# INTEL CORP. V. HAMIDI: TRESPASS TO CHATTELS AND A DOCTRINE OF CYBER-NUISANCE

*By Steven Kam*

> It stands to reason that the faster a technology develops, the more rapidly it will surpass preexisting law, and the more prominent common law theories may become . . . . It is not surprising, therefore, that as the Internet geometrically expands its speed . . . intellectual property owners again must consider the common law as a source of protection . . . .[1]

The revival of the once moribund action of trespass to chattels exemplifies the truth of this statement. In *Intel Corp. v. Hamidi*, the California Supreme Court became the first state high court to recognize the application of this tort to networked computers.[2] The court affirmed the tort's expansion as a pragmatic answer to the problem of electronic invasions, but also imposed restraints to prevent the degradation of the Internet's usefulness through misuse of this tort.[3] The court's discussion of harms and benefits also transcended the rule-based construction of trespass to chattels. A reading of the analysis suggests that the tort may well come to resemble a doctrine of nuisance in cyberspace or pave the way for cyber-nuisance as an action unto itself.[4] The economic foundations of nuisance law adapt readily to the social and commercial realities of cyberspace, where the consequences of interconnected behavior demand a more balanced and nuanced analysis than bright-line rules can offer.

---



1. 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).

2. Intel Corp. v. Hamidi, 30 Cal. 4th 1342 (2003).

3. *See generally* Dan Hunter, *Cyberspace as Place and the Tragedy of the Digital Anticommons*, 91 CALIF. L. REV. 439 (2003). Misuse could lead to a "tragedy of the anticommons," in which the Internet never achieves its full potential due to excessive transactions costs (in this case, in the form of burdensome litigation and licensing procedures). *Id.* at 444. The court's opinion reflects that concern by quoting amici curiae, including Professor Mark Lemley, who note that such a tangle of property rights would significantly impede everyday activities on the Internet. *See Hamidi*, 30 Cal. 4th at 1362-63.

4. *See* Dan L. Burk, *The Trouble with Trespass*, 4 J. SMALL & EMERGING BUS. L. 27, 53-54 (2000) (suggesting "nuisance to websites" or "cyberspace nuisance" are better foundations than a doctrine of trespass for property rights in cyberspace).

Part I of this paper provides a primer on the technical terminology and concepts needed to understand the issues presented by the new generation of trespass to chattels cases. Part II summarizes modern treatment of trespass to chattels prior to *Hamidi*. Part III explains the facts of *Hamidi* and the court's addition of considerable flexibility in allowing the doctrine of trespass to chattels to reflect the realities of networked computers. It also discusses the selective rigidity which the court imposes for the sake of preventing overbreadth. Part IV discusses the court's balancing analysis of harms and benefits, which steps outside the literal, bright-line boundaries of personal property law and into the territory of nuisance law. Part V illustrates possible applications of nuisance law to cyberspace and demonstrates its relative advantages in governing activity on the Internet.

## I. TECHNICAL PRIMER

*Intel Corp. v. Hamidi*, on its most basic level concerns the permissibility of one of the most common forms of electronic communication on the Internet: e-mail. Intel Corporation owns and operates an e-mail system for use by its employees in business and reasonable personal use.[5] An ex-employee, Kenneth Kourosh Hamidi, sent several unsolicited e-mails to thousands of addresses on Intel's system, the contents of which were unsympathetic to Intel.[6] Intel then sought both technical and legal means to forbid Hamidi that use of its system.[7] By itself, e-mail is just a form of electronic communication, but its use in both commercial advertising as well as personal and business communication has given rise to many questions concerning its proper use.

### A. Basic Architecture of the Internet

Though any privately-owned computer qualifies as personal property, it must be understood that connecting such a computer to the Internet makes it accessible to many other entities attached to the architecture. The Internet is a network of computers which transmit information and data to one another through an established series of protocols.[8] Its utility increases exponentially as more computers are connected to it due to the phenomenon of "network benefits."[9] Each computer, as a point on the network,

5. *Hamidi*, 30 Cal. 4th at 1349 n.1.

6. *Id.* at 1349, 1356.

7. *Id.* 1348-49.

8. *See generally* CompuServe Inc., v. Cyber Promotions, Inc., 962 F. Supp. 1015, 1018 (S.D. Ohio 1997); ACLU v. Reno, 929 F. Supp. 824, 837-38 (E.D. Pa. 1996).

9. *See generally* Burk, *supra* note 4, at 50-51; Michael L. Katz & Carl Shapiro, *Network Externalities, Competition, and Compatibility*, 75 AM. ECON. REV. 424 (1985);

possesses a permanent or temporary IP address and often an associated alphanumeric domain name.[10] A prearranged protocol[11] uses these addresses to route "packets" of data, containing anything from digital video to malicious viruses or worms, across one or more computers for delivery at its final destination.

## B. Network Congestion

Network congestion adversely affects the speed of Internet communications. Though Internet Service Providers (ISPs)[12] strive to provide facilities that allow fast and uninterrupted flows of information, a deluge of data can still create excessive traffic at individual points on the network. While the Internet's infrastructure regularly deals with simultaneous transfers to the same address, the intermediaries between two computers may be overwhelmed when the frequency of requests and data packets saturates the server's capacity.[13] When a legitimate user cannot access the online resource because another party, legitimately or not, occupies it, a "denial of service" has occurred.[14] Moreover, when large amounts of wanted or unwanted data arrive at their destination, they take up storage space on the destination computer.[15] These occurrences constitute denial of service on the Internet, and such actions purposely undertaken to deny access to a given online resource are called denial of service attacks.[16]

---

Stan J. Liebowitz & Stephen E. Margolis, *Network Externality: An Uncommon Tragedy*, 8 J. ECON. PERSP. 133, 135, 139-40 (1994). "Utility" is a general measure of value or usefulness, and though it is an abstract concept, economists often use monetary value as a convenient stand-in. "Network effects" describe increases in utility that benefit disproportionately from increased membership, with communications networks being an excellent example.

10. *See generally* Alan Silverstein, Under the Hood of the World Wide Web, LearntheNet.com, *at* http://www.learnthenet.com/english/html/70alan.htm (last visited Mar. 16, 2004).

11. Howard Gilbert, Introduction to TCP/IP, *at* http://www.yale.edu/pclt/COMM/TCPIP.HTM (last updated Feb 2, 1995).

12. *See Reno*, 929 F. Supp. at 832-34; s*ee Silverstein, supra* note 10.

13. *See CompuServe*, 962 F. Supp. at 1028.

14. *See* Denial of Service, CERT Coordination Center, Carnegie Mellon Software Engineering Institute, *at* http://www.cert.org/tech_tips/denial_of_service.html (last visited Dec. 17, 2003).

15. *See CompuServe*, 962 F. Supp. at 1022.

16. *See* Denial of Service, *supra* note 14.

## C. Spam

Communication over the Internet is fast, inexpensive, and convenient; a boon to private users as well as to commercial entities.[17] Spam refers to any unwanted unsolicited bulk e-mail ("UBE") or unsolicited commercial e-mail ("UCE").[18] While most think of spam as unwanted e-mail, the broad definition of spam can include webpages and "pop-up" ads which arrive in the course of ordinary web surfing[19] or through "adware" or "spyware" which a remote party installs on a computer, often without the owner's knowing or intended acquiescence.[20] The intent behind the transmission of spam is sometimes commercially "legitimate," but often it is fraudulent.[21] Even proponents of free speech and open access rarely advocate, much less defend, the practice of "spamming."[22] Private parties sometimes attempt to stem the tide of spam on their own, generally through the use of filters[23] that selectively block IP addresses or identify unwelcome messages by their e-mail address or message headers. Spam-

---

17. *See CompuServe*, 962 F. Supp. at 1018; Carol Jones, *E-Mail Solicitation: Will Opening a "Spam-Free" Mailbox Ever Be a Reality?*, 15 LOY. CONSUMER L. REV 69, 70-72 (2002) (sending spam is so inexpensive that even a low response rate gives a better return on marketing over the Internet than through junk mail).

18. *See generally* Scot M. Graydon, *Much Ado about Spam: Unsolicited Advertising, the Internet, and You*, 32 ST. MARY'S L.J. 77, 78 (2000); David E. Sorkin, *Technical and Legal Approaches to Unsolicited Electronic Mail*, 35 U.S.F. L. REV. 325, 327-36 (2001).

