University of Dayton Law Review

Volume 25
Number 1 *25th Anniversary Edition*

Article 10

10-1-1999

Legal Relief from Spam-Induced Internet Indigestion

Jeffrey L. Kosiba
University of Dayton

LEGAL RELIEF FROM SPAM-INDUCED INTERNET INDIGESTION

Jeffrey L. Kosiba[*]

TABLE OF CONTENTS

I. INTRODUCTION

The Internet has become one of the most important modes of communication throughout the world because of its high speed, competitive cost, and relative convenience.[1] Increasingly, private individuals and corporations alike are taking advantage of this far-reaching

---

[*] Executive editor, 1999-2000, University of Dayton Law Review. J.D. expected, May 2000, University of Dayton School of Law; B.S. Microbiology, 1988, University of Massachusetts.

[1] *See, e.g.*, Michael W. Carroll, *Garbage In: Emerging Media and Regulation of Unsolicited Commercial Solicitations*, 11 BERKELEY TECH. L. J. 233, 253 (1996).

method of communication and incorporating it into personal and business routines. In order to increase revenues, commercial marketing companies capitalize on the opportunities associated with online communications and transmit millions of unsolicited commercial e-mail messages to Internet users.[2] Such unsolicited commercial e-mail, also termed "junk e-mail" or "spam,"[3] is the cyberspace equivalent of the unsolicited advertisements receive in mailboxes every day or telemarketing calls that annoy people while they eat dinner.[4] However, as Internet service providers ("ISPs") and e-mail subscribers are quickly discovering, ridding one's computer system of huge volumes[5] of junk e-mail is not as simple as merely tossing unwanted mail into the trash.

As a result of this large amount of spam being sent,[6] Internet e-mail subscribers must reject or delete the unwanted mail from their e-mail accounts. Because many subscribers pay for Internet access on a per minute or hourly basis,[7] they pay to read and discard the junk mail sent to them by "spammers."[8] Subscribers also face delays in their online service due to the massive drain on the ISPs' computer resources which results from processing and storing the bulk spam.[9] Thus, in the eyes of the

---

[2] In fact, one Internet service provider, America Online, reported that its users received over one million junk e-mail messages a day from just one of the many marketing agencies currently using the Internet to advertise to subscribers. David J. Loundy, *Junk E-Mailers Face Attack On Several Fronts*, 144 CHI. DAILY L. BULL. 5 (1998). One estimate puts the average amount of spam sent over the Internet at twenty-five million messages per day. James W. Butler, *Courts Can Spam, But Legislators May Breathe New Life Into Practice*, 220 N.Y.L.J. 5 (1998).

[3] The term spam, refers to junk e-mail, most often comprised of advertisements, that is not solicited by the party to which it is sent. Harry Newton, NEWTON'S TELECOM DICTIONARY 666 (1998). Usually, spam is sent to thousands of e-mail subscribers in large quantities, thereby constituting "bulk junk e-mail." *Id.* This Comment will only address issues regarding unsolicited commercial e-mail, not unsolicited non-commercial e-mail. A "spammer" is a person who sends unsolicited commercial electronic mail. The term "spamming" refers to the practice of sending bulk unsolicited commercial electronic mail. *See* Robert Craig Waters, *An Internet Primer (Part II)*, 44 FED. LAWYER 72 (1997).

[4] A further analogy between spam and regular junk mail has been made to the extent that spam is more akin to junk mail that arrives with postage due. Mark Grossman, *Removing Spam From Your Computer's Diet*, TEX. LAWYER, Nov. 2, 1998, at 36. Many e-mail subscribers pay for their Internet service on a per minute basis. *Id.* Because subscribers must be connected to the Internet in order to read their e-mail, they are essentially paying to read spam they never requested in the first place, similar to paying postage due on unsolicited commercial mail. *Id.*

[5] *See supra* note 2 and accompanying text.

[6] *See supra* note 2 and accompanying text.

[7] *See supra* note 4 and accompanying text.

[8] *Id.*

[9] *See, e.g.*, Clint Swett, *Unsolicited E-Mail a Problem*, THE SACRAMENTO BEE, May 19, 1997, *available in* 1997 WL 3288426 (noting that one ISP's computer network slowed as a result of mass spamming, thereby causing subscribers to suffer a three-hour access delay); *see* Barbara Cole-Gomolski, *Servers Slow Spoofs, Spam: Message Managers Aim To Control Junk E-mail*, COMPUTER

average e-mail user, spam is more than just a mere annoyance because it decreases the quality and value of the Internet.

As bothersome as spam can be for subscribers, ISPs incur the highest costs of spamming. ISPs face thousands of complaints of annoyed customers per day and requests for the discontinuance of service.[10] In the highly competitive Internet service market, ISPs quickly lose revenue as their customers become irritated with spamming and switch to another provider. Unfortunately for subscribers, even discontinuing service with one ISP will not necessarily solve the problem. The result is that the subscriber is inconvenienced by having to evaluate and choose a new ISP, and the ISP is out a customer and the subscription fee that came with him. Moreover, ISPs must also deal with the real burden of processing the large volume of rejected or undeliverable spam that clogs their servers and memory resources. Because spam is often sent with a false return address, such as the name of an ISP for example, ISPs can also face damage to their business reputation or even trademark dilution if their famous trade name or trademark becomes appropriated by a spammer.[11] In the end, junk mail solicitors reap the rewards of their low-cost, mass advertising campaigns while ISPs and subscribers are left to pay for and sort through the mountain of e-mail dumped on their computers.

As the sheer volume of spam has increased, ISPs and subscribers have looked to courts and legislatures for relief. This Comment argues that while ISPs and subscribers have successfully sued spammers under common law tort theories including trespass to chattels,[12] trademark infringement,[13] and tortious interference with a contractual relationship,[14] such common law remedies are not universally applicable, resulting in the

---

WORLD, May 5, 1997, at 59 ("Spam can suck up bandwidth, clog mailboxes and force users to upgrade servers and networking gear to account for the overloads.").

[10] *See, e.g.*, Compuserve, Inc. v. Cyber Promotions, Inc., 962 F. Supp. 1015, 1019 (S.D. Ohio 1997). Internet service providers are not the only people who are listening to the spamming complaints of subscribers. In fact, the Federal Trade Commision's Bureau of Consumer Protection receives up to 2,500 complaints a day concerning spam. *You've got Spam*, CONSUMER REPORTS, Mar. 1999, at 9.

[11] *See infra* notes 91, 101 and accompanying text.

[12] *See, e.g.*, *Compuserve*, 962 F. Supp. at 1015 (ISP successfully sued spammer under a trespass to chattels theory); Thrifty-Tel, Inc. v. Bezenek, 46 Cal. App. 4th 1559, 1567 (1996) (subscriber successfully sued a spammer under the same theory).

[13] *See, e.g.*, America Online, Inc. v. IMS, 24 F. Supp. 2d 548 (E.D. Va. 1998).

[14] *See, e.g.*, Anne E. Hawley, Comment, *Taking Spam Out of Your Cyberspace Diet: Common Law Applied to Bulk Unsolicited Advertising via Electronic Mail*, 66 U.M.K.C. L. Rev. 381, 409 (1997) (citing Concentric Network Corp. v. Wallace , Case No. C-96-20829 RMW (N.D. Cal. Nov. 5, 1996)).

protection of only part of the growing population affected by spam.[15] Moreover, although several state legislatures have enacted statutes regulating or prohibiting unsolicited commercial e-mail,[16] many of the statutes are limited in their application because jurisdiction over spammers is limited to intrastate, rather than interstate, spamming activities.[17] Consequently, uniform federal legislation is required for full protection of both ISPs and subscribers.[18]

This Comment discusses a number of legal remedies available to ISPs and subscribers for relief from spamming. Part II provides background information regarding the Internet, e-mail, and spam, and discusses the problems associated with spamming.[19] Part III of this Comment examines common law remedies based on theories such as trespass to chattels, tortious interference with contractual relations, and trademark law.[20] Part III further provides a review of current state legislative efforts to control or provide relief from spamming.[21] Finally, Part III concludes with a discussion of why federal legislation is needed to provide uniform relief from spamming and to ensure the protection of all those who suffer from its effects.[22]

II. BACKGROUND

A. The Internet and E-mail

The Internet, originally developed for use by the Department of Defense,[23] is a decentralized, worldwide telecommunication network that

---

[15] *See* discussion *infra* Part III.A.

