Chapman Law Review

Volume 7 | Issue 1 Article 3

2004

Punitive Damages in Cyberspace: Where in the World is the Consumer?

Michael L. Rustad

Punitive Damages in Cyberspace: Where in the World is the Consumer?

Michael L. Rustad[*]

I. INTRODUCTION[**]

The Internet offers American consumers a global marketplace open 24 hours a day, 365 days a year. By 2004, online commerce is projected to account for nearly seven trillion dollars.[1] Currently, there are 262.3 million English-speaking Internet users with 280 million projected for 2004.[2] The worldwide online population is projected to be between 709 and 945 million.[3] In the United States there are 182.1 million people online, accounting for 65% of that population.[4] "With the ability to reach millions of Internet users simply by establishing a website, tens of thousands of companies are expected to take advantage of electronic commerce, 'redefining and restructuring the distribution of goods and services.'"[5]

[*] Michael L. Rustad, Ph.D., J.D., LL.M. is the Thomas F. Lambert Jr. Professor of Law and Co-Director of the Intellectual Property Law Concentration at the Suffolk University Law School in Boston. Sandra Paulsson, who is a law graduate of the University of Lund in Sweden and an LL.M. student at Suffolk, provided excellent research and editorial assistance. I would also like to thank my wife, Chryss J. Knowles, for her editorial suggestions. Finally, I would like to express sincere appreciation to my research assistants Michael J. Bauer and Patty Nagle for their diligence, and to the entire *Chapman Law Review* staff, and in particular to Kenny Saffles, Brian Bedinghaus, Trent Evans, Sherry Fuller, Kevin Morriss, Steve Ruden, and Matt Taylor for their efforts in editing this article.

[**] The research for this article included examining several cases only available in jury verdict databases and jury verdict reporting publications. These cases were obtained from LEXIS, Verdict Library, Allver File; and WESTLAW, LRP-JV database (Jury Verdict and Settlement Summaries). Citations to these jury verdict databases are made to the LEXIS or WESTLAW database.

1 *Forrester Projects $6.8 Trillion for 2004 ($ B)*, Global Reach, *at* http://glreach.com/eng/ed/art/2004.ecommerce.php3 (last revised Nov. 23, 2001).

2 *Global Internet Statistics (by Language)*, Global Reach, *at* http://www.glreach.com/globstats/ (last revised Sept. 30, 2003).

3 CyberAtlas staff, *Population Explosion!*, ClickZ Network, *at* http://www.clickz.com/stats/big_picture/geographics/print.php/5911_151151 (Sept. 22, 2003).

4 *Id*.

5 Brian K. Epps, Maritz, Inc. v. CyberGold, Inc.*: The Expansion of Personal Jurisdiction in the Modern Age of Internet Advertising*, 32 GA. L. REV. 237, 239 (1997) (quoting Louise Kehoe, *Surge of Business Interest*, FIN. TIMES (London), Mar. 1, 1995, at XVIII).

The risks to consumers in this global marketplace are many. Consumers are flooded with virus-infected e-mail, spam, and a variety of fraudulent online scams. Online criminals use the technique of "phishing" to trick consumers into giving their credit card numbers by sending fraudulent e-mails posing as banks, financial service providers, or Internet Service Providers ("ISP").[6] The e-mails often have direct hyperlinks to unaffiliated web sites that mirror the sites of trusted institutions.[7]

The Internet makes it effortless for impostors to assume false identities, and therefore, it is a seamless haven for identity theft. The seamy side of the Internet is rapidly becoming a global Petri dish for new torts and crimes perpetrated against consumers. Consumers face a multitude of potential risks as the result of unsavory practices by Internet retailers. The following three horror stories illustrate the systematic ways wrongdoers are preying upon consumers in cyberspace:

The Naked Internet Consumer—In June of 2001, Eli Lilly and Co. inadvertently released the e-mail addresses of 669 medical patients who had registered at its web site[8] to receive messages regarding health-related matters, such as reminders to take certain medications.[9] Eli Lilly settled with the states, but no individual obtained a damages award in this significant compromising of consumer privacy.[10]

Consumers as "Phish" Food in Online Auctions—The majority of consumer frauds arise out of online auction sales.[11] This is due in large part to online fraudsters who use a technique called "phishing" to defraud consumers who use eBay.[12] When phishing, a con artist sends a consumer what appears to be an "'official' e-mail message directing the person to a counterfeit site where they are encouraged to 'update their account.'"[13] The

6 Cade Metz, *Can E-Mail Survive?*, PC MAG., Feb. 17, 2004, at 65, 66.

7 Troy Wolverton, *Wells Fargo Latest Target in Scams*, CNET News.com, *at* http://news.com.com/2100-1017-857177.html (last modified Mar. 11, 2002).

8 *Eli Lilly Strikes Deal Ending E-Mail Privacy Suit by Eight States*, 4 E-BUS. L. BULL. 14, 14 (2002) [hereinafter *Eli Lilly*].

9 Julekha Dash, *ACLU Knocks Eli Lilly for Divulging E-Mail Addresses*, Computerworld, http://www.computerworld.com/managementtopics/ebusiness/story/0,10801,62050,00.html (July 9, 2001).

10 The settlement of the e-mail privacy lawsuit was with the states of California, Connecticut, Idaho, Iowa, Massachusetts, New Jersey, New York, and Vermont. *Eli Lilly*, *supra* note 8, at 14.

11 *Internet Fraud Statistics*, National Fraud Information Center, *at* http://www.fraud.org/2002intstats.htm (last visited Jan. 29, 2004) [hereinafter *Internet Fraud Statistics*].

12 *eBay Email Hoax and Web Page*, *at* http://www.millersmiles.co.uk/identitytheft/101303ebay1.htm (Oct. 13, 2003) (noting that since October 2003 there has been a hoax web page to capture consumer information).

13 Kyle Stock, *Auction Site Can Turn Crime Scene for Unwary*, POST & COURIER

criminal uses the information provided by the consumer to hijack his or her credit card and identity.[14] A survey of Internet fraud found that online auctions accounted for 90% of consumer losses in 2002.[15] The government's Internet Fraud Complaint Center reports that online auction fraud has comprised 46% of complaint referrals since 2000.[16]

Stalking Children in the Internet's Red Light District—Con artists frequently target children online. In one instance, a notorious "typosquatter" registered domain names that employed misspellings of other popular Internet domain names for children-oriented websites, such as Teletubbies and Disneyland, in order to attract children to adult entertainment sites.[17] When children accidentally misspelled the domain names for the children's sites, they were redirected to adult entertainment sites where fees were automatically charged for each child's click stream.[18]

As demonstrated by the above examples, many of the online injuries suffered by consumers are the product of truly reprehensible wrongdoing deserving of punitive damages. This Article presents the results of the first empirical study of the role that punitive damages have played in redressing consumer injuries during the first decade of Internet-related litigation. It provides definitive data on the number, size, post-verdict history, and factual circumstances underlying punitive damages in cyberspace. Currently, punitive damages play no meaningful role in protecting consumers in cyberspace despite the epidemic of wrongdoing that goes undetected and unpunished by public authorities.

Tort law has always evolved to address new forms of misbehavior. In the latter half of the twentieth century punitive damages were awarded against product manufacturers who

(Charleston, S.C.), Dec. 26, 2003, at 1A, 11A, *available at* http://www.charleston.net/stories/122603/loc_26ebay.shtml.

14 *Id*.

15 *Internet Fraud Statistics*, *supra* note 11.

16 NAT'L WHITE COLLAR CRIME CTR. & FED. BUREAU OF INVESTIGATION, IFCC 2002 INTERNET FRAUD REPORT 3 (2003), *available at* http://www.ifccfbi.gov/strategy/statistics.asp (last visited Feb. 22, 2003) [hereinafter IFCC 2002 INTERNET FRAUD REPORT].

17 *US Authorities Redirect 'Most Wanted' Cybersquatter to Jail*, INTERNET MAG. 011 (Nov. 2003) ("John Zuccarini registered common misspellings of the names of popular children's websites . . . and earned up to $1 million (£600,000) per year in affiliate commissions by redirecting people to pornographic websites. Visitors to the sites were often trapped by pop up ads, forcing them to reboot their computers."), http://web2.infotrac-custom.com/pdfserve/get_item/1/s4waebw3_2/sb635_02.pdf [hereinafter *US Authorities*].

18 *Feds Nab Alleged Porn Piper*, *at* http://www.cbsnews.com/stories/2003/09/04/tech/printable571499.shtml (Sep. 4, 2003).

knowingly marketed their products with excessive, preventable danger.[19] Tort remedies have the potential of filling the gap left by ineffective criminal sanctions against cyberwrongs such as online stalking.[20] Public enforcement needs to be augmented by consumers operating as "private attorneys general"[21] who pursue punitive justice against corporate wrongdoers. "The primary function of punitive damages is to punish, to deter private actors from making particularly egregious decisions harmful to society."[22]

Part II examines the case characteristics of Internet lawsuits where plaintiffs initiated causes of action in state and federal courts in the United States between 1992 and 2002.[23] The analysis of plaintiffs' victories in Internet cases has a domestic focus, employing a database that includes virtually all U.S. plaintiff victories in Internet cases. This database permits the first comprehensive examination of: (1) the frequency of punitive damages in Internet cases; (2) the specific causes of action on which the remedy was based; (3) plaintiff and defendant characteristics; and (4) the role punitive damages plays in the cyber-litigation system. A content analysis of all Internet-related cases reveals that no consumer obtained punitive damages during a decade of cyberlaw litigation.[24]

---

19 *See* Michael Rustad, *In Defense of Punitive Damages in Products Liability: Testing Tort Anecdotes with Empirical Data*, 78 IOWA L. REV. 1, 16, 18 nn.87-88 (1992) (noting that punitive damages in products liability cases evolved as a remedy beginning in the mid-1960s).

20 Lisa A. Karczewski, Comment, *Stalking in Cyberspace: The Expansion of California's Current Anti-Stalking Laws in the Age of the Internet*, 30 MCGEORGE L. REV. 517, 518 (1999) (arguing that the legal system has yet to develop effective remedies against online stalking).

21 Judge Jerome Frank of the Second Circuit Court of Appeals coined the term "private Attorney Generals [sic]" to refer to "any person, official or not," who brought a proceeding "even if the sole purpose is to vindicate the public interest." Associated Indus. of N.Y. State, Inc. v. Ickes, 134 F.2d 694, 704 (2d Cir. 1943), *vacated*, 320 U.S. 707 (1943). *See generally* Michael L. Rustad, *Smoke Signals from Private Attorneys General in Mega Social Policy Cases*, 51 DEPAUL L. REV. 511, 518 (2001) (arguing that "[t]he rubric under which all the definitions for the private attorneys general fall is the emphasis on private action for the public interest. It is only the possibility of private attorneys general receiving a contingency fee that permits lawsuits to be brought to vindicate the public interest").

22 *In re* Simon II Litig., 211 F.R.D. 86, 159 (E.D.N.Y. 2002).

23 The only foreign cases included in the research universe were lawsuits filed against non-U.S. defendants in state or federal courts.

24 The definition of a consumer for purposes used in this study is used by many state and federal statutes. A consumer transaction in cyberspace includes commercial transactions in which an individual is purchasing goods or services online for personal, family or household use. The definition of consumer is widely accepted and incorporated in such consumer statutes as the Truth in Lending Act ("TILA"). TILA's scope is limited to "consumer" credit transactions, which are defined as transactions in which "the money, property, or services which are the subject of the transaction are primarily for personal, family, or household purposes." 15 U.S.C. § 1602(h) (1998).

At present, punitive damages serve as a form of corporate self-help to assist corporations in protecting rights and consolidating market share in cyberspace. Part III explores the reasons why punitive damages have not yet developed as a consumer protection remedy in cyberspace. This Article will demonstrate that punitive damages are a necessary deterrent against Internet wrongdoers where the probability of discovery is low and the harm to consumers is generally undetected and unpunished by public authorities.

II. EMPIRICAL STUDY OF PUNITIVE DAMAGES IN CYBERSPACE

A. Research Methods

To obtain a more complete understanding of the roles that judges and juries play in the rapidly evolving arena of cyberspace litigation, all Internet-related cases in which a plaintiff received a punitive damages award were surveyed. This database of punitive damages awards in cyberspace was drawn from a variety of published and unpublished court opinions from the decade of 1992 to 2002. The appendix to this article describes the research methods and sources consulted to assemble the database on punitive damages in cyberspace. The research universe for this study is all Internet-related cases decided in state and federal courts during the first decade of Internet litigation.[25] Each of the reported findings is drawn from a larger universe of 484 cases in which plaintiffs received legal or equitable relief in an Internet-related case in a U.S. state or federal court between 1992-2002. The research findings reported below focus upon the cases in which prevailing cybertort plaintiffs received a punitive damages award.

25 For each Internet case, background information and data was compiled on the characteristics of plaintiffs, defendants, size of awards, and post-trial adjustments.

B. Research Findings

1. Punitive Damages in Cyberspace Are Increasing and Being Awarded at a Higher Rate than in Traditional Tort Caseloads

Table One

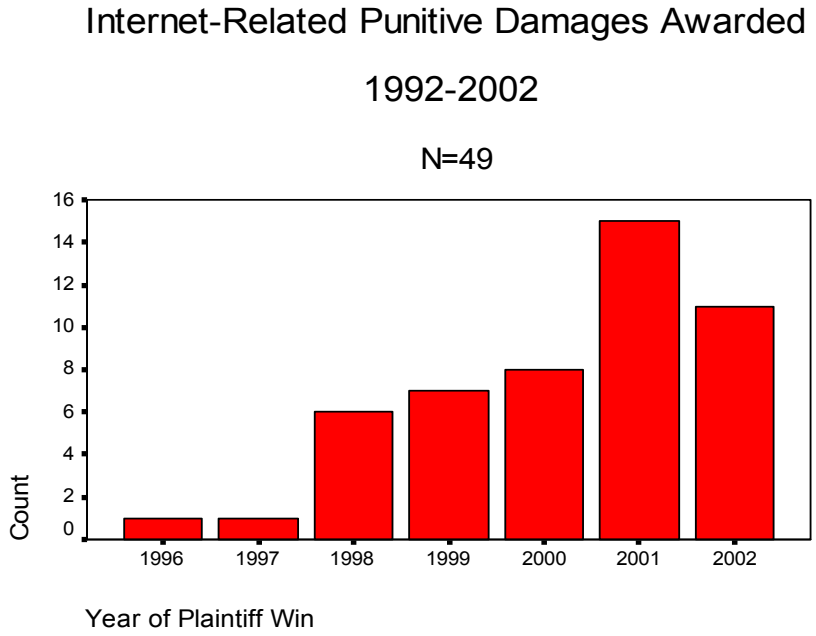


Table One depicts the forty-nine Internet related cases in which a plaintiff received a punitive damages award in all state and federal courts for the decade ranging from 1992 to 2002. The overall rate of punitive damages was roughly 10% of all Internet cases (49 of 484) in which either equitable or legal remedies were granted. Punitive damages are far more likely to be awarded in cybertort cases in which at least some monetary award was made. In the 187 cyberspace cases where money damages were awarded, punitive damages were also assessed in 49 cases (26%).

Table One suggests that the overall rate of punitive damages is greater in the Internet realm than in the real space world. All of the empirical studies of punitive damages agree that the rate of punitive damages is less than one in ten in cases where the

plaintiff prevailed.[26] The most comprehensive study of punitive damages in state courts was completed by researchers at the Bureau of Justice Statistics ("BJS").[27] The BJS study of civil courts of seventy-five of the largest American counties found that "[o]f the 12,026 verdicts in the sample, plaintiffs won a total of 364 punitive damages awards," which was less than 6% of the cases.[28] All prior empirical studies of the rate of punitive damages confirm that the overall rate is substantially lower than in cyberspace cases.[29] The higher overall rate of punitive damages may be explained by the fact that every case involved a defendant whose conduct was intentional. Another explanation would be that many of the cases involved repeat offenders such as spammers, pornographers, or wrongdoers who fled the jurisdiction.

Still, there were less than fifty punitive damages awards in a decade in all state and federal courts. The high-water mark for punitive damages in Internet cases occurred in 2001 with a total of only fifteen awards in all state and federal courts. As these numbers demonstrate, punitive damages are still a thimble-full of cases in the ocean of litigation.

---

26 As one scholar reports:

> Studies conducted by researchers at the RAND Corporation found that punitive damages are only awarded in 1-8% of civil cases. Other studies have found punitive damages to be awarded at similar rates. In the sample of cases examined by Daniels and Martin, punitive damages were awarded in only 4.9% of civil cases and in 8.8% of cases in which the plaintiff prevailed.

Jennifer K. Robbennolt, *Determining Punitive Damages: Empirical Insights and Implications for Reform*, 50 BUFF. L. REV. 103, 161 (2002) (internal citations omitted).

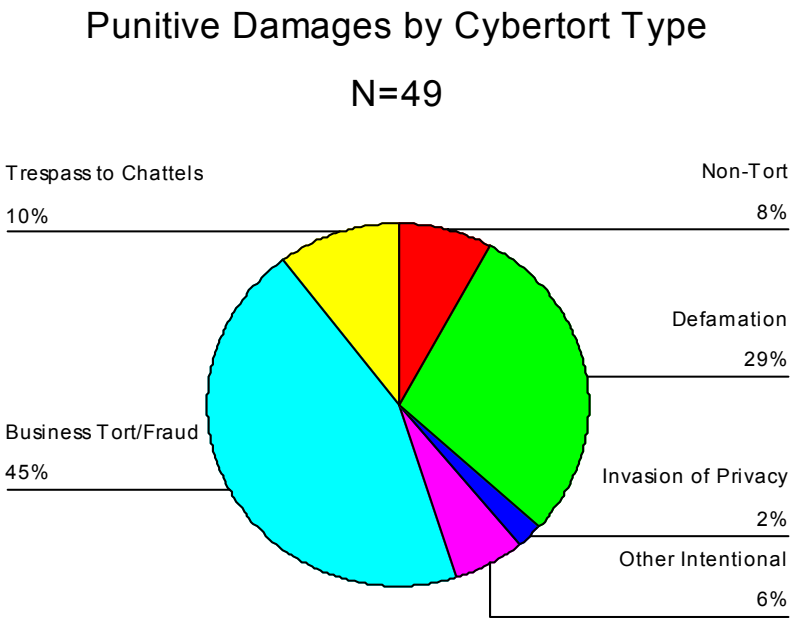
27 Bureau of Justice Statistics, U.S. Dep't of Justice, *Civil Justice Statistics*, *at* http://www.ojp.usdoj.gov/bjs/civil.htm (last revised Oct. 1, 2001).