19. *See, e.g.*, Reuters, *FTC Accuses Pop-Up Maker of 'Extortion'*, CNN.COM, Nov. 7, 2003, *at* http://www.cnn.com/2003/TECH/internet/11/07/microsoft.popup.reut/index.html.

20. *See* Stefanie Olsen, *Gator Sheds Skin, Renames Itself*, CNET NEWS.COM, *at* http://news.com.com/2100-1024_3-5099212.html (last modified Oct. 29, 2003).

21. *See generally* Calvin Whang, Comment, *An Analysis of California's Common and Statutory Law Dealing with Unsolicited Commercial Electronic Mail: An Argument for Revision*, 37 SAN DIEGO L. REV. 1201 (2000).

22. *See generally* Burk, *supra* note 4, at 54; Hunter, *supra* note 3, at 478; Sorkin, *supra* note 18, at 344-57; Whang, *supra* note 21.

23. *See* What is Firewall?, Webopedia Computer Dictionary, *at* http://www.webopedia.com/TERM/F/firewall.html (last visited Feb. 2, 2004). The Webopedia defines "firewall" as

> [a] system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially intranets. All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria.

*Id.*

mers often employ techniques that circumvent such measures.[24] The problem of spam has reached such magnitude that Congress, after several false starts, recently passed the "CAN-SPAM" Act, the first federal statute aimed at curbing fraudulent and unduly burdensome advertising through electronic communications.[25] In addition, services such as Brightmail[26] turn a profit by selling services specifically designed to thwart or intercept spam.[27] The result is a free-for-all between senders of spam, unwilling recipients of spam, and third parties seeking to turn a profit by aligning themselves with or against one side or the other.[28]

### D. Spiders and Robots

Spiders, webcrawlers, and robots are all computer programs that automate the process of cataloguing information available on the web.[29] A human web-surfer can peruse pages and copy information of particular interest. A spider does the same thing, requesting webpages or other data from other computers connected to the Internet and combing through such data or text for particular information. These requests and data transfers constitute electronic communication, just like e-mail, instant messages, or other exchanges of information. This activity comprises part of the traffic on the Internet and therefore can contribute to congestion, depending on the frequency and intensity of the spider's activity.[30]

---

24. *See generally* Intel Corp. v. Hamidi, 30 Cal. 4th 1342, 1371 n.2 (2003) (Brown, J., dissenting); Sabra-Anne Kelin, Note, *State Regulation of Unsolicited Commercial E-Mail*, 16 BERKELEY TECH. L.J. 435 (2001); Whang, *supra* note 21, at 1205-08.

25. *See generally* Associated Press, *Bush Signs Anti-Spam Bill*, CNN.COM, Dec. 16, 2003, *at* http://www.cnn.com/2003/ALLPOLITICS/12/16/bush.bills.ap/index.html; Grant Gross, *U.S. Senate Approves Antispam Bill*, InfoWorld, Dec. 16, 2003, *at* http://www.infoworld.com/article/03/10/25/HNantispambill_1.html. The bill was approved on December 19, 2003, and codified at 15 U.S.C. §§ 7701-7713 (2000).

26. *See* Jones, *supra* note 17, at 73.

27. *Id.*

28. *See, e.g.*, Reuters, *FTC Accuses Pop-Up Maker of 'Extortion'*, CNN.COM, Nov. 7, 2003, *at* http://www.cnn.com/2003/TECH/internet/11/07/microsoft.popup.reut/index.html.

29. *See generally* Stephen T. Middlebrook & John Muller, *Thoughts on Bots: The Emerging Law of Electronic Agents*, 56 BUS. LAW. 341 (2000) (describing the technology behind spiders and laws which bear on automated search and indexing).

30. *See, e.g.*, eBay, Inc. v. Bidder's Edge, Inc., 100 F. Supp. 2d 1058 (N.D. Cal. 2000). Bidder's Edge's robots accessed eBay's site approximately 100,000 times per day. *Id.* at 1063. While a search engine aggregating website locations and subject matter might need to visit a site only periodically to make sure its data is up-to-date, Bidder's Edge was in the business of aggregating auction data. *Id.* at 1061-62. Timeliness of information in an online auction is, of course, critical to bidders, and time-sensitivity is a feature of many subjects of online commerce besides auctions. *See, e.g.*, Press Release, Smith

As with e-mail, an entity may employ spiders for good aims or ill purposes. Search engines, indispensable in the realization of the Internet's utility,[31] use spiders to aggregate indexing information.[32] But spiders also enable spammers to comb webpages for personal and commercial e-mail addresses that they can add to their distribution lists.[33]

## II. LEGAL BACKGROUND: PRIOR APPLICATIONS OF TRESPASS TO CHATTELS TO CYBERSPACE

Several years of litigation preceding *Hamidi* produced a substantial body of cases which revived the doctrine of trespass to chattels by applying it to Internet activities.[34] Essentially moribund, the tort caught the attention of creative attorneys seeking a private cause of action applicable to the concept of trespass on the Internet. Although metaphors and analogies relating cyberspace to real property pervaded academic literature and case law,[35] courts began to view such arguments with suspicion during the 1990s.[36] But even if analogies comparing cyberspace to real property fail under legal scrutiny, computers still qualify as personal property. Armed with this reinvigorated doctrine, plaintiffs succeeded in obtaining selective injunctions against outsiders' intrusions on their computers.[37]

---

School of Business Gets $2 Million NSF Grant to Study e-Markets, Robert H. Smith School of Business, University of Maryland (Aug. 26, 2002), *at* http://www.rhsmith.umd.edu/pr/news-nsf.htm.

31. *See, e.g.*, Laura Quilter, Note, *The Continuing Expansion of Cyberspace Trespass to Chattels*, 17 BERKELEY TECH. L.J. 421, 436 (2002).

32. *See* Maureen O'Rourke, *Property Rights and Competition on the Internet: In Search of an Appropriate Analogy*, 16 BERKELEY TECH. L.J. 561, 570-74 (2001).

33. *See* Jones, *supra* note 17, at 71-31. For example, a spider may search for text strings within the code of personal and commercial websites, whether text or HTML markup, that matches the format of an e-mail address. Public, unprotected publishing on the World Wide Web makes the e-mail address available by default to anyone with Internet access.

34. *See, e.g.*, Ticketmaster Corp. v. Tickets.com, No. 99CV7654, 2000 WL 1887522 (C.D. Cal. Aug. 10, 2000); *eBay*, 100 F. Supp. 2d 1058; Am. Online, Inc. v. IMS, 24 F. Supp. 2d 548 (E.D. Va. 1998); CompuServe, Inc. v. CyberPromotions, Inc., 962 F. Supp. 1015 (S.D. Ohio 1997); Thrifty-Tel v. Bezenek, 46 Cal. App. 4th 1559 (1996).

35. *See* Hunter, *supra* note 3, at 443.

36. *Id.* at 447.

37. *See generally* Burk, *supra* note 4, at 37 (noting that the harm associated with spam is "unwanted content, and not some fictional lessening of goodwill or the capacity of the proprietary network," because if the spam were offering something desirable, for instance "certificates for free beer, or $100 in e-cash—not a word would have been said"); 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); Hunter, *supra* note 3, at 483; Quilter, *supra* note 31, at 428-36.

The original tort provided redress for unauthorized use of, or intermeddling with, the personal property of another.[38] The tort requires proof of intentional physical contact, causation, and the infliction of actual, substantial harm to the chattels.[39] The definitions of "intentional physical contact" and "actual harm" underwent radical changes in order to apply this ancient doctrine, more associated with livestock disputes, to the World Wide Web.

### A. Electron Trespass as Physical Trespass

In the 1996 decision of *Thrifty-Tel, Inc. v. Bezenek*, a case involving phreaking (unorthodox access to telephone systems) in telephone networks, a California Court of Appeal held that a flow of electrons is sufficiently physical to satisfy the requirement of intentional physical contact for purposes of Trespass to Chattels.[40] *CompuServe, Inc. v. Cyber Promotions, Inc.* followed in 1997, explicitly applying *Thrifty-Tel*'s doctrine of electron trespass directly to electronic communications on the Internet.[41] But electronic communications of any sort inherently involve this kind of electron "trespass," leaving the element of "intentional physical contact" completely trivial when applying trespass to chattels to activity in cyberspace.[42]

### B. Courts Broaden "Actual Harm" to Include "Threatened Harm"

"Substantial" actual harm, originally meant harm that amounted to more than a mere theoretical or de minimis deprivation,[43] but when faced

---

38. Quilter, *supra* note 31, at 424-26.

39. PROSSER AND KEETON ON TORTS § 14, at 85-86 (5th ed. 1984).

40. 46 Cal. App. 4th 1559, 1567 n.6 (1996); Burk, *supra* note 4, at 29 (describing "phreaking" and the *Thrifty-Tel* court's reliance on other cases which hold that colloquially "intangible" interferences such as dust or sound waves constitute trespass when they result in tangible harm); *see also* Fairview Farms, Inc. v. Reynolds Metals Co., 176 F. Supp. 178, 186-88 (D. Or. 1959) (holding that advancements in science have allowed for the apprehension and measurement of gases, shockwaves, and particulates once considered uncertain and intangible for purposes of trespass); Martin v. Reynolds Metals Co., 342 P.2d 790 (Or. 1959) (holding that gases and particulates, while invisible to the naked eye, can be agents of direct trespass).

