E-NUISANCE: UNSOLICITED BULK E-MAIL AT THE BOUNDARIES OF COMMON LAW PROPERTY RIGHTS

JEREMIAH KELMAN*

I. INTRODUCTION

E-mail, the most revolutionary advancement in communication since the printing press, has now become the single most important means of intrusion into our daily lives. Because of its inherent convenience and efficiency, e-mail facilitates an unprecedented level of constant, unchecked disturbances from unsolicited bulk messages, also known as spam. As a result of the Internet's decentralized architecture and flawed technical underpinnings,[1] consumers and businesses face daily mass invasions via e-mail. These continuous transmissions of low value unsolicited e-mails are invasions to property interests. In sum, spam is nuisance.

This Note will analyze the extent to which nuisance law can be applied to the unwanted intrusion of unsolicited bulk e-mail. To date, no

* Class of 2005, University of Southern California Law School; B.A. 1999, University of California, Berkeley. I would like to thank Christopher Stone for his guidance and comments. I would also like to thank my colleagues on the *Southern California Law Review* for their dedication and hard work in editing this Note. Finally, I would like to thank my wife Tamar for her love and support.

1. Simple Mail Transfer Protocol, or SMTP, is the standard protocol for relaying e-mail messages over the Internet. The protocol contains no built-in means of verifying the identity of the sender or origination of the message. Created at a time when the Internet was used almost exclusively by academics, SMTP completely trusts that senders are who they claim to be. *See, e.g.*, Paul Festa, *End of the Road for SMTP?*, CNET NEWS.COM, Aug. 1, 2002, *at* http://news.com.com/2100-1038-5058610.html. It has been suggested that a new protocol needs to be written from scratch. *See id*. According to Steve Linford, head of anti-spam activist group Spamhaus, any technological solution to the spam problem will be "an arms race that will go on until the SMTP protocol is rewritten." Will Knight, *Internet Engineers Planning Assault on Spam*, NEWSCIENTIST.COM, Jan. 29, 2004, *at* http://www.newscientist.com/news/news.jsp?id=ns9994620.

adequate legal or technical remedy has been fully tested or put into place to properly protect the inbox from unwanted intrusions. The computer industry has lagged in organizing the massive task of implementing wide scale changes to the e-mail system and currently available technical remedies have done little to stem the enormous tide of spam.[2] Legal solutions applied thus far (via the U.S. Congress and courts) have suffered from confusion, ineffectiveness, and poor tailoring to the core problem. Although a few tough, potentially effective anti-spam laws have been enacted in states such as California, they have since been largely preempted by the recently passed, and widely criticized, Federal Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 ("CAN-SPAM").[3] Significant steps, however, have been made in utilizing the common law in fighting senders of spam ("spammers").[4] Several cases have been successfully brought against spammers under the common law doctrines of trespass to chattels or personal property.[5] While these trespass arguments continue to be experimented with by courts, the law of nuisance

2. For an overview of the problems with spam-filtering software see Margaret Kane, *Building a Better Spam Trap*, CNET NEWS.COM, Jan. 17, 2003, *at* http://news.com.com/Building+a+better+spam+trap/2100-1023_3-981177.html. Several solutions to the spam problem involving major technical overhauls have been proposed. *See* Jo Best, *Gates Reveals His 'Magic Solution' to Spam*, CNET NEWS.COM, Jan. 26, 2004, *at* http://news.com.com/2100-1028_3-5147491.html?part=rss&tag=feed&subj=news. The most intriguing proposal is the idea of creating a system of e-stamps. *See* Associated Press, *Gates: Buy Stamps to Send E-mail*, CNN.COM, Mar. 5, 2004, *at* http://www.cnn.com/2004/TECH/internet/03/05/spam.charge.ap/. Stamps would force spammers to internalize the externalities of spam by imposing nominal postage on each e-mail sent to a U.S. Internet Service Provider ("ISP"). *See id.* While a one cent postage rate for e-stamps has been suggested, even a half-cent per e-mail charge would make current spam practices cost prohibitive. *See id.* At the same time, any costs to legitimate businesses and consumers from the stamps might be avoided if the government were to allot a certain amount of e-stamps per e-mail user. Alternatively, the government could collect the nominal fees into an escrow account, which would be used to pay judgments from spam lawsuits or administrative hearings. Users who comply with standards and do not send spam would get credited back annually.

3. CAN-SPAM Act of 2003, Pub. L. No. 108-187, § 877, 117 Stat. 2699 (codified as amended at 15 U.S.C.A. §§ 7701–7707 (West Supp. 2004); 18 U.S.C.A. § 1037 (West Supp. 2004)).

4. The newly passed Federal CAN-SPAM Act preempts state law specific to spam, but explicitly does *not* preempt the use of generally applicable common law theories in litigating against spam. *Id.* § 7707 ("This chapter shall not be construed to preempt the applicability of—(A) State laws that are not specific to electronic mail, including State trespass, contract, or tort law . . . .").

5. *See, e.g.*, America Online, Inc. v. IMS, 24 F. Supp. 2d 548 (E.D. Va. 1998) (applying Virginia law of trespass to chattels to a spammer's activities); America Online, Inc. v. LCGM, 46 F. Supp. 2d 444 (E.D. Va. 1998) (same); Compuserve, Inc. v. Cyber Promotions, Inc., 962 F. Supp. 1015 (S.D. Ohio 1997) (applying Ohio common law of trespass to chattels to a spammer's activities). *Cf.* Register.com, Inc. v. Verio, Inc., 126 F. Supp. 2d 238 (S.D.N.Y. 2000) (applying New York law of trespass to chattels to the use of software spiders to extract online data).

may be an alternative and possibly preferable avenue of redress that has yet to be fully explored in the context of spam.[6]

Nuisance law has been one of the most flexible doctrines, making adjustments to cover sounds, sights, fears, and odors.[7] By logically taking into account the unique circumstances that e-mail technology and spam bring to the analysis, this Note will discuss the potential of the nuisance framework as an effective and flexible means of curbing the rampant onslaught of spam. Part II will provide a background on the nature of the problem of spam and the initial policy implications involved in legally defining spam. Part III will outline the current state of the law with regard to spam, shedding light on the need for new approaches legislatively and through common law. Part IV will discuss the potential of nuisance law as an effective means of litigating against spam. Part V will conclude that while common law theories of trespass to chattels and nuisance may effectively address the worst cases of spam, a more appropriate response would be a limited, trespass-like, statutory solution at the federal level.

6. The application of nuisance law to spam was proposed by Dan Burk as part of his criticism of the trespass to chattels framework. *See* Dan L. Burk, *The Trouble with Trespass*, 4 J. SMALL & EMERGING BUS. L. 27, 53–54 (2000). Adam Mosoff has addressed the threshold question of whether the traditional nuisance framework can apply to spam by arguing that e-mail is a type of 'use' of property subject to protection by nuisance law. *See* Adam Mossoff, *Spam—Oy, It's Such a Nuisance*, 19 BERKELEY TECH. L.J. 625, 646–54 (2004). Steven Kam has discussed the application of the nuisance balancing test to the unique facts of *Intel Corp. v. Hamidi*, 71 P.3d 296 (Cal. 2003). *See* Steven Kam, Note, Intel Corp. v. Hamidi*: Trespass to Chattels and a Doctrine of Cyber-Nuisance*, 19 BERKELEY TECH. L.J. 427 (2004). This Note adds to the recent scholarship by (1) further addressing the threshold inquiry of whether the traditional real property law of nuisance can be extended to spam (in other words, by moving beyond simply conceiving of e-mail as a use of land, but seeing the computer as a conduit into real property) and (2) providing an in-depth analysis of the nuisance framework as applied specifically to the most common real-world scenarios of disturbance by spam e-mail. Nuisance in the form of electronic transmissions to a computer system has appeared in cases at the trial level, including several cases that have settled out of court, but it has never been dealt with in an in-depth published opinion. *See, e.g.*, Compl., Parker v. C.N. Enters., No. 97-06273 (Dist. Ct. Travis County Nov. 10, 1997), *at* http://legal.web.aol.com/decisions/dljunk/parkero.html (order finding spamming activities "constituted a common law nuisance and trespass" subject to injunction); Compl., Web Sys. Corp. v. Cyber Promotions, Inc., No. 97-30156 (Super. Ct. Harris County), *at* http://legal.web.aol.com/decisions/dljunk/websysc.html (ISPs petition for injunction against spammer, alleging fraudulent spamming constituted private and public nuisance); Compl., Carstens v. Bonzi Software, Inc., No. 02-207199-1 (Super. Ct. Spokane County), *at* http://www.lukins.com/bonzi/files/complaint.pdf (class action alleging nuisance from pop-up ads that mimicked Windows operating system warnings).

7. *See* DAN B. DOBBS, THE LAW OF TORTS § 463 (2000).

II. BACKGROUND AND POLICY STARTING POINTS

Spam[8] annoys e-mail users with every imaginable disreputable product or activity. Spam e-mails commonly advertise offers for prescription drugs—fake and real, sexual enhancement pills and devices, phone sex lines, ads for pornography websites, pyramid schemes, mortgage refinancing, loan refinancing, credit cards, get-rich-quick schemes, scams, and every sort of fraud. The cumulative effect of spam amounts to more than just an annoyance—it has become a widespread assault on the economy.

A. THE VOLUME OF SPAM IS GROWING

The need for an effective legal approach to spam is becoming increasingly urgent as the spam problem grows exponentially and expands into new areas of digital communication. With no effective technical[9] or legal remedy available to consumers and the methods of obtaining e-mail addresses becoming less expensive,[10] the volume of spam continues to explode. In April of 2003, America Online claimed to have blocked 2.37 billion spam e-mails in one day and typically blocks about 80% of all incoming Internet e-mail traffic as spam.[11] According to recent studies, the percentage of total Internet e-mail identified as spam grew from 45% to 65% of all e-mail between March 2003 and July 2004; an average increase of 1.25% per month.[12] Experts have predicted that at current growth rates the ratio of spam to legitimate e-mail will approach nine to one.[13]

8. For purposes of this paper and as the basis for setting legal policy, spam can be defined generally as a digital communication that is sent (a) in bulk, (b) with little or no current or prior relationship between the sender and recipient, (c) without explicit, revocable consent and (d) that gives a disproportionate benefit to the sender and/or places a burden on the recipient. For a more in depth explanation of the definition of spam, see *infra* Part II.

9. For a good summary of the technical approaches to spam and their limitations, see David E. Sorkin, *Technical and Legal Approaches to Unsolicited Electronic Mail*, 35 U.S.F. L. REV. 325, 344–56 (2001).

10. *See* Mike France, *Commentary: Needed Now: Laws to Can Spam*, BUSINESSWEEK ONLINE, Sept. 26, 2002, *at* http://www.businessweek.com/smallbiz/content/sep2002/sb20020926_5958.htm ("Marketers currently pay $150 for a compact disc with 70 million e-mail addresses.").

11. Sandeep Junnarkar, *AOL Touts Spam-Fighting Prowess*, CNET NEWS.COM, Apr. 30, 2003, *at* http://news.com.com/2100-1025-998944.html.

12. BRIGHTMAIL LOGISTICS & OPERATIONS CTR., SPAM STATISTICS (2004) (on file with the Southern California Law Review) [hereinafter BRIGHTMAIL STATISTICS]. Similarly, a UK-based e-mail filtering company found that 62.7% of all global e-mails sent in December 2003 were spam, up from 55.1% the prior month. Will Knight, *Worsening Spam Epidemic Chokes the Net*, NEWSCIENTIST.COM, Jan. 13, 2004, *at* http://www.newscientist.com/news/news.jsp?id=ns99994562.