28 Marc Galanter, *Real World Torts: An Antidote to Anecdote*, 55 MD. L. REV. 1093, 1127 (1996).

29 Michael L. Rustad, *Unraveling Punitive Damages: Current Data and Further Inquiry*, 1998 WIS. L. REV. 15, 17-33 (1998) (reporting the results of nine empirical studies of punitive damages and concluding that the rate of punitive damages is low).

2. Show Me the Money: Punitive Damages Are Mostly Found in Intentional Tort Cases Filed By Businesses To Recoup Economic Loss

Table Two



The first decade of punitive damages in cyberspace shares common ground with eighteenth-century English law where the elite used the legal system to achieve greater power.[30] Forty-five of the forty-nine punitive damages awards arose out of predominately cybertort cases, but every tort cause of action in the cyberlaw punitive damages sample arose out of an intentional tort. Most punitive awards arose in business tort cases filed by online or bricks-and-mortar[31] businesses. Cybertort punitive damages were predominately awarded in

30 Michael L. Rustad & Thomas H. Koenig, *Taming the Tort Monster: The American Civil Justice System as a Battleground of Social Theory*, 68 BROOK. L. REV. 1, 11 (2002) (describing Blackstone's Commentaries on English Law as reflecting the values of property owners and wealthy elites) [hereinafter Rustad & Koenig, *Taming the Tort Monster*].

31 A bricks-and-mortar business is an established company with a physical headquarters in the real space world as opposed to a purely online business with only a virtual presence.

economic loss cases rather than personal injury cases, which are the province of traditional tort law. Punitive damages in Internet-related cases have not yet developed in cases based upon negligence or strict liability.

The few cases where individuals obtained punitive damages often were in cases involving reputation or privacy injuries.[32] In fact, online defamation cases alone accounted for 29% of all punitive damages awarded in cyberspace cases during the ten-year period of the study.[33] For example, a doctor defamed by an Internet posting charging him with taking kickbacks led to a punitive damages award.[34] In another case, a University of North Dakota physics professor won a large punitive damages award against a former graduate student who accused him in online postings "of being a pedophile and having odd sexual habits."[35] In a Florida case awarding punitive damages, an Internet web page contained numerous defamatory postings pertaining to the plaintiff and his children.[36]

The most interesting aspect of Table Two is the cases that were not developed. No consumer was awarded punitive damages in a products liability action for bad software, the transmittal of a virus, or a faulty Internet security product. No consumer prevailed in a medical malpractice case arising out of telemedicine.[37] Moreover, not a single punitive damages award was handed out in any substantive area of the law predicated upon either negligence or strict liability.

Surprisingly, there were no personal injury lawsuits arising out of a decade of Internet sales or services. Punitive damages in cyberspace cases were predicated upon intentional tort causes of action, generally in business disputes. The business tort cases,

---

32 *See infra* Appendix A. *See also* Varian Med. Sys., Inc. v. Delfino, No. 780187, 2001 WL 1904203 (Cal. Super. Ct. Dec. 17, 2001) (assessing $350,000 in punitive damages for "more than 14,000 defamatory and sometimes vulgar messages on more than 100 Internet message boards" accusing company executives of having illicit sexual relations and other bad acts).

33 *See, e.g.*, Matos v. Am. Fed'n of State, County & Mun. Employees, No. CV980578747, 2001 WL 1044632, at *1 (Conn. Super. Ct. Aug. 13, 2001) (reporting defamation claim by corrections department employee against union).

34 Graham v. Oppenheimer, JVR No. 382280, 2000 WL 33232110 (E.D. Va. Oct. 2000) (awarding $350,000 in punitive damages).

35 Scott Carlson, *North Dakota Professor Sues Former Student and a Web Site Over Allegations in an Article*, CHRON. HIGHER EDUC., Jan. 19, 2001, at A33.

36 Bagwell v. Phillips, No. 97-13631, 1998 WL 1656174 (Fla. Cir. Ct. Nov. 23, 1998) (awarding $15,000 in punitive damages).

37 "The Institute of Medicine has defined telemedicine to encompass telephone, video and electronic transmission of medical information using telephone or digital technology." Alissa R. Spielberg, *Online Without a Net: Physician-Patient Communication by Electronic Mail*, 25 AM. J.L. & MED. 267, 287-88 (1999) (citing COMM. ON EVALUATING CLINICAL APPLICATIONS OF TELEMEDICINE, INST. OF MED., TELEMEDICINE: A GUIDE TO ASSESSING TELECOMMUNICATIONS IN HEALTHCARE 16-17 (1996)).

which accounted for nearly half of the punitive damages awards (45%), included actions for the intentional interference with contract, unfair and deceptive trade practices, intentional interference with economic opportunities, intentional interference with noncommercial opportunities, unfair competition, fraudulent misrepresentation, and the misappropriation of trade secrets. However, most of the Internet-related business tort cases involved large companies suing rivals or other companies interfering with their businesses.[38]

A typical business tort case where punitive damages were awarded occurred when one dot-com company sued another dot-com over a generic domain name.[39] Punitive damages were also awarded in a wrongful discharge case against a former dot-com company.[40] Bitter internecine business disputes between online companies and employees accounted for another large segment of cases.[41]

The legally protected interest in the vast majority of cybertort awards was to protect intellectual property interests such as trademarks, domain names, or trade secrets. A court levied a $65 million judgment against an online pornographer for pirating the sex.com domain name.[42] The court's award included $25 million in punitive damages to punish the defendant's fraudulent scheme perpetrated by a forged letter to a domain name registrar.[43]

In *Brookfield Communications, Inc. v. West Coast Entertainment Corp.*,[44] the Ninth Circuit reversed the district

38 *See, e.g.*, eBay, Inc. v. Bidder's Edge, Inc., 56 U.S.P.Q. 2d (BNA) 1856 (N.D. Cal. 2000) (involving rival Internet companies suing over alleged anticompetitive conduct, such as tortious interference with an advertising contract).

39 Xuan-Thao N. Nguyen, *Shifting the Paradigm in E-Commerce: Move Over Inherently Distinctive Trademarks – The E-Brand, I-Brand and Generic Domain Names Ascending to Power?*, 50 AM. U. L. REV. 937, 977 (2001) (describing a case where E-cards.com was awarded $1 million in punitive damages in its unfair competition action against Ecards.com).

40 Moreau v. Direct Express, No. BC 222666, 2001 WL 761748, at *1 (Cal. Super. Ct. Mar. 21, 2001).

41 *See, e.g.*, *Home Interactive Corporation Wins $11 Million Verdict*, *at* http://www.marketwire.com/mw/release_html_b1?release_id=36285 (Dec. 21, 2001) (reporting that a jury ordered the former president of a software company to pay punitive damages for stealing company property, disabling the plaintiff's web site, emptying the company's bank account, and generally interfering with the plaintiff's business after he resigned).

42 Laurie J. Flynn, *Cybersquatting Draws Heavy Penalty*, N.Y. TIMES, Apr. 6, 2001, at C4.

43 Robyn Weisman, *Sex.com Plaintiff to Get US $65 Million*, *at* http://www.newsfactor.com/perl/story/8699.html (Apr. 4, 2001). *See* Kremen v. Cohen, 325 F.3d 1035 (9th Cir. 2003) (certifying question to the California Supreme Court).

44 174 F.3d 1036 (9th Cir. 1999).

court's denial of an injunction prohibiting a competitor's use of its rival's trademark in a domain name as well as in metatags on its web site.[45] The dispute grew out of the defendant's use of metatags with its rival's trademark to increase the traffic to another web site. The court compared the misuse of metatags and the diversion of web traffic from the rightful trademark owner's site to "posting a sign with another's trademark in front of one's store."[46] On remand, the District Court denied summary judgment for punitive damages, holding that there was a triable fact as to whether West Coast was aware of Brookfield's rights at the time.[47]

The dataset demonstrates that punitive damages have not yet evolved as a sanction to punish and deter unfair or deceptive practices against consumers in cyberspace. Few plaintiffs found any legal remedy for violations of Internet security, data mining, or the invasion of privacy, although hardly a day passes when there is not a media account of some egregious breach of Internet privacy.

---

45 *Id*. at 1066-67.

> Metatags are HTML code intended to describe the contents of the web site. There are different types of metatags, but those of principal concern to us are the "description" and "keyword" metatags. The description metatags are intended to describe the web site; the keyword metatags, at least in theory, contain keywords relating to the contents of the web site.

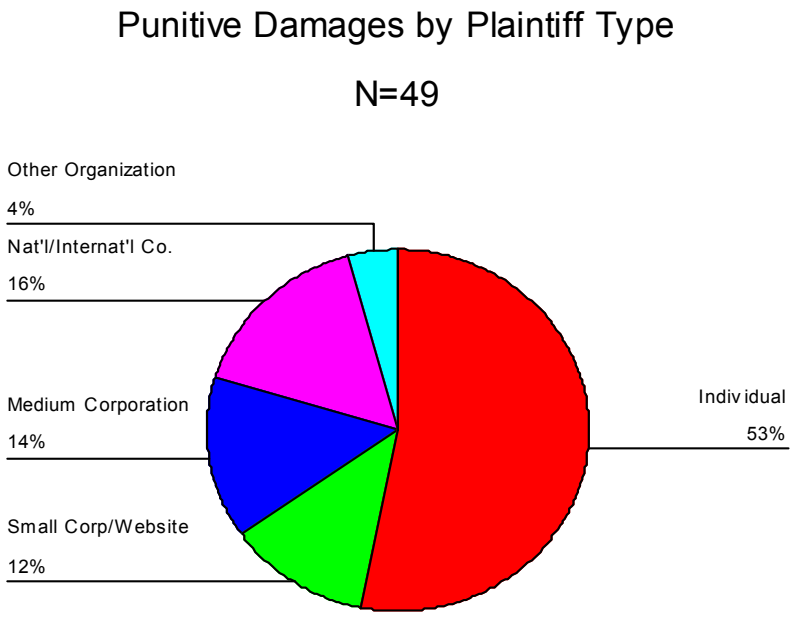
Id. at 1045.

46 *Id*. at 1064.

47 Brookfield Communications, Inc. v. W. Coast Entm't Corp., No. CV 98-9074, 1999 U.S. Dist. LEXIS 23251, at *25-26, 28 (C.D. Cal. June 10, 1999).

3. Punitive Damages Do Not Arise Out of Consumer Transactions

Table Three



Many individual plaintiffs obtained punitive damages for aggravated misconduct growing out of the employment relationship. Although individuals were the largest prevailing plaintiff category, these cases did not arise out of business-to-consumer transactions. For example, no consumer won an award against an Internet seller or renderer of services in a decade of cyberlaw cases.[48] Rather, 100% of the punitive damages awarded to individuals in cyberlaw cases were non-consumer in nature. It is remarkable that for a ten year period, in all U.S. federal and state courts, not a single consumer prevailed in a cyberlaw case in which punitive damages were awarded.

Individuals were the plaintiffs in one of every two punitive damages verdicts in Internet tort cases. However, punitive damages in cyberlaw cases played no meaningful role as a means of consumer protection for individuals. In a decade of punitive

48 The plaintiff and defendant characteristic as well as the aggravating circumstances for each of the forty-nine cyberlaw cases were systematically coded. *See infra* Appendix A.

damages awards, no case arose out of an online sale or service which could be classified as a consumer transaction.[49] Punitive damages, for example, were not awarded for the failure of online merchants to deliver goods or defective software. Furthermore, no consumer received punitive damages for non-consented transfers of their personal information.

Punitive damages awarded in favor of individuals arose out of non-consumer contexts such as the employment relationship or in disputes between individuals. When punitive damages were awarded to individuals, it was often in the context of ugly disputes arising out of incendiary exchanges on listservs, web sites, or e-mails. Nasty neighborhood disputes sometimes morphed into full-scale punitive damages warfare. The category of cases awarding punitive damages to individuals involved online stalkers,[50] vengeful neighbors,[51] and sexual harassers.[52] For example, when a neighbor published derogatory statements on an Internet web page about a family, the target obtained punitive damages in a Florida court.[53] In that case, the defendant also published photographs of the plaintiff's minor child as well as the child's name, address, and telephone number on the web site.[54] The plaintiff's punitive damages award was based on the common law torts of trespass, slander, nuisance, and intentional infliction of emotional distress.[55]

Many of these non-consumer cases involved business torts where an individual filed suit against a company. In one highly publicized case, two former research scientists employed by a high tech company published over 14,000 defamatory and vulgar messages on their web site and on over 100 Internet message boards.[56] The postings targeted two current corporate executives,

---

49 The Magnuson-Moss Warranty—Federal Trade Commission Improvement Act, for example, defines consumer products as meaning "any tangible personal property which is distributed in commerce and which is normally used for personal, family, or household purposes." 15 U.S.C. § 2301(1) (1998). Consumers are defined in the online context as a plaintiff filing an action against a seller or provider of services for actions such as the invasion of privacy, release of defective software, failure to deliver merchandise or similar actions.

50 Tim Doulin, *Jurors Order Stalker to Pay Victims for Internet Harassment*, COLUMBUS DISPATCH (Ohio), Feb. 21, 2002, at C12 (awarding $105,000 to two female musicians who were stalked over the Internet).

51 Bagwell v. Phillips, No. 97-13631, 1998 WL 1656174 (Fla. Cir. Ct. Nov. 23, 1998).

52 *See, e.g.*, Butler v. Krebs, No. 96-1204096, 1998 WL 2023763 (Tex. Dist. Ct. June 8, 1998) (awarding punitive damages against a Continental Express pilot for superimposing plaintiff's photograph onto other female bodies and transmitting the images over the Internet).

53 *Bagwell*, 1998 WL 1656174.

54 *Id.*

55 *Id.*

56 Varian Med. Sys., Inc. v. Delfino, No. 780187, 2001 WL 1904203 (Cal. Super. Ct. Dec. 17, 2001) (noting that plaintiffs alleged libel, invasion of privacy, breach of contract,

accusing them of "having extramarital affairs, videotaping office bathrooms, chronically lying and hallucinating."[57] In another case, a urologist obtained punitive damages against a defendant pathologist and his affiliated medical corporation for anonymous postings on the Internet.[58] Punitive damages were based upon the false accusation that the plaintiff was accepting kickbacks from a bidding company.[59]

Many individual plaintiffs obtained punitive damages for aggravated wrongdoings growing out of the employment relationship. In one bizarre case, a female employee received punitive damages when another employee and his son used the Internet to harrass her by exposing her to web sites devoted to sexual perversion.[60] In another instance, Internet America and its executives were assessed $100,000 in punitive damages, with a total verdict of more than $6 million, in an Internet-related lawsuit for defrauding their former financial officer.[61] The former Internet America executive's contention was that the president of the company defrauded her by convincing her to sell off her stock at a mere $0.80 per share just prior to a successful Initial Public Offering ("IPO").[62]

The second largest plaintiff category is national or international corporations (16%) followed by medium (14%) and small (12%) companies. Court decisions have aided large stakeholders in expanding their identity and intellectual property rights in the new economy. The typical business plaintiff is a "repeat player" or a large corporation with substantial legal and financial resources, such as Playboy Enterprises and America Online ("AOL").[63] According to the survey of cases, the largest stakeholders of the Internet economy

and unfair business practices, and sought compensatory and punitive damages).

57 *Id*. "A Santa Clara County jury awarded $775,000 in compensatory and punitive damages to a business and two of its employees after finding two former employees had libeled the plaintiffs with defamatory and vulgar statements posted on the Internet." *Id*.

58 Graham v. Oppenheimer, No. 00-CV-57, 2000 WL 33381418, at *1 (E.D. Va. Dec. 15, 2000).

59 *Id*. *See also* Graham v. Oppenheimer, JVR No. 382280, 2000 WL 33232110 (E.D. Va. Oct. 2000).

60 Kelly v. Whitley County, No. 00-CV-388, 2002 WL 31932414 (E.D. Ky. Sept. 18, 2002) (awarding $230,000 damages against jailor and county in case involving retaliatory discharge).

61 Carradine v. Internet Am. Inc., No. 05-01-01577-CV, 2001 WL 1825528 (Tex. Dist. Ct. Mar. 26, 2001), *vacated*, 106 S.W.3d 906 (Tex. App. 2003) (vacating due to settlement).

62 *Id*.

63 *See, e.g.*, Am. Online, Inc. v. Nat'l Health Care Disc., Inc., 174 F. Supp. 2d 890 (N.D. Iowa 2001) (awarding $100,000 punitive damages for willful and wanton actions); Am. Online, Inc. v. IMS, No. 98-0011-A, 1998 U.S. Dist. LEXIS 20448 (E.D. Va. Nov. 20, 1998) (magistrate's report recommending award of punitive damages for bad faith actions), aff'd No. 98-0011-A, 1998 U.S. Dist. LEXIS 20645 (E.D. Va. Dec. 30, 1998). *See also* cases cited *infra* notes 156, 157, 164.

were using punitive damages as a tool for consolidating their market share in the Internet economy. Therefore, most cyberlaw cases in the business context feature large Internet companies suing newly-established companies or individuals.

Cybersquatters[64] were frequently sued by powerful Internet industry stakeholders for trademark infringement.[65] John Zuccarini, a notorious cybersquatter, earned millions by registering domain names based upon the common misspellings of trademarks, a practice called "typosquatting."[66] For example, in one case, Zuccarini was ordered to pay damages and attorney fees based upon a finding that the defendant's use of domain names was "confusingly similar," thereby constituting a violation of the federal Anti-Cybersquatting Consumer Protection Act,[67] and an infringement of a famous trademark[68] The court ordered greater damages because the defendant was a recidivist who had been enjoined from registering misspelled names in suits brought by other companies.[69] In another case, America Online sought injunctive relief, compensatory damages, and punitive damages against AT&T, a competing ISP, in a trademark infringement action because AT&T was using the terms "Buddy List," "You have Mail!," and "IM Here."[70]

While large corporations are often plaintiffs in these cases, they rarely find themselves on the defense side of cyberlaw lawsuits. In cases where large corporations were named defendants, punitive damages were rarely awarded.[71] Likewise, the government was a defendant in fewer than 2% of cyberlaw cases—primarily Internet speech cases. Again, punitive damages

64 Cybersquatting is "the practice of registering 'well-known brand names as Internet domain names' in order to force the rightful owners of the marks 'to pay for the right to engage in electronic commerce under their own brand name.'" Virtual Works, Inc. v. Volkswagen of Am., Inc., 238 F.3d 264, 267 (4th Cir. 2001) (quoting S. REP. NO. 106-140, at 5 (1999)).