41. *See* CompuServe, Inc. v. CyberPromotions, Inc., 962 F. Supp. 1015, 1021-22 (S.D. Ohio 1997).

42. *See* Burk, *supra* note 4, at 34 ("Such 'dispossession' by impinging electrons amounts to a rule of inviolability—the equipment was contacted by electrons, not touched, not damaged, not removed, not rendered inoperable. One wonders where the limits of such 'trespass by electrons' might lie.").

43. RESTATEMENT (SECOND) OF TORTS § 218 cmt. i (1965) ("A mere momentary or theoretical deprivation of use is not sufficient unless there is a dispossession.").

with Internet-related cases, courts expanded their interpretations to include threatened, inchoate harms. Prosser and Keeton write that, despite a "surprising dearth of authority" on the lower bounds of the requirement,

> [T]he dignitary interest in the inviolability of chattels . . . is not sufficiently important to require any greater defense than the privilege of using reasonable force when necessary to protect them. Accordingly it has been held that nominal damages will not be awarded, and that in the absence of any actual damage the action will not lie.[44]

The line of cases which expanded actual harms to include threatened harms involved various uses of spiders or robots. In *Register.com, Inc. v. Verio, Inc.*, defendant Verio used spiders to cull information from Register.com's publicly accessible database in furtherance of its spamming activities.[45] In *eBay, Inc. v. Bidder's Edge, Inc.*, defendant Bidder's Edge sent spiders 100,000 times daily[46] to eBay's site for the purpose of maintaining an online auction data aggregation service.[47] In both cases, the courts found no significant actual harm but granted judgment for the plaintiffs because of the potential for copycat crime.[48] Though actual harm had yet to occur, these courts found it likely that others would copy the defendants' behavior, collectively causing congestion or creating unintended but foreseeable denial of service if not preemptively enjoined.[49]

---

44. PROSSER & KEETON, *supra* note 39, at 87. The Restatement (Second) of Torts contains a comment which says substantially the same thing: "The interest of a possessor of chattel in its inviolability, unlike the similar interest of a possessor of land, is not given legal protection by an action for nominal damages for harmless intermeddlings with the chattel." RESTATEMENT (SECOND) OF TORTS § 218, ¶ e.

45. 126 F. Supp. 2d 238, 249-51 (S.D.N.Y. 2000).

46. 100,000 is not necessarily a large number in context. This activity caused no visible end-user impact on the service. Computer systems vary widely in power and purpose, and numbers should always be read with any relevant technical facts in mind. eBay, Inc. v. Bidder's Edge, Inc., 100 F. Supp. 2d 1058, 1063-65 (N.D. Cal. 2000).

47. *Id.* at 1061-62.

48. *See Register.com*, 126 F. Supp. 2d at 250 (quoting Register.com's VP for technology's declaration, "I believe that if Verio's searching of Register.com's WHOIS database were determined to be lawful, then every purveyor of Internet-based services would engage in similar conduct"); *see also eBay*, 100 F. Supp. 2d. at 1071-72 ("[I]f the court were to hold otherwise, it would likely encourage other auction aggregators to crawl the eBay site, potentially to the point of denying effective access to eBay's customers.").

49. *See, e.g., Register.com*, 126 F. Supp. 2d at 252. The court found:

> [I]t is highly probable that other Internet service vendors would also use robots to obtain this potential customer information were it to be permitted . . . . If the strain on Register.com's resources generated by

However, not all courts adopted such lenient standards for inchoate harms. The court in *Ticketmaster Corp. v. Tickets.com, Inc.* found for the defendant.[50] Although it noted that no actual harm had occurred, it distinguished *eBay* on the ground that in its present case, there was no "specter of dozens or more parasites joining the fray, the cumulative total of which could affect the operation of business," implicitly accepting the *eBay* court's interpretation of cognizable harms, only disagreeing as to the threshold of harm.[51]

The application of trespass to chattels against senders of spam was not nearly as controversial because the volume of spammers' activities provided straightforward, plausible measurements of actual harm.[52] The *CompuServe* court also found that actual harm had occurred because CompuServe's end users experienced significant degradations in utility and increases in cost.[53] These harms resulted from the defendant's activity on CompuServe's chattels, but the inconvenience to end users was certainly one degree removed from the computers' literal physical condition or functionality.[54]

### C. Creeping Strict Liability

Scholars, judges, and commentators began to fear a creeping doctrine of strict liability for any unwanted or unsolicited electronic trespass, since the plaintiffs were winning most of the cases even when the defendant was not sending spam or engaging in spam-related activities.[55] In the absence

---

> robotic searches becomes large enough, it could cause Register.com's computer systems to malfunction or crash.

*Id.*

50. Ticketmaster Corp. v. Tickets.com, No. 99CV7654, 2000 WL 1887522, at *4 (C.D. Cal. Aug. 10, 2000).

51. *Id.* The *Ticketmaster* court was quite cognizant of the holding in *eBay*, but held for the defendant, stating that the threat of copycat behavior was too low in this case to find for the plaintiff.

52. *See* Hotmail Corp. v. Van$ Money Pie, Inc., No. 98-20064 JW, 1998 U.S. Dist. LEXIS 10729, at *7 (N.D. Cal. 1998); Am. Online, Inc. v. LCGM, Inc., 46 F. Supp. 2d 444, 451-52 (E.D. Va. 1998); Am. Online, Inc. v. IMS, 24 F. Supp. 2d 548, 550-51 (E.D. Va. 1998); CompuServe, Inc. v. CyberPromotions, Inc., 962 F. Supp. 1015, 1015 (S.D. Ohio 1997).

53. *CompuServe*, 962 F. Supp. at 1019.

54. *See id.* at 1022.

55. *See* Intel Corp. v. Hamidi, 30 Cal. 4th 1342, 1350 (2003) (quoting the dissenting justice in the prior decision, who stated that the Court of Appeal's affirmation of the doctrine's expansion would "expand the tort of trespass to chattel in untold ways and to unanticipated circumstances"); *see also* Burk, *supra* note 4, at 32 (noting that, at the time, the lower court's injunction against Hamidi "further suggests that the claim of 'trespass' is mutating from an innovative claim to deter commercial spam into a more general claim

of any appellate decisions, writers had to speculate as to the doctrine's ultimate reach. While some writers defended the expanded doctrine's usefulness in filling a legislative void,[56] many more worried that trespass to chattels had been expanded beyond reasonable bounds as a nearly unbridled cause of action in cyberspace, capable of defending an interest in inviolability that the old doctrine did not countenance.[57] Even *Ticketmaster*, despite its relative restraint, still respected *eBay*'s standard of potential or threatened harm.[58] Writers predicted that continued broad application of trespass to chattels would eventually create a tragedy of the anticommons, an over-protection of private rights which would hamper basic activities on the Internet.[59]

## III. INTEL V. HAMIDI: THE CALIFORNIA SUPREME COURT

### A. Factual Background

Intel Corporation maintains and operates an intranet,[60] which it uses to transmit messages among its employees, its customers, and other third par-

---

to deter unwanted messages. This change has troubling implications for the free flow of information on the network . . . " ).

56. *See, e.g.*, Mark D. Robins, *Electronic Trespass: An Old Theory in a New Context*, 15 No. 7 COMPUTER LAW. 1 (1998).

57. *See generally* Burk, *supra* note 4, at 35 (attributing the expansion of the doctrine to a blurring between the traditional divide between real property law and personal property law); Hunter, *supra* note 3, at 487; Quilter, *supra* note 31, at 440-42. Real property trespass recognizes a legally defensible interest in inviolability and injunction is a natural remedy for this kind of right. It is argued that the power of these remedies should not be allowed to leak into other theories of trespass unless it addresses an interest of similar gravity.