[16] *See, e.g.*, CAL. BUS. & PROF. CODE § 17538.45 (West 1998 & Supp. 1999); NEV. REV. STAT. § 207.325 (West 1997); VA. CODE ANN. § 18.2-152.3 (Michie 1996); WASH. REV. CODE. ANN. § 19.190.030 (West 1998); *see also* discussion *infra* Part III.B.

[17] *See, e.g.*, CAL. BUS. & PROF. CODE § 17538.4 (West 1998 & Supp. 1999) (stating that "this section shall apply when the unsolicited e-mailed documents are delivered to a California resident via an electronic mail service provider's . . . equipment located [in California]").

[18] Jeri Clausing, *More States Consider Laws Restricting Junk E-Mail*, N.Y. TIMES (Feb. 11, 1999) (visited Apr. 14, 1999) <http://www.nytimes.com/library/tech/99/oz/cyber/articles/llspam.html>.

[19] *See infra* notes 23-44 and accompanying text.

[20] *See infra* notes 45-112 and accompanying text.

[21] *See infra* notes 113-133 and accompanying text.

[22] *See infra* notes 134-166 and accompanying text.

[23] Barry M. Leiner et al., *Internet Society (ISOC) All About the Internet: A Brief History of the Internet* (visited Aug. 20, 1999) <http://www.isoc.org/internet-history/brief.html>.

interconnects countless groups of smaller computer networks.[24] These networks communicate with each other by using a shared protocol, i.e. "an agreed-upon format for transmitting data between two devices."[25] Data transmitted between computers on the Internet is broken up into smaller "packets" in a process called "packet switching."[26] By using "packet switching," the smaller pieces of data arrive and are reassembled at the same predetermined destination although they may travel very different routes over the network.[27] Packet switching, therefore, imbues the Internet with tremendous flexibility because as communication routes become congested individual packets can be re-directed to a clear path in order to reach their final destination.[28]

Individuals and companies seeking access to the Internet can either obtain a direct link to a computer network that is physically linked to the Internet or connect to the Internet through a dial-up service.[29] Internet access through the use of a dial-up service is accomplished by the connection of a modem in a personal computer, through telephone lines, to a network that has a direct link to the Internet.[30] Whichever type of access an individual seeks, a variety of commercial and non-commercial entities, called Internet or online service providers, are available to make the Internet connection.[31] ISPs, such as America Online ("AOL"), Prodigy, and Earthlink, provide access for a subscription fee, typically on a monthly, hourly, or per minute basis.[32] Thus, practically anyone who has access to a personal computer, a modem, and approximately twenty dollars a month can obtain access to the Internet.[33]

One of the first significant uses of the Internet was to transmit electronic messages, "e-mail," from one computer to another.[34] To send e-mail, subscribers type a textual message on a computer linked to the Internet and send the message to the e-mail address of the intended recipient. An ISP

---

[24] ACLU v. Reno, 929 F. Supp. 824, 830-31 (E.D. Pa. 1996).

[25] *PC Webopedia* (visited Aug. 20, 1999) <http://webopedia.internet.com/TERM/p/protocol.html> (defining the word "protocol").

[26] *Reno*, 929 F. Supp. at 832.

[27] *Id.*

[28] *Id.*

[29] *Id.*

[30] *Id.*

[31] *Id.* at 833.

[32] *Id.*

[33] Randall Broberg et al., *Internet Providers Fight Back Against Spammers*, 219 N.Y.L.J. S7 (1998).

[34] Leiner, *supra* note 23.

receives the incoming message and stores it in the recipient's e-mail account, or "post office box," located on the ISP's computer system or "server." The message remains unopened until the recipient accesses it.

In contrast to postal mail, an individual may transmit the same e-mail message to hundreds of people on the Internet for the cost of the time spent online to send the message; which is a fraction of their subscription fee.[35] Today millions of people across the world are "wired," communicating by e-mail every day. ISPs offer subscribers a gateway to the Internet through which they can exchange messages with the entire online world. Unfortunately for subscribers and ISPs, spammers have also taken advantage of the efficiency and cost effectiveness of e-mail to send volumes of unsolicited commercial messages.

B. Spam, Spam, Spam

The practice of sending unsolicited junk mail to consumers is not new. Junk mail, junk faxes, and even telemarketing calls are all unsolicited means by which advertisers promote their products. With the invention of the Internet and e-mail, advertising companies have been provided with a more efficient and cost effective method of reaching potential customers around the globe. For example, if an individual mails one thousand letters within the United States, it would currently cost them $330 per mailing. The cost for sending the same number of e-mail messages each month, excluding buying the necessary equipment, would be drastically less considering the average ISP subscriber pays a flat rate of less than $20 per month for unlimited Internet access.[36] In fact, in order to get started, electronic marketing and advertising companies need only purchase the necessary computer equipment, obtain and pay for access to the Internet through an ISP, and purchase a list of e-mail addresses from a variety of sources.[37]

As a result of the low start-up cost and ease of obtaining worldwide access, Internet mass marketing companies send billions of unsolicited commercial e-mail messages ("spam") to the consternation of ISPs and e-

---

[35] *Reno*, 929 F. Supp. at 834.

[36] Coalition Against Unsolicited Commercial Email, *CAUCE Warns that "Anti-Spam" Amendment to Phone Slamming Bill is Victory for Spammers* (visited Aug. 20, 1999) <http://www.cauce.org/pressreleases/pr6.html>.

[37] Alan Cohen, *Can the Spam: Bills Declare War On Junk E-mail But Some Wonder If Laws Are The Answer*, 218 N.Y.L.J. S2 (1997). For example, e-mail addresses are extracted from chat rooms, list servers, Internet web sites, and newsgroups. *Id.* Such lists containing millions of addresses range in price from $10 to $40. *Id.*

mail subscribers alike.[38] When spam reaches an ISP for delivery to a subscriber, the subscriber must access, review, and either save, return, or discard the unsolicited mail.[39] Until the subscriber processes the unsolicited message, the spam occupies part of the limited amount of storage space on an ISP's computer network.[40] Once the subscriber has reviewed the spam, he may wish to return it to its sender. However, because spammers often use false return e-mail addresses,[41] the returned spam will bounce back to the ISP's server as undeliverable mail, which once again depletes the ISP's limited storage capacity.[42]

The sending of large amounts of spam, or "bulk spam," can so seriously absorb the resources available to the ISP that the network may "crash" or operate at a significantly diminished capacity.[43] Diminished storage capacity can result in a decrease in the quality of the Internet service provided, thereby creating unsatisfied customers who may choose not to renew their subscriptions.[44]

The deluge of spam places a heavy burden on ISPs who must reroute or delete each piece of unclaimed or rejected junk e-mail that reside on their server. Moreover, since many e-mail subscribers pay for Internet access on a per minute or per hour basis, using those paid minutes to access, review, and return or discard unsolicited mail that was deposited into their e-mail accounts is, in essence, paying for spam. Consequently, subscribers rightfully become annoyed by the volume of spam they receive and attempt to rectify the problem by entreating the ISP or the spammer to cease and desist.

---

[38] *See e.g.*, America Online, Inc. v. IMS, 24 F. Supp. 548, 549 (E.D. Va. 1998) (noting that one electronic marketing company, IMS, sent over sixty million unsolicited commercial e-mail messages to customers of America Online over a ten-month period).

[39] Compuserve, Inc. v. Cyber Promotions, Inc., 962 F. Supp. 1015, 1019 (S.D. Ohio 1997).

[40] *Id.*

[41] People v. Lipsitz, 663 N.Y.S.2d 468, 471 (N.Y. Sup. Ct. 1997).

[42] *Compuserve*, 962 F. Supp. at 1022.

[43] *See, e.g.*, Cyber Promotions, Inc. v. America Online, Inc., 948 F. Supp. 436, 438 (E.D. Pa. 1996) (stating that the sending of millions of e-mail messages by plaintiff resulted in the overload of defendant's e-mail servers).

[44] *Compuserve*, 962 F. Supp. at 1023 (noting that "[m]any subscribers have terminated their accounts specifically because of the unwanted receipt of bulk e-mail messages").

III. ANALYSIS

Fortunately for ISPs and subscribers, some legal relief from spamming can be found both in the application of common law tort principles and newly enacted state "anti-spamming" legislation.[45] However, because the sending of spam affects ISPs and subscribers the same way in every state in which it occurs, current remedies for persons affected by spam need to be applied in a uniform manner in order to provide ISPs and subscribers full protection.[46]

A. Common Law Theories Under Which ISPs May Sue for Spam

Over the past few years, ISPs and subscribers have successfully found refuge from the flood of spam in the venerable common law theories of trespass to chattels,[47] tortious interference with contractual relations,[48] and trademark law.[49] However, each of these common law remedies are limited in utility, thereby leaving subscribers' and ISPs' spam problems unaddressed.