65 *See, e.g.*, Shields v. Zuccarini, 254 F.3d 476, 479-81, 487 (3d Cir. 2001); Elecs. Boutique Holdings Corp. v. Zuccarini, 56 U.S.P.Q. 2d (BNA) 1705 (E.D. Pa. 2000).

66 *US Authorities*, *supra* note 17.

67 15 U.S.C. § 1125(d) (1998 & Supp. 2003); 113 Stat. 1501, 1537 (1999). Congress enacted the Anti-Cybersquatting Consumer Protection Act to deter the increasing practice of cybersquatting. *Virtual Works, Inc.*, 238 F.3d at 267.

68 *Elecs. Boutique Holdings Corp.*, 56 U.S.P.Q. 2d (BNA) at 1710-11.

69 *Id*. at 1713.

70 Am. Online, Inc. v. AT & T Corp., 243 F.3d 812, 814, 823 (4th Cir. 2001).

71 *See, e.g.*, Amazon.com, Inc. v. Barnesandnoble.com, Inc., 239 F.3d 1343 (Fed. Cir. 2001) (holding that Amazon.com was not entitled to injunctive relief because barnesandnoble.com had raised a substantial challenge to the validity of their "1-click" patent); GoTo.com, Inc. v. Walt Disney Co., 202 F.3d 1199 (9th Cir. 2000) (reinstating preliminary injunction prohibiting Disney from using confusingly similar logo); PlayMedia Sys., Inc. v. Am. Online, Inc., 171 F. Supp. 2d 1094 (C.D. Cal. 2001) (enjoining America Online because its use of software exceeded the license agreement).

were rarely assessed.[72] Rather, defendants such as spammers and online pornographers accounted for most of the punitive damages awards in business tort cases.[73] In cyberspace, the "repeat players" such as America Online and other large Fortune 500 companies have the economic and legal resources needed to successfully litigate punitive damages lawsuits.[74]

No straightforward enforcement mechanism exists for enforcing tort judgments against web site providers who have no physical presence within the United States. Cyberspace judgments are only enforceable if the defendant has assets subject to legal process in the plaintiff's forum state. American courts require the plaintiff to prove minimum contacts sufficient to satisfy due process over a nonresident defendant.[75] Courts have declined jurisdiction in many Internet-related cases, ruling that a passive web site alone is an insufficient basis for jurisdiction.[76] For a court to exercise jurisdiction, the defendant

---

72 *See, e.g.*, PSINet, Inc. v. Chapman, 108 F. Supp. 2d 611 (W.D. Va. 2000); Mainstream Loudoun v. Bd. of Trs. of Loudoun County Library, 24 F. Supp. 2d 552 (E.D. Va. 1998).

73 *See, e.g.*, Am. Online, Inc. v. Nat'l Health Care Disc., Inc., 174 F. Supp. 2d 890 (N.D. Iowa 2001) (imposing punitive damages for sending spam e-mail on dental and optical plans); Mattel Inc. v. Internet Dimensions Inc., 55 U.S.P.Q. 2d (BNA) 1620 (S.D.N.Y. 2000) (enjoining pornographer's use of the phrase "Barbie's play pen" on its adult entertainment web site on the grounds that it diluted Mattel's trademark "Barbie" for dolls); Hollywood Entm't Corp. v. Hollywood Entm't, Inc., No. C 98-3670, 1999 U.S. Dist. LEXIS 6466 (N.D. Cal. May 4, 1999) (entering default judgment in favor of family video rental store against pornographic video rental store using identical trademark); Archdiocese of St. Louis v. Internet Entm't Group, Inc., 34 F. Supp. 2d 1145 (E.D. Mo. 1999) (enjoining use of PapalVisit.com domain name by adult entertainment web site because it tarnished the Catholic Church's trademark); Hotmail Corp. v. Van$ Money Pie Inc., 47 U.S.P.Q. 2d (BNA) 1020 (N.D. Cal. 1998) (enjoining defendants from using its trade name and service marks in spam e-mail); Hasbro Inc. v. Internet Entm't Group, Inc., 40 U.S.P.Q. 2d (BNA) 1479 (W.D. Wash. 1996) (enjoining pornographer's misuse of CANDYLAND trademark in domain name).

74 Marc Galanter, *Why the "Haves" Come Out Ahead: Speculations on the Limits of Legal Change*, 9 LAW & SOC'Y REV. 95, 97-114 (1974).

75 A threshold issue in many Internet cases is whether an out of state defendant may be subject to process in the forum. The inquiry frequently focuses on whether the defendant's web site activities are interactive or passive:

> The great majority of these cases have adopted the analytical framework of Zippo Manufacturing Co. v. Zippo Dot Com, Inc., 952 F. Supp. 1119, 1124 (W.D. Pa. 1997). In *Zippo* – also a case of specific jurisdiction – the court examined the few cases that had previously addressed the issue of whether a Web site could provide sufficient contacts for specific personal jurisdiction. It applied the results of these cases to the traditional personal jurisdiction analytical framework, noting that "the likelihood that personal jurisdiction can be constitutionally exercised is directly proportionate to the nature and quality of the commercial activity that an entity conducts over the Internet."

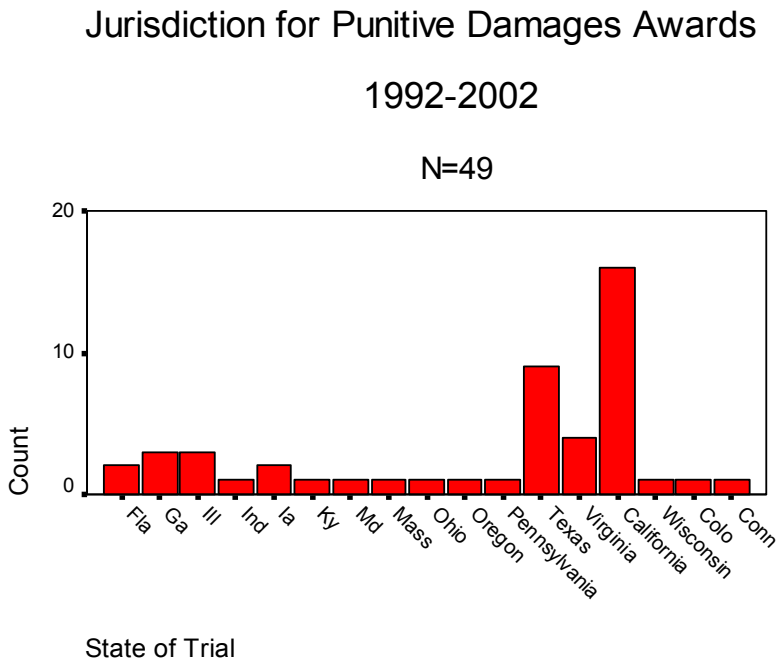
Lakin v. Prudential Secs., Inc., 348 F.3d 704, 710 (8th Cir. 2003) (affirming the district court's finding that the plaintiff had not proven minimum contacts to satisfy due process, but reversing on the issue of general jurisdiction ordering additional discovery).

76 *See generally* MICHAEL RUSTAD & CYRUS DAFTARY, E-BUSINESS LEGAL HANDBOOK § 7.03 (2003 ed.).

must have sufficient "minimum contacts" such that they have "purposefully availed" themselves of the privilege of doing business in the forum.[77] The issue of purposeful availment turns on factual circumstances such as whether the web site targeted residents in the plaintiff's jurisdiction.[78]

4. Punitive Damages Are Awarded In Internet Economy Strongholds

Table Four



Punitive damages in cyberspace between 1992-2002 were handed down in only a handful of states. The state of California accounted for approximately one in three punitive damages awards (N=16, 33%). Texas ranked second with 9 of the 49

77 *See, e.g.*, Bridgeport Music, Inc. v. Still N the Water Publ'g, 327 F.3d 472, 480-84 (6th Cir. 2003) (reversing district court's purposeful availment determination as to record company), cert. denied, 124 S. Ct. 399 (2003); Neogen Corp. v. Neo Gen Screening, Inc., 282 F.3d 883, 890 (6th Cir. 2002) (holding that the purposeful availment requirement is satisfied "if the website is interactive to a degree that reveals [that the defendant] specifically intended interaction with residents of the state"); Biometics, LLC v. New Womyn, 112 F. Supp. 2d 869, 872-73 (E.D. Mo. 2000) (selling products on web site to state residents constituted purposeful availment).

78 The leading case in this area is *Zippo Manufacturing Co. v. Zippo Dot Com, Inc.*, which developed a continuum where the middle ground is the borderline between passive and active web sites. 952 F. Supp. 1119, 1124 (W.D. Pa. 1997).

punitive damages awards (18%) followed by Virginia with four (8%) and Georgia and Illinois with three each. These five states were the only jurisdictions that handed down three or more punitive damages awards in Internet-related cases during that ten-year period.[79] Seventy-one percent of punitive damages in cyberspace cases were awarded in these five jurisdictions (N=35). Only twelve other states had one or more punitive damages awards during a decade of Internet-related litigation in all federal and state courts.[80]

Table Four documents that punitive damages coalesced in the epicenters of the Internet economy and were correlated with the location of key Internet companies. Table Four also confirms that the cyber-jurisdictional hot spots roughly correspond to centers of the Internet economy. A disproportionate number of punitive damages awards were made in states with powerful computer-based, entertainment or software industries. Two information-age leaders, California and Texas, accounted for greater than half of the punitive damages awards handed down in the decade 1992-2002. In many of these cases the plaintiff was a Texas or California corporation seeking redress against domain name entrepreneurs, cyberpirates, or online business competitors.

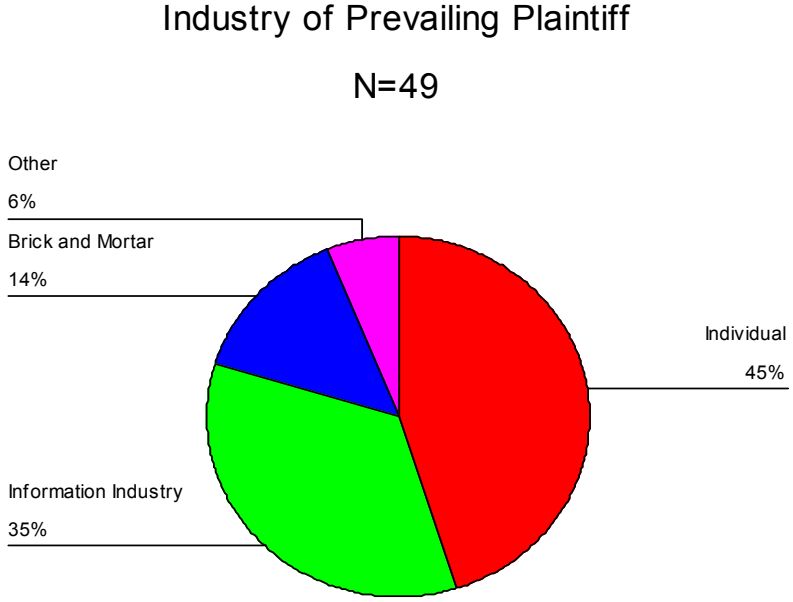
The greater incidence of punitive damages may be partially explained by the prominence of these states in the information economy. California's robust pattern of litigation is due to the dominance of the entertainment, high technology, and software industries. Similarly, Texas is rapidly becoming an epicenter of the computer software industry. Another notable mention is the Northern District of Virginia, where a flurry of anti-spam cases filed by America Online accounts for almost all of Virginia's punitive damages caseload in the decade studied. As we shall see, the empirical evidence suggests that punitive damages served primarily as a corporate means of legal control to protect the information industries in these states from spammers, cyberpirates, infringers, and other Internet wrongdoers.

79 In the larger study of torts in cyberspace, seventy percent of the cybertorts were decided in only five states: California (33%, N=38), Illinois (4%, N=5), New York (6%, N=7), Texas (13%, N=15) and Virginia (13%, N=15). *See infra* Appendix A.

80 Professor Saks, University of Iowa, concludes that no reliable data exists on plaintiff wins or even the size of awards over time in traditional tort litigation. Michael J. Saks, *Do We Really Know Anything About the Behavior of the Tort Litigation System – And Why Not?*, 140 U. PA. L. REV. 1147, 1154 (1992).

5. Punitive Damages Act as a Form of Corporate Self-Help

Table Five



a. Corporate Dominance in Cyberspace

Forty-nine percent of the cyberlaw punitive damages awards were assessed in favor of companies classifiable as either predominately a brick-and-mortar company or one in the information industry.[81] A content analysis of the cases in these industries confirms that corporate America is a major beneficiary of the punitive damages sword. Companies in all industries outnumber individual plaintiffs and many of the disputes involve powerful Internet stakeholders vindicating their rights in

81 The largest component of the "information industry" is made up of ISPs, online service providers, and telecommunication providers, which together account for 15% of all cases. Computer software companies, such as Microsoft, Adobe, Intel, and the larger ISPs were the big winners in cyberspace. Internet-based companies with a bricks-and-mortar presence constituted the single largest plaintiff class among the non-individual plaintiffs. ISPs accounted for the next largest plaintiff category industry, followed by other online sales and services. Miscellaneous organizations accounted for only two punitive damages awards. The information industry plaintiffs included companies that predominately involved the transfer of intangible products such as software, entertainment content, and other intangibles. ISPs such as America Online and Earthlink constituted one of the largest sectors of the information industry in the sample. Other organizations included non-profits. The research universe did not include governmental organizations as prevailing plaintiffs.

cyberspace.[82] The individual plaintiffs depicted in Table Five prevailed in cases arising out of non-consumer claims.[83] Stockholders, investors, or employees received punitive damages in only three of the forty-nine (6%) Internet-related cases involving securities fraud or the failure to pay stock options.[84] The residual "other" category included a few nonprofit organizations.[85] The next subsection examines the functions of punitive damages for corporate plaintiffs in business-to-business transactions.

b. Corporate Self-Help Remedy in Cyberspace

i. Protecting Trade Secrets in Cyberspace

In the Internet economy, the crown jewels of a company may be confidential information such as source code or methods of doing business online. Accordingly, companies have used punitive damages as a tool to redress the misappropriation of trade secrets. Trade secrets on the Internet may be lost at the

82 *See, e.g.*, EarthLink, Inc. v. Smith, 13 Internet L. & Reg. (P&F) 94, (N.D. Ga. July 9, 2002) (awarding punitive damages against spammer in favor of large ISP); Am. Online, Inc. v. Nat'l Health Care Disc., Inc., 174 F. Supp. 2d 890 (N.D. Iowa 2001) (awarding punitive damages to AOL); Schmerin v. CD Titles, Inc., No. SUCV95-07061, 1998 WL 1754045 (Mass. Super. Ct. Mar. 30, 1998) (awarding punitive damages to business against small web site). *See also* Nguyen, *supra* note 39, at 977 (noting the award of punitive damages in a business tort dispute over domain name between E-cards.com and ECards.com); *Neon Systems Says It Won $39 Million Verdict*, N.Y. TIMES, June 6, 2001, at C4 (punitive damages awarded in business torts case).

83 Non-consumer cases frequently arose out of the employment relationship. *See, e.g.*, Butler v. Krebs, No. 96-1204096, 1998 WL 2023763 (Tex. Dist. Ct. June 8, 1998) (awarding punitive damages against airline and co-workers for superimposing nude image of female pilot on web site and intranet among other acts of online harassment); Franza v. Hayes, No. 802402, 2001 WL 1137243 (Ga. Fulton County Ct. May, 2001) (awarding punitive damages to employee in workplace case).

84 There were a few Internet-related securities fraud cases in which punitive damages were awarded for new dot-com businesses that allegedly defrauded investors. In one case, investors were awarded $250,000 in punitive damages when directors of an educational web site misrepresented that its stock would be registered and that the investors would receive stock in another web site company. Chee v. PinkMonkey.com, Inc., No. 00-38766, 2002 WL 1919479 (Tex. Dist. Ct. June 11, 2002).

85 The research sample excludes actions by the Federal Trade Commission ("FTC"), Securities & Exchange Commission, and other government agencies prosecuting actions against cyberspace defendants. The sample includes cases where an individual or corporate entity files suits against a government agency as a wrongdoer. Civil penalties filed by the FTC in cyberspace cases are increasing rapidly. The cases in the FTC sample disproportionately included defendants advertising miracle health products, get rich business schemes, false credit repair schemes, deceptive investment opportunities, pyramid schemes, deceptive adult entertainment sites, spam e-mailers, and other marginal businesses. In recent years, FTC enforcers are expanding their enforcement sweeps to include mainstream companies. Gateway.net, for example, was fined for advertising free Internet services without the disclosure that long distance charges were not free. The FTC is also expected to expand its enforcement against web sites surreptitiously collecting consumer personal information. *Gateway Settles FTC Charges Over Free Internet Service Claims*, *at* http://www.ftc.gov/opa/2001/05/gateway.htm (May 15, 2001).

click of the mouse and must be protected by measures to guard the secrecy of information transmitted. Some of the first cyberlaw cases involved litigation to vindicate the misappropriation of trade secrets. The first online trade secrets cases arose out of the Church of Scientology's attempt to enjoin further distribution of church doctrine on web sites.[86] In one case, the Church of Scientology filed suit against the Washington Post for publishing portions of Scientology doctrine entitled "Advanced Technology," which were claimed as trade secrets.[87] The federal district court denied injunctive relief finding that the defendants' actions were protected by the fair use doctrine of federal copyright law and that the disputed documents were no longer a trade secret as they had already been posted on the Internet.[88]

Trade secrets in the online world deserve the same protections as in the bricks-and-mortar world. Internet trade secrets are particularly vulnerable because the interconnected system of computers makes it possible for hackers, ex-employees, and experts in corporate espionage to steal information without leaving physical evidence. The Internet economy is known for a rapid turnover in employees, and online companies face the constant danger that an ex-employee will misappropriate trade secrets for use in a competitor's business. For example, Monster.com recently settled a trade secret lawsuit against its former president and eighteen ex-employees who left the company to join a rival Internet company.[89]

The misappropriation of trade secrets is a popular cause of action to protect the intangible assets of companies connected to the Internet.[90] In *DoubleClick, Inc. v. Henderson*,[91] several employees of a prominent Internet advertising company planned to leave in order to form a dot-com startup.[92] DoubleClick

86 *See, e.g.*, Religious Tech. Ctr. v. Netcom On-Line Communication Servs., Inc., 907 F. Supp. 1361, 1365-66 (N.D. Cal. 1995) (refusing to enjoin bulletin board service which posted church documents); Religious Tech. Ctr. v. Lerma, 908 F. Supp. 1362, 1369 (E.D. Va. 1995) (granting defendant's motion for summary judgment because there was no trade secret misappropriation).