58. Quilter, *supra* note 31, at 433.

59. *See generally* Burk, *supra* note 4, at 42; Hunter, *supra* note 3, at 509-14; Quilter, *supra* note 31, at 441. Quilter writes,

> [t]he doctrine has become completely malleable, able to fit any and all situations. With trespasses as they have now been defined, and without a harm requirement, it would be difficult to conceive of anything that might not constitute a trespass; trespass is effectively defined purely at the owner's will and can encompass almost any kind of act.

Quilter, *supra* note 31, at 441. The California Supreme Court also notes academic opinions that warn against propertization of the Internet which would have resulted from enforcement under Intel's theory. *Hamidi*, 30 Cal. 4th at 1362-63. Anticommons concerns were also anticipated in the literature. For example, Edward Chang states that "cybertrespass theory will curtail the free flow of price and product information on the Internet by allowing website owners to tightly control who and what may enter and make use of the information housed on its Internet site." Chang, *supra* note 37, at 459.

60. *Hamidi*, 30 Cal. 4th at 1349 n.1 ("An 'intranet' is 'a network based on TCP/IP protocols (an internet) belonging to an organization, usually a corporation, accessible

ties. Though Intel maintains the intranet to facilitate business, its policy also allows employees to make "reasonable nonbusiness use" of the intranet.[61] Kenneth Kourosh Hamidi, a former Intel employee, had an acrimonious falling out with Intel and subsequently founded FACE-Intel (Former and Current Employees of Intel).[62] For a period of over twenty-one months Hamidi, as president of FACE-Intel, sent six unsolicited mass e-mails to a list of thousands of addresses.[63] The contents of these e-mails criticized Intel's employment practices, warned employees that work at Intel was damaging to their health and to their careers, encouraged employees to leave Intel and work elsewhere, and invited them to visit www.faceintel.com.[64] Intel disapproved of the messages, asked Hamidi to stop sending them, and engaged in technical self-help in an attempt to block the messages.[65] Hamidi used techniques similar to those of spammers to circumvent Intel's self-help, but did not actually breach any security barriers or hack into Intel's computers in the process.[66] No evidence suggests that Hamidi's unsolicited e-mails adversely affected the technical performance of any part of Intel's computer systems. The missives were only e-mails, and the system handled them as it handled all e-mail.[67] Though Hamidi refused to heed Intel's requests to cease sending his unsolicited e-mails, he did include within his messages an opt-out provision for the end recipients, which Hamidi honored.[68]

## B. The Holding

The California Supreme Court held that, in California, the common law tort of trespass to chattels did "not encompass, and should not be extended to encompass, an electronic communication that neither damages the recipient computer system nor impairs its functioning."[69] The court also stated that the dispositive issue in a case such as this was whether the

---

only by the organization's members, employees, or others with authorization.' <http://www.webopedia.com/TERM/i/intranet.html> [as of June 30, 2003]. Hamidi used only a part of Intel's computer network accessible to outsiders.").

61. *Id.* at 1346.

62. *See* Ken Hamidi WON, Intel LOST, FACE Intel, *at* http://www.faceintel.com/kenwonintellost.htm (last visited Dec. 17, 2003) (providing a comprehensive account of this case and its preceding history from Hamidi's point of view).

63. *Hamidi*, 30 Cal. 4th at 1349, 1356 (noting that the extent of Hamidi's activity is miniscule compared to that of a typical spammer).

64. *Id.* at 1348-49.

65. *Id.*

66. *Id.*

67. *Id.*

68. *Id.* at 1346.

69. *Id.* at 1347.

activity "caused *or threatened* to cause damage," in an explicit acceptance of the doctrine's expansion in *eBay*, *Register.com*, and *Ticketmaster*.[70]

### 1. *Demonstrating Flexibility in the Common Law*

The court thus adopted the changes imposed upon trespass to chattels by federal district courts in California. In so doing, the court recognized the need for a limited private cause of action against trespass to personal computers. At the very least, the court's decision makes it clear that trespass to chattels, though ancient in its lineage, includes trespass to networked computers.[71] Without this adaptation of the common law, individuals would be limited to statutorily-defined theories of relief, which are typically slow to arrive.[72] As a first step, however, this change to trespass to chattels remained consistent with the historical adaptability of trespass law to changing times and technologies. If this adaptability to cyberspace extends to other forms of trespass law, the result may be a doctrine of cyber-nuisance. This has the potential to thwart any anticommons problems that the Internet and its successors would otherwise face in the future.

### 2. *The California Supreme Court Embraces the Holdings of Prior Courts*

If the California Supreme Court wished to repudiate the trend towards breadth in trespass to chattels, it could have done so.[73] It instead embraced the prior decisions—including *eBay*, which is the most controversial of the spidering cases—and from their holdings harmonized a new threshold of harm for the tort.

---

70. *Id.* at 1353 (emphasis added).

71. *Id.* at 1361 ("The plain fact is that computers, even those making up the Internet, are—like such older communications equipment as telephones and fax machines—personal property, not realty."). The court made this point and avoided settling the "cyberspace as real property" debate, and thus, it would actually be quite premature to call this doctrine "Trespass to Chattels in Cyberspace" given its implicit real-property bias.

72. Legislative progress is notoriously slow, while communications technology has advanced rapidly in the past few decades. The motivations for other courts' extensions to trespass to chattels are obvious enough. *See* Quilter, *supra* note 31, at 435-36. This is not to say that the legislature has been inactive, however—gridlock and political considerations have caused the demise of several federal anti-spam measures. *See generally* Associated Press, *supra* note 25; Gross, *supra* note 25.

73. *Hamidi*, 30 Cal. 4th at 1357 n.5 (concluding that a federal magistrate judge in Oyster Software, Inc. v. Forms Processing, Inc., No. C-00-0724 JCS, 2001 U.S. Dist. LEXIS 22520, at *37-38 (N.D. Cal. Dec. 6, 2001), "incorrectly read *eBay* as establishing, under California law, that mere unauthorized use of another's computer system constitutes an actionable trespass" and that the court did "not read *eBay* . . . as holding that the actual injury requirement may be dispensed with").

a) Trivial Trespass: Electronic Communication is Intentional Physical Trespass

The court implicitly accepted the theory of trespass by electrons without substantive criticism. At no time during its review of electronic trespass cases, including telephone,[74] spamming,[75] and spidering cases[76] did the court question whether trespass by electrons legally satisfied the intentional physical trespass element. If the court had decided to reject the theory, it could not have endorsed any of these cases as good law and would not have even needed to analyze the issue of harm to find for Hamidi.

b) Expanded Harms: Either Actual Harm or Threatened Harm Sufficient to Sustain Cause of Action

By focusing on the holdings of the spidering cases, the court also endorsed the expansion of the requirement of actual harms to include physical harms. As noted above, no evidence supported a finding of substantial or actual harm in *eBay*, *Register.com*, or *Ticketmaster*. Though fact patterns varied in each of these cases, a common thread was the courts' determinations of the probability or improbability of "copycat crime." *eBay* and *Register.com* held for the plaintiffs because the courts believed that they would suffer from overwhelming copycat activity if they lost their cases.[77] *Ticketmaster* found copycats situationally unlikely and held for the defendant.[78]

---

74. *Id.* at 1353 (discussing Thrifty-Tel v. Bezenek, 46 Cal. App. 4th 1559 (1996)).

75. *Id.* at 1353-54 (discussing 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 Pie, Inc., No. C 98-20064 JW, 1998 U.S. Dist. LEXIS 10729 (N.D. Cal. Apr. 16, 1998); CompuServe, Inc. v. Cyber Promotions, Inc., 962 F. Supp. 1015 (S.D. Ohio 1997)).

76. *Id.* at 1354-56 (summarizing "unauthorized robotic data collection" in Register.com, Inc. v. Verio, Inc., 126 F. Supp. 2d 238 (S.D.N.Y. 2000); Ticketmaster Corp. v. Tickets.com, No. 99CV7654, 2000 WL 1887522 (C.D. Cal. Aug. 10, 2000); eBay, Inc. v. Bidder's Edge, Inc., 100 F. Supp. 2d 1058 (N.D. Cal. 2000)).

77. *Register.com*, 126 F. Supp. 2d at 251-52; *eBay*, 100 F. Supp. 2d at 1071-72.

78. *Ticketmaster.com*, 2000 WL 1887522, at *4.

