the flowers.com web address, also a plaintiff in the case, was helpless as its server crashed under the avalanche of thousands of e-mails coming from the defendants. The court ruled that this "massive, unwanted delivery of the Defendants' garbage to the Plaintiffs' doorstep inflicted substantial harm, including substantial service disruptions, lost access to communications, lost time, lost income and lost opportunities."¹⁴⁷ Moreover, the evidence indicated that defendants continued to send spam using the unauthorized flowers.com return address, causing ongoing harm to the plaintiffs. The court thus ruled that defendants'

143. See *supra* note 132, and accompanying text (discussing Verizon's lawsuit against spammer Alan Ralsky).

144. See *supra* note 140, and accompanying text.

145. See *supra* notes 113-121, and accompanying text.

146. No. 97-06273 (D.C. Travis County Nov. 10, 1997).

147. *Id.*

spamming activities “constituted a common law nuisance and trespass.”¹⁴⁸ Plaintiffs requested and received a permanent injunction against the spammers, as well as payment of actual damages in the amount of \$13,910 and attorneys’ fees in the amount of \$5,000.

The specific injuries recognized by the *Parker* court are the same as those repeatedly identified by ISPs and other companies: “substantial service disruptions, lost access to communications, lost time, lost income and lost opportunities.”¹⁴⁹ And with total damages of approximately \$19,000, this case represents a small fraction of the legal and equitable remedies available to Verizon, NortelNetworks, BellSouth, AOL, Intel, and the litany of other businesses currently suffering hundreds of thousands—if not millions—of dollars in losses attributable to spam.

V. LITIGATING SPAM AS NUISANCE: COST-BENEFIT ANALYSES AND DEFENSES

Although it is seemingly an easy task to frame the injuries caused by spam to ISPs and other businesses as an ongoing substantial and unreasonable interference with their business operations, this does not end the nuisance inquiry. If a plaintiff pursues a nuisance claim against a spammer, a court will balance the utility of the parties’ respective activities against each other. If a plaintiff also requests an injunction, which is likely because most ISPs and businesses simply wish to stop the spam, then a court must similarly “balance the equities.” A court performing this utility calculus may permit some activities to continue unabated (although payment of damages remains a viable remedy) after balancing the benefits of the alleged nuisance-creating activity against its costs. Spammers might also assert the affirmative defense of “coming to the nuisance,” in which a plaintiff asserting a nuisance claim arrived on the scene *after* the alleged nuisance-creating activity had begun. In such cases, as with the balancing of the equities, an activity may cause a substantial and unreasonable interference, but the defendant may escape some of the more harsh results of liability. Finally, there are basic procedural concerns, such as whether spammers are unreachable for purposes of personal service of summons and complaints.

In private nuisance suits in many jurisdictions, courts assess the utility of the parties’ respective activities.¹⁵⁰ Accordingly, a court may determine

148. *Id.*

149. *Id.*

150. RESTATEMENT (SECOND) OF TORTS § 829A (discussing the nuisance test for gravity of harm to plaintiff versus utility of defendant’s behavior and listing cases in

that a defendant's actions result in a *substantial interference* with the use of a plaintiff's property, but that the interference is not unreasonable or that the utility of the defendant's operations outweighs the disutility of its harm.¹⁵¹ This utility assessment gives a court some discretion in determining whether an alleged spamming tortfeasor has committed a sufficiently substantial violation to justify an award of legal or equitable remedies, or both.¹⁵²

In the final analysis, however, this discretionary characteristic of nuisance doctrine is unlikely to relieve the spammer of liability. Although a spammer may invoke the value of his "God-given right to spam,"¹⁵³ a court would balance the value of this "right" against the costs imposed on innocent third parties, such as Verizon's claim for \$37 million damages as a result of the exercising of such a right.¹⁵⁴ The same would be true for the spammers who caused damages to servers and company goodwill in past trespass to chattels cases.¹⁵⁵ A court may find that such damages are substantial enough to justify finding the spammer's activities unreasonable as

various jurisdictions). *But see* *Jost v. Dairyland Power Coop.*, 45 Wis. 2d 164, 174-5 (1969) (noting in nuisance case that the court knows of no damages rule in Wisconsin that permits someone engaged in important and desirable enterprises to injure with impunity those who are engaged in enterprises of lesser economic significance).