87 *Lerma*, 908 F. Supp. at 1364-65.

88 *Id*. at 1367-68. *See also* Religious Tech. Ctr. v. F.A.C.T.NET, Inc., 901 F. Supp. 1519 (D. Colo. 1995) (denying preliminary injunction where balance of harms weighed against the plaintiff in case involving Church doctrine allegedly protected as trade secrets).

89 *Monster.com Ends Suit on Ex-Workers*, N.Y. TIMES, May 1, 2001, at C7.

90 *See, e.g.*, SNA, Inc. v. Array, 51 F. Supp. 2d 554 (E.D. Pa. 1999) (enjoining use of plaintiff's domain name as trademark infringement and enjoining meta tagging of plaintiff's trademarks as unfair competition), *aff'd sub nom.*, Silva v. Karlson, 259 F.3d 717 (3d Cir. 2001).

91 No. 116914/97, 1997 WL 731413 (N.Y. Sup. Ct. Nov. 7, 1997).

92 *Id*. at *3.

confiscated one of the employee's laptops and found information on the hard drive, including e-mails and future business plans that provided evidence suggesting the misappropriation of trade secrets.[93]

Punitive damages are increasingly used as a corporate tool to punish and deter competitors that misappropriate trade secrets.[94] The Uniform Trade Secrets Act[95] ("UTSA") provides a wide array of remedies for trade secret misappropriation, including preliminary injunctive relief, monetary damages, lost profits, consequential damages, lost royalties, and attorneys' fees.[96] Section 3 of UTSA also gives the court the power to award "exemplary damages in an amount not exceeding twice any award."[97]

In October 2003, the Internet Truckstop, a web site devoted to improving efficiencies in freight services,[98] received a $120,000 punitive damages award against a competitor, Getloaded.com for the theft of trade secrets.[99] The judge imposed punitive damages after the jury found Getloaded.com liable for hacking into Internet Truckstop's computer system and misappropriating computer codes and other trade secrets.[100]

In yet another case, a California court imposed $2.25 million in punitive damages and $4.3 million in compensatory damages against a Seattle firm for misappropriating an Internet company's technology for pop-up ads.[101] The defendants, who were in the business of selling cameras, used the plaintiff's pop-up technology to feature "cameras trained on scantily clad women."[102] The plaintiffs charged the defendant with failing to pay online advertising revenues and with misappropriating client lists that were used to start the defendant's own company.[103]

---

93 *Id*.

94 *See, e.g.*, Bob Mims, *Overstock.com Sues Two Former Employees*, SALT LAKE TRIB., Dec. 9, 2003, at E9 (reporting that an Internet closeout retailer filed a trade secret claim seeking punitive damages against former employees who allegedly sold customers' e-mail addresses to spammer).

95 THE NAT'L CONFERENCE OF COMM'RS ON UNIF. STATE LAWS, UNIF. TRADE SECRETS ACT WITH 1985 AMENDMENTS §§ 3-4 (1985).

96 *Id*. at § 3.

97 *Id*.

98 The services offered by the Internet Truckstop included freight matching and its corporate goal is to "'[f]ill empty trailers.'" John D. Schulz, *Attacking Inefficiencies*, TRAFFIC WORLD, Sept. 18, 2000, at 33 (quoting Internet Truckstop executive, Scott Moscrip).

99 *Trucking Site Appeals $510K Verdict, $120K in Punitives in CFAA Case*, 16 SOFTWARE L. BULL. 3 (Oct. 2003).

100 *Id*.

101 Claire Luna, *Court Victory for Firm Run by 3 Brothers*, L.A. TIMES, Nov. 19, 2003 (Orange County ed.), at B3.

102 *Id*.

103 *Id*.

In general, large, established companies prevail in cybertort cases against smaller rivals, startups, or web sites. Punitive damages have been imposed in questionable business torts cases where the evidence of aggravated circumstances was weak or non-existent. The typical domain name dispute is a control struggle between an established trademark owner and an Internet entrepreneur who has registered a domain name containing the same trademark.

ii. Punitive Damages and Domain Name Warfare

Domain name disputes typically arise when the registrant, in an effort to attract Internet users, obtains the right to use a domain name that is substantially similar or identical to the trademarks or the name of a famous company or person. The impact on the trademark owner's business may be dramatic because of the confusion created by a misleading domain name address.

In *Kremen v. Cohen*,[104] ex-convict Stephen Cohen forged a letter to a domain name registrar, Network Solutions, claiming it was a letter he received from Online Classifieds.[105] The forged letter tricked the registrar into assigning Kremen's rights to the domain name, sex.com, to Cohen.[106] Cohen's letter "claimed the company had been 'forced to dismiss Mr. Kremen,' but 'never got around to changing our administrative contact with the internet registration [sic] and now our Board of directors has decided to *abandon* the domain name sex.com.'"[107] Judge Alex Kozinski observed:

> Despite the letter's transparent claim that a company called "*Online* Classifieds" had no Internet connection, Network Solutions made no effort to contact Kremen. Instead, it accepted the letter at face value and transferred the domain name to Cohen. When Kremen contacted Network Solutions some time later, he was told it was too late to undo the transfer. Cohen went on to turn sex.com into a lucrative online porn empire.[108]

Kremen filed a lawsuit against the perpetrator of the fraud as well as an action for conversion against the registrar for permitting the fraudulent transfer of sex.com.[109] The district court concluded that the letter had been forged, and accordingly,

104 337 F.3d 1024 (9th Cir. 2003).
105 *Id*. at 1039.
106 *Id*.
107 *Id*.
108 *Id*. at 1027.
109 337 F.3d at 1027-28.

directed the defendant to return the domain name to Kremen.[110] The court also invoked the constructive trust doctrine as well as California's unfair competition statute and ordered disgorgement of the defendant's profits.[111] The evidence was undisputed that Cohen had forged the letter, whereby the owner, Kremen, through his housemate, purportedly transferred the "sex.com" domain name.[112] The district court, however, ruled that the registrar was not liable since domain names could not be converted.[113] The Ninth Circuit reversed, holding that Network Solutions could be held liable for conversion in transferring Kremen's domain name to a con artist since California's law of conversion covers the theft of intangibles.[114] However, the defendant fled to Mexico, thumbing his nose at the court by secreting his assets in offshore locations beyond the reach of process.[115]

In *Simon Property Group, L.P. v. mySimon, Inc.*,[116] Simon Property Group ("SPG"), a bricks-and-mortar company that designed and managed shopping malls, brought suit against mySimon, a dot-com company that had launched a web site in October 1998.[117] Six months after mySimon's launch, SPG started "a corporate 'branding' campaign to inform consumers that it owned and managed certain shopping malls," although it had never considered such a campaign necessary in its 40 years of existence.[118] "SPG demanded that mySimon stop using the 'mySimon' name," but the dot-com refused.[119] SPG filed a trademark infringement lawsuit under the Lanham Act as well as business tort claims under Indiana state law.[120]

The gravamen of SPG's claim was that it had exclusive rights to the "Simon" name, and therefore, "that mySimon's name, Web address, and cartoon mascot named 'Simon' infringed on its rights."[121] The appeals court noted that SPG presented weak evidence that the "'Simon' name had attained secondary

110 *Id*. at 1027.

111 *Id*. The lower court "awarded $40 million in compensatory damages and another $25 million in punitive damages" under California's unfair competition statute. *Id.*

112 Kremen v. Cohen, No. C 98-20718, 2000 WL 1811403, at *1 (N.D. Cal. Nov. 27, 2000).

113 337 F.3d at 1036 (affirming dismissal of plaintiff's conversion claim against domain name registrar).

114 *Id*.

115 *Id*. at 1027 ("The district court froze Cohen's assets, but Cohen ignored the order and wired large sums of money to offshore accounts.").

116 282 F.3d 986 (7th Cir. 2002).

117 *Id*. at 987-88.

118 *Id*. at 988.

119 *Id*.

120 *Id*.

121 *Simon Prop. Group*, 282 F.3d at 988.

meaning or that consumers were likely to confuse SPG with mySimon."[122] MySimon presented a highly probative consumer survey "demonstrating that there was no likelihood of confusion between mySimon and SPG."[123] Despite this compelling defense to SPG's claim of trademark infringement, the jury handed down an $11.5 million compensatory damages award against mySimon, even though the record showed that mySimon had not yet earned profits.[124] The jury also awarded $5.3 million for corrective advertising and $10 million in punitive damages.[125] Finally, the court permanently enjoined mySimon from using or incorporating the terms "Simon" or "my Simon" in any Internet site and from using its "Simon" cartoon mascot on its web site.[126]

However, the trial judge "found that requiring mySimon to change its name provided sufficient relief," and therefore, reversed the $11.5 million damages award.[127] The judge also reduced the $10 million punitive damages award to $50,000 as required by Indiana's tort reform statute.[128] Finally, the judge "ordered a new trial on the corrective advertising issue, subject to SPG's acceptance of a *remittitur* to nominal damages of $10."[129] The Seventh Circuit dismissed SPG's appeal on the grounds that the company had "voluntarily abandoned its quest for a preliminary injunction after the district court denied its TRO motion," and because "[t]he potential threat to SPG's name [was] questionable."[130] In this case, the court apparently found that the corporate plaintiff was "pushing the envelope" in using punitive damages to protect its rights and defend its market position.

iii. Protecting Corporate Reputations in Cyberspace

Bitter disputes arise over the use of the Internet to impugn the reputation of companies by posting allegedly false information. In *Amway Corp. v. Procter & Gamble Co.*,[131] Amway brought suit against Procter & Gamble ("P & G") after a third party published on the Internet a complaint P&G had filed in another case. P & G's posted complaint contained allegedly defamatory statements about Amway, its officers, and its

122 *Id*. at 988, 991.
123 *Id*. at 989.
124 *Id*.
125 *Id.*
126 *Simon Prop. Group*, 282 F.3d at 989.
127 *Id*.
128 *Id*. at 989-90.
129 *Id*.
130 *Id*. at 990-91.
131 346 F.3d 180 (6th Cir. 2003).

business practices, asserting that Amway was operating as an illegal pyramid scheme.[132] The district court granted P & G's motion for summary judgment and found that Michigan's Reporting Privilege protected the accurate posting of the publicly available court documents.[133] The Sixth Circuit affirmed the dismissal, finding that even if the statements in the original document were defamatory, their publication on the Internet did not constitute an additional act of libel on P & G's part.[134] Disputes between business competitors over Internet activities may amount to legal warfare. The Sixth Circuit observed that the "hate-filled history between P & G and Amway would take a writing as long as both the Old and New Testaments and involve at least one of the Good Book's more prominent players."[135]

The Internet makes it easy to falsify return e-mail addresses, allowing web site posters to defame corporate actors anonymously.[136] The corporate plaintiffs are sometimes forced to subpoena ISPs in order to discover the identity of these John Doe defendants.[137] The use of John Doe subpoenas to unveil Internet corporate critics creates a conflict between tort law and the rights of free speech.

A California company and two of its executives filed a libel and invasion of privacy-based lawsuit against two ex-employees who posted a series of messages on an Internet bulletin board devoted to the company's publicly traded stock.[138] The offending "messages maligned the company's products and suggested that the two executives were incompetent and dishonest and that one of them, a woman, might have obtained her position by having sex with a supervisor."[139] A California jury found the ex-employees liable for invasion of privacy, libel, breach of contract, and conspiracy, and awarded $425,000 in general damages and

132 *Id*. at 181.

133 *Id*. at 187.

134 *Id*.

135 *Id*. at 182 (internal footnote omitted).

136 Trade libel is similar to an ordinary defamation case in that a defendant has published a false and derogatory statement about a company. Vondran v. McLinn, No. C 95-20296, 1995 U.S. Dist. LEXIS 21974, at *14 (N.D. Cal. July 5, 1995). The test for business defamation is "'whether, in the circumstances, the writing discredits the plaintiff in the minds of any considerable and respectable class of the community.'" Smith v. Suburban Rests., Inc., 373 N.E.2d 215, 217 (Mass. 1978) (quoting Muchnick v. Post Publ'g Co., 125 N.E.2d 137, 138 (Mass. 1955)).

137 *See* Am. Online, Inc. v. Anonymous Publicly Traded Co., 542 S.E.2d 377 (Va. 2001) (involving a corporation seeking to force America Online to reveal the identities of anonymous web posters).

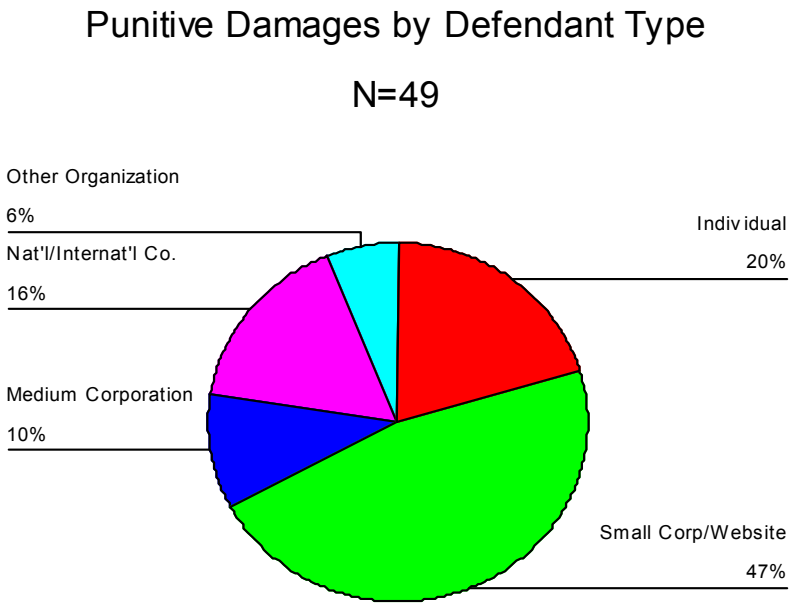
138 *Varian Wins $775,000 Jury Verdict in Internet Libel Case*, *at* http://www.orrick.com/news_events/releases.asp?action=article&articleID=56 (Dec. 18, 2001).

139 David Watson, *C.A.: Defamatory Internet Posting Libel, Not Slander*, METROPOLITAN NEWS-ENTERPRISE (Los Angeles), Nov. 14, 2003, at 1.

$350,000 in punitive damages.[140] The trial judge enjoined the defendants from posting additional defamatory information.[141] It is becoming clear that corporations are using punitive damages as a form of self-help to protect their intellectual property and intangible assets, and to punish trade libel.

6. Punitive Damages Are Assessed Against Corporate Mice Not Elephants

Table Six



a. Small Companies Comprise the Largest Category of Cybertort Defendants

Table Six suggests that small companies are more likely to be defendants in cyberspace tort cases than large or medium corporations.[142] A total of 47% (N=23) of the punitive damages

140 *Id.*

141 *Id.*

142 Punitive damages were rarely awarded in favor of small companies against large companies. Of the awards handed down against large corporate defendants, individuals won five of these cases. Two of three were won by a medium sized company and only one punitive damages award was in favor of a small company against a large company. In contrast, seven out of eight punitive damages awards won by large companies (defined as companies with a Fortune 500 presence or nationally known brand) were awarded against small corporate web sites or startup companies.

defendants were either small online companies or web sites. Medium-sized companies were defendants in only five cyberlaw cases in which punitive damages were awarded. Of the five cases, three awards were in favor of employees of that corporation. Of the remaining two awards assessed against medium-sized companies, one award was to another medium-sized company and the other to a national company. No small company prevailed against a medium-sized company in a decade of cyberlaw cases. The pattern suggests that small online companies are frequently targeted in punitive damages litigation. Still, the overall numbers of punitive damages awards are low. It is suprising that there would be less than fifty successful punitive damages claims in a decade of Internet boom. It is quite likely that there may be additional barriers to litigating in cyberspace. Even powerful corporate actors such as America Online or Microsoft may find it difficult to pursue elusive defendants in cyberspace. The cases that did not result in punitive damages or that were never even brought because of barriers to litigating in cyberspace are the really interesting aspects implied by Table Six.

The Internet allows anonymous communications that are virtually impossible to trace through Internet nodes. Cyber-tortfeasors frequently use false e-mail headers and anonymous remailers to make it difficult to retrace the steps of wrongdoing. Computer records are easy to alter and it is likely that spoliation of electronic evidence is widespread. Internet fraud is frequently launched from an offshore haven. For instance, the large numbers of Nigerian bank fraud schemes are hard to control because the perpetuators are located in West Africa.[143]

b. Punitive Justice Against Infringing Mice

The metaphor of Internet "elephants" and "mice" developed by Peter Swire is helpful in understanding the large number of cyberlaw wrongdoers who escape punitive justice.[144] Professor

143 Lagos and Lome-Togo, Nigeria are the places of origin for most Nigerian Letter Scams. *Nigerian Letter Scams*, Internet Fraud Complaint Center, *at* http://www.ifccfbi.gov/strategy/nls.asp (last visited Jan. 20, 2004). Congo-Zaire, Sadton, Cote d Ivoire, Accra Ghana, Eleme, Festac Town, Ivory Coast, and Sierra-Leone are other African cities where these scams have developed. *Id.* Interestingly, "Canada and the United Kingdom have [also] been identified as originating countries for this scam." *Id.* Given these diverse locations, it will be expensive to obtain redress for the loss of funds, even if the "dot conster" is identified.

144 Peter P. Swire, *Of Elephants, Mice, and Privacy: International Choice of Law and the Internet*, 32 INT'L LAW 991, 993, 1019-23 (1998) (arguing that large multi-national corporations are elephants easy to regulate on the Internet because they frequently have assets that can be attached, versus "mice," who are small, mobile actors that can easily elude enforcement because they have the capacity to disappear or hide in an off-shore haven).