## IV. FIRST STEPS TOWARD A DOCTRINE OF CYBER-NUISANCE

### A. Legal Primer: The Real Property Doctrine of Private Nuisance

The nuisance doctrine has its genesis in real property law,[79] but embodies an economic rule of conduct, consequences, and context that would make an excellent foundation for a rule of liability in cyberspace. Nuisance evolved to handle "nontrespassory" invasions of the public or private interest in the use and enjoyment of land.[80] A modern understanding of physics blurs the line between actions that qualified traditional trespass, such as bodily intrusion and bricks thrown through windows and "intangible" invasions now understood to be "physical," such as particulate matter (smog, industrial fumes) and electromagnetic energy.[81] The semantic niceties of "invasion" or "interference" and the involvement of real property serve as the gatekeepers to this doctrine, which otherwise is chiefly concerned with aggregate social utility and efficient economic outcomes.[82]

---

79. RESTATEMENT (SECOND) OF TORTS § 822 cmt. b (1965) (discussing the growth of modern nuisance doctrine from the former rule of strict liability articulated in *Fletcher v. Rylands*, L.R. 1 Ex. 265 (1866), and affirmed in *Rylands v. Fletcher*, L.R. 3 E. & I. App. 330 (H.L. 1868)). Early in its history, strict liability encompassed some of the legal territory covered by nuisance law. Strict liability's doctrinal inflexibility was incompatible with the realities of the then-dawning Industrial Age, and so the nuisance doctrine developed, a sensible compromise necessitated by the proximity and press of modern living. *See* RESTATEMENT (SECOND) OF TORTS § 822 cmt. f ("Not every intentional and significant invasion . . . is actionable, even when he is the owner of the land in fee simple absolute . . . . Life in organized society and especially in populous communities involves an unavoidable clash of individual interests."). A similar development is presently in the works, as the previous extensions of TTC in cyberspace began establishing a doctrine of near-strict liability. Only *Ticketmaster* and *eBay* suggested any resistance to this trend until *Hamidi*'s authoritative limitations. *See Ticketmaster*, 2000 WL 1887522 at *4; *eBay*, 100 F. Supp. 2d at 1065-66. The earlier cases could be seen as an Information Age analog to *Fletcher v. Rylands*, which was an early doctrine of strict liability developed for a situation in which there was no established tradition of case law. *See, e.g.*, Am. Online, Inc. v. IMS, 24 F. Supp. 2d 548; *CompuServe*, 962 F. Supp. 1015; *Thrifty-Tel*, 46 Cal. App. 1559. But the aggregate realities of the Internet demand a rule of give and take, so the common law must move past cyberspace's *Fletcher v. Rylands* and into the land of nuisance.

80. See RESTATEMENT (SECOND) OF TORTS § 822 cmt. a.

81. Fairview Farms, Inc. v. Reynolds Metal Co., 176 F. Supp. 178, 186-88 (D. Or. 1959).

82. RESTATEMENT (SECOND) OF TORTS § 829 cmt. d, illus. 2 states:

> A and B own small farms on the outskirts of a village. Their farms are on opposite sides of a highway and their residences are directly opposite one another and about 75 yards apart. A makes a practice of breeding livestock in his front yard and in full view of persons in the front

An action for private nuisance arises when an activity or invasion is both intentional and unreasonable.[83] The determination of unreasonableness is principally an economic question, turning upon whether the gravity of the harm caused by the defendant's conduct outweighs its social, or aggregate, utility.[84] Unreasonableness alternatively may exist if the activity is meritorious but the defendant fails properly to internalize the costs of his activity, thereby imposing a negative externality on society in addition to whatever social utility his activity provides.[85] Section 827 of the Restatement Second of Torts lists five disjunctive[86] factors which weigh the gravity of the harm caused by the defendant's conduct in context:

---

> rooms of B's house. This is a source of considerable annoyance and embarrassment to B and his family. A's conduct is indecent and he is subject to liability to B.

*Id.* Section 829 states that an actionable nuisance can consist solely of sight and sound, when the principle object of the conduct is to cause harm to the other or is contrary to common standards of decency. *Id.* § 829.

83. *Id.* §§ 822, 825-31. These balancing tests to not apply to unintentional conduct, which was not at issue in *Hamidi*. Nuisance doctrine deals with such questions separately. *See id.* § 822(b) cmt. a. The legislature may deem certain activities, even if unintentional, to be inherently unreasonable, which obviates the need for a nuisance analysis. Judicial rules for determining unreasonableness otherwise reside in §§ 519-20. *See also id.* § 822 cmt. j. Some courts, often informally, consider certain activities so inherently risky that they apply a standard similar to strict liability. Though damages for worms, viruses, and hacker intrusions are usually adjudicated under the Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (2000), it stands to reason that such activities that have the power to cripple the Internet and inflict billions of dollars in damage or endanger human life in the hundreds or more would qualify as ultrahazardous activities. *See, e.g.*, Philip W. Esbenshade, *Hacking: Juveniles and Undeterred Recreational Cybercrime*, 23 J. JUV. L. 52, 58 (2003) (describing an incident where another juvenile hacker unwittingly shut down the FAA control tower at Worcestor airport); Rebecca Allison, *Hacker Attack Left Port in Chaos*, GUARDIAN UNLIMITED, Oct. 7, 2003 (detailing a case being heard in the UK, where a 19-year-old hacker disabled a major Texas port through a denial-of-service attack intended only for one individual user's computer; the interconnected, relatively decentralized structure of the Internet makes it all the more likely that a denial-of-service attack may have serious but unanticipated consequences), *at* http://www.guardian.co.uk/online/news/0,12597,1057454,00.html. The creation and release of malicious viruses might also be considered ultrahazardous activities. *See, e.g.*, Melissa Virus Creator Jailed, BBC NEWS, May 2, 2002, *at* http://news.bbc.co.uk/1/hi/world/americas/1963371.stm; House Science Subcomm. on Tech., *The Love Bug Virus: Protecting Lovesick Computers from Malicious Attack* (May 10, 2000), *available at* http://www.nist.gov/hearings/2000/lovebug.htm.

84. RESTATEMENT (SECOND) OF TORTS §§ 822(a), 826(a).

85. *Id.* § 826(b). *But see id.* § 830 cmt. c, illus. 2, 3 (noting that if the defendant reasonably internalizes the costs to the extent possible, he may not always be liable even though the conduct causes both utility and harm).

86. The Restatement suggests:

> the extent of the harm involved;
> the character of the harm involved;
> the social value that the law attaches to the type of use or enjoyment invaded;
> the suitability of the particular use or enjoyment invaded to the character of the locality; and
> the burden on the person harmed of avoiding the harm.[87]

Still, the defendant's conduct may be excused or justified if it does more good than harm. Section 828 lists three conjunctive[88] factors which analyze the utility of the defendant's conduct:

> the social value that the law attaches to the primary purpose of the conduct;
> the suitability of the conduct to the character of the locality; and
> the impracticability of preventing or avoiding the invasion.[89]

## B. First Steps Toward a Nuisance Doctrine in Cyberspace

Several parts of the court's analysis, especially those sections justifying the expansion of traditional thresholds, resounded with reasoning that would be appropriate under an analysis of nuisance. At least one other court had read past case history to mean that trespass to chattels embodied

---

> Since the gravity of harm is its seriousness from an objective standpoint, it is the product of all relevant factors. There is no general rule as to the relative weight of the particular factors in all the ever-varying cases . . . . The list of factors here stated is not intended to be exhaustive.

*Id.* § 827 cmt. b.

87. *Id.* § 827(a)-(e).

88. *Id.* § 828 cmt. c.

> It is only when the conduct has utility from the standpoint of *all the factors as a whole* that its merit is ever sufficient to outweigh the gravity of the harm it causes. If the conduct has no utility from the standpoint of *one* of the factors, the fact that it has utility from the standpoint of other factors is not controlling.

*Id.* (emphasis added). Supposing for the sake of argument that nuisance does apply to cyberspace, if an ISP were to send a mail bomb back to a spammer, it would fail this test outright. The ISP nonetheless may attempt to excuse its retaliatory self-help by arguing that the social value the law attaches to the use or enjoyment invaded—a spammer's capacity to attack spam—has almost no social value, and that a spammer could easily avoid the retaliation by not subjecting the ISP and its customers to outrageous amounts of spam in the first place.