1. Trespass to Chattels

Trespass to chattels occurs when a person either dispossesses another of his chattel (personal property) or uses or intermeddles with the chattel in the possession of another, resulting in some type of injury.[50] Under this theory, trespass liability attaches when a person, without authorization, intentionally makes physical contact, or intermeddles,[51] with personal

---

[45] *See, e.g.*, CAL. BUS. & PROF. CODE § 17538.45 (West 1998 & Supp. 1999); NEV. REV. STAT. § 207.325 (West 1997); VA CODE ANN. § 18.2-152.3 (Michie 1996); WASH. REV. CODE ANN. § 19.190.030 (West 1998).

[46] States may differ in the application of tort law to the context of the Internet, as well as in the scope of statutory provisions against spamming. In order to provide a consistent means with which ISPs, subscribers, and spammers may resolve disputes, Congressional legislation that applies uniformly across the nation is desirable.

[47] *See* discussion *infra* Part III.A.1.

[48] *See* discussion *infra* Part III.A.2.

[49] *See* discussion *infra* Part III.A.3; *see also* United Drug Co. v. Theodore Rectanus Co., 248 U.S. 90, 97 (1918), *superseded by statute as stated in* Foxtrap, Inc. v. Foxtrap, Inc., 671 F.2d 636 (D.C. Cir. 1982) (stating that trademark law is merely a part of the broader common law principles of unfair competition).

[50] Restatement (Second) of Torts § 218 (1965).

[51] "Intermeddling" is defined as "intentionally bringing about a physical contact with the chattel." *Id.* § 217. Courts have found the presence of intermeddling where an electronic marketing

property in the rightful possession of another.[52] The level of intent required is that the trespasser knows that "intermeddling will, to a substantial certainty, result from the act."[53] However, liability for trespass to chattels is found where the defendant's use or contact materially harms the quality, physical condition, or value of the possessor's chattel.[54]

a. Protection for ISPs

Applying trespass to chattels theory in the context of spam, courts have recognized that ISP's have a possessory interest in their chattel, namely their computer equipment and software.[55] This possessory interest is impacted when a spammer, without authorization, affirmatively acts to transmit junk e-mail resulting in contact with the ISP's server, thereby diminishing the quality or value of the interest.[56]

The recent case of *Compuserve v. Cyber Promotions*[57] serves as an example. In *Compuserve*, an ISP brought a trespass to chattels action against Cyber Promotions, a company notorious for its spamming activities.[58] It was determined that Cyber Promotions had intermeddled with Compuserve's possessory interest in its computer equipment by its unauthorized and intentional use of the ISP's equipment to send unsolicited commercial e-mail.[59] The court found that the harm resulting from Cyber Promotions' intermeddling was a decrease in the value the ISP placed on

---

company made an unauthorized mailing of unsolicited bulk e-mail causing the value of an ISP's computer equipment to be diminished although it was not physically damaged. Compuserve, Inc. v. Cyber Promotions, Inc., 962 F. Supp. 1015, 1022 (S.D. Ohio 1997).

[52] Restatement (Second) of Torts § 217 (1965).

[53] *Id.*

[54] *Id.* § 218.

[55] *Compuserve*, 962 F. Supp. at 1021 (stating that "[i]t is undisputed that [Internet service providers have] a possessory interest in [their] computer systems"); *see also*, America Online, Inc. v. IMS, 24 F. Supp. 2d 548, 550-51 (E.D. Va. 1998).

[56] *Compuserve*, 962 F. Supp. at 1022. Making contact with an ISP's server by sending spam is considered physical contact because "[e]lectronic signals generated and sent by computer have been held to be sufficiently physically tangible to support a trespass cause of action." *Id.* at 1021 (citing Thrifty-Tel, Inc., v. Bezenek, 46 Cal. App. 4th 1559, 1567 (1996)).

[57] 962 F. Supp. at 1015.

[58] *Id.*; Broberg et al., *supra* note 33, at S14.

[59] *Compuserve*, 962 F. Supp. at 1024-25. Cyber Promotions use of the computer equipment was considered unauthorized because Compuserve had repeatedly demanded that defendant cease and desist from sending spam through its server. *Id.*

its equipment to serve its subscribers.[60] Specifically, the court explained that although spamming did not physically damage the ISP's equipment, the value of the equipment was still diminished because the ISP was unable to access the resources necessary for efficient provision of services to its subscribers.[61]

Furthermore, the court noted that the strain placed on plaintiff's resources resulted in a loss of revenue due to unsatisfied customer subscription cancellation, causing harm to Compuserve's business reputation and "goodwill," which is also actionable under the trespass to chattels doctrine.[62] It would appear, therefore, that ISPs have a valid common law means with which to protect themselves from the evils of spamming.

b. Limited Protection for Subscribers

The common law protection of trespass to chattels is not as effective in situations in which only subscribers are harmed by spam. Like ISPs, Internet subscribers have a possessory interest in their e-mail accounts and the transmission of electronic signals through such accounts.[63] This interest arises from the contract between the ISP and the subscriber, thereby conferrring upon the subscriber the legal right to "occupy" e-mail account space on the ISP's server.[64] The possessory interests of paying subscribers in their e-mail accounts are violated because spamming diminishes the quality or value of those interests. Therefore, subscribers

---

[60] *Id.* at 1022 (noting that "[A]ny value CompuServe realizes from its computer equipment is wholly derived from the extent to which that equipment can serve its subscriber base"). Arguably, the value an ISP places on its equipment can also include the cost of the equipment and its maintenance and the labor cost in terms of time to operate the system and the time necessary to remove spam from its network servers.

[61] *Id.*

[62] *Id.* at 1023. The court issued a preliminary injunction prohibiting Cyber Promotions from sending spam to any e-mail addresses maintained by Compuserve. *Id.* at 1028. Other ISPs have also successfully sued spammers under the theory of trespass to chattels. *See, e.g.*, Hotmail Corp. v. Van Money Pie, Inc., No. C 98-20064 JW, 1998 U.S. Dist. LEXIS 10729 (N.D. Cal. Apr. 16, 1998); America Online, Inc. v. LCGM, Inc., 46 F. Supp. 2d 444 (E.D. Va. 1998); America Online, Inc. v. IMS, 24 F. Supp. 548 (E.D. Va. 1998).

[63] *See* People v. Barela, 286 Cal. Rptr. 458, 460 (Cal. App. 1989) (stating that a possessory interest is "[the] possession of property or the right to possess property" including the legal right to control, own, possess, or occupy the property at issue). As previously noted, electronic signals are considered property interests sufficient to maintain a trespass to chattels action. *Compuserve*, 962 F. Supp. at 1021.

[64] *Barela*, 286 Cal. Rptr. at 460.

may also have a cause of action under trespass to chattels theory to protect themselves from the effects of spam.

Subscribers who pay for Internet service may do so on a monthly, hourly, or per minute basis. The rates paid by subscribers are set by ISPs and may be raised to account for the costs the ISP incurs as a result of spam. When spam is delivered to a subscriber's e-mail account, he must expend time, and therefore money, to view and remove the various pieces of unsolicited mail. Thus, the paid service diminishes in its value to the subscriber as the result of spamming because money expended to obtain access to and use of the Internet is spent deleting unwanted commercial e-mail.[65] In other words, the paid subscriber does not "get his money's worth." Consequently, although jurisprudence addressing the application of trespass to chattels by subscribers in the context of spam is lacking, a paid subscriber could, theoretically, sue a spammer for diminishing the value of his Internet service through intermeddling with the possessory interest in his e-mail account.

However, the applicability of trespass to chattels to a situation where the affected e-mail account holder has not obtained a contract for service from an ISP or paid for such service is not clear. Many states provide that recovery in an action for trespass to chattels is limited only to the actual damage suffered by the owner of the possessory interest as a result of the defendant's intermeddling with the possessory interest.[66] In fact, the Restatement (Second) of Torts notes that an intentional intermeddler is subject to liability only where "his intermeddling is harmful to the possessor's *materially valuable* interest" in the value of the chattel.[67] Presumably, this limitation in recovery poses a problem for subscribers who, through non-profit organizations or educational institutions, do not pay for their Internet access or e-mail account. Although non-paying subscribers experience Internet service delays and must expend time to delete spam, such time would have to be quantified in terms of damages incurred as a result of spamming in order to recover under the trespass to chattels theory. Since the subscriber did not pay for the Internet service, the quantification process becomes much more difficult.