Swire defines corporate "elephants" as "large organizations that have major operations in a country. Elephants are powerful and have a thick skin, but are impossible to hide. They are undoubtedly subject to a country's jurisdiction."[145] In other words, when a corporate elephant such as a national corporation commits wrongs in cyberspace, there will frequently be assets to attach and officers to receive process. For example, companies like AOL, Amazon.com, eBay, and Yahoo! are classified as "elephants" because they are subject to regulation everywhere. On the other hand, "mice" are the exact opposite.[146]

Even when a prevailing plaintiff wins a large punitive damages award, collecting it is a different matter. Collecting a punitive damages award is difficult because a number of wily Internet mice either fail to make an appearance, file bankruptcy, or simply disappear after the plaintiff obtains a judgment.[147] Default judgments outnumbered cases decided by juries in the larger cybertort dataset. The plaintiffs in cases against Internet mice have almost no chance of collecting their judgment.[148] In *John Does v. Franco Productions*,[149] forty-six young men were awarded $506 million against Franco Productions and Internet Distributors for compensatory and punitive damages in a case in which the defendants secretly filmed college athletes and sold the videotapes on the Internet.[150] The defendants secretly videotaped college athletes in locker rooms, restrooms, and showers.[151] The tapes carried names like "Straight Off the Mat" and "Voyeur Time," and depicted hundreds of young athletes who had unknowingly been photographed in various degrees of nudity.[152] However, since the primary defendant was likely offshore, and thus failed to make an appearance to defend the action, this multi-million dollar award is largely symbolic.

145 *Id*. at 993.

146 *Id*.

147 *See, e.g.*, Doe v. GTE Corp., 347 F.3d 655, 656 (7th Cir. 2003) (noting that online pornographer defaulted in a case filed by college athletes for secret filming and sale of videos online); Kremen v. Cohen, 337 F.3d 1024, 1027 (9th Cir. 2003) (reporting that primary defendant moved assets to an off-shore haven and defaulted); Caton v. Trudeau, 157 F.3d 1026, 1028 (5th Cir. 1998) (reporting that defendant filed bankruptcy after Internet libel judgment was rendered).

148 *See, e.g.*, *GTE Corp.*, 347 F.3d at 656-57 (observing that there was little chance in recovering $500 million award against defaulting primary defendant in decision dismissing claim against GTE for enabling sale of unauthorized tapes by defendant).

149 No. 99 C 7885, 2002 U.S. Dist. LEXIS 24032 (N.D. Ill. Nov. 25, 2002), *aff'd sub nom.*, Doe v. GTE Corp., 347 F.3d 655 (7th Cir. 2003).

150 *Id*. at *1; Does v. Franco Prods., No. 99 C 7885, 2000 U.S. Dist. LEXIS 9848, at *2 (N.D. Ill. July 12, 2000).

151 *Franco Prods.*, 2000 U.S. Dist. LEXIS at *2.

152 Jere Longman, *Videotaped Athletes Victorious in Court*, N.Y. TIMES, Dec. 5, 2002, at D8.

An Internet company "can reopen immediately after being kicked off of a server or can move offshore."[153] As Professor Swire notes, "Mice breed annoyingly quickly—new sites can open at any time."[154] When "harm over the Internet is caused by mice, hidden in crannies in the network, traditional legal enforcement is more difficult."[155] The large number of default judgments in cyberlaw reflects the reality that it is easy for web sites to disappear or assets to be transferred. The next subsection illustrates how large corporate actors ("elephants") are in a better position to litigate against elusive web site wrongdoers ("mice") than are consumers.

In the cyberlaw sample, corporate elephants were seldom defendants in punitive damages litigation. From the beginning of cyberlitigation, it has been the large corporate elephants that have prevailed in lawsuits against mice. In the field of intellectual property law, it is the owners of famous trademarks and trade names who frequently file lawsuits against small companies. Playboy Enterprises, for example, has the legal resources to file intellectual property lawsuits to protect its trademarks and copyrighted images in cyberspace.[156] Internet elephants frequently enjoy advantages as repeat players in cyberlitigation. In many cases, only the corporate elephants have the legal resources to vindicate their rights. Again, Playboy Enterprises is a good example of a major cyberlitigator who frequently files lawsuits to protect its corporate name and intellectual property rights. Frequently, the corporate elephant is litigating against smaller companies, some of which are located in foreign venues.[157]

---

153 Swire, *supra* note 144, at 993.

154 *Id*.

155 *Id*.

156 *See, e.g.*, Playboy Enters., Inc. v. Netscape Communications Corp., 55 F. Supp. 2d 1070 (C.D. Cal. 1999) (denying Playboy's motion for a preliminary injunction against Netscape for using Playboy's Internet-related trademarks in keywords of search engine), *aff'd*, 202 F.3d 278 (9th Cir. 1999); Playboy Enters., Inc. v. Universal Tel-A-Talk, Inc., 48 U.S.P.Q. 2d (BNA) 1779 (E.D. Pa. 1998) (holding that plaintiff failed to allege necessary facts for a trademark counterfeiting claim).

157 *See, e.g.*, Playboy Enters., Inc. v. Welles, 279 F.3d 796 (9th Cir. 2002) (rejecting Playboy's arguments that former playmate who used the phrase "Playmate of the Year" on her web site and in metatags violated trademark law); Playboy Enters., Inc. v. Sanfilippo, 46 U.S.P.Q. 2d (BNA) 1350 (S.D. Cal. 1998) (awarding damages to Playboy based upon the web site's unauthorized copying of Playboy's copyrighted images); Playboy Enters., Inc. v. AsiaFocus Int'l, Inc., No. 97-734-A, 1998 U.S. Dist. LEXIS 10359 (E.D. Va. Feb. 2, 1998) (reporting copyright infringement action versus small foreign company); Playboy Enters., Inc. v. Webbworld, Inc., 991 F. Supp. 543 (N.D. Tex. 1997) (awarding damages to Playboy based upon the web site's unauthorized copying of Playboy's copyrighted images), *aff'd*, 168 F.3d 486 (5th Cir. 1999); Playboy Enters., Inc. v. Russ Hardenburgh, Inc., 982 F. Supp. 503 (N.D. Ohio 1997) (finding bulletin board liable for direct and contributory infringement for posting Playboy's copyrighted and trademarked images for access by paying subscribers); Playboy Enters., Inc. v. Frena, 839 F. Supp.

The overall problem that there are too few punitive damages awards in cyberspace appears to be due to the huge costs involved in tracking down anonymous wrongdoers. It is likely that few consumers have the technical expertise to determine who is tracking their click-streams, unleashing viruses, or sending fraudulent offers. The small number of punitive damages cases may be partially explained by the fact that defendants may be mice who are difficult to trace. In traditional torts, it is generally not a problem to determine the identity of a wrongdoer. In contrast, cyber-tortfeasors are not physically present at the scene of the misdeed. Computers can be the target of a tortious act, such as when information is misappropriated from a database or a computer network. Furthermore, a network or web site may be the target of viruses or vandalism that constitutes a property tort.

Owners of famous trademarks such as Playboy, Mattel, Victoria's Secret, and America Online have been successful litigants in cyberspace because of their superior legal resources. These companies have used the courts to not only vindicate their traditional rights against Internet mice but also to expand intellectual property protections in this new medium.[158] In many cases, large national enterprises were filing lawsuits against companies that existed only in cyberspace. In *Playboy Enterprises, Inc. v. Webbworld, Inc.*,[159] for example, a web site was found liable for copyright infringement for offering a subscription service to adult images protected by copyright.[160]

Mice, on the other hand, have far more flexibility and can disappear at the click of a mouse or seek an offshore haven. The anonymity of individual Internet users makes it easy to commit civil wrongs without consequence. Enforcement by individuals is frustrated by the ease with which individual users may simply disappear from cyberspace. Individuals subject to various cyberspace laws or controls may simply "'exit' from the regime defined by those laws."[161]

1552, (M.D. Fla. 1993) (finding that a small company's web site infringed Playboy's trademarks and copyrights in posting images to its site).

158 The typical complaint by a trademark owner against the owner of a domain name is litigated under diverse causes of action, including (1) trademark infringement, (2) trademark dilution (federal and state), (3) domain name piracy, (4) false designation of origin, and (5) unfair competition. Trademark owners frequently seek injunctive relief to enjoin the use of the domain name or a transfer of the domain name. Courts may enjoin commercial content on a domain name's web sites but are reluctant to enjoin the use of the domain name for noncommercial purposes.

159 991 F. Supp. 543 (N.D. Tex. 1997), *aff'd*, 168 F.3d 486 (5th Cir. 1999).

160 *Id*. at 548.

161 Elizabeth Longworth, *The Possibilities for a Legal Framework for Cyberspace*, *in* THE INTERNATIONAL DIMENSIONS OF CYBERSPACE LAW 16 (UNESCO Publ'g 2000).

An Italian designer, Alfredo Versace, for example, was enjoined from marketing clothing and other items in the United States because the federal court ruled that he was using trademarks confusingly similar to trademarks registered by the famous designer, Gianni Versace.[162] Undeterred by the federal court order, Alfredo simply used offshore Internet sites to advertise and distribute his products in the United States.[163]

c. Anti-Spam Initiatives Against Online Mice

Punitive damages lawsuits against commercial e-mailers accounted for approximately 10% of all awards. In every punitive damages award, it was the ISP, rather than the consumer, who won punitive damages, even though the injuries were suffered primarily by consumers through spam e-mail. For example, an unsolicited bulk e-mail health solicitation was sent to millions of AOL subscribers stating: "The answer to cancer has been know [sic] for years. This website proves that eating inexpensive apple seeds and/or apricot seeds completely cure [sic] most cancers. The theory also states that by eating just a few seeds per day will [sic] 99.95% guarantee that you will never develop cancer."[164] The commercial e-mail messages made claims regarding their "cancer cures" and typically directed recipients to a web site where they could purchase products such as Laetrile, a videotape, and a book promoting the defendant's cancer treatment.[165]

In the vast majority of the cases, it is the ISP rather than the consumer who seeks punitive damages and other relief against the spammer. AOL, for example, "has undertaken various technical efforts to permit its members to opt out of receiving messages from domains and IP addresses that are or have been the subject of member complaints regarding unsolicited bulk e-mail."[166] However, the wily spammer continually develops new methods for bypassing ISP controls. The spammer transmits e-mail "from multiple and varying domains, employ[s] random and varying user names, relay[s] their messages through the servers of innocent third parties, or falsif[ies] the headers on their e-mails to indicate that their messages are from domains that AOL

162 Gianni Versace, S.p.A. v. Versace, No. 01 Civ. 9645, 2003 U.S. Dist. LEXIS 14858, at *47-48 (S.D.N.Y. Aug. 27, 2003).

163 *Id*. at *15-16.

164 Am. Online, Inc. v. Christian Bros., No. 98 CIV 8959, slip op. at 9 (S.D.N.Y. Dec. 9, 1999) (quoting example of defendant's bulk e-mailing practices), *available at* http://legal.web.aol.com/decisions/dljunk/christian.html.

165 *Id*. at 10.

166 *Id*. at 11.

does not filter (*e.g.*, 'msn.com' or 'aol.com')."[167] Despite the best efforts of the ISP community, computer systems are unable to detect and filter much of the tidal wave of unsolicited bulk e-mail targeting consumers.

This tidal wave of spam has greatly increased the costs associated with running an ISP. For example, a director of one ISP claimed "that [spam] [had] added 500 percent to 700 percent to the ISP's costs over nearly three years."[168] Punitive damages are increasingly being used by large ISPs in punishing and deterring the widespread social problem of spam e-mail. Amazon.com, for example, has recently filed lawsuits seeking punitive damages against eleven e-mail marketers who spoofed the company's e-mail addresses.[169] The e-mail forgeries were "promoting, among other things, home appliances and penis enlargement."[170]

In one case, a California software manufacturer was sued for deceptive business practices in a Washington class action.[171] The software vendor used deceptive Internet advertising banners that impersonated computer error messages with "headings that read 'security alert,' 'warning' and 'message alert,' with messages that include[d]: 'you[r] computer is currently broadcasting an Internet IP address. With this address, someone can immediately begin attacking your computer.'"[172] Internet users receiving this message were urged to click "OK" to the message.[173] Allegedly, "viewers who click an 'OK' button [were] forwarded to a commercial Web site promoting Bonzi software for preventing Internet intrusions or speeding up Internet connections."[174] The lawsuit, filed on behalf of consumers in eight states, was settled when the company agreed to label its "security alert" as an advertisement.[175]

In a typical day, the average consumer has an e-mail inbox full of offers to make fast money. ISPs such as America Online seek to enjoin these unsolicited advertisements to their millions

167 *Id.*

168 Drew Clark, *E-Commerce: Internet Firms Share Horror Stories About Costs of Spam*, NAT'L J. TECH. DAILY, May 1, 2003, *at* LEXIS, Nexis Library NAT'L J. TECH. DAILY File.

169 Matthew Heller, *Lost in the Cyber-Kudzu*, L.A. TIMES, Dec. 21, 2003 (Magazine), at 24.

170 *Id.*

171 *Software Manufacturer Accused of Using Deceptive Internet Ad Banners*, MEALEY'S LITIG. REP.: CLASS ACTIONS, Dec. 19, 2002, at 4.

172 *Id.*

173 *Id.*

174 *Id.*

175 *Error Copycat Pop-up Will Be Labeled as Ad*, CAP. TIMES (Madison, Wis.), May 29, 2003, at 6E.

of subscribers by arguing that these unwanted messages trespass upon their personal property. Consequently, ISPs such as America Online were the first to employ punitive damages as an anti-spam remedy.[176] A large service provider such as AOL suffers damages due to spammers' use of false return addresses. In responding to subscriber complaints regarding spam e-mail, AOL incurs costs in wasted bandwidth, traffic slowdowns, decline in user productivity, and time.[177]

America Online employs punitive damages to punish those who flood their subscribers with unwanted e-mail. In *America Online, Inc. v. National Health Care Discount, Inc.*,[178] the court found that the spammer's e-mail actions constituted a trespass to chattels as well as a violation of state and federal computer abuse laws.[179] The court calculated damages by charging the spammer $2.50 per thousand pieces of spam for a total of $337,500.[180]

In yet another case, *America Online, Inc. v. Prime Data Systems, Inc.*,[181] the court entered a default judgment granting a permanent injunction and awarding compensatory and punitive damages.[182] The court found that the mass e-mailer's conduct warranted the "imposition of punitive damages both to punish defendants' conduct and to deter others' tortious behavior that threatens the vitality of Internet e-mail communication."[183] The magistrate judge set the level of punitive damages at "three times AOL's proven per-message cost of $.00078."[184] Thus, punitive damages were assessed at a rate of $.00234 per message.[185] The court found that the punitive damages assessed were consistent with treble damages authorized by state and federal statutes for aggravated misconduct.[186] However, the *Prime Data* court was forced to reduce the punitive damages award due to a 1988 tort reform statute that required judges to reduce awards to the upper limit of $350,000.[187]

176 *See, e.g.*, Am. Online, Inc. v. IMS, 24 F. Supp. 2d 548, 549 (E.D. Va. 1998) (awarding punitive damages against a spam e-mailer).

177 Am. Online, Inc. v. IMS, No. 98-0011-A, 1998 U.S. Dist. LEXIS 20448, at *3 (E.D. Va. Nov. 20, 1998).

178 174 F. Supp. 2d 890 (N.D. Iowa 2001).

179 *Id*. at 900.

180 *Id*. at 901.

181 No. 97-1652-A, 1998 U.S. Dist. LEXIS 20226 (E.D. Va. Nov. 20, 1998).

182 *Id*. at *14-16.

183 *Id*. at *10.

184 *Id*. at *13.

185 *Id*.

186 *Prime Data Systems*, 1998 U.S. Dist. LEXIS 20226, at *13-14.

187 *Id*. at *11 (citing VA. CODE § 8.01-38.1).

Fraudulent uses of unsolicited commercial e-mail victimize millions of Internet users. Accordingly, ISPs have filed hundreds of lawsuits seeking punitive damages to punish spammers, but tort law is just beginning to accomplish this goal. Even a corporate elephant such as America Online must muster substantial resources to successfully litigate against elusive spam e-mailers who engage in such deceptive practices as falsified or redirected addresses.

Despite the havoc that spam creates for Internet consumers, no individual plaintiff has ever won a victory against a spammer outside of small claims court judgments. A Pennsylvania court expressly ruled that the federal Telephone Consumer Protection Act[188] could not be used by consumers to punish and deter the sending of solicited commercial e-mail.[189]

The CAN-SPAM Act of 2003[190] that went into effect on January 1, 2004 prohibits consumers and ISPs from filing lawsuits against spam e-mailers under the federal statute.[191] Section 7 of the CAN-SPAM Act provides for exclusive enforcement by the FTC and certain other agencies, rather than by ISPs or consumers.[192] State attorneys general are not permitted to file anti-spam lawsuits if there is a pending federal civil or administrative enforcement action by the FTC.[193] Furthermore, the new federal anti-spam statute preempts all state anti-spam legislation, even those that provide consumers with a cause of action against commercial e-mailers.[194] A number of states enacted anti-spam statutes that permitted consumers to sue e-mail senders who used misleading subject lines, transmission paths, or third-party domain names without permission.[195] In 2001 alone, anti-spam statutes were introduced in twenty-six states, and each of these statutes is preempted by CAN-SPAM.[196] The nationalization of anti-spam legislation further marginalizes the role of consumers in directly redressing abuses due to unsolicited e-mail. In the end, commercial e-

188 47 U.S.C. § 227 (2003).

189 Aronson v. Bright-Teeth Now, LLC, 824 A.2d 320, 320-21 (Pa. Super. Ct. 2003).

190 Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003 (CAN-SPAM Act of 2003), Pub. L. No. 108-187, 117 Stat. 2699 (codified as amended in scattered sections of 15 U.S.C., 18 U.S.C., 28 U.S.C., and 47 U.S.C.).

191 *See* CAN-SPAM Act § 7.

192 *Id*.

193 *Id*.

194 *Id*. § 8. Section 8 supersedes any state statute or regulation governing commercial e-mail, but it does not address the use of tort remedies against spam. *Id*.

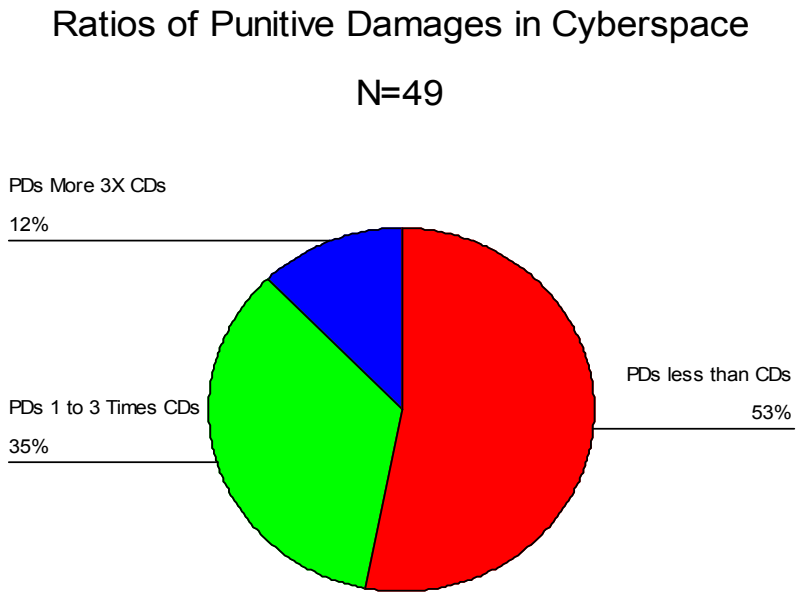
195 *See, e.g.*, State v. Heckel, 24 P.3d 404, 407, 413 (Wash. 2001) (upholding state of Washington anti-spam statute and rejecting defendant's argument that it unduly burdened interstate commerce).