89. *Id.* § 828(a)-(c).

a rule approaching strict liability,[90] a ruling which the California Supreme Court authoritatively denounced in *Hamidi*.[91]

*1. Employing Nuisance-Like Reasoning*

Proper analysis of actual harms under trespass to chattels is a quantitative discipline that emphasizes categorical rules and measurable effects, but the substance of the court's opinion emphasizes utilities and harms in a manner reminiscent of the balancing tests in the nuisance doctrine.[92] Literature analyzing the traditional doctrine of trespass to chattels states that deprivations must occur for a substantial or measurable period of time and cannot be merely theoretical.[93]

a) The Gravity of the Harm (§ 827)

The court noted that though Hamidi employed evasive tactics in sending his UCEs to Intel's servers, he never actually breached any security barriers.[94] This fact has relevance in the calculation of damages only in the negative because the calculation of employee time and resources spent in deleting Hamidi's e-mails from the system could not contain figures for time and resources *not* expended on damages that did not occur. The court implicitly made value judgments on the nature of Hamidi's behavior that would weigh upon the extent and the character of the harm involved.[95] The court also noted that the extent of the harm of Hamidi's conduct was miniscule compared to the impact of a typical spammer's activity, which was the cornerstone of its finding in favor of Hamidi under trespass to chattels.[96]

---

90. Oyster Software, Inc. v. Forms Processing, Inc., No. C-00-0724 JCS, 2001 WL 1736382 (N.D. Cal. Dec. 6, 2001).

91. Intel Corp. v. Hamidi, 30 Cal. 4th 1342, 1357 n.5 (2003).

92. *See generally* PROSSER & KEETON, *supra* note 39; RESTATEMENT (SECOND) OF TORTS § 218. The Restatement notes that for an interference or intermeddling to give rise to an action, the deprivation of use "must be for a time so substantial that it is possible to estimate the loss caused thereby. A mere momentary or theoretical deprivation of use is not sufficient unless there is a dispossession." RESTATEMENT (SECOND) TORTS § 218.

93. *See* RESTATEMENT (SECOND) OF TORTS §§ 218-19.

94. *Hamidi*, 30 Cal. 4th at 1346, 1349, 1353.

95. Recall that these are the first two listed factors weighing against the defendant's activity or behavior. RESTATEMENT (SECOND) OF TORTS § 827(a)-(b).

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

b) The Utility of the Conduct (§ 828)

i) Social Value and Purpose

For the defendant to justify or excuse his activity, the law must attach some social value to the primary purpose of the conduct.[97] The court did *not* decide *Hamidi* on First Amendment grounds,[98] but there was a hint of similar sympathy in the court's characterization of Hamidi's UBEs as "occasional advocacy messages," not spam.[99]

ii) Suitability

Secondly, the court must consider the suitability of the conduct to the character of the locality.[100] The court placed special emphasis on the fact that Hamidi merely used an e-mail system connected to the Internet for the transmission of e-mail. Specifically, the court found that Hamidi did not use Intel's system "in any manner in which it was not intended to function . . . ."[101] Intel's e-mail system was equipment designed for speedy communication between employees and the outside world; Hamidi communicated with Intel employees over that system in a manner entirely consistent with its design."[102] The court had no need to make statements such as these in an analysis of damages. Within the confines of trespass to chattels doctrine, it would have sufficed to say that the effect of six UBEs in twenty-one months consumes negligible storage space and computing power.[103] Applied to nuisance analysis, however, these statements would

97. RESTATEMENT (SECOND) OF TORTS § 828(a).

98. *Hamidi*, 30 Cal. 4th at 1364-65. First Amendment issues were important to a number of people working on this case. Hamidi considered them the most important aspect of the case and was disappointed that the court chose not to answer these questions. *See* Ken Hamidi WON, Intel LOST, *supra* note 62.

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

100. THE RETATEMENT (SECOND) OF TORTS § 828(b).

101. *Hamidi*, 30 Cal. 4th at 1353.

102. *Id.* at 1360-61 n.7. The Court also stated,

> Intel connected its e-mail system to the Internet and permitted its employees to make use of this connection both for business and, to a reasonable extent, for their own purposes. In doing so, the company necessarily contemplated the employees' receipt of unsolicited as well as solicited communications from other companies and individuals. That some communications would, because of their contents, be unwelcome to Intel management was virtually inevitable.

*Id.* This language should bring to mind the "give-and-take," "live and let live" characterizations in RESTATEMENT (SECOND) OF TORTS § 822 cmt. g.

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

reduce the weight of harm in the context of the "suitability of the conduct to the character of the locality."[104]

iii) Unavoidable/Unpreventable Harm

Finally, there must be some impracticability of preventing or avoiding the invasion, without which the defendant cannot excuse his conduct despite its value, as otherwise the defendant inflicts unnecessary harm.[105] The court noted that Intel's employees would have had an easy time opting out of Hamidi's mailings, as Hamidi made this option explicit and genuine in the content of his UBE.[106] The court in effect emphasized that the burden on the person harmed of avoiding the harm[107] was slight, and hence, the harm was also small.[108] Certainly, Hamidi could have avoided completely any distraction to Intel's employees by not sending the UBE. Still, by including an opt-out provision in his messages, Hamidi went to lengths to notify recipients of their right to refuse further missives and his willingness to abide by their wishes, which demonstrates respect for the intent behind § 828(c).[109]

*2. Rigid Categorization: This is Still Not Cyber-Nuisance*

Fundamentally, trespass to chattels still only protects possession and related interests in personal property. Though the analysis in *Intel v. Hamidi* often sounds like nuisance-based reasoning, the decision does not rest primarily upon balancing economic efficiency or social utility, but upon categorical pronouncements of what constitutes "harm" and "interests" under the rules of the tort.[110] Thus, the decision does not actually create a common-law doctrine of cyber-nuisance under the name of trespass to chattels. The court made rigid and categorical rejections of em-

---

104. RESTATEMENT (SECOND) OF TORTS § 828(b).

105. *Id.* § 828(c).

106. *Hamidi*, 30 Cal. 4th at 1346, 1349.

107. RESTATEMENT (SECOND) OF TORTS § 827(e).

108. *Hamidi*, 30 Cal. 4th at 1352-53.

109. RESTATEMENT (SECOND) OF TORTS § 828 cmt. h. This comment on clause (c) states,

> An invasion is practicably avoidable by the actor if the actor by some means can substantially reduce the harm without incurring prohibitive expense or hardship. Thus, if the actor can carry on his activity with more skill or care or in a different manner or at a different time and thereby avoid a substantial part of the harm without substantially diminishing the value of his own enterprise, the invasion is practicably avoidable.

*Id.*

110. *Hamidi*, 30 Cal. 4th at 1352-53, 1356, 1358-60.

ployee time and productivity as interests in the "condition, quality, or value" of the computer system.[111] Therefore, practitioners seeking to employ trespass to chattels against unwanted electronic communications must be able to identify a defensible interest attaching tightly to the basic interest of possession; an interest too tangential or remote from possession or technical performance is likely to face dismissal. Nuisance law countenances no such rigidity; "enjoyment and use" covers any legally protectible interest, weighted by utility and harm.[112]

The court kept trespass to chattels lashed to its foundations, despite some newfound flexibility. It dismissed several metaphors equating cyberspace and real property[113] and flatly stated that "computers, even those making up the Internet, are . . . personal property, not realty."[114] Though trespass to chattels has been extended to include trespass to networked computers, this did not create a distinct theory of trespass via cyberspace. In addition, the court categorically rejected characterizations of employee time and attention as interests in computers or their functionality.[115] The court also viewed the loss of consumer goodwill and economic revenues recognized by the *CompuServe* court with suspicion.[116] Common sense suggests that the user or owner of a personal computer has an interest in a mailbox free of spam and a computer free from unwanted spyware,[117] but Intel's complaint was only indirectly related to the computer system's functional condition.[118] Even so, quantities of spam and pop-ups will harm a private user's utility long before the computer itself suffers actual degra-

111. *See* RESTATEMENT (SECOND) OF TORTS § 218(b).

112. In economic terms, these are benefits and costs, respectively. *See generally* JOSEPH W. SINGER, PROPERTY LAW 322-23 (3d ed. 2002).

113. *Hamidi*, 30 Cal. 4th at 1360-61.

114. *Id.* at 1361 (describing networked computers as being literally similar to other communications networks, like telephones and fax machines, whereas comparison of such computers to real property requires a metaphor).

115. *Id.* at 1347, 1359. ("Whatever interest Intel may have in preventing employees from receiving disruptive communications, it is not an interest in personal property, and trespass to chattels is therefore not an action that will lie to protect it."). As part of this argument, the California Supreme Court quoted Burk, *supra* note 4, at 36: "The Restatement test clearly speaks in the first instance to the impairment of the chattel . . . . But employees are not chattels (at least not in the legal sense of the term)." *Hamidi*, 30 Cal. 4th. at 1359.