13. Knight, *supra* note 1.

B. THE ECONOMICS OF SPAM

Any solution to the spam problem must take into account the basic economic factors involved. First, the response rate to unsolicited e-mail marketing is extremely low. It has been suggested that the response rate to spam is as low as .005%.[14] In other words, the average spam message draws a positive response from only fifty out of a million people.[15]

A second economic factor is the costs of sending bulk e-mail, which are negligible. A spammer's main business expenses are simply a standard personal computer, an Internet Service Provider ("ISP") account (around $20–$30 per month), a one-time purchase of spam mailing software ("spamware"[16]), and a good bulk list of e-mail addresses.[17] The subsequent marginal costs of sending spam are, for all practical purposes, zero.[18]

Finally, on the other side of the economic equation of spam are the massive aggregate costs that are shifted onto businesses and consumers who use the Internet.[19] On a systemic level, spam places substantial costs onto ISPs who must upgrade their storage space, central processing unit ("CPU") power, and filtering software.[20] They also suffer from "denial of service attacks"—overloads that temporarily shut down service and increase support costs, including the need for additional filtering software and customer service representatives.[21] The costs to consumers include

14. France, *supra* note 10.

15. *Id.*

16. Commercial spam software, or "spamware," harvests e-mail addresses from the Internet, allowing marketers to send messages in bulk while employing an assortment of actions to evade detection and blocking by ISPs. *See* ANDREW LEUNG, TELUS CORPORATION, SPAM: THE CURRENT STATE 5 (2003) (on file with author). The cost of spamming has dropped rapidly as more sophisticated, cost-efficient harvesting programs have been developed. *See* France, *supra* note 10.

17. For example, in the Spring of 2003, marketers could purchase 70 million e-mail addresses, representing 3500 potential new customers, for less than $200. *See* France, *supra* note 10.

18. The economics of spam also explain its continuous unchecked growth. Because almost all costs of sending spam are shifted to the recipient, there is virtually no built-in market force to limit its growth. *See* Ian Ayres & Matthew Funk, *Marketing Privacy*, 20 YALE J. ON REG. 77, 83 (2003). The cost structure of spam marketing and its corresponding unfettered growth is in direct contrast to the stable growth levels of "junk mail" sent the old fashioned way via the United States Postal Service. *See* Michael Osterman, *Spam Not at Economic Equilibrium*, NETWORK WORLD FUSION, Feb. 11, 2003, *at* http://www.nwfusion.com/newsletters/gwm/2003/0210msg1.html. Junk mail entails relevant per-parcel costs (paper, printing costs, and postage) and response rates that are well known and remain constant. *Id.* Because of these factors, junk mail remains at a constant economic equilibrium, comprising a relatively small portion of the average household's postage. *Id.* Because the cost of sending spam is virtually nonexistent, it, unlike junk mail, is not at economic equilibrium. *Id.*

19. For details on the costs involved, see Coalition Against Unsolicited Commercial Email, *The Problem*, *at* http://www.cauce.org/about/problem.shtml (last visited Nov. 20, 2004).

20. *See id.*

21. LEUNG, *supra* note 16, at 9.

increased time sorting through mail and deleting spam, losing e-mails due to false positives of filtering software, frustration and psychological harms from perceived privacy invasions, and the offensive nature of many of the messages.[22] Further, taking its content into account, spam brings additional, costly problems for consumers. In its worst and most typical form, spam is a vehicle of "get-rich-quick" schemes, fraud, unwanted obscenity,[23] and increasingly, computer viruses[24] and privacy invasion.[25] In the business context, the costs are likewise substantial. [26] U.S. corporations lost an estimated $10 billion to spam in 2003.[27] The average 4.4 seconds it takes to deal with each message accounted for $4 billion in lost productivity.[28] Consumption of IT resources (for example, server

22. *See id*.

23. A survey by the Gartner Group in 1999 found 37% of spam to be "get-rich-quick" schemes and 25% adult advertisements. GARTNER GROUP, ISPS AND SPAM: THE IMPACT OF SPAM ON CUSTOMER RETENTION AND ACQUISITION 5 (1999). A survey by the Federal Trade Commission ("FTC") using data from 2002 and 2003 found spam content to be 18% adult (for example, "pornography and dating services"), 20% business opportunity (for example, "work at home, franchise, and chain letters"), 17% finance (for example, "credit cards, refinancing, insurance, foreign money offers") and 10% health related (for example, Viagra advertisements). FTC, FALSE CLAIMS IN SPAM 3 (2003), *available at* http://www.ftc.gov/reports/spam/030429spamreport.pdf. With respect to the fraudulent nature of spam, the report found that 33% of spam contained a false "From" line, 22% contained a false "Subject" line, and 66% of all spam contained either a false "From" line, a false "Subject," or false text. *Id.* at 3, 5, 10. Additionally, the FTC found that 40% of spam contained signs of falsity in the message body. *Id.* at 8. With respect to the source of such falsehoods, 90% of the spam categorized as "business opportunities" contained signs of falsehood within the body of the message and spam with pornographic imagery contained falsified "Subject" or "From" lines. *Id*. at 8, 15.

24. In 2002, approximately one in two hundred e-mails contained computer viruses, up 50% from the number of viruses sent in 2001. Matt Loney, *Email Viruses Show Dramatic Rise*, ZDNET UK, Dec. 16, 2002, *at* http://news.zdnet.co.uk/business/0,39020645,2127580,00.

25. A growing new digital invasion called spyware secretly gathers information on unsuspecting computer users and turns it over to marketers and identity thieves, implicating serious invasion of privacy concerns. *See* Editorial, *The Spies in Your Computer*, N.Y. TIMES, Feb. 18, 2004, at A18. A type of spyware called adware tracks where a user goes on the Web and reports back to advertisers so they can send targeted advertisements back to the person. *Another Computer Age Nuisance: Spyware* (NPR radio broadcast, Mar. 18, 2004), *available at* http://www.npr.org/templates/story/story/story.php?storyId=1777227. Some spyware goes as far as taking over the computer or sending the Web browser to sites without the user's permission. *Id*. Such programs can be distributed by e-mail, but are usually slyly packaged within software downloads or may invade computers during web surfing. *Id*. An anti-spyware bill that outlaws the software was recently passed in the House of Representatives. H.R. 2929, 108th Cong. (2004). *See also* Jim Hu, *AIM Add-on Prompts Spyware Concerns*, CNET NEWS.COM, Mar. 3, 2003, *at* http://news.zdnet.co.uk/internet/security/0,39020375,39148016,00.htm.

26. *See, e.g.*, Scott Bekker, *Spam to Cost U.S. Companies $10 Billion in 2003*, ENT NEWS, Jan. 9, 2003, *at* http://www.entmag.com/news/article.asp?EditorialsID=5651 (discussing the estimated annual cost of spam to U.S. corporations).

27. *Id.* In 2003, the total annual cost of spam increased 12%, up from an estimated $8.9 billion in 2002. *Id*.

28. *Id*.

capacity, server administration, bandwidth and disk space, and support accounted for the rest).[29]

Although some level of disorder is to be expected of the Internet, an entity largely governed by "anarchic," nonlegal norms,[30] it is becoming clear that users must gain more control over their e-mail addresses either by shifting costs back to the spammers (through law or technology) or through the adoption of new technological standards. Otherwise, the e-mail system as we know it may come to a grinding halt.

C. POLICY STARTING POINT: DEFINING SPAM

Responding to the problem of spam requires a working definition of what exactly "spam" means. Defining spam is essential to targeting the problem. Typical of a novel problem, the category has been shaped to varying levels of broadness. The definition of spam should optimally take into account key factors of consent and cost shifting.

The recently passed CAN-SPAM Act excludes from its definition of spam the type of e-mail that would most restrict the commercial solicitations of "legitimate" Internet businesses.[31] CAN-SPAM sanctions e-mail that, though unsolicited, is not fraudulent and gives the user an opportunity to opt out.[32] It is not surprising that the Direct Marketing Association lobbied Congress for the adoption of a definition of spam along these lines.[33] Although such e-mail may be less pernicious than other unsolicited communications sent with less transparent means, it nonetheless

29. *Id*.

30. On the problems involved in enforcing Internet norms, see Mark. A. Lemley, *The Law and Economics of Internet Norms*, 73 CHI.-KENT L. REV. 1257, 1266–92 (1998). *See also* Margaret Jane Radin & R. Polk Wagner, *The Myth of Private Ordering: Rediscovering Legal Realism in Cyberspace*, 73 CHI.-KENT L. REV. 1295, 1297–98 (1998) (arguing that the Internet, largely enforced through self-organizing, nonlegal norms, will be best governed by a mixed top-down and bottom-up ordering regime). The difficulties of Internet self-governance have come to the forefront in a recent suit brought by VeriSign against nonprofit coordinator/regulator ICANN over who will control key aspects of the Internet domain name system. *See* David McGuire, *Internet Address Sellers Sue ICANN, VeriSign*, WASHINGTONPOST.COM, Feb. 27, 2004, *at* http://www.washingtonpost.com/wp-dyn/articles/A9415-2004Feb26.html.

31. *See* 15 U.S.C.A. § 7704(a)(1)–(5) (West Supp. 2004). *See also* The Spamhaus Project, *The Spam Definition and Legalization Game*, *at* http://www.spamhaus.org/news.lasso?article=9 (last visited Nov. 20, 2004).

32. § 7704(a)(1)–(5).

33. *See* The Spamhaus Project, *supra* note 31. *See also* The Direct Marketing Association, *The CAN SPAM Act of 2003: What to Look for, What to Look Out For*, *at* http://www.the-dma.org/anti-spam/E-mail_Chart.pdf (last visited Nov. 20, 1004) (advocating a new, legitimate spam—unsolicited and bulk like illegal spam, but distinguished by the truthfulness of the headers, subject line, and message body).

shifts costs to recipients and requires an active response to reject unsolicited communication.[34] When one considers key concepts of consent, cost-shifting, and economic and social utility, this definition fails to address the factors that make unsolicited e-mail problematic.[35]

Spam has also been defined as Unsolicited Commercial E-mail ("UCE").[36] UCE excludes from its scope such messages as fundraising, opinion surveys, religious messages, and political advertisements.[37] Spam was defined on such lines by California's anti-spam laws, which regulated e-mail that was commercial and sent to a recipient who (a) "has not provided direct consent to receive advertisements . . . [and (b)] does not have a preexisting or current business relationship . . . with the advertiser . . . ."[38] Thus, the California approach does not require e-mail to be sent in bulk (eliminating gray areas of deciding what is considered "bulk"), and does not include noncommercial unsolicited e-mail. The California definition of UCE may be seen as a good start at addressing much of the problematic spam. At least on a theoretical level, however, the UCE definition may be underinclusive because noncommercial unsolicited bulk mail often shifts costs and breaches consent in ways that are just as harmful as unsolicited commercial e-mail. [39] Additionally, it may be

34. *See infra* Part III.A.2 (discussing the criticism of the opt-out approach).

35. Defining spam as broadly as possible—as *all* unsolicited e-mail—is also unworkable in that generally, unsolicited e-mails, commercial or personal, that are not also *bulk* usually have some level of utility or implied consent. Examples of nonbulk, unsolicited messages include: a message sent to someone the sender thinks might be a long lost relative or friend, a question to the author of a website, or a request from one website owner to another to exchange links. *See* Sorkin, *supra* note 9, at 335 n.43. Such unsolicited e-mail is rarely considered to be spam, by consumers and academics alike, for a variety of reasons. First, even if one explicitly revokes consent to a nonbulk, noncommercial e-mail, there are independent public policy reasons—for example, promoting Internet growth or respecting Internet norms of consent—or nonetheless implying consent. Nonbulk unsolicited e-mail, often the source of valuable new personal and business relationships, creates exactly the positive social connections that make e-mail such a powerful medium of communication. Thus, in order to encourage positive "network effects"—the phenomenon by which something becomes more useful in proportion to the number of users it gains—a fenceless, open network is the best framework for nonbulk e-mail communication, solicited or otherwise. *See* Burk, *supra* note 6, at 50–51 (explaining the existence of network effects in cyberspace). Additionally, there are stronger constitutional implications with respect to blocking such messages than with blocking UBE or UCE. *See* Sorkin, *supra* note 9, at 335.

36. For further comments on legally defining spam, see generally Sorkin, *supra* note 9, at 327–36.

37. *See id*. at 333.