The measurement of actual damages becomes almost impossible because the victim has not expended anything to obtain access to the

---

[65] The time and money expended throwing away spam is in direct contrast to the minimal effort and lack of expense in discarding unwanted junk mail left in a mailbox.

[66] *See, e.g.*, Itano v. Colonial Yacht Anchorage, 267 Cal. App. 2d 84, 90 (1968); State v. Kern, 140 N.W.2d 920, 921 (Iowa 1966); Glidden v. Szybiak, 63 A.2d 233 (N.H. 1949).

[67] RESTATEMENT (SECOND) OF TORTS § 218 (1965) (emphasis added).

Internet.[68] Furthermore, such a victim has no contractual agreement with an ISP expressly giving him a possessory right in an e-mail account. However, the non-paying Internet user still suffers the same extreme annoyance of receiving spam and the expense of time required in removing it from his e-mailbox as his paying brethren. Hence, although ISPs and their paying subscribers may find refuge in the doctrine of trespass to chattels, such a cause of action is not applicable in all cases.

c. Possible Defenses for Spammers

A further limitation on the application of trespass to chattels in the context of spamming is the possible defenses a spammer can raise to justify conduct that would be otherwise tortious.[69] For example, if a spammer can illustrate that he has a privilege, either created by law or by consent of the ISP, to send unsolicited commercial e-mail through the ISP's server, no tort has been committed.[70]

One such privilege was tested in *Cyber Promotions, Inc. v. America Online, Inc.*,[71] in which Cyber Promotions argued that it had a right or privilege at law to send unsolicited commercial e-mail messages under the "free speech" provisions of the First Amendment of the United States Constitution.[72] However, the court rejected Cyber Promotions' argument and stated that America Online, as a private company with a possessory interest in its private e-mail servers, was not a state actor subject to liability under Cyber Promotions' First Amendment claim.[73] The court concluded that the First Amendment did not give Cyber Promotions an "unfettered right . . . to invade AOL's private property with mass e-mail

---

[68] A further argument can be made that since a non-paying Internet user has not given any value in exchange for his e-mail account then the value of that account cannot be diminished through intermeddling.

[69] *See* RESTATEMENT (SECOND) OF TORTS § 10 (1965) (stating the basis of the privilege defense).

[70] *Id.* Alternatively, the spammer could also defend against a trespass claim if he convinces the court that e-mail is neither chattel nor "real property." However, in the light of a growing body of consistent precedent in supporting the idea that ISPs and subscribers have possessory interests in their computer equipment and e-mail accounts, this alternative seems unlikely. *See, e.g.*, Compuserve, Inc. v. Cyber Promotions, Inc., 962 F. Supp. 1015, 1021 (S.D. Ohio 1997).

[71] 948 F. Supp. 436 (E.D. Pa. 1996).

[72] *Id.* at 440-41.

[73] *Id.* at 456; The Supreme Court has held that First Amendment protection is not a "shield against merely private conduct." Hurley v. Irish-American Gay Group of Boston, 515 U.S. 557, 566 (1995) (citations omitted).

advertisements."[74] Consequently, spammers will not likely be able to assert a privilege defense derived from the First Amendment.

However, a privilege sufficient to constitute a defense can be found where an individual has given his consent, either expressly or implicitly, to a would-be trespasser.[75] An ISP can give such consent where it grants a spammer consent to use its server.[76] In order to transmit spam to e-mail addresses, electronic marketing companies enter into subscription agreements with ISPs to obtain Internet access.[77] Unless the subscription agreement provides to the contrary, the spammer is free to send as much e-mail as he wants, absent applicable state and federal law to the contrary.[78]

For example, in *Compuserve*, the defendant spammer asserted that Compuserve had given its tacit consent to the use of its equipment to send e-mail and therefore, could not maintain an action for trespass to chattels.[79] However, the court rejected this argument because Compuserve had an Internet user policy prohibiting the unauthorized sending of spam through its proprietary computer network, and had expressly notified Cyber Promotions that its use was unauthorized pursuant to that policy.[80]

From the holding in *Compuserve*, the inference can be drawn that if an ISP does not have an express policy against spamming which notifies spammers that such a use of its computer system is unauthorized, companies like Cyber Promotions may be able to successfully assert a privilege defense based on implied consent. Absent a policy prohibiting the sending of spam, an ISP cannot be able to stop a spammer the *first* time he acts under trespass to chattels theory. Since a spammer can bulk e-mail thousands or millions of unsolicited messages at a time, the spammer may have the opportunity to reap his rewards while potentially damaging ISPs

---

[74] *Cyber Promotions*, 948 F. Supp. at 456; *see, e.g., Compuserve*, 962 F. Supp. at 1025-26 (following the holding in *Cyber Promotions* with respect to the First Amendment).

[75] *See* RESTATEMENT (SECOND) OF TORTS § 10 (1965).

[76] RESTATEMENT (SECOND) OF TORTS § 252 (1965).

[77] *See, e.g.*, Broberg et al., *supra* note 33, at S7.

[78] *Compuserve*, 962 F. Supp. at 1023-24. The court in *Compuserve* noted that "there is at least a tacit invitation for anyone on the Internet to utilize plaintiff's computer equipment to send e-mail to its subscribers." *Id.* (citing Buchanon Marine, Inc. v. McCormack Sand Co., 743 F. Supp. 139 (E.D.N.Y. 1990)).

[79] *Id.* at 1024.

[80] *Id.* An example of a subscription agreement prohibiting the use of an ISP's network to send spam can be found in the "Hotmail Terms of Service Agreement" which provides in part that a member may not "use the Service in connection with chain letters, junk email, spamming or any duplicative or unsolicited messages (Commercial or otherwise)." *Hotmail Policy and Member Conduct* (visited Apr. 22, 1999), <http://lc2.law5hotmail.passport.com/cgi-bi.../hminfo_shell.asp?_lang=&beta=&content=nospa>.

and subscribers alike without being subject to liability for his actions in trespass. However, as long as the ISP subsequently notifies the offending spammer that such a use is not authorized, any further mass mailings of spam would subject the actor to liability under trespass tort law.

2. Tortious Interference with Contractual Relations

Other tort theories involving the protection of the business relationship between an ISP and its subscribers may provide some relief from spam. Tort law has evolved, in part, to protect business relationships from the intentional interference of third parties[81] and provides a cause of action for the intentional interference of another's contractual relationship.[82] Such a cause of action requires the finding of the spammer's intent to interfere,[83] and that intent can be found where the interference occurs as a necessary consequence of the conduct the actor engaged in for an entirely different purpose.[84] Although a spammer's intent is to advertise and mass-market its product to e-mail subscribers, its actions may result, as a necessary consequence, in the interference with an ISP's performance of contractual obligations owed to its customers.

Such an interference was examined in *Concentric Network Corp. v. Wallace*,[85] in which an ISP brought a cause of action for tortious interference of a contract which resulted from Wallace's massive spamming campaign targeted at plaintiff Concentric Network Corporation's ("CNC") customers.[86] CNC claimed that as a result of the burden placed on its computer system by the volume of spam intentionally generated by Wallace, it experienced serious delays in processing e-mail and a decrease in the overall performance of its service provider agreements with its subscribers.[87] CNC argued that the resulting decrease

---

[81] W. Page Keeton et al., Prosser and Keeton on the Law of Torts § 14 (5th ed. 1984).

[82] Restatement (Second) of Torts § 766 (1979). This cause of action provides that a person who "intentionally and improperly interferes with the performance of a contract ... between another and a third person by inducing or otherwise causing the third person not to perform the contract, is subject to liability to the other for the pecuniary loss resulting to the other from the failure of the third person to perform the contract." *Id.*

[83] *Id.* § 8a.

[84] *Id.* § 767, cmt. d.

[85] *See* Hawley *supra* note 14.