116. *Id.* at 1357-59.

117. *See generally* Whang, *supra* note 21, at 1203-04; John Simons, *The Battle over Spam Gets Ugly*, U.S. NEWS & WORLD REP., May 12, 1997, at 55.

118. *Hamidi*, 30 Cal. 4th at 1348, 1353 ("In the present case, the claimed injury is located in the disruption or distraction caused to recipients by the contents of the e-mail messages, an injury entirely separate from, and not directly affecting, the possession or value of personal property.").

dation in performance.[119] The receipt of several thousand pieces of spam in one's mailbox might not noticeably affect a computer's technical performance, but it does reduce the usefulness of the e-mail system to the user.

### C. Historical Parallel: The Development of the Original Nuisance Doctrine

*Intel v. Hamidi* added another page in a story that mirrors the development of the original doctrine of private (real-property) nuisance from its beginnings in strict liability. *Fletcher* v. *Rylands* originally established a doctrine of strict liability for trespass to land.[120] This doctrine did not stand unmodified in the face of technological progress. Over time, courts incorporated rules of context and economically-motivated balancing tests into the doctrine, changing it from a landowner's weapon into a mechanism designed to safeguard the economic goals of aggregate utility maximization and cost internalization.[121] For instance, a Texas court held that above-ground reservoirs, which *Rylands v. Fletcher* did not consider a "natural use of the land" in England, were, in fact, a necessary and therefore natural use of Texan land, given the realities of Texan climate.[122] And a series of cases decided during and after the Industrial Revolution repudiated strict liability except in cases of negligence, recklessness, or inherently dangerous activities because the proximity and congestion characteristic of an increasingly mechanized, industrialized urban life demanded that everyone accept a degree of give-and-take.[123]

---

119. *See* eBay, Inc. v. Bidder's Edge, Inc., 100 F. Supp. 2d 1058, 1071-72 (N.D. Cal. 2000). Also, some pop-up ads can be so aggressive as to render the computer unusable until it is rebooted or until the user performs an action dictated by the pop-up maker. Though the computer may still have memory or processing power available for other tasks, the user's ability to enter input or access desired programs may be wholly disrupted. *See, e.g*, Shields v. Zuccarini, 254 F.3d 476, 479-80 (3d Cir. 2001) (affirming a judgment against the defendant for cybersquatting). In conjunction with cybersquatting, the defendant in designed sites that "mousetrapped" visitors, rendering them "unable to exit without clicking on a succession of advertisements." *Id.*

120. Fletcher v. Rylands, L.R. 1 Ex. 265 (1866). The court in *Fletcher* held that
> the person who for his own purposes brings on his lands and collects and keeps there anything likely to do mischief if it escapes, must keep it in at his peril, and, if he does not do so, is prima facie answerable for all the damage which is the natural consequence of its escape.

*Id.*

121. Martin v. Reynolds Metals Co., 342 P.2d 790, 790 (Or. 1959).

122. Turner v. Big Lake Oil Co., 96 S.W.2d 221 (Tex. 1936).

123. *See* RESTATEMENT (SECOND) OF TORTS §§ 822 cmt. b, 828 cmt. g (1965); *see also* Spano v. Perini Corp., 250 N.E.2d 31 (N.Y. 1969) (abolishing the former distinction between "debris" as a tangible agent of trespass and "concussion" as an intangible which

Context, cost internalization, and network benefits are all concerns that favor the development of a doctrine of cyber-nuisance. Whereas nuisance in real property usually affects only neighbors or other landowners in the immediate geographical vicinity, on the Internet, everyone is just an IP address away. This interconnectedness magnifies network benefits—and network harms. That many activities on the Internet have both highly productive and highly destructive uses makes the inclusion of context, costs, and benefits indispensable for fair and efficient adjudications.

The greatest obstacle to the development of cyber-nuisance lies in the formalistic objection that one should not equate cyberspace with realty and that nuisance is, by lineage, a real-property doctrine. Despite this formalistic obstacle, the efficiency aims that comprise the underlying principles of nuisance apply aptly to the problems of inherently communal cyberspace.[124] The networked nature of the Internet leads to the conclusion that a balancing of benefits and harms will achieve results that are superior to the overdeterrence threatened by bright-line rules.[125]

## V. COMPARATIVE ANALYSIS: CYBER-NUISANCE VERSUS TRESPASS TO CHATTELS

### A. Give-and-Take: Nuisance Is the Preferable Rule of Aggregate Utility, While Trespass to Chattels Is Provincial and Absolutist

Trespass to chattels exists to defend possession and related harms, and its harm-based analysis focuses on literal damages but asks few questions as to the worth of the trespassory activity.[126] Had the *Ticketmaster* court employed the California Supreme Court's analysis, it could not have permitted or justified defendant Tickets.com's activity simply because Tickets.com furnished more good (data aggregation that facilitates comparison shopping) than harm (light activity on *Ticketmaster*'s website) to the community. The theory of trespass by electrons, by its very scope, implicates all electronic communications, and as a strict damages analysis,

---

will not support a claim of trespass). Use of the Internet and networked computers for electronic communications would appear to be a "natural use" of such a system, qualified by context. The California Supreme Court states that occasional unwanted communication is inevitable when a computer or system is connected to a network as large as the Internet. *Hamidi*, 30 Cal. 4th at 1359-60. And frequently, as in the case with personal e-mail, unsolicited communication is often welcome.

124. SINGER, *supra* note 112, at 325-31.

125. Recall the "tragedy of the anticommons" described by Hunter, *supra* note 3.

126. *See* PROSSER & KEETON, *supra* note 39, at 85-87. Though there is some analysis as to the trespasser's intent or purpose, the analysis deals more with questions of culpability or thresholds than it deals with utility or defenses.

wholly controls liability. But use of a spider to aggregate data for search engines or comparison shopping and use of a spider to collect e-mail addresses for facilitating spam should be treated differently, though the technical impact of their activity on the visited sites may be similar. Trespass to chattels examines only the harm to the property's owner; the doctrine does not address network harms or benefits.

### B. *Hamidi*: Speech and Advocacy

Assume for the moment that a nuisance doctrine in cyberspace exists.[127] Hamidi's FACE-Intel messages dance on the borderline of UBE versus UCE; Hamidi undoubtedly received some measure of personal satisfaction in the activity and its results, and the court still recognized an aspect of "advocacy" in his speech without a detailed analysis of First Amendment concerns.[128] If the court had considered the speech argument under nuisance, it would have had to consider the social value of Hamidi's speech.[129] The court did not endorse using electronic communication as a means of harassment, but noted that if Intel wished to object to the content or consequences of Hamidi's speech, it had other avenues of relief.[130]

Connecting an intranet to the Internet results in inevitable give-and-take and requires a degree of reasonable tolerance sufficient to grant Hamidi leeway under § 828(b).[131] Moreover, Hamidi mitigated the burden of his conduct upon his audience to the extent possible through an opt-out policy, satisfying § 828(c). In general, the extent of the harm of Hamidi's

---

127. As noted, the only reason why nuisance does not already apply to the Internet is because by tradition it has always been a doctrine protecting "use and enjoyment of land." RESTATEMENT (SECOND) OF TORTS § 827. Therefore, either nuisance must be expressly expanded to include electronic communications in cyberspace (the preferable route) or the academic debate over Cyberspace as Place must be resolved in favor of treating cyberspace as real property (undesirable due to anticommons concerns).

128. *See Hamidi*, 30 Cal. 4th at 1356.

129. *Id.* at 1364-65. The court said nothing specific about the value of Hamidi's speech per se. Its brief discussion of constitutional concerns implied that it would have decided in Hamidi's favor. The court offered no opinion as to whether the content of Hamidi's speech was valuable, nor did it suggest that he had an absolute right to use the Internet as an avenue of expression. The court based its dicta on two facts: that Intel had recourse to self-help, and that it does not find the constitutional right "not to listen" to grant an employer the right to decide when its employees should or should not listen. *Id.*; *see also* RESTATEMENT (SECOND) OF TORTS § 828(a) (providing commentary and examples on evaluating the "social value" the law attaches to the defendant's conduct).

130. *Hamidi*, 30 Cal. 4th at 1347-48.