38. CAL. BUS. & PROF. CODE § 17529.1(o) (West Supp. 2004).

39. It may be helpful at times, for the purposes of enacting legislation, to adopt UCE as the definition of spam. Several reasons have been put forth supporting the use of UCE as a more suitable legal definition: (1) it avoids supposed difficulties in determining whether a message was sent in "bulk"; (2) noncommercial messages (especially political and religious messages) may be protected speech; and (3) regulations confined to commercial messages may be more likely to be adopted than if applicable to both commercial and noncommercial messages. *See* Sorkin, *supra* note 9, at 334.

overinclusive by including in the definition single unsolicited commercial solicitations directed on a one time basis to a specific recipient. While this sort of activity may be without explicit consent, the cost shifting involved, even in the aggregate, does not seem to be particularly substantial.

Finally, Unsolicited Bulk e-Mail ("UBE") is the broadest practical definition of spam. This definition will be adopted for the purpose of this Note because it best tracks issues of consent and cost shifting.[40] If necessary or appropriate, a particular legislative solution can narrow the UBE definition down to exclude noncommercial e-mails by exception.

A good definition of spam as UBE can be derived from the framework provided by anti-spam activist groups: "[a]n electronic message is 'spam' if: (1) the recipient's personal identity and context are irrelevant because the message is equally applicable to many other potential recipients,"[41] (2) little or no connection exists between the recipients and the sender or each other,[42] (3) "the recipient has not verifiably granted deliberate, explicit, and still-revocable permission for it to be sent,"[43] and (4) "the transmission and

Generally, state spam legislation has defined spam as some form of UCE. *See* David E. Sorkin, *Spam Laws: United States: State Laws: Summary*, *at* http://www.spamlaws.com/state/summary.html (last visited Nov. 20, 2004). *See infra* Part III.B for a discussion of California's version of the UCE definition.

40. With respect to the constitutionality of laws based on the UBE definition, it can arguably be viewed as more content-neutral than one focusing on commercial communications. *See* Sorkin, *supra* note 9, at 335. Additionally, such constitutional concerns may be less problematic in the context of common law property framework, where the issue is vindication of one's general right to prevent others from interfering with their private property.

41. Mail Abuse Prevention System, *Definition of "Spam"*, *at* http://www.mail-abuse.org/standard (last visited Aug. 26, 2004); The Spamhaus Project, *The Definition of Spam*, at http://www.spamhaus.org/definition.html (last visited Nov. 20, 2004). *See also* Infinite Monkeys & Co., *Spam Defined*, *at* http://www.monkeys.com/spam-defined/definition.shtml ("Internet spam is one or more unsolicited messages, sent or posted as part of a larger collection of messages, all having substantially identical content.") (last visited Nov. 20, 2004).

42. By adding in the element "and little or no connection exists between the recipients and the sender or each other," the original definition has been adjusted to account for situations of implied consent. The California definition similarly provides for implied consent to unsolicited e-mail in the case where there is an existing personal or business relationship. CAL. BUS. & PROF. CODE § 17538.45(a)(1)–(2). While consent should be explicit with bulk, commercial messages, it may be *implied*, based on social norms, when the recipient has some legitimate social or business connection to the sender and/or the other recipients. Examples of bulk e-mail where consent would be implied on the basis of connection between the sender and recipients would include: forwarding a joke or chain letter on to all of one's friends; "replying all" to a message sent by someone else to all of their friends; or a business sending a holiday greeting message to all of its major suppliers. Such situations, where consent would reasonably be implied based on social expectations or for policy reasons, should be excluded from a legal definition of spam.

43. Mail Abuse Prevention System, *supra* note 41.

reception of the message appears to the recipient to give a disproportionate benefit to the sender."[44]

This revised definition of spam as UBE lacking implied consent breaks the problem of spam into its key components: (1) communication sent in bulk, (2) recipients with little or no legitimate social or business connection to the sender or each other (implied consent), (3) lack of consent, and (4) cost shifting and low to negative utility of the individual transaction to the recipient.

Although this definition addresses the essential problem, the definition will be further delineated with respect to consent, utility, and cost shifting as this Note proceeds to analyze the application of nuisance law's balancing test to spam. The key is that for the purposes of shaping legal policy, the definition of spam should not turn simply on content or veracity, but on the lack of consent, cost-shifting, and low or negative overall utility of an e-mail message.

D. AN E-MAIL AND INBOX PROBLEM

Defining spam does not, however, define the entire problem. Spam may be the mass of unsolicited bulk e-mail, but in the end the problem manifests itself in the inbox. For the purpose of developing legal policy and analyzing common law remedies where consent is relevant, inboxes must be considered independent of other aspects of the Internet such as websites and domain names.[45]

The inbox is the physical server space rented or owned by a user for the purposes of receiving and storing e-mail. The data contained on this server space is usually downloaded, mirrored, and often synchronized to a user's individual computer hard drive space. The inbox is also the virtual space comprised by the graphical representations of lists, files and opened messages displayed by a user's e-mail or text messaging software. More than any other virtual space on the Internet, the inbox has an exclusive quality (at least in the perception of Internet users) comparable to the absolute dominion traditionally bestowed on one's home.[46] While the

44. *Id.*

45. *See* Kenneth C. Amaditz, *Canning "Spam" in Virginia: Model Legislation to Control Junk E-Mail*, 4 VA. J.L. & TECH. 4, paras. 5–9 (1999) (discussing the differences between e-mail as an "active" form of Internet communication and other "passive" forms such as websites).

46. The Gartner Group's survey sheds light on e-mail users' strong negative perception of spam as an invasion of their dominion. *See* GARTNER GROUP, *supra* note 23, at 7 (detailing Internet users' perception of spam). According to the survey, over 30% of e-mail users found spam to be a "significant invasion of their privacy." *Id.* Courts, in adapting the doctrine of trespass to chattels have addressed

server space rented for one's e-mail address is voluntarily placed on an open network, the inbox must be actively reached by typing in a specific address and making direct, personal contact.[47] This distinguishes the inbox from the virtual space of a website that acts primarily as a one-way communicator to the public as a whole, deeply ingrained into the mesh of the World Wide Web ("Web") (via hyperlinks, directories, advertisements, and search engine spiders).[48] The website, by its very nature, may be seen as an irrevocable, open invitation to the public. The inbox, on the other hand, is socially perceived as an invitation-only medium. Presumably, from the perspective of reasonable consumer expectations—at least when it comes to commercial communication—such invitation or consent ideally should be explicit and narrow in scope. Conversely, from the perspective of legitimate marketers having to deal with the practical reality of promoting their businesses via the Web and e-mail, a more flexible view of consent is desirable. Thus, as with the definition of spam discussed above, any legal solution dealing with spam faces the problem of allocating the appropriate balance with respect to consent and the scope of liability between the competing interests of consumers and legitimate marketers.

III. SPAM AND THE LAW TODAY

The current existence of inadequate legal remedies for the growing plague of spam reveals a need for aggressive experimentation in empowering Internet users, either through comprehensive new legislation at the federal level or via the common law. To date, several approaches to spam, both legislatively and in the courts, have met with varying levels of success. Most attempts at curbing spam through legal means have suffered from enforcement deficiencies and have inadequately balanced the competing interests of Internet users and legitimate direct marketers.

virtual spaces, such as e-mail servers and inboxes, in a manner analogous to interests in land. *See generally* Compuserve v. Cyber Promotions, 962 F. Supp. 1015 (S.D. Ohio 1997); Richard A. Epstein, *Cybertrespass*, 70 U. CHI. L. REV. 73 (2003) (arguing that cyberspace can be logically analogized to real property). *But see* Laura Quilter, *The Continuing Expansion of Cyberspace Trespass to Chattels*, 17 BERKELEY TECH. L.J. 421, 442 (2002) (criticizing the courts' expansive common law protections of digital communication mediums by analogizing to real property interests).

47. *See* Amaditz, *supra* note 45, at para. 6.

48. *See* Amaditz, *supra* note 45, at paras. 6–8. This distinction may be a plausible basis for the creation of a right to exclude certain unsolicited digital transmissions to the inbox but not to websites. *But see generally* Burk, *supra* note 6, at 43–47 (arguing that the distinction between websites and e-mail based on consent is illusory).

A. FEDERAL LEGISLATION (CAN-SPAM)

In late 2003, Congress passed the CAN-SPAM Act, the first federal framework for spam.[49] The act is primarily directed towards unsolicited commercial e-mail sent through fraudulent means by illegitimate marketers.[50] Significantly, the act legalizes a class of spam that complies with certain requirements for truthfulness,[51] denies a private right of action,[52] and largely preempts state legislation related to spam.[53]

1. Overview of the Act

a. Requirements

The legislation sets specific requirements for legally sending unsolicited commercial e-mail. Under the Act, marketers generally can send unsolicited bulk e-mail as long as the messages honestly disclose their origin (including a valid postal address), clearly indicate that they are advertisements, and provide a working "opt-out" mechanism.[54] Additionally, the message cannot have been sent by fraudulent means or via illicitly created e-mail lists.[55] Marketers who comply with these requirements can legally send unsolicited messages unless and until the recipient affirmatively executes an opt-out request.[56]

b. Enforcement

The CAN-SPAM Act sets forth limited civil enforcement mechanisms, primarily through the Federal Trade Commission ("FTC"), State authorities, and ISPs.[57] Significantly, recipients of unsolicited messages are not able to sue the senders under the Act.[58]

49. The CAN-SPAM Act of 2003, Pub. L. No. 108–187, § 877, 117 Stat 2699 (codified as amended at 15 U.S.C.A. §§ 7701–7707) (West Supp. 2004); 18 U.S.C.A. § 1037 (West Supp. 2004)).

50. *See id*.

51. *See* 15 U.S.C.A. § 7704(a)(1)–(5) (West Supp. 2004).

52. *See id.* at § 7706(f)–(g). For a directory of online summaries and discussions of CAN-SPAM, see GigaLaw.com, *CAN-SPAM Library*, *at* http://www.gigalaw.com/canspam/articles.html (last visited Nov. 20, 2004).

53. 15 U.S.C.A. § 7707(b).

54. *Id.* § 7704(a)(3)–(5).

55. *Id.* § 7704(b); 18 U.S.C.A. § 1037 (West Supp. 2004) .

56. *Id.* § 7704(a)(3)–(5).

57. *Id.* § 7706(a), (f)(1), (g)(1).

58. *Id.* § 7706.

c. Penalties

The act sets statutory damages on a per message basis, with a cap of $1,000,000 or $2,000,000 per suit, depending on whether an action is brought by the FTC or ISPs.[59] It also allows courts to treble the damages in cases where defendants willfully commit violations or when the messages were sent by evasive or fraudulent methods.[60] Additionally, in the case of messages sent using fraudulent methods, the Act provides for criminal penalties, including incarceration.[61]

2. Criticism of the Act

Technology and legal experts harshly criticize CAN-SPAM for several reasons. First, they argue that it wrongly denies a private right of action. Second, they claim it moves too quickly in preempting stronger state laws. Third, it legalizes spam from so-called legitimate marketers under an "opt-out" approach.[62]

Experts have argued that the Act's limited enforcement authority and the significant costs involved in bringing these lawsuits make it likely spammers will be held liable only for the most egregious of violations.[63] Some instead advocate legislation with enforcement akin to California's Junk Fax law and now preempted spam law, in which private individuals can quickly and cheaply bring spammers to small claims courts and obtain statutory judgments based on easily provable legal standards.[64] Proponents of a statutory framework with such private remedies or alternatively, a system of bounty rewards, argue it would deter spammers by placing de facto postage costs onto spam. In this sense each spam sent out would

59. *Id.* § 7706(f)(3)(B), (g)(3)(B).

60. *Id.* § 7706(f)(3)(C), (g)(3)(C).

61. *See* 18 U.S.C.A. § 1037(D) (West Supp. 2004).

62. 15 U.S.C.A. § 7704(a)(3)–(5). *See also* Amit Asaravala, *With This Law, You Can Spam*, WIRED NEWS, Jan. 23, 2004, *at* http://www.wired.com/news/business/0,1367,62020,00.html; The Spamhaus Project, *United States Set to Legalize Spamming on January 1, 2004*, *at* http://www.spamhaus.org/news.lasso?article=150 (last visited Nov. 20, 2004); Tom Spring, *Why Spammers Love the CAN-SPAM Law: Anti-spam Laws Make Some Spamming Legal and Do Little to Quell the Onslaught*, PC WORLD, Jan. 19, 2004, *at* http://www.pcworld.com/resource/printable/article/0,aid,114363,00.asp; Chris Ulbrich, *Spam Law Generates Confusion*, WIRED NEWS, Jan. 26, 2004, *at* http://www.wired.com/news/business/0,1367,62031,00.html.