[86] *Id.* Wallace, the defendant in this case, is the president of the ill-famed Cyber Promotions. *Id.*

[87] *Id.*

in the system's performance caused customer dissatisfaction to the point that it induced many to discontinue their service contracts with the ISP.[88]

However, the applicability of this tort as a cause of action against spamming is severely limited because a claim arises for tortious interference with a contract only when the actor actually induces a party to breach a contract.[89] However, subscribers may not actually breach their subscription agreements, opting to simply not renew their subscription with that particular ISP. Consequently, ISPs like CNC may have difficulty sustaining a claim for tortious interference with their subscription agreements.[90] Furthermore, subscribers bringing a tortious interference claim must also face the burden of showing that the spammer induced an ISP to breach its contractual obligation to provide Internet service.[91] Since ISP subscription agreements often include clauses disclaiming liability for interruptions in service,[92] proving that an ISP breached its service provision contract is difficult. By agreeing to the ISP's terms of service, the subscriber acknowledges that interruptions of service are anticipated between the two parties, and that the ISP is not liable for the type of temporary loss of service that may result from the system being overloaded by spam.[93] Because ISPs disclaim liability for interruptions in service and attempt to remedy interruptions of service in a timely manner, subscribers also will have difficulty showing actual inducement of breach of contract by a spammer.[94]

---

[88] *Id.*

[89] RESTATEMENT (SECOND) OF TORTS § 766 (1979).

[90] Nonetheless, the court in *Concentric Networks* entered a stipulated judgment whereby Wallace agreed to an injunction prohibiting Cyber Promotions from using CNC's accounts to send or receive e-mail. Ian C. Ballon, *Linking, Framing And Other Hot Topics In Internet Law And Litigation*, 520 PLI/Pat 167, 297 (1998).

[91] *See* Restatement (Second), *supra* note 82.

[92] For example, CNC's ISP liability disclaimer provides "CNC expressly disclaims any representation or warranty that the CNC service will be error-free, secure, or uninterrupted." *ConcentricHost Terms of Service and Acceptable Use Policy* (visited Aug. 20, 1999) <http://www.concentric.net/support_center/ex_tos.html>.

[93] *Id.*

[94] Other recourse may be availabe for ISPs under contract law based on the breach of a subscription agreement between an ISP and a spammer. If the agreement, or "terms of service" specifically prohibit the use of an ISP's network to send spam, any violation of that agreement could give rise to an action for breach of contract, or the discontinuance of service by the ISP. *See, e.g.*, Hotmail Corp. v. Van Money Pie, Inc., No. C 98-20064, 1998 U.S. Dist. LEXIS 10729, at *3, *17 (N.D. Cal. Apr. 16, 1998). Because only ISPs, and not subscribers, are protected under the breach of subscription agreement approach, this remedy is also limited in its scope of application.

3. Violation of Trademark Law

Fortunately for ISPs at least, other causes of action are available for relief from spamming based on principles of state and federal trademark law.[95] Federal trademark law is designed to "secure to the owner of the mark the goodwill of his business and to protect the ability of consumers to distinguish among competing producers."[96] ISPs, such as AOL and HOTMAIL, often incorporate their trademark name within their Internet domain names.[97] Spammers often enter false return addresses in the messages they send[98] and sometimes even go so far as to enter the name of an ISP in order to avoid receiving rejected mail or requests to cease and desist from subscribers.[99] If a spammer uses such a domain name in conjunction with its own advertising service in a manner that causes confusion as to the origin of its service, the spammer may be liable for trademark infringement or fraud.[100]

Similarly, if a spammer uses an ISP's domain name trademark in a manner that results in the "dilution of the distinctive quality" of the mark, the spammer may be liable for trademark dilution.[101] However, in order to succeed in a trademark dilution claim, a trademark owner must show that

---

[95] Both state and federal trademark law, embodied in the Lanham Act, were derived from common law principles of unfair competition. *See* United Drug Co. v. Theodore Rectanus Co., 248 U.S. 90, 97 (1918) *superceded by statute* Foxtrap, Inc. v. Foxtrap, Inc., 671 F.2d 636 (D.C. Cir. 1982) (stating that trademark law is merely a part of the broader common law principles of unfair competition).

[96] Advanced Resources Int'l v. Tri-Star Petroleum, 4 F.3d 327, 333 (4th Cir. 1993).

[97] Domain names are an alphanumeric designation of a site's Internet address. Porsche Cars North America, Inc. v. Porsche.com, No. 99-0006-A, 1999 U.S. LEXIS 8750 at *2 (E.D. Va. June 8, 1999). America Online, or "AOL," has their trademark incorporated in their domain name "aol.com." Similarly, HOTMAIL is known by its domain name "hotmail.com."

[98] *Ameritech.net Swamped by Spam, Blocks E-mail From America Online*, The Daily Record (Baltimore), July 29, 1998, at 2A.

[99] *Id.*

[100] The Lanham Trademark Act makes actionable the misleading use of a trademark in connection with services in commerce that results in the likelihood of confusion as to the origin or sponsorship of such services. The Lanham Trademark Act of 1946, 15 U.S.C. § 1125(a) (1946). In order for a false designation violation to occur the accused must use a false designation which deceives as to origin, ownership, or sponsorship of the service. *Id.* Moreover, the owner of the mark must believe that he is likely to be damaged by such false designation. *Id.* An example of a use that would constitute a § 1125(a) violation would be found where a spammer enters the name "aol.com" in the return address or "from" fields of the unsolicted e-mail message. *See, e.g.*, America Online, Inc. v. IMS, 24 F.Supp. 2d 548, 551 (E.D. Va. 1998). Consumers of the Internet service through which the spam is sent could become confused into thinking that the source of the spam was the ISP, AOL, and not the spamming service itself. *See id.*

[101] 15 U.S.C. § 1125(c).

he owns a famous and distinctive mark and that the alleged use of the mark is likely to result in its dilution through blurring or tarnishment.

In *America Online, Inc. v. IMS*,[102] an ISP successfully brought suit against a spammer under both of the above theories of trademark law.[103] ISP, AOL, successfully brought false designation of origin[104] and trademark dilution actions against IMS, an electronic marketing company.[105] AOL alleged that the defendant improperly sent over 60 million unauthorized e-mail messages to AOL subscribers.[106] The court held that defendant's use of the AOL domain name trademark in their message headers[107] created a "false designation of origin" in violation of trademark law because any subscriber seeing the familiar domain name in the header would mistakenly conclude that the spam either originated with or was sponsored by AOL.[108] The court also determined that AOL used its famous trademark as a domain name[109] and concluded that because AOL's customers made negative associations between their ISP and the junk e-mail sent by IMS, defendant's use of the domain name tarnished the mark resulting in the dilution of its distinctiveness.[110]

Although some ISPs such as AOL have been successful in their trademark claims against spammers, even the application of trademark law cannot completely stop the flow of spam over the Internet. Trademark infringement only occurs when a spammer uses a trademarked domain name. Therefore, spammers can avoid liability for false designation of origin by simply making sure they do not enter a trademarked domain name into the return address field. The spam will still get through, but it may be rejected and returned to some other unlucky person or an ISP that does not have a trademark.

Similarly, because trademark owners bear the burden of proving that their mark is indeed distinctive and famous in an action for trademark

---

[102] 24 F.Supp.2d 548.

[103] *Id.*

[104] *See supra* note 100 and accompanying text.

[105] *America Online*, 24 F. Supp. 2d at 548.

[106] *Id.* at 549.

[107] *PC Webopedia* (visited Aug. 20, 1999) <http://www.pcwebopedia.com> (defining the word "header" as follows: "In word processing, one or more lines of text that appears at the top of each page of a document").

[108] *America Online*, 24 F. Supp. 2d at 551.

[109] *Id.* at 552. The court stated that the AOL trademark was "distinctive" and "used and recognized throughout the world in association with AOL's online products and services." *Id.*

[110] *Id.* Although the court in *America Online* deferred ruling on damages, *Id.*, IMS will most likely be permanently enjoined from further use of the "aol.com" domain name.

dilution,[111] owners of trademarks not reaching such a threshold of fame will not have trademark dilution available to relieve them from spamming. This gap in coverage, inherent in the law, allows electronic marketing companies to seek out and utilize less famous ISPs without fear of an action for trademark dilution in response to their spamming practices. However, ISPs that do not have famous marks can still sue for false designation of origin if the spammer uses the ISP's trademark in a spam message header.[112] Nonetheless, the application of trademark causes of action to the context of spamming is still limited in that it provides relief from spamming to only some of those affected by the spamming efforts of direct marketing companies. Subscribers and ISPs affected by spam must turn to the state and federal legislatures for uniform protection from the ill effects of spam.