151. RESTATEMENT (SECOND) OF TORTS § 822, cmt. i (noting that "the actor's conduct may have sufficient utility . . . to outweigh a certain quantum of risk to another's use and enjoyment of land"). *See, e.g.*, *Nissan Motor Corp.*, 544 F. Supp. at 1118 (recognizing interference of paint spray with plaintiff's business but holding defendant not liable because "the utility of defendant's conduct outweighs the gravity of the occasional harm which Nissan has sustained"); *Ferguson v. City of Keene*, 111 N.H. 222, 225 (1971) (noting that claim for damages in nuisance suit requires "balancing the utility of the use against the gravity of the harm suffered by the plaintiff"); *Boomer v. Atlantic Cement Co.*, 26 N.Y. 2d 219, 223 (1970) (applying the rule in New York that a nuisance will be enjoined if a utility calculus shows a "marked disparity . . . in economic consequence between the effect of the injunction and the effect of the nuisance"); *Hughes v. Emerald Mines Corp.*, 303 Pa. Super. 426, 441-42 (1982) (affirming in part a nuisance verdict against the defendant because defendant failed to show that the damage caused by its pollution was not unreasonable and that the utility of its conduct outweighed the harm that it caused to the plaintiff).

152. In his brief comments on the possibility of using nuisance to address spam, Burk implicitly invokes the balancing of the equities as an advantage of this doctrine, *see* Burk, *supra* note 19. He says that nuisance is better than trespass because it can "better accommodate the peculiar calculus of benefits and harms in cyberspace." *Id.* at 54.

153. *See supra* note 126.

154. *See supra* note 132, and accompanying text.

155. *See supra* note 84 (detailing nuisance-type injuries in two of the trespass to chattels cases involving an ISP suing a spammer).

a matter of law.¹⁵⁶ If a plaintiff ISP or business suffering the injuries described in the prior section makes it this far in the nuisance analysis, then it seems like an easy sprint to the finish line.

The court's discretion to weigh the respective benefits and costs of each party's actions is also significant because it permits the court to consider variables beyond simple economic or monetary values. As noted earlier, the trespass rule requires a finding of trespass for *any* "impinging electron."¹⁵⁷ This creates over-protection concerns, similar to the specter of over-protection that haunted the REDUCE Spam Act and other proposed legislation.¹⁵⁸ This is why scholars have criticized trespass as "too broad a claim."¹⁵⁹ The deleterious impact on either free speech or the commercial development of the Internet is no less a concern in the context of absolute, exclusionary trespass rules than it is under over-reaching legislation.

A court's cost-benefit assessment, or its balance of the equities, resolves this concern. In applying nuisance, a court has the discretion to distinguish between innocuous or privileged e-mails and truly odious spam—between, for example, e-mail containing constitutionally protected political speech and e-mail sent by mortgage lenders, sellers of Viagra, con-artists, pornographers, and others. A court would also have the ability in adjudicating a nuisance claim to assess the *de minimus* inconvenience caused by the limited number of non-commercial e-mail sent by some netizens, such as the several thousand e-mails sent by Hamidi over Intel's network.¹⁶⁰ In the case of Hamidi, it is a trespass possibly, but it hardly rises to the level of a nuisance, at least by balancing the insignificant damages suffered by Intel against Hamidi's right to use the Internet in ways that are entirely normal and expected of any person paying a monthly access fee.¹⁶¹

156. See RESTATEMENT (SECOND) OF TORTS § 829A cmt. b (1979) (noting that "certain types of harm may be so severe as to require a holding of unreasonableness as a matter of law, regardless of the utility of the conduct").

157. See *supra* note 94, and accompanying text.

158. See *supra* notes 56–65, and accompanying text.

159. See *supra* note 92, and accompanying text (noting how this concern, among other similar criticisms, caused the *Hamidi* court to mangle its trespass analysis).

160. PROSSER § 88, *supra* note 86, at 629 (noting that nuisance liability is "imposed only in those cases where the harm or risk to one is greater than he ought to be required to bear under the circumstances, at least without compensation") (quoting RESTATEMENT (FIRST) OF TORTS, § 822 cmt. j (1939)).