63. *See* Telephone Interview with David Kramer, Partner, Wilson, Sonsini, Goodrich & Rosati (Feb. 20, 2004); Coalition Against Unsolicited Commercial Email, *Statement on Can-Spam Act*, *at* http://cauce.org/news/2003.shtml (Dec. 16, 2003) [hereinafter *Statement of Can-Spam Act*].

64. *See* Kramer, *supra* note 63; Jessica Levine, *Spam and the Law*, PC MAGAZINE, Feb. 25, 2003, *at* http://www.pcmag.com/print_article/0,3048,a=36204,00.asp (noting the view of anti-spam activists urging the use of antifax legislation as a model for anti-spam legislation at the federal level).

entail the future repercussion of defending thousands of small claims lawsuits down the road.[65]

Second, many have argued that the Act is not only ineffective but affirmatively harmful by preempting strong proconsumer remedies for spam in states such as California.[66] In one sense, this argument may, at its core, appeal to the general idea that the Act could have been stronger when compared to the previously enacted state laws, not the issue of whether federal unification of the law would be beneficial. Marketers have made the sensible argument that the assortment of spam laws made it costly and confusing for them to comply with the various requirements in each state.[67] Nonetheless, as a new problem it could have been helpful to give time for state experimentation with different legal approaches.

Finally, the Act has been heavily criticized for its opt-out approach, which anti-spam activists predict will lead to a new flood of legal spam.[68] The opt-out approach creates a default of consent to all e-mail sent with truthful indicators of origin and status as advertisements, unless and until the recipient actively opts out. From the standpoint of anti-spam groups, this exacerbates the problem by requiring consumers to continually opt out of commercial communications.[69] They point out that if just 1% of the approximately 23 million small businesses in the United States[70] directed just one e-mail per year to a user's inbox, that individual would have to sort through over 600 messages per day.[71] The sheer numbers and cost shifting involved with e-mail have thus led many to question the wisdom of the opt-out approach to spam.[72] As Congressman Gary Miller points out

> [l]egally, opt-out is a step backwards because it accepts the first [s]pam message as legal, thereby granting the [s]pammer an extraordinary legal

65. *See* Kramer, *supra* note 63. *See also* Asaravala, *supra* note 62.

66. *Id*.

67. *See* Grant Gross, *State Spam Laws and the New CAN-SPAM*, INFOWORLD, Feb. 27, 2004, *at* http://www.infoworld.com/article/04/02/27/09FEspamstates_1.html?security (noting the "compliance headache" for e-mail marketers).

68. *See* Coalition Against Unsolicited Commercial Email, *CAUCE Does the Math—Why Can't the Marketing Industry?*, *at* http://www.cauce.org/pressreleases/math.shtml (last visited Nov. 20, 2004). *See also Statement on Can-Spam Act*, *supra* note 63.

69. *See* Coalition Against Unsolicited Email, *supra* note 68.

70. SMALL BUSINESS ASS'N, OFFICE OF ADVOCACY, SMALL BUSINESS BY THE NUMBERS 1 (2004), *available at* http://www.sba.gov/advo/stats/sbfaq.pdf.

71. *See* Coalition Against Unsolicited Commercial Email, *supra* note 68.

72. An additional problem with the opt-out approach is that given the difficulties in identifying truthful from untruthful spam, users may be encouraged to follow through with opt-out links in spam e-mails, which in most cases only confirm to the spammer that the recipient is a valid e-mail address, inviting even further spam as one's e-mail address is added into premium spam CDs. *See* Coalition Against Unsolicited Commercial Email, *supra* note 19.

> right to the ISP's computer in the first instance. Practically, opt-out does not make sense . . . . Once we have granted a [s]pammer one free bite at the apple, we are better off with no law at all.[73]

On the whole, many assert that with its limited avenues for enforcement and opt-out scheme, CAN-SPAM does little to deter spammers and creates a new set of problems by empowering direct marketers with legal means of spamming.[74]

B. ATTEMPTED STATE LEGISLATION AS AN ALTERNATIVE STATUTORY MODEL

Prior to the enactment of CAN-SPAM, a patchwork of laws to curb spam had been enacted in thirty-eight states.[75] Similar to CAN-SPAM, most states provided for an opt-out approach, with required disclosures for e-mail advertisements.[76] Significantly, however, California, Delaware, and Washington adopted more proconsumer positions on spam, with an opt-in approach and potentially effective means of civil enforcement.[77] The California law targets unsolicited commercial e-mail, defined clearly as any electronic message with the purpose of promoting the sale of goods or services sent to a recipient who (a) "has not provided direct consent to receive advertisements [and (b)] does not have a preexisting or current business relationship . . . with the advertiser."[78] In providing for enforcement, the law parallels the state's previous junk fax legislation by allowing individual recipients of such unsolicited commercial e-mail to obtain liquidated damages of $1,000 per e-mail advertisement.[79] Consistent with a bright-line trespass rule, California's law generally follows a strict liability regime. It does, however, allow courts to reduce the liquidated damages to $100 per message when the defendant acted reasonably in implementing procedures designed to prevent the sending of unsolicited e-

73. Gary Miller, *How To Can Spam*, 2 VAND. J. ENT. L. & PRAC. 127, 130 (2000).

74. *See* Asaravala, *supra* note 62.

75. *See* Sorkin, *supra* note 39.

76. *See id*. *See generally* Sorkin, *supra* note 9, at 368–84 (detailing state legislative approaches to spam).

77. CAL. BUS. & PROF. CODE § 17529 (West Supp. 2004); DEL. CODE ANN. tit. 11, §§ 931, 937–38 (2004); WASH. REV. CODE § 19.190.070 (2004). *See also* Sorkin, *supra* note 39.

78. CAL. BUS. & PROF. CODE § 17529.1(o). As in the definition of spam in Part II *infra*, California provides for implied consent to unsolicited e-mail in the case where there is a preexisting or current personal or business relationship. *Id.* The California approach differs in that its definition does not require e-mail to be sent in bulk (eliminating gray areas of deciding what is considered "bulk") and does not include noncommercial unsolicited e-mail. *Id*.

79. *Id.* § 17529.8(a)(1)(B).

mail.[80] The California Act, by providing a limited trespass-like entitlement, may be a good blueprint for how federal lawmakers could enact a better, more efficient anti-spam law based on a bright-line rule.[81] Thus, it is important to consider the now preempted California law in comparison to the new federal scheme in considering appropriate alternative legal means for approaching spam.

C. SPAM UNDER THE COMMON LAW DOCTRINE OF TRESPASS TO CHATTELS

1. Trespass Meets the Internet

While a patchwork of state laws of varying strength have been enacted and subsequently preempted, ISPs have successfully obtained damages and injunctions against spammers on the common law theory of trespass to chattels. Trespass to chattels is a tort that provides remedy for the unauthorized intentional removal or damage of personal property.[82] Unlike trespass to land, however, liability is not provided for purely nominal damages.[83] According to the *Restatement (Second) of Torts* ("Restatement"): "The interest of a possessor of a chattel in its inviolability . . . is not given legal protection by an action for nominal damages for harmless intermeddlings with the chattel . . . . [The] conduct must affect some other and more important interest of the possessor . . . ."[84]

80. *Id.*

81. The law is efficient in providing a level of deterrence in that, like the successful California and federal laws for junk faxes, it sets clear standards and liquidated damages that allow enforcement through quick and inexpensive individual lawsuits. *See* 47 U.S.C.A. § 227 (West. 2002); CAL. BUS. & PROF. CODE § 17529.8(a)(1)(B). *See also* JUNKFAX.ORG, HOW TO GET $2500 OR MORE PER JUNK FAX YOU RECEIVE, *at* http://www.junkfax.org/fax/action/how_to_sue.html (explaining the relatively simple process of obtaining judgments in California small claims courts under the junk fax laws). In a typical junk fax case, the plaintiff simply has to establish: (a) "I received a fax from [junk faxer] on date y"; (b) "the fax was sent without . . . express invitation"; and, in order to obtain treble damages, (c) the fax was sent willfully or knowingly. *Id*. *But see* Ryan Singel, *Fax.com Still Dodging Legal Slaps*, WIRED NEWS, Jan. 12, 2004, *at* http://www.wired.com/news/print/0,1294,61861,00.html (detailing the difficulties involved in collecting a large judgment from one of the biggest and most evasive fax marketing companies). By contrast, a typical big lawsuit against a single spammer brought by an ISP, under either a common law theory or CAN-SPAM, entails legal fees upward of $250,000. *See* Kramer, *supra* note 63.

82. *See* RESTATEMENT (SECOND) OF TORTS §§ 217–218 (1965) [hereinafter TORTS]; W. PAGE KEETON, DAN B. DOBBS, ROBERT E. KEETON, & DAVID G. OWEN, PROSSER AND KEETON ON THE LAW OF TORTS § 14, at 85–88 (5th ed. 1984) [hereinafter PROSSER & KEETON]; Epstein, *supra* note 46, at 76–79.

83. *See* TORTS, *supra* note 82, § 218.

84. *Id*. § 218 cmt. e.

The leading case applying trespass to chattels to spam is *Compuserve v. Cyber Promotions, Inc.*[85] Cyber Promotions, a spam marketing service, sent a high volume of unsolicited e-mail to users of the Compuserve network.[86] Compuserve received complaints from subscribers threatening to cancel the service and claimed the high volume of messages placed a significant burden on the finite processing and storage capacity of its servers.[87] The ISP notified Cyber Promotions that it was not permitted to use its equipment to store and process its e-mail.[88] Nonetheless, the volume of spam subsequently increased as Compuserve's efforts to filter out the continuing transmission of unwanted e-mails were circumvented by Cyber Promotions through typical means such as concealing the origins of the messages.[89]

Although the application of the law of trespass to e-mail had never been previously addressed, the court turned to the precedent of *Thrifty-Tel, Inc. v. Bezenek*, a case involving a minor who had hacked into a telephone system with his computer.[90] *Thrifty-Tel* held that electronic signals generated by a computer to a telephone system were sufficiently tangible to support a cause of action for trespass to chattels.[91] The court in *Compuserve* adopted this view in reaching the threshold determination that the transmission of e-mail to an ISP's computer equipment could be properly addressed within the trespass to chattels framework.[92] In turn, the court followed the Restatement's guidance on the type of situations in which trespass to chattels can be actionable.[93] According to the Restatement:

> [O]ne who commits a trespass to a chattel is subject to liability to the possessor of the chattel if, but only if:
>
> (a) he dispossesses the other chattel, or
>
> (b) the chattel is impaired as to its condition, quality, or value, or
>
> (c) the possessor is deprived of the use of the chattel for a substantial time, or

85. Compuserve, Inc. v. Cyber Promotions, Inc., 962 F. Supp. 1015, 1020–27 (S.D. Ohio 1997).
86. *Id*. at 1017.
87. *Id*. at 1019.
88. *Id*. at 1017.
89. *See id*. at 1019.
90. Thrifty-Tel, Inc. v. Bezenek, 54 Cal. Rptr. 2d 468, 471 (Ct. App. 1996).
91. *See id.* at 472–74.
92. *See Compuserve*, 962 F. Supp. at 1021.
93. *See id*. at 1021–22.

> (d) bodily harm is caused to the possessor, or harm is caused to some person or thing in which the possessor has a legally protected interest.[94]

The court held that the value of Compuserve's equipment was diminished even though it was not physically harmed because the high volume of mail from the defendant placed demands on the storage space and processing power of its servers, which in turn diminished the services it was able to afford its customers.[95] Alternatively, under section 218(d) of the Restatement, the court found that the aggregate economic effects of its customers sifting through unwanted messages amounted to harm to the legally protected interest in its goodwill and business reputation.[96] The court additionally took note that in order to impose liability for such damages under the Restatement, plaintiffs must exhaust self-help measures.[97] Subsequently, several cases with similar facts applied a trespass to chattels theory to e-mail following the reasoning laid out in *Compuserve*.[98]

2. The Extension of Trespass to Chattels Critiqued—A Slippery Slope?

The doctrine soon exploded into a sort of "trespass to websites," in cases brought to limit access to websites by search-engine-like software.[99] Automated software is often used by websites to access content from the databases of other websites (such as sports scores or auction results) in order to summarize the information for Internet users. In *eBay v. Bidder's Edge*, a court found a company's use of such software to access auction results posed a potential for harm to the capacity of eBay's servers sufficient to support a trespass to chattels claim and was thus grounds for a permanent injunction.[100]

The prospect of such expansion and the potential for even broader use of the doctrine led some, such as Dan Burk, to question the benefits of

94. TORTS, *supra* note 82, § 218.

95. *See Compuserve*, 962 F. Supp. at 1022.