B. Legislative Efforts to Remove Spam

1. State Anti-Spam Laws

ISPs and subscribers may be able to find relief from spamming from the legislative efforts of their states of residence. However, state anti-spam statutes are limited in their utility to provide relief for subscribers and ISPs because they often only prohibit or provide remedies for *intrastate* spamming activities or have nominal penalties which act as only a weak deterrent to spammers. Nonetheless, several states, in an effort to supplement common law solutions to the spam problem, have proposed or enacted their own "anti-spam" laws.[113] The themes of such laws focus on providing a civil cause of action for damages or injunctive relief for

---

[111] 4 J. THOMAS MCCARTHY, MCCARTHY ON TRADEMARKS AND UNFAIR COMPETITION § 24:89 (4th ed. 1997). Specifically, the plaintiff in a trademark dilution claim must plead and prove that he is the owner of a famous mark:

> as measured by the totality of the eight factors listed in [15 U.S.C. § 1125(c)(1)], . . . [t]he defendant is making commercial use, . . . [i]n interstate commerce, . . . [o]f a mark or trade name, . . . defendant's use began after the plaintiff's mark became famous, [and that] defendant's use causes dilution by lessening the capacity of the plaintiff's mark to identify and distinguish goods or services.

Id.

[112] *See* discussion *supra* Part III.A.3.

[113] *See, e.g.*, CAL. BUS. & PROF. CODE § 17538.45 (West 1998 & Supp. 1999); NEV. REV. STAT. § 207.325 (West 1997); VA. CODE ANN. § 18.2-152.3 (Michie 1996); WASH. REV. CODE ANN. § 19.190.030 (West 1999).

recipients of spam,[114] imposing criminal liability for spamming,[115] levying fines against spammers,[116] and imposing restrictions on spamming.[117]

Recently, Virginia passed the Virginia Computer Crimes Act that provides, in relevant part, that any person who uses a computer network "without authority and with the intent to . . . [c]onvert the property of another" is guilty of computer fraud in violation of the Act.[118] Under this computer fraud law, both ISPs and subscribers are provided a private cause of action for the unauthorized use of their computer networks or computers by spammers.[119] Although the Virginia law itself does not specifically outlaw or regulate spam, it can be applied in some cases.

For example, in *America Online, Inc. v. LCGM, Inc.*,[120] the Federal District Court for the Eastern District of Virginia held that the defendant, LCGM, violated the Virginia computer fraud law by sending unsolicited commercial e-mail through AOL's server without authorization.[121] AOL argued that LCGM's use of its "aol.com" domain name allowed the defendant's unsolicited e-mail to circumvent spam-filtering devices in place,[122] thereby resulting in an unauthorized use of AOL's service and free advertising at the expense of AOL.[123] The court granted summary judgment in favor of plaintiff on its computer fraud claim.[124] Thus, AOL was able to successfully apply the Virginia computer fraud law to the context of spamming indirectly.[125]

---

[114] *See, e.g.*, VA CODE ANN. § 18.2-152.3 (Michie 1996).

[115] *See, e.g.*, NEV. REV. STAT. § 207.325 (West 1997).

[116] *See, e.g.*, WASH. REV. CODE ANN. § 19.190.040 (West 1999).

[117] *See, e.g.*, CAL. BUS. & PROF. CODE § 17538.45 (West 1998 & Supp. 1999).

[118] VA. CODE ANN. § 18.2-152.3(3) (Michie 1996).

[119] *See Id.* Recently, the State of Virginia has amended its Computer Crimes Act to make the use of a false online identity in conjunction with the sending of unsolicited bulk e-mail a misdemeanor trespass offense. The Associated Press, *Virginia Passes Law Against Unsolicited E-mail*, N.Y. TIMES, (Feb. 25, 1999) <http://www.nytimes.com/library/tech/99/02/biztech/articles/25spam.html>.

[120] 46 F. Supp. 2d 444, 451 (E.D. Va. 1998).

[121] *Id.*

[122] *Id.* Depending upon the e-mail software of a recipient or ISP, software that contains a program for filtering e-mail can sort and filter-out spam by the name of its sender, its subject matter, or other parameters based on message headers. *See* Hiawatha Bray, *Getting Rid of Junk E-Mail*, BOSTON GLOBE, Sept. 26, 1996, at D1.

[123] *America Online*, 46 F. Supp. 2d at 453 (stating that because many spammers forge e-mail message headers or enter false information, spam still slips through, rendering filtering mechanisms helpful but not entirely effective).

[124] *Id.*

[125] VA. CODE ANN. § 18.2-152.3(3) (Michie 1996). *See also* The Associated Press, *supra* note 119.

Other states have enacted legislation expressly directed at regulating spamming.[126] Both Washington and California have enacted laws prohibiting the unauthorized sending of unsolicited commercial e-mail and the entering of false or misleading information in e-mail subject lines.[127] However, the California statute only covers intrastate spamming activities and provides in part that, in the context of e-mail, "this section shall apply when the unsolicited e-mailed documents are delivered to a *California resident* via an electronic mail service provider's service or equipment *located in this state*."[128]

Further examples of state legislative efforts against spamming are found in both the Washington statute and a similar Nevada statute, which indicate that a violation of their "anti-spamming" laws is considered only a misdemeanor punishable by a small fine.[129] For example, the Washington statute provides that damages for a subscriber affected by spam is limited to the greater of $500 or actual damages for each piece of spam received.[130] The statute further limits the recovery of damages by ISPs to the greater of $1000 or actual damages.[131] Such a minimal punishment will not act as a strong deterrent for spammers who can generate huge advertising revenues at a minimum cost.[132] Although these new anti-spam laws provide state residents some relief from spamming, their utility in stopping spam is limited because of the imposition of only minimal penalties and their inapplicability to non-resident spammers.

Furthermore, many state statutes are targeted at controlling only intrastate spamming activities.[133] Unfortunately, Internet activities that traverse jurisdictional boundaries could create enforcement difficulties and leave state residents open to the efforts of out-of-state spammers. Thus, even state legislative efforts do not have the ability to completely protect their own resident ISPs and subscribers from the nuisance of spam.

---

[126] *See, e.g.*, CAL. BUS. & PROF. CODE § 17538.4 (West 1998 & Supp. 1999); NEV. REV. STAT. § 207.325 (West 1997); WASH. REV. CODE ANN. § 19.190.030 (West 1998).

[127] CAL. BUS. & PROF. CODE § 17538.4(a)(b) (West 1998 & Supp. 1999); WASH. REV. CODE ANN. § 19.190.030(1) (West 1998).

[128] CAL. BUS. & PROF. CODE § 17538.4(d) (West 1997 & Supp. 1999) (emphasis added).

[129] *See* NEV. REV. STAT. § 207.325(3) (West 1997); *See* H.B. 2752, 55th Leg., Reg. Sess. (Wash. 1998).

[130] *See* H.B. 2752, 55th Leg., Reg. Sess. (Wash. 1998).

[131] *Id.*

[132] Arguably, more severe penalties in the form of larger fines could act as a disincentive for marketing companies considering spamming.

[133] For example, both the California and Washington anti-spam laws only cover cases where the spam is sent by a computer in that state, to a resident of that state. CAL. BUS. & PROF. CODE § 17538.4(d) (West 1998 & Supp. 1999); *see* H.B. 2752, 55th Leg., Reg. Sess. (Wash. 1998).

2. Federal Efforts to Regulate the Flow of Spam

State remedies for spammimg provide only limited protection for subscribers and ISPs.[134] Common law causes of action are difficult to prove.[135] Trademark law's narrow scope only protects ISPs and owners of famous trademarks.[136] Moreover, state statutory remedies are also of limited utility because they are often directed at only intrastate spamming, or provide only a small fee or penalty for non-compliance.[137] Given these limitations, comprehensive federal legislation provides the best hope for the complete and uniform protection of all persons in the United States who are harmed by unsolicited commercial e-mail.[138] In fact, Congress has recently recognized the size of the problem and started listening to consumer groups and ISPs who wish to stop the flow of spam. Both consumer advocacy groups and marketing associations have pushed Congress to either amend existing law or enact new law regulating the sending of unsolicited commercial e-mail.[139]

One example of such Congressional efforts was a bill proposed by Representative Chris Smith of New Jersey, designed to amend the Telephone Consumer Protection Act of 1991.[140] The bill's goal is to "ban the transmission of unsolicited advertisements by electronic mail, and to require that sender identification information be included with electronic mail messages."[141] Anti-spam groups strongly supported the bill's prohibition of spam because it required the spammer to divulge its true identity and provided a strong monetary disincentive for non-compliance.[142] However, the bill met strong opposition by both the American Civil Liberties Union and AOL on First Amendment grounds

---

[134] *See* discussion *supra* Part III.B.1.

[135] *See* discussion *supra* Part III.A.

[136] *See* discussion *supra* Part III.A.3.

[137] *See* discussion *supra* Part III.B.1.

[138] Advocates of state law efforts to regulate spamming have expressed concern that "a patchwork of different laws across the country could hamper legitimate online marketing." Clausing, *supra* note 18.