161. See *Borland v. Sanders Lead Co.*, 369 So. 2d 523, 529 (Ala. 1979) (recognizing in nuisance doctrine that "there is a point where the entry is so lacking in substance that

Unlike trespass, nuisance affords spammers another potential defense (beyond asserting the economic or social value of their work): they may claim that a plaintiff “came to the nuisance,” and thus knowingly exposed themselves to a preexisting condition.¹⁶² Unfortunately for the spammers, the scope of this defense is limited and unlikely to succeed. It is not an absolute defense, but simply serves as another factor for the court to take into consideration in weighing the propriety of equitable and legal relief.¹⁶³ Even if the defense is accepted by a court, most ISPs, such as AOL, CompuServe and MSN, offered e-mail services *before* the spam deluge began in earnest, and similarly so for any business that had connected its network to the Internet before spam’s dramatic rise in volume around the turn of the century. Again, nuisance does not force a court to create a legal fiction of a dispossessed network, but rather requires a court to assess the actual impact of the parties’ behavior in both its quantitative and temporal dimensions.

Finally, before an ISP or business could sue a spammer for private nuisance, it must first locate the spammer and serve the individual (or business representative) with a summons and complaint. This raises two potential problems: first, a plaintiff may be unable to locate a potential defendant, particularly when most spammers work behind well-constructed electronic veils of secrecy, and second, if the spammer is located overseas, any potential claim lying in U.S. jurisdictions would be frustrated.

Although it may seem a daunting task with billions of spam flooding the Internet each day, identifying those responsible for creating this nuisance is not as difficult as some might think. For instance, Verizon was

the law will refuse to recognize it, applying the maxim *de minimis non curat lex*—the law does not concern itself with trifles”).

162. *See, e.g.*, Page County Appliance Ctr., Inc., 347 N.W. 2d at 175 (recognizing in nuisance doctrine that “[p]riority of occupation and location—‘who was there first’—is a circumstance of considerable weight”); *Spur Indus., Inc. v. Dell E. Webb Dev. Co.*, 494 P.2d 700, 708 (1972) (affirming an injunction ordered against a nuisance defendant, but requiring the plaintiff to indemnify defendant for the cost of shutting down or moving the business as the plaintiff “brought people to the nuisance to the foreseeable detriment” of the defendant).

163. RESTATEMENT (SECOND) OF TORTS § 840D (noting that this claim is “not in itself sufficient to bar [plaintiff’s] action, but it is a factor to be considered in determining whether the nuisance is actionable”). *See, e.g.*, *Burt v. Beautiful Savior Church of Bloomfield*, 809 P.2d 1064, 1069 (Colo. Ct. App. 1990) (rejecting “moving to the nuisance” defense because this “would, in effect, allow defendant to condemn part of the value of [plaintiff’s] property”); *Patrick v. Sharon Steel Corp.*, 549 F. Supp. 1259, 1267 (N.D.W.V. 1982) (recognizing that the “majority view rejects the doctrine of coming to the nuisance as an absolute defense to a nuisance action”) (quoting *Lawrence v. Eastern Airlines, Inc.*, 81 So. 2d 632, 634 (Fla. 1955)).

able to identify and sue the lone individual who caused its networks to crash twice under a torrent of spam.¹⁶⁴ The numerous ISPs and Internet companies, such as eBay, that have successfully sued in the past for trespass to chattels were also able to identify and serve the persons responsible for damaging their networks and their businesses.¹⁶⁵ Studies indicate that approximately 200 spammers are solely responsible for 90 percent of the world's spam.¹⁶⁶ Given the billions of spam sent out each day, this is an amazingly small number of perpetrators, and it is a list that is easily manageable for a company such as BellSouth or NortelNetworks with the will, the resources, and the substantial interests at stake.