96. *See id*. at 1022–23.

97. *See id*. at 1023.

98. *See* Marjorie A. Shields, Annotation, *Applicability of Common-Law Trespass Actions to Electronic Communications*, 107 A.L.R. 5th 549 (2003); Quilter, *supra* note 46, at 430.

99. *See, e.g.*, Register.com, Inc. v. Verio, Inc., 126 F. Supp. 2d 238 (S.D.N.Y. 2000); eBay, Inc. v. Bidder's Edge, Inc., 100 F. Supp. 2d 1058 (N.D. Cal. 2000). *Cf.* TicketMaster Corp. v. Tickets.com, Inc., No. CV997654HLHVBKX, 2003 WL 21406289, at *3 (C.D. Cal. Mar. 7, 2003) (finding that the "mere use of a spider to enter a publicly available website to gather information" without evidence that the use or utility of the computer was adversely effected is insufficient to satisfy the harm requirement of trespass to chattels).

100. *See eBay*, 100 F. Supp. 2d at 1071–73.

granting a right to exclude unwanted electronic transmissions to Internet devices.[101] Burk suggests that the *Compuserve* decision draws trespass to chattels so broadly that it can be extended to any electronic invasion imaginable, including trespass to phones, faxes, and even toasters.[102] He argues that the trespass approach applied to the Web could eliminate the public benefits from an open cyberspace network through what he describes as "over-propertization."[103] Burk bases much of his analysis on the proposition that the Web is a digital "commons" in the sense that the Web-enabled public shares a common communications resource by plugging into the Internet.[104] He sums up the economic theory behind the use of trespass as a means of protecting against abuse of the common resource of the Internet as follows:

> The claim of trespass is to some extent an attempt to avoid a negative externality, that is, the cost imposed by spammers upon network users . . . . Spammers may use the digital commons . . . without considering the external costs of their usage . . . . Typically, external costs . . . may be internalized by creating private property interests that give users an incentive to consider the full cost of their usage, or seek

101. *See* Burk, *supra* note 6, at 48–53. *See also* Dan Hunter, *Cyberspace as Place and the Tragedy of the Digital Anticommons*, 91 CAL. L. REV. 439, 500–13 (2003) (arguing that the cyberspace as place metaphor is resulting in propertization of the Internet that will lead to a "digital anti-commons"). For further discussion of the legal implications of applying property metaphors to cyberspace, see Mark A. Lemley, *Place and Cyberspace*, 91 CAL. L. REV. 521, 523–28 (2003); Maureen A. O'Rourke, *Property Rights and Competition on the Internet: In Search of an Appropriate Analogy*, 16 BERKELEY TECH. L.J. 561, 586–93 (2001) (arguing that more flexible rules are needed to govern access to websites in order to avoid unintended anticompetitive consequences of applying rules or access to traditional real or personal property). *But see* Epstein, *supra* note 46, at 79–84 (arguing that old property torts such as trespass to land and trespass to chattels can adapt well to new problems posed by e-mail); David McGowan, *Website Access: The Case for Consent*, 35 LOY. U. CHI. L.J. 341, 375–85 (arguing in favor of a property rule to govern website access, conditioned by a default of consent as the best way to facilitate bargaining on terms so likely to increase net social welfare and disputing the view that right to exclude at the website level will lead to an anti-commons); Jane K. Winn, *Symposium: Technology, Values, and the Justice System: Crafting a License to Know from a Privilege to Access*, 79 WASH. L. REV. 285, 286–87 (suggesting that the scope of trespass to chattels can be refined by conditioning the right to exclude with a defense of constructive consent—an affirmative privilege of reasonable access to Internet resources); I. Trotter Hardy, *The Ancient Doctrine of Trespass to Web Sites*, 1996 J. ONLINE L. art. 7, para. 6, *at* http://www.wm.edu/law/publications/jol/95_96/hardy.html (supporting the application of trespass theory to websites).

102. The law already provides protection against unwanted invasions of telephones and fax machines without employing a balancing test. *See* 47 U.S.C.A. § 227(b)(1)(B) (West 2003) (prohibiting calls to residential phone lines using artificial or prerecorded voice without consent); *Id*. § 227(b)(1)(C) (prohibiting unsolicited fax advertisements); *Id*. § 223(a)(1)(E) (banning use of phone repeatedly for harassment). *See also* Tom W. Bell, *Internet Law Chapter 6: Trespass to Chattels*, *at* http://www.tomwbell.com/NetLaw/Ch06.html (last visited Nov. 20, 2004). The difference of course is that such limited statutory rules do not run the risk of even further expansion. *See id*.

103. Burk, *supra* note 6, at 48–54.

104. *Id*. at 48.

> permission to impose usage costs upon the property of another. Thus, propertizing the Net may initially seem an attractive way to accomplish this: by granting local system operators a right to exclude . . . .[105]

He goes on to argue, however, that the propertization of the Internet may have separate, adverse effects of creating hold-out problems and an anti-commons: the state in which property rights become divided up to the point where they prohibit the feasibility of performing business transactions because of the many licenses that must be obtained.[106] Additionally, he adds that the Web creates positive network effects, or benefits accrued as more people use the system.[107] Thus, he predicts that using trespass to close off the Internet may cause adverse effects that could ultimately outweigh the benefits of forcing spammers to internalize the cost of their activities.[108] Therefore, assuming trespass to chattels can be applied almost without limit wherever one decides to withdraw consent on the Internet, Burk suggests that the better property theory would be nuisance. He notes that nuisance would avoid the problems of trespass by allowing courts to balance the interests of various users of the Internet as a common resource.[109] Alternatively, he suggests that a trespass-like property approach could work if limited through targeted legislation.[110]

3. Expansion of Trespass to Chattels Curtailed

The continuing expansion of trespass to chattels has come into question, in light of the California Supreme Court's decision in *Intel v. Hamidi*, which narrowed the doctrine.[111] In *Hamidi*, a former Intel employee sent mass e-mails to the company's employees, criticizing its employment practices.[112] Hamidi evaded Intel's efforts to block his e-mails and continued to send out mass mailings despite the company's demand that he stop.[113] The court held that trespass to chattels does not encompass an electronic communication that neither damages nor impairs the functioning of a recipient computer system.[114] The court noted, however, that damage to the chattel could occur in the case when an ISP's servers

105. *Id*. at 48–49.
106. *See id*. at 49.
107. *See id*. at 50.
108. *See id*. at 51.
109. *See id*. at 53–54.
110. *See id*.
111. *See* Intel Corp. v. Hamidi, 71 P.3d 296 (Cal. 2003).
112. *Id*. at 300–01.
113. *Id*.
114. *Id*. at 304, 306–07.

was overloaded by spam to the extent that the spam was slowing down the overall e-mail traffic on the ISP's system.[115] Thus, according to the *Hamidi* Court, its decision did not run contrary to the holding of *Compuserve* recognizing such direct harms.[116] The indirect harm of declining productivity by workers, however, was found to be outside the reach of trespass to chattels.[117]

IV. THE FUTURE OF PROPERTY TORTS APPLIED TO SPAM

The common law has incrementally developed a logical coherence in the area of balancing and allocating property entitlements that can be helpful in legally approaching the problem of unsolicited bulk e-mail invading the inbox. Trespass to chattels has served as a gap-filler in lieu of the development of effective spam legislation. The baseline definition of spam arrived at in Part II above suggests that adoption of a complete entitlement would be optimal. Nonetheless, there are reasons for moving towards a looser or "muddy" legal rule. As Burk points out, the use of trespass can become detrimental to the Internet's growth as an open system if it extends into the protection of websites against unwanted invasions caused by search engines and hyperlinks.[118] Burk's criticism of trespass to chattels can be countered, however, by considering consent as a limiting concept. His argument that a trespass entitlement will lead to a balkanization of the Internet implicitly assumes that (a) *Compuserve* represents the application of a potentially ever-expansive nominal damages rule, imposing liability for mere electronic transmission and (b) it will be difficult for courts to delimit trespass to chattels on the basis of implied consent or privilege.[119] The proposition that trespass, under *Compuserve*, applies to anywhere that electrons impinge on another's computer device may not fully account for basic notions of consent.[120] Under standard social expectations certain types of communications are impliedly consented to regardless of whether they are "unwanted."[121] Thus, common notions of implied consent or a policy-defined privilege of constructive consent might effectively serve the courts as boundaries of trespass.[122] For example, as discussed in Part I, implied consent distinguishes the inbox

115. *See id*.
116. *Id*. at 307–08.
117. *Id*. at 308.
118. *See* Burk, *supra* note 6, at 48–52.
119. *See id*. at 29, 53–54.
120. *See* Epstein, *supra* note 46, at 85.
121. *Id*.
122. *See id*; Winn, *supra* note 103, at 286–87.

from websites. Nonetheless, the potential expansion of trespass is not unrealistic. Additionally, on a practical level, even if one concludes that e-mail would be optimally dealt with under a trespass framework, there are benefits to the parallel application of nuisance law because of its ability to cover situations beyond the line drawn by *Hamidi*. For example, under nuisance, a plaintiff could recover damages in the form of declining productivity and personal discomfort, whereas under the *Hamidi* interpretation of trespass to chattels, such claims would not be recognized. This section explores the extent to which invasions of spam on the inbox can fit within the outer edges of nuisance and the practical limitations on enforcement of e-mail entitlements through the common law.

A. E-NUISANCE—OVERVIEW AND THRESHOLD INQUIRIES

1. Nuisance—Private Nuisance Overview[123]

Private nuisance law primarily addresses the right to use and enjoy one's land free of intangible invasions.[124] At one time, nuisance law, as described by William Prosser, was an "impenetrable jungle," having meant "all things to all people," and applied broadly to everything from "an alarming advertisement to a cockroach baked in a pie."[125] It is possible, however, to set up a coherent framework of private nuisance on the basis of a type of harm to the plaintiff—diminished enjoyment of rights in land.[126] Nuisance can be defined generally as an activity that intentionally[127] interferes with the use and enjoyment of land through intangible invasions that are unreasonable.[128]

123. The law of nuisance varies from state to state. For the purpose of analysis and breadth of coverage, this Note will generally follow the framework of the *Restatement (Second) of Torts*.

124. *See* DOBBS, *supra* note 7, § 462, at 1319.

125. PROSSER & KEETON, *supra* note 82, § 86, at 616.

126. *See* DOBBS, *supra* note 7, § 462, at 1321.

127. The intent requirement is usually satisfied on the basis of knowledge or purpose—if the actor acts with the purpose of causing an invasion or knows that the invasion is occurring or is substantially certain to result. S*ee* TORTS, *supra* note 82, § 825; PROSSER & KEETON, *supra* note 82, § 87, at 624–25. Additionally, most nuisance suits involve recurring or continuing conduct. *See* TORTS, *supra* note 82, § 825 cmt. d. Thus, in cases where no knowledge existed at the first instance of engaging in the activity, it becomes intentional when continued after the actor knows it is causing invasions. *See id*. The act of spamming in most cases would easily satisfy intent on the basis of knowledge to substantial certainty. It might be found unintentional, however, in situations such as when a company purchases a bulk mailing list it believes contains e-mail addresses that have been obtained with consent. In such cases, it might be necessary for plaintiffs to first contact spammers via cease and desist notices or opt-out requests in order to satisfy this requirement. Thus, to some extent, nuisance's intent requirement may give companies that hire spammers at least one bite of the apple to send out mass mailings.

128. *See* TORTS, *supra* note 82, §§ 821–830; DOBBS, *supra* note 7, § 463, at 1321.