[139] *Id.*

[140] The Netizen Protection Act, H.R. 1748, 105th Cong. (1997).

[141] *Id.*

[142] Coalition Against Unsolicited Commercial Email, *The Smith Bill - H.R. 1748*, (visited Aug. 20, 1999) <http://www.cauce.org/hr1748.html>. The bill provided a private cause of action for spam recipients who did not have a pre-existing relationship with the spammer or did not consent to receiving spam. *Id.* If a spammer did not have consent or a pre-existing relationship with the recipient, the recipient could collect $500 for each piece of spam received. *Id.*

because it singled out commercial speech based on its content.[143] Ultimately, unable to obtain the support of both houses of Congress, the bill died in the 105th Congress.[144]

Other attempts at regulating spamming through federal legislation have also met with failure. The Murkowski-Torricelli bill, for example, would have allowed spam to be sent as long as it was "tagged" as an advertisement so that subscribers could "opt-out" of receiving it.[145] This bill was strongly criticized as legitimizing spam and failing to prevent the sending of annoying junk e-mail in the first place.[146] Consumer advocacy groups feared that if spam was legitimized it would "open the floodgates," making it possible to legally deliver vast quantities of spam to Internet subscribers, without providing any relief for ISPs from the increased burden of spam on their facilities.[147]

Another anti-spam law, proposed by Congressman William Tauzin, of Louisiana, provided for the establishment of guidelines regarding commercial marketing through unsolicited e-mail and interactive computer services.[148] Consumer advocacy groups condemned the Tauzin bill as being totally ineffective because compliance with its federal spamming

---

[143] Cohen, *supra* note 37. Cohen quoted AOL's Jill Lesser as stating her First Amendment objection was that "[t]he legislation picks out a particular type of content, commercial [e]-mail." *Id.* (holding that legislatures may regulate truthful commercial speech in a reasonable time, place, and manner as long as the means is the least restrictive available, furthers a substantial governmental interest, and leaves open alternative channels of communication). *See* Central Hudson Gas v. Public Service Comm. of New York, 447 U.S. 557 (1980) (holding that legislatures may regulate truthful commercial speech in a reasonable time, place, and manner as long as the means is the least restrictive available, furthers a substantial governmental interest, and leaves open alternative channels of communication). Spam constitutes commercial speech because it "refers to a brand name or product or service" and is "made by a speaker with a financial interest in the sale of the advertised service, in the sale of competing product or service, or in the distribution of the speech" itself. Thomas W. Merrill, Comment, *First Amendment Protection for Commercial Advertising: The New Constitutional Doctrine*, 44 U. CHI. L. REV. 205, 236 (1976) (defining commercial speech).

[144] Coalition Against Unsolicited Commercial Email, *Pending Legislation*, (visited Aug. 20, 1999) <http://www.cauce.org/legislation.html>.

[145] Coalition Against Unsolicited Commercial Email, *S. 1618 / H.R. 3888*, (visited Aug. 20, 1999) <http://www.cauce.org/s1618_hr3888.html>.

[146] *Id.* The bill required spammers to instruct recipients on how to opt-out of their mailing lists. Alan Cohen, *Slamming The Door On Spam*, 220 N.Y. L.J. T2 (1998). The bill further provided that it was illegal for a spammer to falsify the origin of its e-mail messages. *Id.* The biggest objection to S. 1618 voiced by anti-spam groups was that spammers were allowed "one free bite" and only had to obtain consent for subsequent mailings. Coalition Against Unsolicited Commercial Email, *S. 1618 / H.R. 3888*, (visited Jan. 27, 1999) <http://www.cauce.org/s1618_hr3888.html>.

[147] Cohen, *supra* note 146, at T2.

[148] The Data Privacy Act of 1997, H.R. 2368, 105th Cong. (1997). The Tauzin bill sought "to promote the privacy of interactive computer service users through self-regulation by the providers of such services [ISPs], and for other purposes." *Id.* This bill was much more relaxed in terms of its prohibition of spamming and the imposition of guidelines for bulk e-mail advertisers. *See id.*

guidelines was purely voluntary on the part of spammers. Consumer groups feared that the opt-out approach would be unenforceable against large mass marketing organizations, thereby keeping ISPs and subscribers at the receiving end of large volumes of spam.[149] As a result of lack of support by, and agreement between, both consumer advocacy groups and marketing associations, the Tauzin and Murkowski-Torricelli bills met their demise in the 105th Congress.[150]

3. Future Attempts to Protect Persons Against Spam

Despite the past failure of Congress to enact legislation regulating unsolicited commercial e-mail, Congress continues to consider the impact of spam on ISPs and subscribers, as well as the opposing views of the consumer protection and marketing groups. By repeatedly attempting to enact effective anti-spam legislation applicable on a national scale, Congress has recognized both the harm incurred by ISPs and subscribers as a result of spam and that the problems associated with unsolicited commercial e-mail cannot be resolved solely under state statutory and common law. Congress must also recognize that in order to gain support from both consumer advocacy groups and marketing associations, some form of compromise is necessary to protect subscribers and ISPs.

Federal legislation should be enacted that would provide uniform protection for all victims of spamming, ISPs and subscribers alike. Congress should look to previously enacted telecommunications laws prohibiting other infamous marketing practices, such as telemarketing and "junk faxing," for guidance on how to best protect all those affected by spam.[151] The creation of a private federal cause of action for victims of spammimg would be able to fill the gaps left in the "protective barrier" against spam by the application of common law principles without completely preempting applicable state law remedies.[152] Nonetheless,

---

[149] Coalition Against Unsolicited Commercial Email, *S. 1618 / H.R. 2368*, (visited Aug. 20, 1999) <http://www.cauce.org/hr2368.html>.

[150] Coalition Against Unsolicited Commercial Email, *Pending Legislation*, (visited Aug. 20, 1999) <http://cauce.org/legislation.html>.

[151] *See, e.g.*, Telephone Consumer Protection Act of 1991, 47 U.S.C. § 227 (West 1998). This act prohibits the sending of unsolicited advertisement facsimiles and the use of automated dialing devices in telemarketing practices. *Id.*

[152] *See* discussion *infra* Part III.A.1-2. Much of the proposed federal legislation provided that state law applicable to protect against spam would not be preempted by a federal anti-spam law. *See, e.g.*, H.R. 3888, 105th Cong. (1998).

Congress must consider the conflicting viewpoints of consumer advocacy groups and marketing organizations.

a. Balancing Opposing Viewpoints

Consumer groups push for an all out ban of spam, but this approach is condemned by advertisers as being unconstitutional under First Amendment protections for commercial speech. On the other side of the spectrum, marketing organizations favor "opt-out" approaches or voluntary self-regulation based on congressional guidelines. For federal anti-spam legislation to gain support from both of these competing factions, and to pass both houses of Congress, some level of compromise is necessary.

In designing anti-spam legislation, Congress must determine the breadth of the prohibition of spam, the manner in which spam may be regulated to allow the lawful use of unsolicited commercial e-mail, and the parties for which a private cause of action would be available. Such legislation cannot have a scope so broad as to amount to a total ban on spam at all times, in every place, and in every manner without violating the First Amendment protections afforded advertising companies in their commercial speech.[153] Such a total ban on spam would likely be considered unconstitutional because it is more extensive than necessary to further a substantial governmental interest.[154] Furthermore, a complete ban on spam would not take into account the legitimate sending of spam to subscribers who actually want to be solicited. Congress must take an approach consistent with First Amendment commercial speech jurisprudence and limit its regulation of speech to a reasonable time, place, and manner.

On the other hand, voluntary self-regulation left in the hands of spammers is undesirable and unlikely to meet with success. One only has to look at the history of Internet self-regulation in the case of the dissemination by website owners of private information collected from Internet users during online registration. The Federal Trade Commission ("F.T.C.") was forced to file an action against one such website owner, Geocities, for collecting and disseminating personal information of people

---

[153] *See* Cohen *supra* note 146, at T2; Central Hudson Gas v. Public Serv. Comm. of New York, 447 U.S. 557, 566 (1980). However, the First Amendment does allow the prohibition of false or misleading commercial speech. *Id.* at 563-64. Accordingly, an anti-spam law could provide express prohibitions against false or misleading unsolicited commercial e-mail.