Furthermore, while a plaintiff cannot plead nuisance against a spammer in a foreign country, this is a problem for *any* domestic legal remedy for spam. In any lawsuit or agency enforcement action, the defendant must be identified and served, regardless of whether the charge is a violation of the CAN-SPAM Act, trespass to chattels, or private nuisance.¹⁶⁷ The international dimension of the spam problem can be addressed only through international treaties, regardless of the legal options available under U.S. law.¹⁶⁸ Still, ISPs and other businesses need an effective remedy today against the spammers causing substantial and unreasonable interference with their computer networks. Thus far, the studies indicate, and the case law confirms, that most offenders or at least the most egregious offenders, reside or work within the United States.¹⁶⁹

VI. THE BROADER PERSPECTIVE: HOW TO PROTECT THE PROPERTY ENTITLEMENT AT ISSUE IN SPAM CASES

In reversing the trial and appellate courts' rulings that Hamidi was liable for trespass to chattels, the California Supreme Court revealed that it found the concerns expressed in the academic literature about property

164. See *World's Top 10 Spammers*, *supra* note 132, and accompanying text.

165. See *supra* note 76 (listing trespass to chattels cases).

166. Sullivan, *supra* note 4.

167. See, e.g., Hansell, *supra* note 71 (describing hundreds of lawsuits filed under the CAN-SPAM Act in March 2004 against defendants residing in the United States).

168. See Declan McCullagh, *Be Wary of Washington's Spam Solution*, CNET NEWS.COM (Sept. 9, 2002), at <http://news.com.com/2010-1071-957024.html> (noting criticism of proposed CAN-SPAM Act and REDUCE Spam Act bills pending before Congress that they will only force spammers to go overseas, thereby evading the reach of the federal government).

169. Nancy Anderson, Deputy General Counsel for Microsoft, stated in March 2004 that "[m]ost of the individuals involved in spam live in the United States." Hansell, *supra* note 71.

metaphors in the digital realm to be convincing.¹⁷⁰ Such metaphors require the courts to construct legal fictions of “dispossession” of computers by encroaching ones and zeros of digital code.¹⁷¹ Worse yet, the *Hamidi* court recoiled at the logical implications of holding *any* intruding byte (or even a bit) of code liable for trespass. Although the *Hamidi* court ultimately came to the wrong conclusion, these concerns are legitimate.

Trespass rules protect an absolute and impenetrable property right. It is trespass, more than any other property doctrine, that implements in the law the distinctive Anglo-American social norm that every person’s home is his castle.¹⁷² This explains the lack of any substantiality requirement in finding trespass liability. It is the invasion of the property—the dispossession *per se*—that is the wrong committed, not the extent of the damages resulting from this invasion. If a homeowner wishes to be a hermit, or a student refuses to loan out her bicycle, the law protects these choices absolutely. Both the hermit and the student are secure in the knowledge that they may sue for trespass any person who attempts to dispossess them of their home or bicycle.

This strict protection of the right to exclude is inconsistent with the nature of the property entitlement at issue in a spam case: a computer server that is, by its nature, connected to a world-wide computer network dedicated to the exchange of information. A company that connects to the Internet, or the ISP whose sole service is providing access to the Internet, is arguably consenting to receiving e-mail from third parties. It is not the

170. See *supra* notes 91–100, and accompanying text; see, e.g., Jonathan H. Blavin & I. Glenn Cohen, Note, *Gore, Gibson, and Goldsmith: The Evolution of Internet Metaphors in Law and Commentary*, 16 HARV. J. L. & TECH. 265 (2002) (discussing generally the rise and use of the “internet as real space” metaphor); Mark A. Lemley, *Place and Cyberspace*, 91 CALIF. L. REV. 521, 523 (2003) (discussing in part “why the cyberspace as place metaphor is not a particularly good one”); Michael J. Madison, *Rights of Access and the Shape of the Internet*, 44 B.C. L. REV. 433 (2003) (discussing, in part, the implications of property metaphors applied to the Internet); Edward Lee, *Rules and Standards for Cyberspace*, 77 NOTRE DAME L. REV. 1275 (2002) (critiquing the implicit legal formalism in the use of property metaphors); Maureen A. O’Rourke, *Property Rights and Competition on the Internet: In Search of an Appropriate Analogy*, 16 BERKELEY TECH. L.J. 561, 598–613 (2001) (noting general anticompetitive policy implications in applying property metaphors to the Internet).