Examples of nuisance include activities by defendants that cause disturbances to occupants through dust, smoke, gas, odors, chemicals, loud noises, or excessive light.[129] Nuisance has also been found with disturbances of peace of mind, for example, from the presence of a nearby house of prostitution.[130]

a. The Outer Bounds of Nuisance Law—Precedents for Applying the Framework to Spam

Several cases set a precedent for finding nuisance in electronic signals creating disturbances analogous to those found in the Internet and e-mail contexts. First, nuisance has been applied several times to excessive phone calls.[131] Additionally, the law has been applied to an electronic invasion affecting the use of a more portable, personal property item: the television.[132]

Courts have granted liability for abusive phone calls under nuisance theory.[133] In *Brillhardt v. Ben Tipp*, the Washington Supreme Court found as a threshold matter that frequent phone calls resulted in an actual invasion to the "right to enjoy . . . property without unreasonable interference."[134] Thus, under nuisance doctrine, the court imposed liability on the finding that the phone calls constituted an unreasonable annoyance.[135]

In *Wiggins v. Moskins Credit Clothing Store*, a federal district court similarly held that harassing daily phone calls over a three-month period amounted to nuisance.[136] The court found that the repeated phone calls were "an intrusion into [the] home and an interference with the peaceful enjoyment thereof."[137] Thus, the court held that these phone calls were an

129. *See* DOBBS, *supra* note 7, § 463, at 1322; PROSSER & KEETON, *supra* note 82, § 87, at 619–20.

130. *See, e.g.*, Tedescki v. Berger, 43 So. 960, 961 (Ala. 1907) (holding that a house of prostitution was a nuisance); Crawford v. Tyrrell, 128 N.Y. 341, 345 (1891) (same).

131. *See, e.g.*, Wiggins v. Moskins Credit Clothing Store, 137 F. Supp. 764 (E.D.S.C. 1956); Macca v. Gen. Tel. Co. of the Northwest, 495 P.2d 1193 (Or. 1972); Brillhardt v. Ben Tipp, Inc., 297 P.2d 232 (Wash. 1956).

132. *See* Page County Appliance Ctr. Inc., v. Honeywell, Inc., 347 N.W. 2d 171 (Iowa 1984). For a discussion of the application of nuisance to junk faxes, see Jennifer L. Radner, Comment, *Phone, Fax, and Frustration: Electronic Commercial Speech and Nuisance Law*, 42 EMORY L.J. 359, 397–401 (1993).

133. *See, e.g.*, *Wiggins*, 137 F. Supp. 764; *Macca*, 495 P.2d 1193; *Brillhardt*, 297 P.2d 232.

134. *Brillhardt*, 297 P.2d at 235.

135. *See id*. at 234.

136. *See Wiggins*, 137 F. Supp. at 764, 767.

137. *Id*. at 767.

"invasion of a proprietary interest of [the] plaintiff in her home . . . by conduct tantamount to a nuisance."[138]

In a later case, *Macca v. General Telephone Co. of the Northwest*, the Oregon Supreme Court found that the listing of the plaintiff's phone number as an "after-hours" floral shop, thereby resulting in numerous phone calls, resulted in an invasion of the right to use and enjoy property free from unreasonable interference.[139] As such, the court held that the disturbance caused by these phone calls was governed by the law of private nuisance.[140]

One court, however has taken a more cautious approach. In *Sofka v. Thal*, several calls during the day were found not to be nuisance.[141] The court noted in dicta that phone calls were a nuisance only if the number or frequency of calls was "great enough to seriously annoy a person of ordinary sensibilities."[142] Surprisingly, the court added that "[r]epeated telephone calls are an accepted feature of everyday life, and maintaining telephone service evidences the expectation if not the hope of calls from time to time."[143] Today, at least in the context of telemarketing, the popularity of the national do-not-call list suggests the more common views is quite the opposite.[144]

Nuisance has also been applied to electronic disturbances to television reception. *Page County Appliance Center v. Honeywell* held that a jury could find that radiation emitted from a computer installed in a nearby travel agency that caused the disturbance of television reception was a legal nuisance.[145] The court noted the ubiquity of televisions "in almost every home," implying that such activities would not be considered abnormal to general residential or business use of property.[146] Today, similar observations can be made with respect to the use of computers and sending e-mail.

138. *Id*.
139. *Macca*, 495 P.2d at 1193–94, 1196.
140. *See id*. at 1195.
141. *See* Sofka v. Thal, 662 S.W.2d 502, 509 (Mo. 1983).
142. *Id*.
143. *Id*.
144. Caroline E. Meyer, *In 1 Year, Do-Not-Call List Passes 62 Million*, WASH. POST, June 24, 2004, at E05.
145. Page County Appliance Ctr., Inc. v. Honeywell, Inc., 347 N.W.2d 171, 176 (Iowa 1984).
146. *Id*.

2. Adapting Private Nuisance Law to Spam—Are Analogies Necessary?

Nuisance law protects the use and enjoyment of land from intangible nontrespassory invasions.[147] Thus, as a preliminary matter, in addressing the abuse of e-mail under a nuisance framework, courts will have to pass a threshold issue of whether this cause of action, traditionally confined to disturbances to real property,[148] can be applied to spam. Because the disturbance created by e-mail may be somewhat tangentially related to land, there are two possible ways that courts would approach it under the nuisance framework. First, nuisance could be applied directly under the traditional framework by viewing the computer either as a conduit into real property or as a type of "use" of real property. Second, nuisance law could be extended into the realm of personal property.[149]

a. Nuisance Applied to Spam Under the Traditional Framework: The Computer as a Conduit into Real Property.

Common law has proven to be very flexible, but with its incremental movements and the weight of precedent, it can be slow to adapt. Courts may thus hit a wall when approaching the traditional application of nuisance as a cause of action applying to the use and enjoyment of land. This may be especially true considering that courts have several cases before them characterizing the problem as an invasion to personal property under the trespass to chattels framework. Nonetheless, logically, this should not prevent the application of nuisance to e-mail. Several cases discussed above have applied the theory to electronic invasions affecting the use of personal property such as telephones[150] and televisions.[151] Similarly, the sending of spam can be directly approached under traditional

147. *See* DOBBS, *supra* note 7, § 462, at 1319.

148. *See* PROSSER & KEETON, *supra* note 82, § 86, at 618. Public nuisance does not require an activity to affect the use and enjoyment of private land. DOBBS, *supra* note 7, § 467, at 1335. This Note will not address public nuisance in depth. Such suits against spammers are viable and could clearly be enforced by public authorities. *See id*. To be brought by private parties, the public nuisance must also be a private nuisance to the plaintiff or cause "special harm to the plaintiff in the exercise of the public right." *Id*. ISPs or, perhaps in the case of pornographic spam, households with children might have a special harm in the exercise of a public right. For the most part, however, other private parties would likely not be able to bring a public nuisance action without also having a viable private nuisance claim.

149. In theory a court could address spam by analogy to nuisance as a new sort of digital property tort. This possibility will not be addressed in detail here because it is highly unlikely that a court would make such substantial gap-filling leaps under the common law. Additionally, a new tort specific to spam, unless broadly applicable to all Internet property, would probably be preempted by CAN-SPAM. *See* 15 U.S.C.A. § 7707 (West Supp. 2004).

150. *See, e.g.*, Brillhardt v. Ben Tipp, Inc., 297 P.2d 232, 234 (Wash. 1956).

151. *Page County*, 347 N.W. 2d at 175–76.

nuisance law as an invasion on the use and enjoyment of land if the inbox is viewed as a conduit to and use of real property.[152]

In reaching the conclusion that e-mail falls within the framework of nuisance, one can start by comparing spam to unsolicited telephone calls. Like the telephone, e-mail inboxes are a form of personal property that permit electronic invasions that interfere with the use and enjoyment of land. Or, more directly, communicating on a computer through e-mail is in itself a type of use of one's land subject to protection from interference by nuisance law.[153]

One may argue that, unlike the telephone, the computer might not be a necessary part or common use of one's home. Computers are not usually attached fixtures and, as such, can be easily replaced. Further, the e-mail account accessed by the computer can be seen as even less permanent. Thus, it can be argued that the inbox should not be seen as an ingrained, open window into real property space or a use of land because use of the inbox reflects an individual choice of the property owner. This assumption that e-mail is unnecessary can be countered, however, by considering the level to which e-mail has become as integral to the home as the telephone. We are not far off from a world in which e-mail is as basic a technology as the telephone (arguably it has already has reached this level of acceptance). Like the telephone, e-mail has become so essential in our society that increasingly one cannot reasonably be expected to avoid it as a mode of communication.[154] Just as one would not unplug one's phone at dinner

152. This line of argument characterizing the inbox as conduit or window gets into the realm of disturbance to the use and enjoyment of property in a general residential or business sense. Of course, viewing the inbox or computer as a conduit may not even be necessary when looking at the communication with e-mail on a computer itself as either part of general residential use or else as a *type* of use and enjoyment of land. For example, use of one's backyard for a mink farm is a type of *use* of land involving personal property (the minks) sensitive to certain types of invasions (i.e. vibrations from plane over flights) that will not affect residential uses. Similarly, one can use their home as residentially connected to the outside world by the e-mail system. Alternatively, in today's world, residential use likely includes e-mail use. *See Page County*, 347 N.W. 2d at 176 (noting the ubiquitous use of televisions within residential properties).

153. With respect to ISPs attempting to bring a cause of action for nuisance the analysis is slightly different. In that case, the ISP would not be arguing nuisance on behalf of their customers, but based on the use of its land for the maintenance of computer systems as part of the business of providing Internet access and solicited e-mail. Thus, damages of overloaded servers, slowed e-mail traffic, declines in employee productivity, time spent dealing with customer complaints, and loss of good will would be characterized as disturbance of the use and enjoyment of property of the Internet service. *C.f.* Compuserve, Inc. v. Cyber Promotions, Inc., 962 F. Supp. 1015, 1022–23 (finding diminished capacity of equipment and loss of good will as sufficient damages for a trespass to chattels suit brought by an ISP against a spammer).

154. The social value of e-mail as an activity will be relevant in the balancing analysis of nuisance discussed *infra* Part IV.B.

time as a solution to incessant telemarketing, one should not be expected to stop using e-mail, or to continually change one's e-mail address in order to avoid spam.

Just as the telephone has been found to be a possible entry point for disturbances to real property interests,[155] the computer may properly be seen as an audio-visual window through which unwanted invasions can enter. Upon recognizing the essential quality of one's inbox as a communicative medium connecting occupants of real property, one can then reasonably view the e-mail account itself as a fixed aspect of real space. If the inbox is as fundamental to our society as the telephone, one can accept that e-mail users should not have to change their e-mail accounts every three months in order to avoid abusive commercial senders.[156] In this way, the inbox can be viewed either as a fixed (or at least, semi-fixed) conduit into real property or an inherent part of residential use itself. Thus, e-mail may be logically approached within the boundaries of the nuisance law.

b. Nuisance Applied by Extension of Law to Personal Property

If courts are unwilling to accept the argument that e-mail can affect the use and enjoyment of land, nuisance law could alternatively be applied by analogy to or extension into personal property[157] along the lines of a novel nuisance to chattels theory. While it may seem awkward to fit e-mail into old property frameworks, such increments in the case law are a necessary part of the common law's adaptation to technological developments. Richard Epstein supports this view, arguing that leaps by extension and analogy are logical common law responses to changes in technology. [158] He writes:

155. *See supra* Part IV.A.1.a.

156. For a discussion of one's right to use self-help "abatement" measures in the form of counter-strikes against the senders of potential digital nuisances such as computer viruses, see generally, Curtis E. A. Karnow, Strike & Counterstrike: The Law on Automated Intrusions and Striking Back, (Feb. 27, 2003) (unpublished manuscript), *at* http://www.blackhat.com/presentations/win-usa-03/bh-win-03-karnow-notes.pdf). Karnow's presentation proposes interesting questions, including whether an ISP, in carrying out cyber counterattacks (otherwise illegal under federal laws) against a sender of harmful digital invasions, could argue the privilege of abatement under public nuisance law. *See id*. *See also* PROSSER & KEETON, *supra* note 82, § 89, at 641–43 (discussing the privilege of abatement).