[154] *See Central Hudson*, 447 U.S. at 564.

who accessed their website.[155] Although data collection by website owners is lawful and unregulated in the Internet context, Geocities came under fire because it had promised not to give out personal information collected during user registration without the consent of the user.[156] Left to its own devices, Geocities was found to have sold the private information it collected to other website owners without receiving the permission of its users.[157]

The irony of the situation is that Geocities could have collected and disseminated the information with impunity if it had not implemented its no disclosure without consent policy.[158] In the self-regulated realm of cyberspace, websites are not required to have policies of non-disclosure and there is no incentive for a website owner to develop such a policy. Allowing spammers to self-regulate or voluntarily comply with federal spamming guidelines would similarly be ineffective because there would be no incentive to comply and no disincentive against increased mass spamming efforts. Thus, self-regulation of spammers would not address the harms incurred by ISPs and subscribers as the result of spam.

A legislative approach that mandates compliance with reasonable time, place, or manner restrictions would offer a compromise between the conflicting desires of consumer advocacy groups and marketing organizations. Congress could work with the Internet Corporation for Assigned Names and Numbers ("ICANN"), a non-profit group who will oversee the Internet's domain name[159] and addressing system,[160] to set up specific domains on the Internet that would be either "spam" or "spam free" zones. For example, certain Internet domains have been reserved for

---

[155] Joel Brinkley, *F.T.C. 'Losing Patience' With Business on Web Privacy*, N.Y. TIMES (Sept. 21, 1998) <http://www.nytimes.com/library/tech/98/09/biztech/articles/21privacy.html>.

[156] *Id.*

[157] Jeri Clausing, *Trade Commission Says GeoCities Violated Privacy Rules*, N.Y. TIMES (Aug. 13, 1998) <http://www.nytimes.com/library/tech/98/08/cyber/articles/13geocities.html>. Geocities' conduct amounted to an 'unfair and deceptive trade practice' in the eyes of the F.T.C. *Id.* In seeking to avoid a lawsuit by the F.T.C., Geocities accepted a settlement under which it was to restructure its data privacy policy. *Id.*

[158] Brinkley, *supra* note 155.

[159] A domain name is "[a] name that identifies one or more [Internet Protocol] addresses. . . . Domain names are used . . . to identify particular Web pages . . . . Every domain name has a suffix that indicates [to] which top-level (TLD) domain" the webpage belongs. *PC Webopedia* (visited Aug. 20, 1999) <http://www.pcwebopedia.internet.com/TERM/d/domain_name.html> (defining the term "domain name"). For example, "aol.com" is the domain name for AOL's Internet address, having a top-level domain name of ".com."

[160] Jeri Clausing, *New Internet Board Responds to Government Requests*, N.Y. TIMES (Nov. 23, 1998) <http://www.nytimes.com/library/tech/98/11/cyber/articles/24domain.html>.

government agencies and have a domain name which ends in ".gov."[161] The same type of Internet domain reservation could be applied to the context of keeping part of cyberspace free of spam. There would simply be a large zone of Internet addresses that would be considered "no spam" zones, allowing ISPs and subscribers to decide whether they want spam in their Internet diets, such as www.ihatespam.nospam. If a subscriber wanted to receive spam, he could sign-up with an ISP who had an Internet domain or address that would enable him to receive spam such as www.spam-me.spam.

Such a limited restriction on spam as commercial speech would be constitutional as a reasonable time, place, or manner restriction because it would leave open other channels of communication through which spam could be sent.[162] Moreover, this approach would serve the interests of all involved. Subscribers would have the choice to receive spam or to be shielded from it. ISPs would also benefit from this approach because they could set up their web interface in a spam free zone if they desired. For example, if AOL wanted to offer a service free of spam, it could obtain a second Internet name of AOL.com.nospam and decrease its overall costs of processing unwanted spam and mechanical problems associated with overburdened servers.

Finally, spammers would benefit because they could send unsolicited messages to subscribers and ISPs who expect to receive it. In a spamming zone, marketing groups could flourish without being subject to litigation for truthful spamming. However, the "spam zoning laws" could still constitutionally prohibit spam that contains false or misleading information such as a false return address, and impose harsh pecuniary or criminal penalties for non-compliance, thereby providing a level of protection for those subscribers and ISPs who elect to receive spam.[163] The needs of spammers, ISPs, and subscribers would all be addressed by a "spam zoning" approach because it would offer shelter for ISPs and subscribers from the effects of spam while ensuring the First Amendments protections that spammers have in their commercial speech.

---

[161] *See supra* note 159 and accompanying text. Other examples of reserved domains include ".org" for non-profit institutions, ".edu" for educational institutions, and ".mil" for websites operated by the military. *Id.*

[162] The United States Supreme Court has held that zoning requirements for theatres showing pornography, which is speech protected by the First Amendment, are constitutional as reasonable time, place, and manner restrictions. Young v. American Mini-Theatres, 427 U.S. 50 (1976).

[163] *See* NEV. REV. STAT. § 207.325(3) (West 1997); *see* H.B. 2752, 55th Leg., Reg. Sess. (Wash. 1998).

b. "A Civil Action"

As noted previously, legislation that does not provide a private cause of action or harsh fines for violations of anti-spam regulations is undesirable to consumer advocacy groups as ineffective because the monetary incentives to send spam are not outweighed by the potential penalties for doing so.[164] In order to discourage spammers under a spam zoning approach, remedies must be available to subscribers and ISPs to use against spammers who send unsolicited commercial e-mail across the border into spam-free territory. Providing a private, civil cause of action to anyone who is injured by spamming, coupled with a considerable statutory damages provision, is necessary because it would subject spammers found in violation of the spam-free cyberspace to civil liability and fines for non-compliance. Spammers could be subjected to harsh fines, or even treble damages, for non-compliance when knowingly invading a spam-free zone.[165]

A caveat to the private cause of action approach is the difference in the financial position of marketing companies and subscribers. Although marketing and advertising groups who generate huge revenue as a result of their spamming practices could afford to litigate, many subscribers would find themselves unable to finance a civil action. Thus, for an anti-spam statute to be effective, it must insure that all persons affected by spam in a non-spam zone can utilize such a cause of action by providing for the award of reasonable attorneys fees to the prevailing party.[166]

A spam zoning approach which restricts truthful spamming in a reasonable time, place, and manner, coupled with a statutory private cause of action for violations of spam-free zones, represents a compromise between the interests of ISPs, subscribers, consumer groups, and marketing organizations alike. All those affected by spam who are not protected by the limited utility of state common law and statutory remedies would have a way in which to recover for harm incurred by willful spammers. ISPs and subscribers who desire to be sheltered from spam and the effects it has

---

[164] *See supra* notes 130-132 and accompanying text.

[165] *See* discussion *infra* Part III.B.2 (discussing the Smith bill which provides for a $500 fine per piece of spam sent in violation of the law); *see also* Coalition Against Unsolicited Commercial Email, *The Smith Bill - H.R. 1748*, (visited Aug. 20, 1999) <http://www.cauce.org/hr1748.html>. If a spammer was shown to have willfully or knowingly violated the spam law, the damages were trebled to $1500 per piece of spam sent. *Id.*

[166] The award of attorney's fees should not be limited to just the plaintiff because just as many subscribers could not afford to maintain a lawsuit. Fledgling spamming companies also may not have the resources to defend themselves.

on their computers and computer networks may seek refuge in "no spam" zones. Meanwhile, spammers are free to send their unsolicited commercial e-mail through Internet facilities that allow it, to consumers who expect and desire it. With a strong monetary disincentive for false or misleading spam and violations of spam-free zones, spammers will have no motive to cross over the "no spam" line drawn in the electronic sands of cyberspace.

IV. CONCLUSION

Although the common law provides some relief for ISPs and subscribers, comprehensive federal legislation is required to stem the tide of unsolicited commercial e-mail and to provide uniform protection against spam. Congress should draft legislation that will fill in the gaps in protection found in the common law and in many state anti-spam laws in terms of their inapplicability to interstate spamming transactions.

Accordingly, legislation should be drafted to address the concerns of both consumer advocacy groups and marketing companies by restricting spam in a reasonable manner. Such restrictions, if violated, must give rise to a private cause of action for all affected by spamming, regardless of the indeterminacy of their pecuniary loss or their place of residence. A spam zoning approach would allow legitimate spamming to continue in a limited forum of those who wish to receive it. Providing a private cause of action and statutory damages for spammers who knowingly violate spam-free cyberspace will act as a strong deterrent to non-compliance. Furthermore, allowing the award of reasonable attorney's fees to the prevailing party would insure that both plaintiffs and defendants would be able to finance a civil action under the statute. Given the limited utility of state common law and statutory remedies currently available for spamming victims, only through federal legislative efforts will ISPs and subscribers obtain relief from spam.