171. See *Am. Online, Inc. v. IMS*, 24 F. Supp. 2d 548, 550–51 (E.D. Va. 1998) (holding that defendant did not rebut plaintiff AOL’s claim that “its possessory interest in its computer network [has] been diminished by the bulk e-mailing”).

172. See 2 WILLIAM BLACKSTONE, COMMENTARIES *2 (describing the “right to property” as “that sole and despotic dominion which one man claims and exercises over the external things of the world, in total exclusion of the right of any other individual in the universe”).

right to exclude that is at issue in a spam case,¹⁷³ it is the injuries arising from the *misuse* of the access right granted by the owner.¹⁷⁴ A factory may have the right to produce a minimal amount of pollutants that drift onto neighboring homes, but this does not justify this factory's decision to increase its production of pollutants by a thousand-fold simply because homeowners accept responsibility for the previously produced minimal amounts. The same is true for a computer server processing e-mails from third parties to customers and employees.

In this sense, the doctrine of trespass does not properly reflect the nature of the property entitlement that an ISP or business is attempting to protect. The *Hamidi* court recognized this somewhat in discussing the problems associated with erecting impenetrable virtual "walls" on the Internet, particularly when the *raison d'être* of domains and e-mail addresses is facilitating interaction and communication between customers, employees and third parties.¹⁷⁵ This is the operative fact underlying the spam cases that is obscured by the "dispossession" metaphor of trespass to chattels.¹⁷⁶

Attempting to escape the ill-effects of using trespass to chattels in a case that highlighted the fundamental disconnect between this legal doctrine and the property entitlement at issue in spam cases, the *Hamidi* court made a further mess of the law. The *Hamidi* court trumpeted its rejection of confusing property metaphors,¹⁷⁷ but its decision revealed its own blind

173. This is not to say that in some contexts the strict protection of the right to exclude is a valid means of protecting a property entitlement on the Internet. This is the case with cybersquatting, in which people illegitimately use trademarks on the Internet. *See, e.g.*, *Virtual Works, Inc. v. Volkswagon of Am., Inc.*, 238 F.3d 264 (4th Cir. 2001) (affirming summary judgment for Volkswagon against Virtual Works's use of "vw.net"); *Sporty's Farm L.L.C. v. Sportsman's Mkt., Inc.*, 202 F.3d 489 (2d Cir. 2000) (affirming injunction against domain name owner of "sportys.com" in favor of catalog owner's trademark).

174. *Cf. Bidder's Edge, Inc.*, 100 F. Supp. 2d at 1065-66 (rejecting eBay's analogy to defendant's act as equivalent to an invasion of a "brick-and-mortar store" by robots as an "admittedly formalistic" and "inappropriate" comparison).

175. *Hamidi*, 30 Cal. 4th at 1363 (recognizing loss of "ease and openness of communication and . . . lost network benefits" in treating "undesired communications" on the Internet as a trespass violation); *Id.* at 1364 (rejecting the proposed "rigid property rule of computer server inviolability").

176. *See IMS*, 24 F. Supp. 2d at 550-51 (holding defendant did not rebut plaintiff AOL's claim that "its possessory interest in its computer network [has] been diminished by the bulk e-mailing").

177. *See supra* note 99, and accompanying text.

commitment to a fundamentally confused seven-year-old jurisprudence.¹⁷⁸ Although Justice Cardozo was right to chastise courts who blindly follow metaphors, it is equally wrong for a court to follow blindly an improper legal doctrine in the name of rejecting an improper metaphor.¹⁷⁹

Nuisance sweeps all of these problems aside, because it does not require a court to consider whether a portion of the Internet—more specifically, a website or a company network or an e-mail inbox—is property that is susceptible to being trespassed. To the contrary, nuisance asks a court to consider only whether a computer is a tool that is similar to any other machine or animal used in a company's business operations. And the legal issue before the court in such a case is simply whether the plaintiff's use of that tool has been substantially and unreasonably interfered with by the defendant's activities. Accordingly, nuisance keeps a court focused on objective facts in the real world, and, unlike trespass to chattels, supports a finding of liability only on the basis of such real-world actions. There is no need for a court ruling on a private nuisance claim to find a constructive or metaphorical "dispossession" of a company's computer network by a spammer.