157. Intel argued such a nuisance action, claiming that the spam "continues to interfere with Intel's use and enjoyment of its computer system" in its original complaint against Hamidi. Compl., Intel v. Hamidi, No. 98AS05067 (Super. Ct. Sacramento County), *at* http://www.faceintel.com/intellawsuit.htm. Intel voluntarily dismissed the nuisance claim, however, before the courts could address its viability. *See* Intel Corp. v. Hamidi, 71 P.3d 296, 300 (Cal. 2003).

158. *See* Epstein, *supra* note 46, at 73–74.

> As a general proposition, new forms of technology create the opportunity for new forms of resource use. These uses might not map well with the existing framework of property rights. A common law system . . . should be able to respond to these changes both by preserving what makes sense in the older system and by changing what does not.[159]

E-mail technology has created new competing property uses within the framework of a digital commons (in the form of network bandwidth and storage) in which spammers are able to infinitely shift costs onto the other users of the system. Therefore, it makes sense that nuisance law, developed to maximize the overall cost-benefit calculus of competing real property uses, can lend itself to adjusting the economic imbalance between e-mail users and spam marketers. Thus, if necessary to hone in on the effects of spam on personal property (the computer and e-mail account), courts can avoid thorny real versus personal property distinctions by extending the common law to e-mail as a new form of nuisance to personal property.

B. E-NUISANCE—APPLYING THE FRAMEWORK

After providing a brief overview of nuisance law's balancing test, this section will discuss its application to spam under various scenarios. In analyzing the applicability of nuisance to spam, two distinct types of defendants will be considered: (1) the typical illegitimate spammer who sends UBE by fraudulent means; and (2) the legitimate marketer who sends UBE via truthful methods. Because of the flexibility of nuisance, as discussed below, the analysis shifts depending on whether the defendant is an illegitimate spammer or a legitimate marketer sending out UBE.[160] Intuitively, one can recognize inherent differences between AT&T sending out unsolicited bulk e-mail with valid opt-out requests, the Red Cross mass e-mailing calls to donate blood, the unscrupulous marketer sending out advertisements for herbal Viagra, and the pornographer sending out graphic advertisements for sex websites. Not surprisingly, as will be seen below, nuisance law, by virtue of its balancing approach, is able to formally address the intuitive considerations involved in each of these situations.

159. *Id.*

160. The hypothetical plaintiffs considered will be individual e-mail users and businesses. ISPs are additional potential plaintiffs with completely different interests and harms. The nuisance analysis in such situations will not be discussed in depth. In any event, given a high enough volume of spam sent to an ISP, the analysis of nuisance would be similar to the circumstances of individual users with the exception that the harms will likely be greater and more easily quantifiable. Thus, in a balancing analysis, it may be easier to establish the unreasonableness of spamming activities when the plaintiff is an ISP rather than an individual e-mail user.

1. The Nuisance Framework: Unreasonableness

The law of nuisance does not attempt to cure every slight annoyance that comes from living within a community.[161] An invasion of a plaintiff's use and enjoyment of land must be unreasonable.[162] Generally, an intentional invasion of another's interest in the use and enjoyment of land is unreasonable "if the gravity of the harm outweighs the utility of the actor's conduct."[163]

According to the Restatement an activity is unreasonable if "(a) the gravity of the harm outweighs the utility of the actor's conduct or (b) the harm caused by the conduct is serious and the financial burden of compensating for this and similar harm to others would not make the continuation of the conduct not feasible."[164]

In determining unreasonableness, the weighing of utility against the actor's conduct is essentially a problem of relative valuation determined by a trier of fact in light of the facts of each case.[165] The balancing is determined objectively based on whether a reasonable person viewing the

161. PROSSER & KEETON, *supra* note 82, § 88, at 626.

162. *See* TORTS, *supra* note 82, §§ 822, 826.

163. *Id.* § 826.

164. *Id.* The second prong usually applies only when damages are sought, the harm is substantial, and the utility of the conduct is high. This prong will not be applied for purposes of this Note. It generally would not apply to spam which in most cases involves difficult to calculate damages and/or a low utility activity. One may notice that the second prong seems self-contradictory in that if something is "unreasonable" then it shouldn't matter if the compensation for its harms would make the conduct unfeasible. The comments to the Restatement, however, express the rationale behind this concept: the second prong is primarily for situations where the plaintiff is seeking damages, the harm is substantial, and although the utility outweighs the harm, it is nonetheless unreasonable because compensating for the harms caused would not make the continuation of the activity unfeasible. *See id.* § 826 cmt. f. It is essentially a rule to encourage Pareto efficiency (where at least one is better off and nobody is made worse off), rather than Kaldor-Hicks efficiency (where the net result of benefits and harms to society from an activity is positive), in cases where the harm is substantial. In other words, it might be reasonable to carry out a beneficial activity if compensation is provided, but unreasonable to carry it on without paying. *See id*. However, the rule does not approach Kaldor-Hicks efficiency if the provision of damages makes the continuation *not* feasible because the plaintiff may thus get nothing. According to Jennifer Radner, this prong may apply in a nuisance suit brought against junk faxes, where the damages are easily quantifiable. Radner, *supra* note 132, at 399–401.

165. *See* TORTS, *supra* note 82, § 826 cmt. b. Certain types of intentional invasions are unreasonable as a matter of law. *See id*. Such crystallization can be in a statutory enactment defining certain activities as unreasonable, or in a series of cases. *See id*. States could facilitate the application of nuisance in this way by defining spamming activities as unreasonable. Such specific legislation, however, would likely fall into the realm of preemption by the CAN-SPAM Act. *See* 15 U.S.C.A. § 7707 (West. Supp. 2004). In addition to such crystallized determinations, certain general rules have developed for guiding triers of fact in weighing the gravity of the harm against utility. *See* TORTS, *supra* note 82, §§ 826–828. For example, generally, an invasion is unreasonable if the defendant's conduct is done only to harm the plaintiff, such as in the case of a spite-fence. *See id*. § 829 cmt. c.

costs and benefits of the activity would find it unreasonable.[166] Several factors are relevant to determining the gravity of harm: (1) the extent of the harm, (2) the character of the harm, (3) the social value that the law attaches to the type of use or enjoyment invaded, and (4) the burden on the person harmed of avoiding the harm.[167] In determining the utility of the activity two factors are relevant: (1) the social value of the primary purpose of the conduct and (2) the ability of the plaintiff to avoid the harm.[168]

An additional consideration in balancing the gravity of harm against the utility of the conduct is the role of aggregated invasions by multiple parties.[169] The Restatement explains:

> Situations may arise in which each of several persons contributes to a nuisance to a relatively slight extent, so that his contribution taken by itself would not be an unreasonable one and so would not subject him to liability; but the aggregate nuisance resulting from the contributions of all is a substantial interference, which becomes an unreasonable one. In these cases the liability of each contributor may depend on whether he is aware of what the others are doing, so that his own conduct becomes . . . unreasonable in the light of that knowledge.[170]

This concept of aggregating the harm of individual contributors to an overall series of similar invasions is particularly important in the context of spam.

2. E-nuisance Applied: When Spam Becomes Unreasonable

a. E-nuisance Type 1: Individual or Business Sent UBE by Illegitimate Spammers

This section will discuss the application of the nuisance unreasonableness analysis to the activity of a typical spammer sending a high volume of e-mails to an individual or business recipient. For the purpose of this discussion, this Note will assume that these spammers are selling borderline, or even illegal products, using fraudulent methods of mass e-mailing.

166. *See id.* § 826 cmt. c.

167. *Id.* § 827. The Restatement lists an additional factor: the suitability of the particular use or enjoyment invaded to the character of the locality. *Id.* It is difficult to imagine a situation in which the use of e-mail would not be suited to a particular locality. Moreover, the physical location does not change one's exposure to such electronic invasions making it a meaningless point of analysis in this situation.

168. *Id.* § 828.

169. *See id.* § 840E. cmt. b.

170. *Id*.

(1) The Gravity of the Harm

The extent of harm from spam sent to a business or individual may be significant if sent repeatedly and continuously over a long period of time. With respect to degree, the harm may be substantial when considering an aggregate of invasions. The invasion of each individual e-mail may only be slightly annoying or damaging. But in the aggregate, harm from multiple spammers may add up to substantial and unreasonable levels. The Restatement gives the example that "it may . . . be unreasonable to pollute a stream to only a slight extent, harmless in itself, when the defendant knows that pollution by others is approaching or has reached the point where it causes or threatens serious interference . . . ."[171] Similarly, with the virtual river of the Internet, the spammer likely knows that counterparts are also polluting inboxes and that the proportion of UBE to regular e-mail has reached substantial levels, even exceeding 60%.[172] Furthermore, given the growth rates of spam, a court could take into account the potential for substantial harm from the continuance of such activities when deliberating over an order for injunction.

The next relevant factor is the character of the harm, which with respect to spam, is largely personal discomfort or annoyance.[173] The standard for such harm is that of the average reasonable person.[174] As discussed in Part I, Gartner's survey from 1999 sheds some light on the strongly negative view of spam by the ordinary person.[175] According to the study, 83% of respondents disliked spam, with 63% saying they "dislike it a lot."[176] Of those who disliked it, over 30% found it to be a "significant invasion of their privacy."[177] This study may only scratch the surface of user perceptions of the gravity of the invasion with respect to personal discomfort. Considering that spam comprised less than 40% of e-mail in 1999 and today amounts to greater than 60%, the perceptions of spam have likely worsened.[178] Thus it is conceivable that the personal discomfort from spam, at least in the aggregate, could be considered substantial. While the harm from spam may not appear substantial compared to repeated telemarketing phone calls, where one is disturbed by continuous ringing

171. *Id*.
172. *See supra* note 12 and accompanying text.
173. *See* TORTS, *supra* note 82, § 827 cmt. d. (suggesting that harm may arise out of personal discomfort or annoyance).
174. *Id*. § 827 cmt. e.
175. *See supra* note 46.
176. Gartner Group, *supra* note 23, at 7.
177. *Id*.
178. *See supra* note 12 and accompanying text.

and disturbing phone conversations, spam disturbs and annoys in a unique way that is compounded by its massive volume. Additionally, considering spam's often offensive content (sometimes visual), and repeated constant distraction, the extent of harm may be high.

The harm from spam sent to businesses may be more directly quantifiable and substantial than the general personal annoyance discussed above. Damages may be calculated by considering resources spent by businesses in response to spam, including software, technical support, and upgrades to computer equipment. Additionally, lost productivity from the time taken to delete messages can add up to substantial figures for corporations.[179]

The next consideration relevant to the gravity of harm is the social value of the use and enjoyment invaded.[180] The use of e-mail, in itself, or as a residential or business use clearly has an intrinsic social value.[181] Residential and business uses generally, according to the Restatement, "are essential to the functioning of organized society and substantial interferences with them under almost any circumstances are relatively serious."[182] E-mail use, specifically, can be seen as having a significant value to society by facilitating an efficient mode of communication and e-commerce.

Finally, the last relevant factor is the burden on the plaintiff of avoiding the harm.[183] The standard means of avoiding e-mail invasions are: (1) filtering; (2) frequently changing one's e-mail address; and (3) not using e-mail. The first two means of avoidance are costly and ineffective. Moreover, the necessary partial avoidance of spam through filtering in itself entails an additional harm equal to the direct harm to be avoided (for example, through mistakenly deleted emails). Some degree of filtering, however, might be reasonably achieved at a low expense through cheaply available filtering software, thereby discounting the gravity of the harm. At this point in time, however, filtering software does not work in such a way. Even after a volume of spam is automatically identified and sorted, the filters are overinclusive, throwing out desirable mail with the spam. Therefore, the user must spend time checking the filtered e-mail to ensure it has not made mistakes. Thus, filtering is generally not considered a reasonable avoidance method. The last approach, abandoning e-mail use

179. *See supra* text accompanying note 26.
180. *See* TORTS, *supra* note 82, § 827.
181. *See id.* § 827 cmt. f.
182. *Id.*
183. *Id.* § 827.

altogether, is the functional equivalent of cementing up one's window to avoid smoke fumes. Abandonment of the use of e-mail is clearly not a viable option.