131. *See id.* at 1359-60; RESTATEMENT (SECOND) OF TORTS § 822 cmt. g. This also implicates § 828(b) because Hamidi's conduct was not beyond the extent of unwanted communications that Intel would expect from connection to the Internet.

conduct under § 827 is quite low.[132] Therefore, the weighing of harms and balances under nuisance would also result in a finding for Hamidi. Note also that if Hamidi's activities achieved a volume approaching commercial spam, a court applying nuisance would find the gravity of the harms under § 827 sufficient to justify enjoining Hamidi. Such conduct would have gone inexcusably beyond what is needed for the dissemination of speech, and as a matter of policy, the extension of unbounded spamming rights to everyone with a private opinion would encourage waste of Internet resources. Intel's employees are not chattels and neither is Intel's interest in their time,[133] but nuisance measures the value of conduct, use, and enjoyment, not just the right of possession.[134] Hamidi's e-mails are neither categorically condoned nor forbidden, but weighed in context.

### C. Spidering: *eBay*, *Ticketmaster*, and *Register.com* Revisited

Nuisance would handle the spidering cases with greater factual consistency than trespass to chattels because its analysis pays heed to the purposes of the spidering. Although the California Supreme Court managed to synthesize a rule from these cases, the outcomes remain awkward. *eBay* and *Ticketmaster* both involve defendants who employ spiders to perform data aggregation services thereafter made available to the public.[135] In both cases, the impact was too small to result in actual harm, yet courts found threatened harm cognizable in *eBay* but not in *Ticketmaster*.[136] A "specter" of copycat auction aggregators was deemed likely, but not a specter of copycat ticket sales aggregators. Why? The *Register.com* court's concern about copycat spammers is legitimate because spammers do not curtail their activities unless an outside agency imposes penalties on their behavior, and spammers are not known for their concern about the impact of behavior beyond their own profit margins or liability for dam-

132. *Hamidi*, 30 Cal. 4th at 1355-56.

133. *Id.* at 1359.

134. *See* RESTATEMENT (SECOND) OF TORTS §§ 822, 828.

135. Ticketmaster Corp. v. Tickets.com, No. 99CV7654; 2000 WL 1887522, *2 (C.D. Cal. Aug. 10, 2000); eBay, Inc. v. Bidder's Edge, Inc., 100 F. Supp. 2d 1058, 1061-62 (N.D. Cal. 2000).

136. *Id.*

ages.[137] But how many data aggregators are likely to enter the same market, where profits derive from competitive popularity of use?[138]

A nuisance analysis would capture this concern under § 828 or its equivalent. Section 828(a) addresses the social value that the law attaches to the *primary* purpose of the conduct. Search engines have proven value in cyberspace and have contributed immensely to the utility of the Internet.[139] But when the *primary purpose* of the spidering is to facilitate spam, the outcome of an application of § 828(a) is clear: the law attaches very little social value to spam. Many states have already enacted anti-spam statutes, with some even imposing criminal liability for failure to comply with provisions that facilitate opt-out mechanisms,[140] and the CAN-SPAM Act, which also provides for per-violation fines for spam-related offenses, was approved on December 19, 2003.[141] This factor alone would be enough to halt fraudulent or misleading spam under nuisance without regard to the resultant degree of harm.[142] Section 828(c) also examines the

---

137. *See* Jones, *supra* note 17, at 70-72 (sending spam is so inexpensive that even a low response rate gives a better return on marketing over the Internet than through junk mail). Much of the cost of dealing with spam is not borne by the spammers themselves, and this failure to internalize the cost of their activity upon the end user results in a predictable, empirically obvious overproduction of spam.

138. Many businesses may pursue the same market, but the field becomes highly competitive. Revenue models employed in Internet business have evolved from support via advertising revenue to actual e-commerce involving fees, transactions, and the sale of actual goods. The result is a crowded space, where generally a few firms pursue similar revenue models but in different fields, waging a constant battle to maintain name recognition. *See generally* Gary P. Schneider, *Chapter 3: Selling on the Web: Revenue Models and Building a Web Presence*, *in* ELECTRONIC COMMERCE (3d ed. 2002), *available at* http://www.course.com/downloads/mis/ecommerce3eoc/ch03.cfm.

139. Quilter, *supra* note 31, at 424 ("[L]ocating any information on the Internet would be an almost impossible task without search engines such as Google, Yahoo, or FindLaw.").

140. *See* Kelin, *supra* note 24, at 441-49.

141. *See* 15 U.S.C. §§ 7701-7713 (2000). The chapter is titled "Controlling the Assault of Non-Solicited Pornography and Marketing" and leaves no doubt as to the contemporary target of the legislation. The act does not make spam illegal per se, but § 7703 imposes mandatory opt-out provisions and prohibits "predatory and abusive commercial e-mail." Section 7704(b) targets other techniques including use of spidering and dictionary attacks as "aggravated violations" when employed in preparation for or execution of spamming activities.

142. RESTATEMENT (SECOND) OF TORTS § 828 cmt. c (1965).

> It is only when the conduct has utility from the standpoint of all of the factors as a whole that its merit is ever sufficient to outweigh the gravity of the harm it causes. If the conduct has no utility from the standpoint of one of the factors, the fact that it has utility from the standpoint of other factors is not controlling.

impracticability of preventing or avoiding the invasion, which would force spammers to comply with any statutes that govern their behavior or face nuisance liability. Compliance with several current statutes is often trivial. For instance, one statute merely requires that the first characters in the subject header be "ADV:", which allows any user of e-mail to employ a filter that automatically screens out every such message.[143] It would be difficult for a spammer to prove that this requirement imposes an unreasonable burden.[144]

Nuisance is also versatile with respect to remedies, with both damages and injunctions available.[145] Bidder's Edge provided a useful service, but did not pay for the impact of its activity.[146] Nuisance analysis would find in favor of Bidder's Edge's spidering under equivalents to § 827(a) and (b) since actual harm was not substantial, and under § 827(d) because spidering is a form of electronic communication that has long existed as an element of other useful information services. The relative lightness of the harm weighs against the utility of the conduct. Section 828(a) would ascribe significant value to the primary purpose of the spidering, in this case legitimate data aggregation.[147] Bidder's Edge would only fail § 828(c) for not paying for the impact of its activity on eBay's servers, but the nuisance doctrine would encourage damages instead of an injunction, allowing society to enjoy the benefits of Bidder's Edge's service while Bidder's Edge internalizes its costs.[148]

---

*Id.*

143. *See* CAL. BUS. & PROF. CODE § 17538.4(g) (West 1997 & Supp. 2003); Kelin, *supra* note 24, at 444-49.

144. *But see* Jones, *supra* note 17, at 76-77. The statement is true if the various spam regulations are internally consistent; if one jurisdiction requires that the message header begin with "ADV:" and another jurisdiction requires that the message header begin with "XXXSPAM:" then literal compliance with both will prove tricky if not impossible. This is a strong argument for preferring a federal anti-spam statute enabled by the Commerce Clause over separate and potentially inconsistent state commercial e-mail statutes.

145. *See* RESTATEMENT (SECOND) OF TORTS §§ 822, 827, 828 cmt. h, 830.

146. *See* eBay, Inc. v. Bidder's Edge, Inc., 100 F. Supp. 2d 1058, 1071 (N.D. Cal. 2000); *see also* RESTATEMENT (SECOND) OF TORTS § 830 (discussing the balancing consideration regarding the defendant's attempt to mitigate the harm imposed by his or her conduct). Even when the overall utility of a defendant's conduct may outweigh the harm it inflicts, this does not by itself excuse the defendant from a duty reasonably to mitigate that harm. *See* RESTATEMENT (SECOND) OF TORTS § 803.

147. *See* Quilter, *supra* note 31, at 424.

148. *See generally* SINGER, *supra* note 112, at 325-31.

## VI. CONCLUSION

The California Supreme Court clarified the newly revived doctrine of trespass to chattels in a way that achieved consistency with the majority of prior case history and harmony with the concerns of economic efficiency and freedom of expression. The expansion reflected the need for ready relief against network congestion in a technology characterized by rapid advances and geometric growth. The court also restricted the tort, anchoring it to its traditional foundation as a means for defending possession in personal chattels, and thereby forestalled the rise of a crippling rule of strict liability in cyberspace. Though a landmark decision in tort law, *Intel v. Hamidi* does not end the controversy regarding trespass law in cyberspace. Rather, it highlights the limitations of one doctrine and encourages further development of a responsible doctrine that prefers an efficient balancing of rights to an awkward system of rigid rules and absolute interests. Law has historically moved to accommodate changes in reality arising from changes in technology, and just as tort law adapted to the advances of the Industrial Age, so too will it adapt to the advances of the Information Age.