This conclusion is admittedly contrary to the generally prevailing attitude today that nuisance is a doctrinal "morass."¹⁸⁰ This prevailing view explains, in part, the shift to statutory solutions for land-use conflicts, such as zoning, and "the disintegration of private law mechanisms for controlling nuisances."¹⁸¹ This view of nuisance is contrary to the thesis of this Article that a private cause of action for nuisance should be used by ISPs and businesses against the spammers who are interfering with their business operations.

This theoretical criticism of nuisance doctrine is not fatal to this Article's proposal. Irrespective of any *general* theoretical failings in traditional nuisance doctrine, the use of nuisance against spammers can and should work to redress the novel harms arising from the new uses of the Internet and e-mail. As with any common law doctrine, the application of the general rules to particular fact patterns would develop over time, creating a body of law that would define the nature of the legal entitlement that ISPs

178. The *Thrifty-Tel* case was decided in 1996, and thus the use of trespass to chattels in Internet cases was only seven years old at the time of the *Hamidi* decision.

179. See *Berkey v. Third Ave. Ry. Co.*, 244 N.Y. 84, 94 (1926) (Cardozo, J.) (stating eloquently that "[m]etaphors in law are to be narrowly watched, for starting as devices to liberate thought, they end often by enslaving it").

180. Robert G. Bone, *Normative Theory and Legal Doctrine in American Nuisance Law: 1850 to 1920*, 59 S. CAL. L. REV. 1101, 1224-25 (1986).

181. See Epstein, *supra* note 104, at 98.

and businesses have in the unfettered use of their computer networks. Certainly, such a development might also occur with trespass to chattels, and one might argue that this is what the *Hamidi* court was doing: defining the boundaries of trespass doctrine as applied to spam. But if courts *de facto* are treating a problem in one way, while *de jure* defining it in an entirely different way that requires them to create legal fictions and indeterminate distinctions, then it is hardly a knockdown criticism that expressly adopting the *de facto* approach might create problems itself. At least in adopting nuisance, the courts will forthrightly face the real problems in assessing the substantial interference, as well as the costs and benefits associated with this interference.

At a minimum, courts should also correlate their legal analyses and remedies to the legal entitlement at issue. The law is filled with enough complexity and problems; there is no reason to add to them by wrestling with the doctrinal equivalent of using a hammer to do the work of tweezers. Given the somewhat unique correlation between the elements of nuisance and the type of injurious interference with property caused by spam, it would be easier and more efficient for the courts to resolve these problems using the legal tool best suited for the job. Although nuisance might be a messy doctrine *generally*, Ockham's razor recommends it for the *particular* problem of spam.

A more fundamental criticism of pleading spam as nuisance is that this proposal entails the same invalid extension of a traditional common law cause of action as the past application of trespass to chattels to computer servers and websites. Nuisance arose to address substantial, nontrespassory interferences with *land*, whether a farm, a factory or a home. Applying this doctrine to computers, even when cast in terms of interferences with business operations, is at least one degree further removed from land than a cow or a piece of lumber. Obviously, a computer firm or ISP owns land only out of necessity, and not because the land itself is integral to the operation of its business. A cow needs grass and crops need soil; both are intimately connected to land. A computer only needs plastic, metal, and silicon. Thus, maybe computers and their networks really are just a world of chattels.¹⁸²

It is true that applying nuisance to spam would be a novel application of this doctrine, bringing a whole new sphere of economic activity within

182. See Richard A. Epstein, *Cybertrespass*, 70 U. CHI. L. REV. 73, 76 (2003) (“[T]he various equipment and facilities that make up the internet are not by any stretch of the imagination real property. Rather, they are a new form of chattel, which are presumptively governed by the law of trespass to chattels.”).

the ambit of a legal cause of action that arose in entirely different circumstances to redress entirely different harms. But is it not a virtue of the common law system that it is adaptable to changing socio-economic circumstances? This criticism really strikes at the basic question of how a legal system can effectively secure legal entitlements and ensure orderly transaction-facilitating behavior in the midst of radical economic and social transformation. Such a topic is far beyond the limited scope of this Article, and a proper justification of the common law as a default system for defining legal rules in the midst of social and economic transformation would require a lengthy monograph in its own right.¹⁸³