In sum, the gravity of harm from UBE sent by illegitimate spammers may be relatively substantial, especially considering the impact of aggregation and the social value of e-mail as a use and enjoyment of land. Additionally, as will become evident in discussing the low utility of spamming, the level of harm from spam invasions may not need to be very high for it to be unjustifiably continued.

(2) The Utility of Spamming—or Lack Thereof

The utility of spamming considers (a) "the social value that the law attaches to the primary purpose of the conduct;"[184] and (b) "the impracticability of preventing or avoiding the invasion."[185]

The typical spamming enterprise can make substantial sums of money for the unscrupulous individuals who engage in such activities. Nonetheless, considering the interests of society as a whole, spamming amounts to conduct of a low to negative social value. Spamming activities can have a lack of social utility for several reasons. First, spam's primary purpose and means are often malicious—using fraud and deception to sell products, many of which are harmful.[186] Second, spam may be illegal, for example by selling fake pharmaceuticals.[187] Third, spam is often contrary to common standards of decency—for example, pornographic spam or spam selling sexual enhancement products.[188] According to the Restatement, conduct carried out for these three purposes so lack utility that the invasion may be unreasonable as a matter of law.[189] However, this rule only applies when the activity is clearly malicious or contrary to common standards of decency and the gravity of harm is significant.[190] Therefore, some e-mail invasions from spammers, by not qualifying as clearly malicious or indecent will require a full balancing of harm and utility.[191] To the extent that spam from the common illegitimate marketer has any social value, however, it will be extremely low. The low social value of the typical spam-advertised product is evidenced by the extremely

184. *Id.* § 828.
185. *Id.* § 828.
186. *See id.* §§ 828 cmt. e, 829.
187. *See id.*
188. *See id.*
189. *Id.* § 828 cmt. e.
190. *See id.* § 829.
191. *See id.* §§ 826, 826 cmt. b.

low response rates to spam. Thus, it is fairly clear on the basis of social value that the utility of a spammer's activities are extremely low at best.

An additional consideration to be taken into account is whether unwanted e-mail invasions can be practically avoided by spammers.[192] When conduct can be practically avoided while still achieving its primary purpose, it lacks utility if the actor fails to take measures to avoid the resulting invasion. If the primary purpose of spam is to advertise goods and services to interested consumers, then the invasion to the remaining 99.995% of Internet users can easily be avoided by maintaining an opt-in mailing list. The real purpose, of course, might be the fishing out of a small number of customers by contacting a mass of people without consent. In that case, harm can only be avoided by the sender ceasing to carry on its spamming activities. The assessment of utility does not change with this variation, however, because the typical spammer's products and services for the most part are of low social value.

(3) The Balance

It is clear that spamming by a typical illegitimate marketer is an activity of low or negative utility. The gravity of harm from spam is less clear and depends on the extent to which the invasions can be aggregated. In weighing the two, it seems very plausible that the extremely low utility of the spamming activities in most cases will be easily outweighed by the harms from the resulting invasions.

b. E-nuisance Type 2: Individual or Business Sent UBE by Legitimate Businesses or Individuals

In the case of suits against a legitimate marketer, the considerations are much the same as above except that the harms with respect to annoyance may be somewhat lower and the utility of the activity potentially higher. In the case of a large, legitimate corporation sending out unsolicited bulk e-mail, the activity is likely to be of low utility because of their ability to prevent the invasions. The legitimate company can easily avoid the disturbance to users from UBE by properly creating and maintaining confirmed opt-in mailing lists. Such low cost avoidance methods may make the sending of UBE a low utility activity even by legitimate companies selling useful products.

On the other hand, the provision of working opt-out mechanisms and clear subject lines might be seen as a means of avoiding unreasonable invasions. After all, the user can opt-out after the first message is sent and

192. *See id.* § 828.

"just one message" is not a substantial harm to outweigh the utility of the products being sold. In this way, spammers may get a few bites at the apple under nuisance because the theory is often associated with continuing activities as opposed to harms caused by one particular act.[193] In this sense, the framework may seem to comport with an opt-out view of spam similar to the CAN-SPAM act.[194] This is troubling when considering the aggregate impact of every legitimate business sending out just one spam each with working opt-out requests. This view of the nuisance framework breaks down, however, when considering the impact of UBE in the aggregate. As discussed in Part II, the aggregate e-mails from just a fraction of small business in the U.S. sending just one message per year to each recipient would flood one's inbox. Add in the time to opt out of each of company's e-mail list and the harm further escalates. Perhaps the user could be expected to take actions to avoid the harm if the Direct Marketing Association provided working opt-out requests, clear subject lines, in addition to an effective "Do-Not-E-mail List." In that case, the gravity of the harm might change because the e-mail user may be able to reasonably avoid the invasion by signing up for the group opt-out list. Nonetheless, at least in the absence of such a hypothetical list, companies should not be free from liability when they knowingly contribute to the volume of UBE, simply by limiting their mailings to one-time events. Thus, just as with assessment of the degree of harm, the aggregate impact of UBE from multiple parties should be taken into account when assessing duration of harm.

The balance may also change if the sender of UBE is a socially valuable nonprofit organization. Thus, we can imagine the high utility of the Red Cross, facing an emergency blood shortage, sending out mass mailings to solicit donations. Such a high utility would likely dwarf any harm caused by the e-mail. Of course, nuisance law's balancing here is reflective of the likely positive response from most users to such e-mail. Most would not take offense, and of course, such a suit would never exist outside of this hypothetical. However, we might be able to imagine some gray area where the sender's activities have a high utility but not enough to justify the method of communicating without recipient consent. For example, a noncommercial UBE might be sent to recipients encouraging them to exercise their right to vote. This may be a high utility activity, but perhaps not high enough to override the disturbance to users, especially when considering the aggregate effects of such e-mails. Or, perhaps the

193. *See* DOBBS, *supra* note 7, § 465, at 1327 n.10.

194. 15 U.S.C.A. § 7704(a)(3)–(5) (West 2004).

opposite conclusion is reached when the sender is for example, a former employee sending UBE to a company's current workers, urging them to quit. In this case, drawn from the facts of *Hamidi*, a court could find the social value of the former employee's targeted communications to outweigh the harm to the company.

A similar case might be a union attempting to organize by sending UBE to nonunionized employees of a company. Because nuisance takes into account the value of the conduct to society as well as to the defendant, the court in such a case would decide whether the union's mailing under the circumstances was of sufficient utility relative to the harm to the company. In such scenarios, because of the ability to avoid the harm by creating an opt-in mailing list, the social value of sending the message to the specific recipients would need to be addressed. Thus, though a union's activities in e-mailing might have a high social value when targeted to the right recipients, it would not if sent to just anyone. Additionally, if the suit was for damages and the harm to the corporation from lost productivity, tech-support requests, or a slow-down of e-mail equipment was serious enough, the sending of UBE might be considered unreasonable even if the utility outweighed the harm.[195] Thus, though an injunction might not be appropriate in such circumstances, the union might be required to compensate the company its damages.[196]

Nuisance law thus provides different legal outcomes for the different types of situations in which unsolicited bulk e-mail could be sent. In sum, nuisance clearly has the potential to logically address invasions to the inbox. It worth noting however, that although the annoyance from UBE is clearly significant and important, it is far from clear whether it is substantial enough to be actionable under nuisance law.[197] Nonetheless, the framework need not fall short of the problems of e-mail users. Within the framework, a range of protection can be justified, from flimsily allowing

195. *See* TORTS, *supra* note 82, § 826(b) cmt. f.

196. *See id*.

197. On a practical level, enforcement difficulties may be an additional hurdle in applying nuisance to spam. First, it is often difficult to track down spammers given the methods used to obfuscate their trails and the overseas bases for much of their activities. However, enforcement is not necessarily an insurmountable hurdle in that 90% of illegitimate spam originates from fewer than two hundred individuals, businesses, and gangs, the majority of which are located within the United States. *See* The Spamhaus Project, *Register of Known Spam Operations ("ROKSO") Database*, *at* http://www.spamhaus.org/rokso/index.lasso (last visited Nov. 20, 2004). Information on these "most wanted" spammers can be found on the ROKSO database that tracks their activities and provides additional sensitive evidence to law enforcement agencies. *See id*. Second, because a large spam lawsuit is expensive, it might be difficult for consumers to utilize class actions without the availability of clearly calculable damages.

marketers one bite at the apple, to providing strong rights to preemptively exclude UBE. It will be up to state courts to flesh out the level of protection granted to e-mail users by the common law of nuisance.

V. CONCLUSION

Whether called a trespass or nuisance, there is an intuitive sense that invasions to the inbox by unsolicited bulk messages violate property rights. Still, questions of the appropriate metaphor for cyberspace remain debated. Nonetheless, several available frameworks—trespass to chattels, targeted legislation, and nuisance—are capable of effectively addressing the problem of spam, while avoiding the risk stifling the beneficial aspects of an open e-mail system.

Complete entitlements such as trespass seem capable of working well in the context of e-mail, given the ability of courts to take implied consent into account. Thus a full exposition of implied or constructive consent, if based on a proper weighing of public policy, will have a similar effect to applying a nuisance balancing approach. The difference is that trespass would be more prone to draw the line in favor of an absolute right to exclude. Additionally, trespass is a satisfactory solution if narrowly applied by statute. In drawing these lines, legislatures might consider allowing the absolute right in the types of situations that would clearly weigh in favor of the recipient's right to exclude under a nuisance balancing analysis. One benefit of such an approach is the ability to preemptively ensure stronger protection to the inbox, accepting some level of spillover into areas where nuisance might find high utility on the part of the sender. Further, statutory rules for spam can potentially better foster consumer enforcement by setting clear liquidated damages.

Nuisance, on the other hand, at least on a theoretical level, may be better equipped to address the conflicts and abuses of cyberspace generally. The framework forces a thorough analysis of policy implications of competing uses and the interests of society as a whole. The Internet and electronic messaging technologies gain significant benefits from a good degree of openness with respect to users' ability to freely interact without obtaining consent for each informational transaction. Thus, as Burk suggests, nuisance may be the optimal generally applicable rule for assigning property rights in cyberspace. Regardless, even setting aside the vigorously debated question of what general property regime is ideal for governing the transactions and issues of cyberspace overall, it is clear that the nuisance framework, by virtue of its flexibility, is logically able to

address the conflicts and abuses of e-mail. As this Note has illustrated, nuisance can be a viable legal theory for spam under a wide range of circumstances. The framework is not, however, without practical limitations. First, the theory may grant some spammers a first bite at the apple as a framework traditionally entailing repeated or continuous events. Second, damages from spam might be too uncertain to drive litigation. Although nuisance might not be the strongest protection for the inbox from every intrusion by UBE, it at least can clearly be used to attack the worst cases—repeated, abusive, excessive spamming and e-mailing of offensive, obscene content. Nuisance applied to spam is a good move forward in that it represents at least a partial recognition of proprietary interests in one's inbox. It can hopefully get at some of the worst abuses of e-mail and the most significant departures from what one would expect people impliedly to consent to by connecting to the open network. At the same time, it is flexible and open enough to avoid problems of a complete exclusory interest like trespass.

In the end, there is a limit to which the law can solve a problem with technical origins at its core. The most successful solution will come from rewriting the protocols behind the Web and e-mail system. New standards could be used to allow reliable authentication of senders, e-stamps, or technical enforcement of an opt-in approach to e-mail. A new e-mail standard could allow users, at their option, to make their e-mail inbox, opt-in only, by allowing reception of only authorized e-mail. As we have seen in the analysis of nuisance applied to spam, competing interests exist in the use of the Internet (i.e., consumers, ISPs, and Web marketers). Therefore it would be beneficial, in addition to attacking spam through purely legal avenues, for the federal government to step in and legally institute a standards body to make sure the technical system implemented best balances interests of consumers and other groups.

Such technical overhauls may not arrive, however, until long after the spam problem exponentially grows and expands into new areas. Therefore, the effectiveness of statutory and common law solutions remains crucial to keeping the intrusion of spam and other harmful digital invasions at bay. Experimentation is needed. Although abuse of communication is as old as the printing press, the 21st century efficiency of e-mail facilitates a new height of annoyance by virtue of degree, duration, and frequency. Nuisance theory provides a set of well-tested background principles worth considering in carving out an effective solution to this irritating variation of an old problem.