196 RUSTAD & DAFTARY, *supra* note 76, at § 5.03[E].

mailers will no longer be subject to consumer lawsuits under state anti-spam statutes.

7. Punitive Damages Are Low-Ratio Awards Often Lower Than Compensatory Damages

Table Seven



In *State Farm Mutual Automobile Insurance Co. v. Campbell*,[197] the U.S. Supreme Court struck down a $145 million punitive damages award on the grounds of substantive due process.[198] The Court observed that "[c]ompensatory damages 'are intended to redress the concrete loss that the plaintiff has suffered by reason of the defendant's wrongful conduct'" whereas "punitive damages . . . are aimed at deterrence and retribution."[199] The Court's constitutional analysis of punitive damages requires the plaintiff to make a showing that the defendant's misconduct is sufficiently reprehensible in order to satisfy due process.[200] The Court's recent revisit of damage award

197 123 S. Ct. 1513 (2003).

198 *Id*. at 1519-21.

199 *Id*. at 1519 (quoting Cooper Indus., Inc. v. Leatherman Tool Group, Inc., 532 U.S. 424, 432 (2001)).

200 *Id*. at 1521. The Court has also noted that reprehensibility is higher where the "target of the conduct had financial vulnerability." *Id*.

ratios in *Campbell* should have little effect on cyberlaw punitive awards. The Court held that a jury's award of punitive damages of $145 million and compensatory damages of $1 million (145:1) was unconstitutionally excessive.[201] The Court came close to stating a per se rule that extreme ratios are presumptively unconstitutionally excessive.[202] Punitive damages in cyberspace are often much smaller in proportion to the compensatory damages. In 53% of the cyberlaw awards, the punitive component of the verdict was actually less than the compensatory damages. In only six instances (12%) were punitive damages three or more times greater than the compensatory award.

Table Seven confirms that there is no problem with skyrocketing punitive damages in cyberspace. The function of punitive damages in the first decade of Internet litigation was generally to assist companies in protecting their rights and consolidating control of the Internet. The traditional role of punitive damages in products liability, premises liability, medical malpractice, and other substantive fields is to provide consumer protection. In cyberspace, consumers were conspicuously missing from the punitive damages equation. Courts have been reluctant to impose legal duties on corporate defendants for inadequate Internet security and for preventing third parties from unleashing viruses, hacking, or stealing consumer information. Furthermore, courts have yet to extend products liability standards to computer software or web sites.

201 *Id*. at 1524.
202 *Id*.

8. Punitive Damages Were Rarely Appealed By Defendant

Table Eight

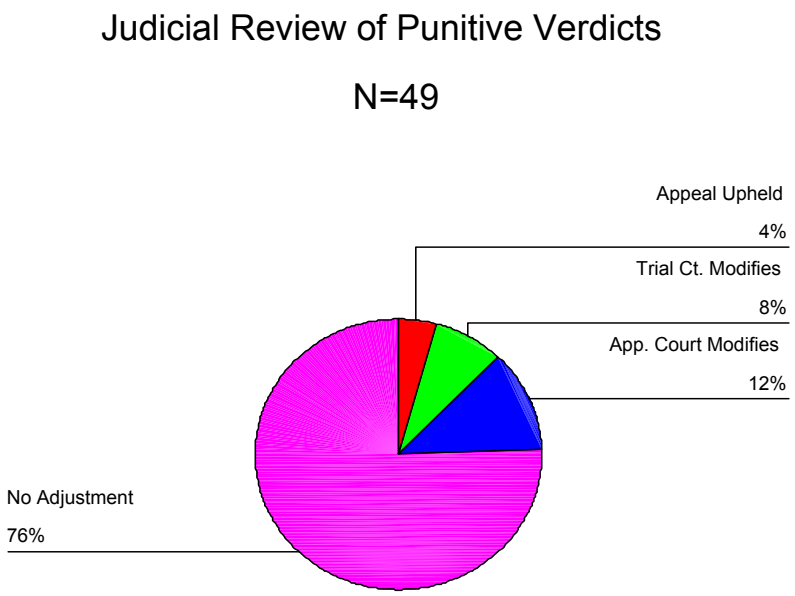


Table Eight reveals that relatively few judicial adjustments were made to punitive damages in cyberspace cases. No appeal or post-verdict adjustment occurred in thirty-seven of the forty-nine cyberlaw punitive damages awards. One reason for so few adjustments is that the ratio of punitive to compensatory damages is generally proportional or lower. The median punitive damages award was only 82% of the size of the compensatory damages, with a mean award only 1.7 times the size of the compensatory component.

Interestingly, defendants who actually challenged punitive damages were frequently successful in getting a reversal or remittal of the award. In the twelve cases where a judicial modification occurred, the trial judge reduced or reversed the punitive damages awards in four instances. Of the eight punitive damages awards reviewed by appellate courts, six verdicts were reduced or reversed. The small number of appeals can be explained by the large number of default judgments in the sample as well as the large number of low ratio awards discussed above. For example, in many of the high profile punitive damages cases, the primary defendant disappeared with a click

of the mouse, and for several of the largest punitive damages awards, the Internet mice disappeared or defaulted.[203]

In a few cases, punitive damages in favor of large corporate actors were capped or limited by tort reforms that were originally enacted to protect companies. The traditional critique of punitive damages is that large corporations suffer at the hands of "jackpot juries."[204] The tort reform movement to limit punitive damages arises from the perception that it is the corporations that are victimized by greedy individual claimants and their lawyers. In 2003 alone, the corporate community convinced legislators in seventeen states to file proposed statutes limiting punitive damages as well as the doctrine of joint and several liability.[205]

One of the unanticipated consequences of tort reform is that it may end up hurting its corporate advocates. The business community in Texas, for example, viewed then governor George W. Bush as "the right man to break the back of the litigious culture in the Lone Star State."[206] As Governor of Texas, Bush "signed seven major bills into law, including ones that capped punitive damages at no more than twice actual damages plus $750,000."[207] In his State of the Union address in January 2003, President Bush noted the importance of enacting federal tort reforms.[208] However, legal backfire, or the law of unanticipated consequences, posits "that a [new] law produces or will produce results directly contrary to one or more of those intended. Legal backfire claims are pervasive, yet potentially misleading and harmful argumentation used primarily to undermine existing law (or policy) or to forestall the enactment of new law."[209]

Any new technology will frequently produce legal backfire because social changes inevitably impact legal institutions in entirely unpredictable ways. The legal backfire from tort reform is that it impairs the corporate community's ability to vindicate its rights in cyberspace. Corporate tort reformers paint the "image of a monstrously destructive civil justice system" that is

203 *See, e.g.*, Kremen v. Cohen, 337 F.3d 1024 (9th Cir. 2003) (imposing liability for conversion against domain name registrar in case in which primary defendant defaulted in $65 million punitive damages award); Jere Longman, *Videotaped Athletes Victorious in Court*, N.Y. TIMES, Dec. 5, 2002, at D8.

204 A search in LEXIS's current news file produced 669 "hits" for the search "jackpot w/5 jury or juries."

205 Mark Ballard, *17-Front Tort War*, NAT'L L.J., May 12, 2003, at 1.

206 Christopher O'Leary, *Lone Star Litigation: Are Huge Jury Awards in Texas a Relic?*, CORP. LEGAL TIMES, May 2003, at 43, 46.

207 *Id*. at 48.

208 *See Doctors and Tort Reform*, WASH. POST, Feb. 16, 2003, at B6.

209 Robert A. Hillman, *The Rhetoric of Legal Backfire*, 43 B.C. L. REV. 819, 819 (2002).

sapping American productivity and competitiveness.[210] Many of the tort reform arguments could be applied with more validity to large corporate stakeholders using litigation to enclose the Internet commons. "Neo-conservatives often employ the theme of a 'culture of victimization gone wild' to ridicule [individual] plaintiffs seeking" redress for personal injury.[211] The general public is amused, angered, and perplexed by accounts of loony tort filings publicized by tort reformers. However, many of the widely disseminated tort stories are totally false or presented in a misleading and pejorative fashion.[212]

The corporate opponents of punitive damages portray the civil justice system "as greedy vulture lawyers against poor oppressed businesses."[213] Ironically, it appears that corporations are actually using punitive damages as a tool to protect their rights in cyberspace. In the tort reform debates, corporate America is not seeking limitations on punitive damages in this area. If punitive damages are evolving as a corporate sword rather than as a shield in cyberspace, the tort reformers may wish to revise their demands to eliminate or cripple the remedy.

Tort reform has played a role in capping punitive damages sought by companies. In the *Simon Property Group* case discussed earlier in this Article, the trial judge reduced a punitive damages award for a state unfair competition claim from $10 million to $50,000.[214] As the court explained, "Indiana law limits punitive damages to the greater of $50,000 or three times compensatory damages."[215] In a Virginia case, a federal court awarded the plaintiff $675,000 including $350,000 in punitive damages, that state's upper.[216] The Virginia cap of $350,000 has also limited punitive damages awards to America Online in their cases against spammers.[217]

---

210 Rustad & Koenig, *Taming the Tort Monster*, *supra* note 30, at 3.

211 *Id*.

212 THOMAS H. KOENIG & MICHAEL L. RUSTAD, IN DEFENSE OF TORT LAW 173 (2001). For example, "[t]ort reformers frequently cite the case of a woman who received $2,699,000 in punitive damages after injuring her back opening a pickle jar." *Id*. However, in the actual case, the court justified the punitive damages based on the defendant's conduct of nearly five years, including retaliation, which was found to be "'willful, mean-spirited acts indicative of an intent to cause physical or emotional harm.'" Marc Galanter, *An Oil Strike in Hell: Contemporary Legends About the Civil Justice System*, 40 ARIZ. L. REV. 717, 730 (1998) (quoting Vandevender v. Sheetz, Inc., 490 S.E.2d 678, 693 (W. Va. 1997).

213 Christina Johns, *Tort Reform*, *at* http://www.cjjohns.com/c_law/tort_reform.html (last visited Dec. 1, 2003).

214 Simon Prop. Group, L.P. v. mySimon, Inc., 282 F.3d 986, 990 (7th Cir. 2002).

215 *Id*.

216 Graham v. Oppenheimer, No. 00CV57, 2000 WL 33232110 (E.D. Va. Oct. 2000); Kathleen Fay, *Defamed MD Awarded Maximum Punitive Damages Award in Va.*, E-COM. L. & STRATEGY, Jan. 2001, at 12.

217 *See, e.g.*, Am. Online, Inc. v. Bluecard Publ'g, No. 98-905-A, slip op. at 9-10 (E.D.

Cyberspace punitive damages flip the historic role of punitive damages in which individuals normally filed suit against powerful companies. The typical plaintiff in Internet punitive litigation is a large corporation suing a defendant in the dark side of the Net. Internet defendants are typically cybersquatters, online pornographers, spammers, or anonymous critics located in an offshore haven.

Few legislators who supported tort reform could have anticipated that one consequence was to handcuff information-industry leaders such as America Online, eBay, and Amazon.com in punishing and deterring spammers and other Internet predators. Lord Devlin approved a large punitive damages award in an aggravated assault case observing that one should think of punitive damages as "a fine which has to hit the defendant hard if he has disregarded the rights of others and show that that sort of conduct does not pay."[218] Punitive damages "should reflect 'the enormity of [the defendant's] offense'" rather than some arbitrary ratio of punitive damages to compensatory damages.[219] The deterrent power of punitive damages is significantly eroded when Internet wrongdoers can compute the cost of wrongdoing in advance.

The next part of this Article explains why punitive damages have yet to develop in cyberspace and why they are necessary to fortify existing consumer protection in cyberspace.

II. EXTENDING PUNITIVE DAMAGES TO INTERNET CONSUMERS

Internet-related consumer fraud complaints skyrocketed from 49,957 to 75,063 from 2001 to 2002.[220] Forty-six percent of the Internet fraud complaints were for losses from online auction fraud with a median loss of $320.[221] The non-delivery of goods accounted for just under a third of complaints with a median loss of $176.[222] Consumer confidence in cyberspace is impaired by worries about the lack of information security, data protection, confidentiality, and the failure of web merchants to deliver goods and services in a timely manner.[223] The Internet is a borderless

Va. Jan. 5, 2000) (reducing punitive damages in cases involving numerous deceptive practices of the spammers to mask their identity), *available at* http://legal.web.aol.com/decisions/dljunk/bluecard.html.

218 Loudon v. Ryder, [1953] 2 Q.B. 202, 209 (1953).

219 BMW of N. Am., Inc. v. Gore, 517 U.S. 559, 575 (1996).

220 IFCC 2002 INTERNET FRAUD REPORT, *supra* note 16, at 4.

221 *Id*. at 6-7.

222 *Id*. at 6.

223 David Byrne, Cyberspace and Consumer Confidence, Address at the Annual Conference of the Kangaroo Group of MEPs (Sept. 18, 2000), *at* http://europa.eu.int/comm/

medium, which makes it imperative that consumers have "access to the legal system and courts in their *own country* [as] an essential part of consumer confidence[.]"[224]

The FTC is the most active Internet enforcer, but even this pro-active agency lacks the necessary resources to patrol cyberspace. It is as if the FTC is trying to hold back a tidal wave of cyberfraud with a broom.[225] The FTC is seeking to increase efforts in Internet-related enforcement, such as the regulation of e-mail list marketing, online auction practices, and e-mail sending software.[226]

Hardly a day goes by without new media reports of consumers harmed in cyberspace, yet punitive damages in Internet cases are rare.[227] Punitive damages awards, sometimes called exemplary, vindictive, penal, or retributory damages, are designed to punish and deter. Section 908(2) of the Restatement (Second) of Torts provides that "[p]unitive damages may be awarded for conduct that is outrageous, because of the defendant's evil motive or his reckless indifference to the rights of others."[228] Consumers are harmed every day in Internet chat rooms, news groups, and computer bulletin boards by conduct that calls for the deterrent hammer of punitive damages. Online chats may seem informal and relaxed, but an online posting in a chat room or on a web site may become the basis of a defamation lawsuit.[229] Few consumers have the resources to vindicate their rights in the online world.

---

dgs/health_consumer/library/speeches/speech55_en.html.

224 *Id*.

225 Internet enforcement is only one small sector of the FTC's responsibilities to protect consumers from unfair and deceptive trade practices:

> The [FTC] enforces 46 federal laws, including many laws that apply to web sites. Under the Federal Trade Commission Act, 15 U.S.C. §§ 41-58, the Commission seeks to: (a) prevent unfair methods of competition, and unfair or deceptive acts or practices in or affecting commerce; (b) obtain money and other relief for injured consumers; (c) define and prevent unfair or deceptive practices; and (d) investigate the business, practices, and management of entities engaged in commerce.

Federal Trade Commission Actions Affecting Web Sites & E-Commerce, *at* http://www.keytlaw.com/FTC/ftcactions.htm (last modified Sept. 2, 2003).

226 *FTC Examining Spam Lists and E-Mail Sending Programs*, WASH. INTERNET DAILY, March 28, 2002, at 1 (LEXIS, CURNWS Library).

227 *See, e.g.*, *Over the Counter – American Websites Selling Fake UK Degrees*, OVERSEAS OVERWHELMED (Higher-Edge), Mar. 12, 2003, *at* http://www.higher-edge.com/oov-archive.htm (shutting down web sites selling fake degrees from universities which used an address in Palmers Green, North London, to make their operations appear respectable, defrauding hundreds of thousands of mostly U.S. customers).

228 RESTATEMENT (SECOND) OF TORTS § 908(2) (1979).

229 *See, e.g.*, Carlson, *supra* note 35, at A33; Am. Online, Inc. v. Anonymous Publicly Traded Company, 542 S.E.2d 377, 379 (Va. 2001); Graham v. Oppenhiemer, No. 00-CV-57, 2000 WL 33381418, at *1 (E.D. Va. Dec. 15, 2000).

A. Why Punitive Damages Have Not Developed For Consumers

1. CDA Immunity Breeds Irresponsibility

The most significant reason why there are so few consumers using the remedy of punitive damages in cyberspace is the blanket immunity granted to ISPs by Congress. One of the unintended consequences of 42 U.S.C. § 230, the Communications Decency Act of 1996 ("CDA"),[230] is that it immunizes unfair, deceptive, and predatory practices in cyberspace. One of the statutory purposes of § 230 was to protect the "infant industry" of online service providers, such as America Online, CompuServe, and Prodigy, from tort liability arising out of postings by customers.[231] Section 230 of the CDA immunizes ISPs for torts committed by subscribers and third parties.[232] The long-term consequence of § 230 is to grant blanket immunity to ISPs for many torts in cyberspace. The courts have extended ISP immunity to nearly every conceivable information-related tort, including invasion of privacy,[233] and negligence.[234] The result has been that ISPs have prevailed in nearly every tort-related case in the last decade.[235] This broad immunity lessens the incentive for ISPs to develop technologies that will detect or control third party wrongdoing on their systems.[236]

---

230 47 U.S.C. § 230 (2001).

231 Zeran v. Am. Online, Inc., 129 F.3d 327, 330-31 (4th Cir. 1997) (stating that one of Congress's purposes was to insulate providers from potentially staggering tort liability).

232 *Id*. at 331.

233 Does v. Franco Prods., No. 99 C 7885, 2000 U.S. Dist. LEXIS 8645, at *13-14 (N.D. Ill. June 21, 2000) (holding that ISPs that host web sites are not liable for postings by customers), *aff'd sub nom.*, Doe v. GTE Corp., 347 F.3d 655 (7th Cir. 2003).

234 In *Lunney v. Prodigy Services Co.*, 723 N.E.2d. 539 (N.Y. 1999), the court held that Prodigy was not negligent in failing to prevent an imposter from opening up an account, posting vulgar messages, and sending threatening e-mails. 723 N.E.2d at 543. The court recognized that if a duty was imposed on an ISP to prevent people from opening up false accounts and committing these types of defamatory acts, it would require an inordinate amount of time and money to study the transactions of millions of subscribers. *Id*. The court reasoned that if Prodigy was held liable for the actions of third parties, it would "open an ISP to liability for the wrongful acts of countless potential tortfeasors committed against countless potential victims." *Id*.