Nonetheless, a few remarks on this subject are in order. At first blush, this criticism actually cuts in favor of a common law solution to the problem of spam, as opposed to enacting legislation or wasting resources on purely defensive technologies that are continuously circumvented. Over the centuries, the common law has survived in Anglo-American jurisdictions precisely because of its highly adaptive capabilities. “The basic common law system of property, tort, contract, and restitution is sensible through[out] changes in scarcity conditions, tastes, and technology. Indeed, the system is sensible precisely because it is a framework for efficient adaptation to changes in scarcity conditions, tastes, and technology.”¹⁸⁴ This is hardly a modern insight. In 1829, Justice Joseph Story praised both the ability of the common law to evolve beyond its origins in the feudal system and its embracing of “general rules, by which rights or actions are to be governed.”¹⁸⁵ Of course, the latter made the former possible.

183. See, e.g., Louis Kaplow, *An Economic Analysis of Legal Transitions*, 99 HARV. L. REV. 509 (1986). Kaplow’s article has sparked a growing field in the academic literature, analyzing the causes and implications of stability in legal doctrines over time. See, e.g., Thomas W. Merrill & Henry E. Smith, *Optimal Standardization in the Law of Property: The Numerus Clausus Principle*, 110 YALE L. J. 1, 37 (2000) (noting that the creation of certain basic and fundamental property rules provides for the efficient development of property regimes over time).

184. Christopher T. Wonnell, *The Noncompensation Thesis and its Critics: A Review of this Symposium’s Challenges to the Argument for not Compensating Victims of Legal Transitions*, J. CONTEMP. LEGAL ISSUES 293, 306 (2003); see also Richard A. Epstein, *Beware of Legal Transitions: A Presumptive Vote for the Reliance Interest*, 13 J. CONTEMP. LEGAL ISSUES 69, 70 (2003) (noting that the presumption of the common law system is that “[w]herever possible try to keep the legal framework constant, and allow the response to societal changes to take place through private adjustments”).

185. Joseph Story, *An Address Delivered Before the Members of the Suffolk Bar, at Their Anniversary on the Fourth of September, 1821, at Boston*, 1 AM. JURIST 1, 1 (1829). This was the inaugural article in the very first American law journal.

The radical transformation of the digital revolution and the rise of the Internet do not necessarily require a similarly radical response by the legal system. The solution to spam is not more likely to be found in new statutes or in new technologies simply because these are as novel as the problem itself. “Let us not vainly imagine,” wrote Justice Story, “that we have unlocked and exhausted all the stores of juridical wisdom and policy.”¹⁸⁶ The common law continues to protect legal entitlements, such as the right to use and enjoy one’s property without substantial interference, and it can continue to redress new forms of injury, such as the harmful effects of spam. The viability of the common law is that it permits private ordering through context-dependent responses in the legal system: private actors invoke general legal rules to redress particular types of harms arising in particular circumstances. This is especially important when the subject matter of legal ordering—the Internet and “high tech” generally—continually outpaces the best efforts of legislators to capture it.¹⁸⁷ Thus, the courts can avoid the problems of over- and under-protection by carefully tailoring their decisions to the circumstances at hand, and do so by calling upon general rules that can assist and guide the relevant parties in their continuing commercial endeavors.

Sometimes the first attempt at a legal solution does not pan out as hoped, as proponents for trespass to chattels discovered in *Hamidi*, but the common law offers several general doctrines for securing the myriad legal property entitlements that exist in our society. Trespass secures the right to exclude and nuisance secures the right to use. Intel’s loss in *Hamidi* indicates that trespass to chattels has led the courts down the proverbial garden path: they were blinded to the proper legal entitlement at issue by the formal elegance of applying the trespass rules. The reasons for the California Supreme Court’s reluctance to affirm trespass liability in *Hamidi* point the way to nuisance.

186. *Id.* at 29.

187. See Bruce P. Keller, *Condemned to Repeat the Past: The Reemergence of Misappropriation and Other Common Law Theories of Protection for Intellectual Property*, 11 HARV. J. L. & TECH. 401, 428 (1998) (noting that “technology in this century has continually outpaced statutory law and litigants have repeatedly turned to judge-made law to protect important rights [A]s the Internet geometrically expands its speed, accessibility, and versatility . . . intellectual property owners again must consider the common law as a source of protection at the end of this century, much as it was at the beginning”).

VII. CONCLUSION

This Article has proposed that ISPs and businesses have missed an important, existing cause of action that may help to remedy the damage caused by spam. Although spammers may believe in their “God-given right to spam,”¹⁸⁸ it is far more relevant to our social and economic interactions that “[t]he ‘great principle of common law’ is that one may not use their property to injure others.”¹⁸⁹ As the FTC concluded in its report to Congress: “spam imposes real costs.”¹⁹⁰ In the economists’ terms, spammers are creating negative externalities through the use of their e-mail accounts. Nuisance doctrine is an ideal legal mechanism for forcing spammers to internalize the costs they impose on innocent third parties.

Nuisance doctrine, of course, is not a panacea. It will not stop the spam deluge alone. As noted in Part I, the various responses to spam are not mutually exclusive. In fact, the problems with spam have been exacerbated in part by the attempts to create a single solution, whether that solution is a spam filter or an all-encompassing statute. There is a place in the anti-spam arsenal for filters. The use of spam filters is no more improper than the use of burglar alarms or water filtration devices, despite laws against burglary and pollution. There is also a place for the sanctioning of fraudulent commercial e-mail (although it is a separate question whether this is best done through new legislation or through existing statutes prohibiting fraud). Criminal statutes, though, do not make related private causes of actions unnecessary or moot; thus, there is a place in the arsenal against spam for a litigation tool that holds non-fraudulent spammers accountable for the costs they knowingly impose on ISPs and other businesses.

The costs imposed by spam arise from its substantial interference with the commercial operations of ISPs and businesses—a classic nuisance-type injury. Spam disrupts the operation and use of the computers that constitute a firm’s commercial exploitation of its property. To put it bluntly, computers are no different to the ISP than are cows to the dairy farmer. The nuisance rule that applies to the latter should apply to the for-

188. See *supra* note 126, and accompanying text.

189. *Moon v. N. Idaho Farmers Ass’n*, No. CV 2002 3890, 2002 WL 32102995, at *7 (D. Idaho Nov. 19, 2002) (quoting *Baltimore & Potomac R.R. Co. v. Fifth Baptist Church*, 108 U.S. 317, 331 (1883)); see also Eric R. Claeys, *The Revolution in American Nuisance Law* (suggesting that nuisance doctrine is internally consistent and coherent if it is assessed as arising from this basic political principle) (manuscript on file with author).

190. See *Prepared Statement of The Federal Trade Commission on “Unsolicited Commercial Email” Before the Senate Committee on Commerce, Science and Transportation*, *supra* note 3, at 13.

mer.¹⁹¹ And, except for spammers, few people dispute the claim that deluging computer networks with billions of unsolicited e-mails is a fundamentally unreasonable act. Legal scholars may disagree about the precise applications on the margins of the context-dependent “reasonableness” standard, but economists and rights theorists would probably find common cause in the judgment that the person(s) responsible for the 2.4 billion spams that AOL filters daily (not counting what actually gets through to AOL’s customers) is unreasonably harming AOL and any other ISP suffering under a similar torrent of spam.¹⁹² Nuisance doctrine exists to protect property owners against such harms.

Spam is a nuisance. As Washington State Attorney General Christine Gregoire declared last year, “It has become obvious our delete key will not solve this problem. We need to make life tough on spammers. They need to know they may have to defend themselves in court.”¹⁹³ Nuisance doctrine can make this a meaningful and viable threat.

191. *See supra* note 121, and accompanying text (noting Wisconsin case affirming nuisance judgment against electric company whose wires produced stray voltage injuring plaintiff’s dairy herd); *see also* PROSSER § 87, *supra* note 86, at 619-20 (discussing application of nuisance to unpleasant odors, smoke, dust, gas, noises, pollution, destruction of crops, and phone calls).

192. *See supra* note 7, and accompanying text.

193. Bob Sullivan, *Microsoft Files 15 Spam Lawsuits*, at <http://msnbc.msn.com/id/3078458> (June 17, 2003).