235 *See, e.g.*, Smith v. Intercosmos Media Group, No. 02-1964, 2002 U.S. Dist. LEXIS 24251, at *14-15 (E.D. La., Dec. 17, 2002) (holding that Intercosmos was entitled to immunity under the Communications Decency Act of 1996 for both damages and injunctive relief for defamation, libel, or negligence based on allegedly defamatory web sites set up by its customers); Doe One v. Oliver, 755 A.2d 1000, 1003-04 (Conn. Super. Ct. 2000) (holding America Online immune from improper e-mail messages sent to plaintiff mother's employer), *aff'd*, 792 A.2d 911 (Conn. App. Ct. 2002), *cert. denied*, 796 A.2d 556 (Conn. 2002); Schneider v. Amazon.com, Inc., 31 P.3d 37, 43 (Wash. Ct. App. 2001) (dismissing defamation lawsuit against Amazon.com for third party's posting of negative comments about the author's book on site).

236 Section 230 immunity for tort liability for ISPs is reminiscent of how the courts constructed harsh doctrines such as contributory negligence, the assumption of risk, and the fellow servant rule to protect nascent industry during the industrialization of America. *See generally* MORTON J. HORWITZ, THE TRANSFORMATION OF AMERICAN LAW,

Courts have extended the impact of § 230 by insulating defendants from an even greater range of tort-based lawsuits filed by consumers.[237] In *Doe v. GTE Corp.*,[238] a court dismissed an action against an ISP that "provided web hosting services to [pornographic web] sites such as 'youngstuds.com' at which the hidden-camera videos were offered for sale."[239] The ISP did not produce or sell the tapes but "provided the usual package of services that enables someone to publish a web site over the Internet."[240] The package of services that GTE provided the X-rated company consisted of:

> (1) static IP (Internet protocol) addresses through which the web sites may be reached (a web host sometimes registers a domain name that corresponds to the IP address); (2) a high-speed physical connection through which communications pass between the Internet's transmission lines and the web sites; and (3) storage space on a server (a computer and hard disk that are always on) so that the content of the web sites can be accessed reliably.[241]

The advertisements for the X-rated tapes passed over GTE's network and were stored on its servers.[242] However, the federal district court held that GTE was entitled to immunity under § 230(c)(1).[243] The court reasoned that this section was not only a definition but also served as immunity in blocking "civil liability when web hosts and other [ISPs] *refrain* from filtering or censoring the information on their sites."[244] The Seventh Circuit affirmed the finding that GTE was neither a publisher nor a speaker and therefore it was immunized under § 230.[245]

In *Barrett v. Rosenthal*,[246] a California appeals court became the first U.S. court to hold that § 230 does not immunize an ISP who republishes defamatory statements authored by a third party after acquiring knowledge that the statements were

1780-1860, ch. 3 (1977) (arguing that the courts subsidized economic growth through the legal system by replacing just compensation for limited liability in tort and other substantive fields of law).

237 Blumenthal v. Drudge, 992 F. Supp. 44, 50 (D.D.C. 1998) (dismissing claim on § 230 grounds in case involving defamatory postings). *See also* Lunney v. Prodigy Servs. Co., 723 N.E.2d 539 (N.Y. 1999) (finding that commercial online service provider was not liable for defamation claim since it did not "publish" allegedly defamatory e-mail message).

238 347 F.3d 655 (7th Cir. 2003).

239 *Id*. at 657.

240 *Id*.

241 *Id*.

242 *Id*.

243 Doe v. GTE Corp., 347 F.3d at 657.

244 *Id*. at 659.

245 *Id*. at 662.

246 9 Cal. Rptr. 3d 142 (Cal. Ct. App. 2004).

false.[247] The plaintiffs, Dr. Polevoy and Dr. Barrett, were two medical doctors "primarily engaged in combating the promotion and use of 'alternative' or 'nonstandard' healthcare practices and products."[248] The plaintiffs maintained Internet "[w]eb sites that expos[ed] 'health frauds and quackery' and provid[ed]" consumers with information about health care alternatives.[249]

One defendant, Rosenthal, was an alternative health practitioner who reprinted and distributed a number of false accusations about the plaintiffs. The defendant's web postings accused the two doctors of running a "Slea[z]y 'Quackbuster' Scam."[250] Dr. Polevoy was accused of stalking women and being a quack.[251] The defendants refused to retract the statements and the plaintiffs filed suit for libel, conspiracy, and libel per se.[252] The trial court struck down their complaint on the grounds that it violated California's anti-SLAPP statute.[253] The trial court also ruled that § 230 protected the defendant from liability and that the defamation claims were not supported by sufficient proof that the plaintiffs suffered monetary losses.[254] The appellate court affirmed the application of the anti-SLAPP statute as to Dr. Barrett, but not as to Dr. Polevoy.[255] The appellate court also ruled that the trial court erred in requiring Dr. Polevoy to prove damages since the defamatory language posted on the web site was libel per se.[256]

The court ruled that the federal immunity of § 230 was inapplicable since Rosenthal was a "user of an interactive computer service" and a primary publisher who was strictly liable for libelous statements.[257] The court ruled that § 230 does not "abrogate the common law principle that one who republishes defamatory matter originated by a third person is subject to [distributor] liability if he or she knows or has reason to know of its defamatory character."[258] The court refused to follow a Fourth Circuit opinion that § 230 "immunized providers and users of interactive computer services from liability not only as *primary*

247 *Id*. at 167.
248 *Id*. at 144.
249 *Id*.
250 *Id*. at 146 (alteration in original).
251 *Barrett*, 9 Cal. Rptr. 3d at 149.
252 *Id*. at 145.
253 *Id*. at 143-44. The court noted that the California statute barred strategic lawsuits against public participation. *Id.*
254 *Id*. at 146.
255 *Id*.
256 *Barrett*, 9 Cal. Rptr. 3d at 146-47.
257 *Id*. at 151.
258 *Id*. at 152 (quoting RESTATEMENT (SECOND) TORTS, § 581(1)) (emphasis omitted).

publishers but also as *distributors*."[259] The court reasoned that providers or users who knowingly distribute defamatory materials produced by third parties should be subject to liability.[260] The court noted that § 230, on its face, did not clearly address whether Congress intended to overthrow the well-established common law principle of distributor liability.[261] However, after a review of the legislative history, the court observed that the survival of distributor liability was consistent with § 230.[262]

It may be that the *Barrett* case is ushering in a new era when courts will begin to retrench and reform § 230 to the balance between immunity and tort responsibility. The court in *Barrett* compared the "lack of clarity as to the boundary of the immunity [in the CDA to] the specificity of the immunity granted under the Digital Millennium Copyright Act" ("DMCA").[263] It may be proper to grant immunity for publishing content supplied by third parties; however, it is improper to extend that liability to transmitting knowingly libelous statements. Congress should make it clear that distributorship liability may be imposed for transmitting defamatory statements after acquiring notice. Congress could, for example, enact safe harbor provisions that parallel the intermediary liability standards of the Digital Millenium Copyright Act. One promising reform would be to implement a "take-down" policy like the one Congress enacted in the DMCA.[264] The DMCA's safe harbor provisions,[265] unlike § 230 of the CDA, balance freedom of expression against copyright infringement.[266]

The DMCA limits the potential liability of ISPs only if they satisfy the safe harbor provisions.[267] With few exceptions, a

259 *Id*. at 153-54 (declining to follow Zeran v. Am. Online, Inc., 129 F.3d 327 (4th Cir. 1997)).

260 *Id*. at 152.

261 *Barrett*, 9 Cal. Rptr. 3d at 155-58.

262 *Id*. at 167.

263 *Id*. at 158 n.11 (citing 17 U.S.C. § 512).

264 The DMCA limits online providers' liability for users' copyright infringement so long as the provider takes down the offending material promptly upon notice. 17 U.S.C. § 512(c) (1996 & Supp. 2003). The DMCA was signed into law by President Clinton in 1998. U.S. COPYRIGHT OFFICE, THE DIGITAL MILLENNIUM COPYRIGHT ACT OF 1998: U.S. COPYRIGHT OFFICE SUMMARY 1 (1998), available at http://www.copyright.gov/legislation/dmca.pdf. The DMCA amends the federal Copyright Act in Title 17 of the United States Code to develop greater protection for materials transmitted in the Internet environment. *Id*. at 3. One of the more controversial provisions of the DMCA is the prohibition against circumventing technological measures controlling access to works provided by the Copyright Act. 17 U.S.C. § 1201 (1996 & Supp. 2003).

265 17 U.S.C. § 512(a), (c).

266 *Barrett*, 9 Cal. Rptr. 3d at 158 n.11.

267 The DMCA does not confer an absolute immunity upon ISPs like 42 U.S.C. § 230 because the immunities of ISPs are limited to specific functions they perform. *See* 17

party satisfying the requirements for one of the safe harbors cannot be liable for monetary, injunctive, or other equitable relief.[268] A reconstructed § 230 of the CDA would only grant ISP tort immunity if it fulfilled the requirements for a safe harbor. An ISP could, for example, be immune from tort liability unless it knew or should have known that the tortious activity was occurring on its system and aided in the accomplishment of the direct tortfeasor's purpose by allowing the postings to continue.

2. Internet Usage of Trade That Waives Consumer Protection

a. Adhesive Internet Consumer Contracts

Another significant reason why punitive damages have not yet evolved to protect consumers in cyberspace is because of contracts of adhesion.[269] Consumers are largely foreclosed from the possibility of seeking punitive damages by adhesive license agreements and web site terms of service agreements.[270] The U.S. Internet and software industry universally require consumers to waive any meaningful warranties and tort remedies and to agree to litigate disputes in distant and inconvenient forums.

i. Internet Choice of Forum Clauses

"Choice of forum" is a contractual provision that predetermines the judicial or arbitral forum in the event of a dispute arising out of an Internet or web site agreement. For example, Disney requires all disputes to be decided in a state or federal court located in Los Angeles County,[271] and Nokia requires disputes to be submitted to an arbitrator in Finland.[272] In addition, America Online's forum selection clause for its members provides that "'exclusive jurisdiction for any claim or

U.S.C. § 512(a), (c).

268 17 U.S.C. § 512 (providing a rather narrow exception under § 512(j)).

269 *See generally* Friedrich Kessler, *Contracts of Adhesion—Some Thoughts About Freedom of Contract*, 43 COLUM. L. REV. 629, 632 (1943) (noting that the concept of adhesion contracts refers to contracts in which the weaker party must adhere to the stronger party's terms).

270 *See, e.g.*, Hill v. Gateway 2000, Inc., 105 F.3d 1147, 1150-51 (7th Cir. 1997) (enforcing an arbitration clause in a shrink-wrap license); ProCD, Inc. v. Zeidenberg, 86 F.3d 1447, 1449 (7th Cir. 1996) (enforcing shrink-wrap license term). *See generally* Michael Rustad & Lori E. Eisenschmidt, *The Commercial Law of Internet Security*, 10 HIGH TECH. L.J. 213, 289-93 (1995).

271 *Jurisdictional Clauses in Current Shrinkwrap and Clickwrap Contracts*, Consumer Project on Technology, *at* http://www.cptech.org/ecom/ucita/licenses/jurisdiction.html (last visited Jan. 31, 2004) (citing clause in Disney's terms of service or license agreement) [hereinafter *Jurisdictional Clauses*].

272 *Id*.

dispute with AOL or relating in any way to your membership with or your use of AOL resides in the courts of Virginia."[273]

ii. Internet Choice-of-Law Clauses

Internet merchants use choice-of-law clauses to predetermine the legal remedies that apply for disputes involving the online contract. Dell Financial Services, for example, requires that the law of Texas govern all claims relating to its web site.[274] The Alturian GPS Software web site applies the law of Belgium in the event of disputes.[275] The licensing agreement of RealNetworks, Inc. requires consumers to resolve all disputes before binding arbitration applying Washington state law.[276]

If, for example, a consumer violated the RealNetworks license agreement by exceeding the scope of its use restrictions, the company could seek an injunction in federal court, a right not granted to consumers.[277] United States courts have been inclined to enforce Internet or software license agreements with terms inimical to consumer welfare such as pro-vendor forum selection clauses, anti-warranties, and limitations of remedies.[278] In general, courts have been willing to enforce Internet contracts so long as the user has an opportunity to review the terms of the contract and manifest assent to the license agreement.[279] During the 1990s, companies were able to avoid many contractual

273 Freedman v. Am. Online, Inc., No. 3:03cvl048, 2003 U.S. Dist. LEXIS 22019, at *2 (D. Conn. Dec. 5, 2003) (quoting America Online Member Agreement), *vacated*, No. 3:03cv1048, 2004 U.S. Dist. LEXIS 1388 (D. Conn. Jan. 30, 2004).

274 *Jurisdictional Clauses*, *supra* note 271.

275 *Id*.

276 *REALNETWORKS, INC. END USER LICENSE AGREEMENT*, RealNetworks, Inc., *at* http://web.nps.navy.mil/nssliao/realplayer/playrlic.html (last visited Jan. 31, 2004).

277 *Id*. RealNetworks ("RN") requires consumers to waive access to U.S. courts while reserving its own rights. For any violation of RN intellectual property rights, "RN may seek injunctive relief, or any other appropriate relief, in any court of competent jurisdiction." *Id*.

278 *See, e.g.*, Hughes v. McMenamon, 204 F. Supp. 2d 178, 181 (D. Mass. 2002) (finding that subscriber agreed to the license agreement and the forum selection clause was enforceable); Caspi v. Microsoft Network, L.L.C., 732 A.2d 528, 530, 532-33 (N.J. Super. Ct. App. Div. 1999) (upholding forum selection clause where subscribers to online software were required to review license terms in scrollable window and to click "I Agree" or "I Don't Agree"); Groff v. Am. Online, Inc., No. PC 97-0331, 1998 WL 307001, at *6 (R.I. Super. Ct. May 27, 1998) (holding user was bound by forum selection clause in online license agreement); Barnett v. Network Solutions, Inc., 38 S.W.3d 200, 204-05 (Tex. App. 2001) (upholding forum selection clause in online contract for registering Internet domain names that required users to scroll through terms before accepting or rejecting them).

279 *See, e.g.*, *Caspi*, 732 A.2d at 532 (enforcing mass market agreement even though the user could assent without scrolling to the bottom of the license agreement by clicking the "I agree" icon on the screen). *See generally* Christina L. Kunz et al., *Click-Through Agreements: Strategies for Avoiding Disputes on Validity of Assent*, 57 BUS. LAW. 401, 402-03 (2001) (citing cases that consider the user's ease or difficulty of viewing terms as a major factor in enforcing licensing agreements).

disputes with consumers by convincing courts to enforce one-sided choice-of-law provisions and other adhesive Internet contracts.

The U.S. market-based approach assumes that it is enough consumer protection for Internet merchants and software vendors to simply make adequate disclosures that the consumers are waiving their legal rights and remedies. The theory underlying "adequate disclosure" is that consumers will choose vendors with more favorable license terms.[280] However, this is not possible in the Internet industry where consumers are required to waive their rights and remedies. The practical reality is that consumers have no legal recourse against Internet merchants.

It is improbable that a U.S. consumer will opt to file a claim that must be filed across the country or in an overseas venue. "[R]equiring consumers to travel to a foreign and oftentimes remote forum to seek redress in an unfamiliar legal system . . . would in many cases effectively deny consumers access to judicial redress."[281]

The Internet challenges choice-of-law principles because it "is not a physical or tangible entity, but rather a giant network which interconnects innumerable smaller groups of linked computer networks."[282] Punitive damages arising out of consumer transactions in cyberspace will be stillborn if U.S. courts continue to enforce choice-of-law and forum-selection clauses. Punitive damages cannot develop if choice-of-law and forum clauses are considered to be "prima facie valid and should be enforced unless enforcement is shown by the resisting party to be 'unreasonable' under the circumstances."[283]

b. Waiver of Internet Consumer's Right to Seek Tort Remedies

A Dilbert cartoon lampoons these adhesion contracts by depicting a licensee who unwraps the shrink-wrap only to learn that he has become Bill Gate's towel boy.[284] In the cartoon, Dilbert states, "I didn't read all of the shrink-wrap license agreement on my new software until after I opened it.

280 Jean Braucher, *Delayed Disclosure in Consumer E-Commerce as an Unfair and Deceptive Practice*, 46 WAYNE L. REV. 1806, 1810 (2000).

281 Karen Stewart & Joseph Matthews, *Online Arbitration of Cross-Border, Business to Consumer Disputes*, 56 U. MIAMI L. REV. 1111, 1126 (2002).

282 CompuServe Inc. v. Cyber Promotions, Inc., 962 F. Supp. 1015, 1018 (S.D. Ohio 1997).

283 The Bremen v. Zapata Off-Shore Co., 407 U.S. 1, 10 (1972).

284 Scott Adams, *Dilbert*, L.A. TIMES, Jan. 14, 1997, at D2.

Apparently, I agreed to spend the rest of my life as a towel boy in Bill Gates'[s] new mansion."[285] Shrink-wrap and web-wrap contracts are standard form contracts for the electronic age. The standard form contract dominates cyberspace just as it dominates every other domain of everyday life.[286]

In the typical mass-market license agreement, consumers routinely waive their right to seek punitive damages and foreclose the possibility of all but the most limited remedy under the UCC. Online users are offered "take it-or-leave it" web-wrap or terms of service consumers agreements that foreclose the possibility of punitive damages and any other tort remedy.[287] Nearly every Internet merchant dictates the choice-of-law as a condition for accessing its services or using its goods. No consumer negotiates with Bill Gates or Jeff Bezos in the Internet economy. Requiring consumers to waive their rights to a jury trial is a controversial practice because the Internet industry is unwilling to give even the most rudimentary implied warranties of quality. One can read thousands of click-stream, click-wrap, shrink-wrap, and terms of service agreements and never find a single Internet vendor willing to provide meaningful warranties or remedies for its software, software products, or services.

The typical Internet-related mass-market license agreement provides no warranties of any kind and forecloses any remedy by requiring the consumer to litigate in a forum of the vendor's choice, which is often in a distant forum. The following anti-warranties clause of an online pharmacy is fairly typical of what consumers encounter in cyberspace:

> Disclaimer of Warranties. YOU EXPRESSLY UNDERSTAND THAT AND AGREE THAT:
>
> a. YOUR USE OF THE SERVICE IS AT [YOUR] SOLE RISK. THE SERVICE IS PROVIDED ON AN "AS IS"

---

285 *Id*.

286 Shrink-wrap contracts are the newest form of standard form contracts that predominate our everyday life. Professor Slawson wrote in 1971 that:

> Standard form contracts probably account for more than ninety-nine percent of all the contracts now made. Most persons have difficulty remembering the last time they contracted other than by standard form; except for casual oral agreements, they probably never have. But if they are active, they contract by standard form several times a day. Parking lot and theater tickets, package receipts, department store charge slips, and gas station credit card purchase slips are all standard form contracts.
>
> . . . The contracting still imagined by courts and law teachers as typical, in which both parties participate in choosing the language of their entire agreement, is no longer of much more than historical importance.

W. David Slawson, *Standard Form Contracts and Democratic Control of Lawmaking Power*, 84 HARV. L. REV. 529, 529 (1971).

287 *See* Braucher, supra note 260, at 1832.

AND "AS AVAILABLE" BASIS. PHARMACY CHOICE EXPRESSLY DISCLAIMS ALL WARRANTIES OF ANY KIND, WHETHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT.

b. PHARMACY CHOICE MAKES NO WARRANTY THAT (i) THE SERVICE WILL MEET YOUR REQUIREMENTS, (ii) THE SERVICE WILL BE UNINTERRUPTED, TIMELY, SECURE, EFFICIENT, OR ERROR FREE, (iii) THE RESULTS THAT MAY BE OBTAINED FROM THE USE OF THE SERVICE WILL BE ACCURATE OR RELIABLE, (iv) THE QUALITY OF ANY PRODUCT, SERVICE, INFORMATION, OR OTHER MATERIAL PURCHASED OR OBTAINED BY YOU THROUGH THE SERVICE WILL MEET YOUR EXPECTATIONS, AND (v) ANY ERRORS IN THE SOFTWARE WILL BE CORRECTED.

c. ANY MATERIAL DOWNLOADED OR OTHERWISE OBTAINED THROUGH THE USE OF THE SERVICE IS DONE AT YOUR OWN RISK AND DISCRETION. YOU WILL BE SOLELY RESPONSIBLE FOR ANY DAMAGE TO YOUR COMPUTER SYSTEM OR LOSS OF DATA THAT RESULTS FROM THE DOWNLOAD OF ANY SUCH MATERIAL.

d. NO ADVICE OR INFORMATION, WHETHER ORAL OR WRITTEN, OBTAINED BY YOU FROM PHARMACY CHOICE OR THROUGH OR FROM THE SERVICE SHALL CREATE ANY WARRANTY NOT EXPRESSLY STATED . . . .

e. NEITHER PHARMACY CHOICE NOR YOU MAY MODIFY OR WAIVE THE DISCLAIMERS PROVIDED FOR IN THIS SECTION . . . . NO ORAL MODIFICATIONS OR WAIVER OF THIS DISCLAIMER SHALL BE VALID OR BINDING ON PHARMACY CHOICE.[288]

Amazon.com's terms of service agreement forecloses consumers from seeking punitive damages or any other type of tort damages.[289] The most popular search engine, Google.com, has a term of service that precludes the possibility of obtaining

288 *Pharmacy Choice Terms and Conditions of Service*, *at* http://www.pharmacychoice.com/home/terms.cfm (last visited Jan. 26, 2004).

289 *Conditions of Use*, *at* http://www.amazon.com/exec/obidos/tg/browse/-/508088/102-6759433-7263313 (last visited Jan. 26, 2004) ("AMAZON.COM WILL NOT BE LIABLE FOR ANY DAMAGES OF ANY KIND ARISING FROM THE USE OF THIS SITE, INCLUDING, BUT NOT LIMITED TO DIRECT, INDIRECT, INCIDENTAL, PUNITIVE, AND CONSEQUENTIAL DAMAGES.").

punitive damages:

> Under no circumstances shall Google be liable to any user on account of that user's use or misuse of Google Web APIs. Such limitation of liability shall apply to prevent recovery of direct, indirect, incidental, consequential, special, exemplary, and punitive damages whether such claim is based on warranty, contract, tort (including negligence), or otherwise, [(]even if Google has been advised of the possibility of such damages).[290]

The eBay User Agreement requires its users to "read, agree with and accept all of the terms and conditions contained in this User Agreement and the Privacy Policy, which include those terms and conditions expressly set out below and those incorporated by reference," before they can access the eBay system.[291] One of the terms of service for eBay is the absolute prohibition on seeking punitive damages under any doctrinal theory.[292]

c. Mandatory Consumer Protection in Cyberspace

The solution to adhesive Internet contracts is to either extend punitive damages to cyberspace or adopt a system of "thick" regulations such as the European Union regime of mandatory consumer protection terms.[293] None of the countries of the European Union other than the United Kingdom recognize the doctrine of punitive damages.[294] The Brussels Regulation, for

---

290 *Terms and Conditions for Google Web API Service*, *at* http://www.google.com/apis/api_terms.html (last visited Jan. 26, 2004).

291 *User Agreement*, *at* http://pages.ebay.com/help/community/png-user.html (last visited Jan. 26, 2004).

292 The user agreement states:

> UNDER NO CIRCUMSTANCES SHALL EBAY BE LIABLE TO ANY USER ON ACCOUNT OF THAT USER'S USE OR MISUSE OF EBAY TOOLBAR. SUCH LIMITATION OF LIABILITY SHALL APPLY TO PREVENT RECOVERY OF DIRECT, INDIRECT, INCIDENTAL, CONSEQUENTIAL, SPECIAL, EXEMPLARY, AND PUNITIVE DAMAGES WHETHER SUCH CLAIM IS BASED ON WARRANTY, CONTRACT, TORT (INCLUDING NEGLIGENCE), OR OTHERWISE, (EVEN IF EBAY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES).

User License Agreement, http://pages.ebay.com/ebay_toolbar/download.html (last visited Jan. 26, 2004).

293 The European Union ("EU") was formed in the 1950s and now includes fifteen member states located in the Eurozone. James E. Pfander, *Member State Liability and Constitutional Change in the United States and Europe*, 51 AM. J. COMP. L. 237, 239 (2003). The EU is set to add another ten member states in 2004. *Id.* "The *European Council* refers to meetings of the heads of state of the 15 [EU] member states." RUSTAD & DAFTARY, *supra* note 76, at § 8.02[A]. The European Union's key consumer protection directives address distance selling, data protection, and e-commerce. *Id.*

294 *See* Christopher Hodges, *Multi-Party Actions: A European Approach*, 11 DUKE J. COMP. & INT'L L. 321, 330 (2001) ("No European jurisdiction generally permits punitive damages . . . ."). *But see* Rookes v. Barnard, 1964 A.C. 1129, 1131 (H.L. 1964) (appeal taken from Eng.) (noting that in the United Kingdom, a restricted form of exemplary damages is recognized in a handful of aggravating circumstances).

example, gives consumers the right to sue suppliers in their home court.[295] It provides that if a business "pursues commercial or professional activities in the Member State," then the consumer may sue in the court where he or she is domiciled.[296] The far-reaching consumer provisions also apply to U.S. companies targeting European consumers in Internet transactions.[297] Therefore, European Union rules will likely become the *de facto* consumer protection law for the Internet since non-European Union countries will be subject to its rules.

The European Union model tacitly assumes that mandatory consumer protection is required in cyberspace and elsewhere. The Distance Selling Directive, for example, requires sellers to provide consumers with information about the identity of the supplier, the main characteristics of goods and services including taxes, delivery costs, arrangements for payment, the existence of a right of withdrawal, the period for which the offer remains valid, and the minimum duration of the contract.[298]

The European Directive on Consumer Goods contains provisions that apply equally well to Internet sales.[299] The Directive, for example, gives consumers a two-year period to exercise rights as to defective products.[300] The Directive presumes that any non-conformity found in the first six months after delivery existed at tender, and European consumers under the Consumer Goods Directive have a right of repair or replacement without charge or inconvenience.[301] Under the Directive, any waiver of rights in a contractual agreement signed by European consumers is not binding.[302]

---

295 The European Union countries are promulgating some of the most extensive regulations of cyberspace. Council Regulation 44/2001 of 22 December 2000 on Jurisdiction and the Recognition and Enforcement of Judgments in Civil and Commercial Matters, 2001 O.J. (L 12) 1. The Brussels Regulation replaces the 1968 Brussels Convention effective March 2002. *Id*. at 14, 16. The Brussels Regulation applies to all EU countries that signed the Brussels Convention of 1968 except Denmark. Id. at 3. The new Brussels Regulation has not yet supplanted the Lugano Convention of 1988. *Id*. at 1, 14-15. The Brussels Regulation governs jurisdiction in civil and commercial disputes between litigants and provides for the enforcement of judgments. *Id*. at 3, 11.

296 *Id*. at 6. Article 15(1)(c) extends the consumer home forum rule to entities that direct activities to Member States. *Id*.

297 *See id*. at 7. The Brussels Regulation has legal force in the Member States of the European Union. However, U.S. companies with a presence in a Member State and conducting business with European consumers would be subject to the pro-consumer home court rule. Thomas C. Vinje and Ann-Charlotte Hogberg, *Whose Law Governs in EU?: Draft "Rome II" Regulation Threatens Certainty of 2000 Directive*, N.Y. LAW JOURNAL, April 30, 2001, at S3.

298 European Parliament & Council Directive 97/7/EC, 1997 O.J. (L 144) 19-27.

299 European Parliament & Council Directive 1999/44/EC, 1999 O.J. (L 171) 12.

300 *Id*. at 15.

301 *Id*.

302 *Id*. at 16.

Internet contracts with European consumers must also comply with the Unfair Terms Directive.[303] The Directive has an express policy of policing unfair terms where there is an imbalance of power between the company and consumer.[304] It applies to a wide range of one-sided Internet contracts where the terms are offered on a "take-it-or-leave-it" basis. Any ambiguity in a consumer contract is construed against the company in favor of the consumer.[305] The central provision of the Unfair Terms Directive is that contractual terms found to be unfair are unenforceable.[306] In contrast, the U.S. market-based approach tends to be opposed to such pro-welfaristic consumer protection regimes. The extension of punitive damages to protect consumers is consistent with the U.S. pro-market approach with its emphasis on flexibility and pragmatism.

B. Extending Punitive Damages for Consumer and Individual Protection in Cyberspace

Few consumer lawyers have the resources to pursue an Internet wrongdoer capable of fleeing the jurisdiction with the click of the mouse. Even if the Internet wrongdoer can be located, there remains a problem with default judgments. Consumers will be more likely to obtain collectible judgments from Internet elephants rather than elusive mice, but may not be aware that attorneys are available to work on a contingency basis. Alternatively, the amount of money involved may be so miniscule for any one Internet user that the victim may not feel that he or she has the time, energy, or expertise to prosecute a fraudulent Internet merchant. Many Internet users may each have a small loss resulting from a pattern and practice of dishonesty.

1. Remedy for Socially Compensable Damages

The legal environment of the Internet is a perfect venue for an expanded remedy of punitive damages. Judge Guido Calabresi drew the classic distinction between specific deterrence that makes the wrongdoer pay the price of wrongdoing and the larger social sanction of general deterrence, which vindicates the harm to society.[307] The concept of general deterrence may be seen in the earliest exemplary damages cases where awards were

303 Council Directive 93/13/EEC, 1993 O.J. (L 95) 29.

304 *Id*.

305 *Id*.

306 *Id*.

307 A. Mitchell Polinsky & Steven Shavell, *Punitive Damages: An Economic Analysis*, 111 HARV. L. REV. 869, 877 & n.13 (1998).

made "for example's sake."[308] Punitive damages against spam e-mailers are good examples of what Judge Calabresi defines as "socially compensatory damages."[309] The purpose of socially compensatory damages is "to make society whole," as opposed to compensatory damages, which are "assessed to make the individual victim whole."[310] Tort law's capacity to efficiently punish and deter conduct through socially compensable damages is central to Judge Calabresi's theory of punitive damages.[311] Judge Calabresi argues that in many cases "compensatory damages are . . . an inaccurate measure of the true harm caused by an activity."[312]

Consumers need a fortified punitive damages remedy precisely for purposes of optimal deterrence. Ordinary damages are an insufficient deterrent where the gain to the defendant exceeds any compensable injury. General deterrence requires punitive damages to convince other Internet wrongdoers that there is no profit in wrongdoing. Merely requiring an Internet company to disgorge the amount by which it was unjustly enriched is an insufficient deterrent. Without the threat of uncapped punitive damages, it would be beneficial for the fraudulent Internet business to wait until it was discovered or sued before disgorging what was owed. As the court stated in *Wangen v. Ford Motor Co.*,[313] if it were not for punitive damages then "[s]ome may think it cheaper to pay damages or a forfeiture than to change a business practice."[314] The purpose of punitive damages in cyberspace is the same as in the bricks-and-mortar world of compensating the larger society for uncompensated external costs.[315] Punitive damages are "an appropriate way of making the injurer bear all the costs associated with its activities."[316] In the first decade of cyberspace punitive damages, there have been some notable examples where the remedy served to root out socially harmful web site activity.

2. Serving as a Death Penalty to Internet Harassment

"Cyberstalking refers to the use of the Internet, e-mail, or other electronic means to repeatedly threaten, follow, or harass

308 Tullidge v. Wade, 95 Eng. Rep. 909, 909 (K.B. 1769).

309 Ciraolo v. City of New York, 216 F.3d 236, 245 (2d Cir. 2000) (Calabresi, J., concurring).

310 *Id*. (Calabresi, J. concurring).

311 *Id*. at 243, 245 (Calabresi, J. concurring).

312 *Id*. at 244 (Calabresi, J. concurring).

313 294 N.W.2d 437 (Wis. 1980).

314 *Id*. at 451 (citing Walker v. Sheldon, 179 N.E.2d 497, 499 (N.Y. 1961)).

315 *In re* Simon II Litig., 211 F.R.D. 86, 159 (E.D.N.Y. 2002).

316 *Ciraolo*, 216 F.3d at 244 (Calabresi, J. concurring).

another person."[317] Internet wrongdoers, for example, have harmed women by maliciously posting personal information on sadomasochistic web sites and by using new morphing technologies to superimpose their victim's face onto pornographic pictures.[318] For example, an online stalker who posted profane, derogatory, and harassing messages threatening violence to female musicians was assessed with punitive damages.[319]

In *Hitchcock v. Woodside Literary Agency*,[320] Jayne Hitchcock, a University of Maryland teaching assistant, alleged she was the victim of a campaign of electronic terror by an online company.[321] Ms. Hitchcock's nightmare began when she answered a web site advertisement soliciting writing samples from "'published and unpublished authors.'"[322] After submitting a writing sample, she received a letter from Woodside Literary Agency ("WLA") praising her writing and soliciting her to forward a full manuscript to the agency, "along with a $75 'reading and market evaluation fee.'"[323] She mailed a second sample of her writing to WLA using her maiden name.[324] WLA responded with a virtually identical letter save for soliciting a $150 reading fee.[325] Ms. Hitchcock concluded that WLA was nothing more than a scam soliciting bogus fees from consumers seeking to become writers.[326] She posted warnings about WLA on various Internet bulleting boards observing that "legitimate literary agencies did not charge 'reading fees.'"[327]

Hitchcock allegedly became the target for a systematic campaign of online harassment by anonymous parties.[328] The harassment took diverse forms, including the posting of messages that falsely claimed that Hitchcock was the author of pornography.[329] She also received a number of crude e-mail messages, which placed her in fear of sexual assault.[330] Her e-mail accounts were flooded, and offensive messages were sent to

317 RUSTAD & DAFTARY, *supra* note 76, at § 5.03[A] (emphasis omitted).

318 *See, e.g.*, Butler v. Krebs, No. 96-1204096, 1998 WL 2023763 (Tex. Dist. Ct. June 8, 1998) (awarding punitive damages against airline and pilot for superimposing nude image of female pilot on web site and intranet).

319 Stockdale v. Baba, 795 N.E.2d 727, 730-33 (Ohio Ct. App. 2003).

320 15 F. Supp. 2d 246 (E.D.N.Y. 1998).

321 *Id*. at 249.

322 *Id*. at 248.

323 *Id*. at 249.

324 *Id*.

325 *Hitchcock*, 15 F. Supp. 2d at 249.

326 *Id*.

327 *Id*.

328 *Id*.

329 *Id*.

330 *Hitchcock*, 15 F. Supp. 2d at 249.

third parties under her name.[331] Despite this clear pattern of systematic online harassment, the federal court dismissed Hitchcock's RICO[332] claim for failure to state a claim since the defendants could not, by law, constitute a criminal enterprise.[333] In the end, the consumer had no remedy available for such pervasive e-mail harassment and the "e-mail bombs" that shut her e-mail account down. The *Hitchcock* case illustrates the need for strong consumer self-help remedies to punish egregious misconduct in cyberspace.

Punitive damages are beginning to be employed to restrain web sites threatening violence. In *Planned Parenthood of Columbia/Williamette, Inc. v. American Coalition of Life Activists*,[334] anti-abortion activists posted "GUILTY" posters identifying the names, addresses, and photographs of physicians that provided abortions.[335] The web site developed by the American Coalition of Life Activists ("ACLA") personally identified the plaintiffs on "Deadly Dozen 'GUILTY'" posters.[336] Additionally, ACLA compiled the "Nuremberg Files" to collect evidence against abortion doctors so that they could one day be placed on trial for crimes against humanity.[337] "The 'GUILTY' posters identifying specific physicians were circulated in the wake of a series of 'WANTED' and 'unWANTED' posters that had identified other doctors who performed abortions before they were murdered."[338]

The plaintiffs argued that the distribution of the Old West-style Deadly Dozen "WANTED" posters identifying the abortion providers constituted a threat of force under the federal Freedom of Access to Clinics Entrances Act.[339] In three prior incidents, a "wanted"-type poster identifying a specific doctor who provided abortion services was circulated, and the doctor named on the poster was killed.[340] The jury returned a verdict in the

331 *Id*.

332 The Racketeer Influenced and Corrupt Organizations Act ("RICO"), 18 U.S.C. §§ 1961-1968 (2003), requires that the plaintiff demonstrate "that a defendant, employed by or associated with an enterprise affecting interstate or foreign commerce, conducted or participated in the conduct of this enterprise's affairs through a pattern of racketeering activity." *Hitchcock*, 15 F. Supp. 2d at 249 (internal quotation marks omitted).

333 *Id*. at 249-50.

334 290 F.3d 1058 (9th Cir. 2002), *cert. denied*, 123 S. Ct. 2637 (2003).

335 *Id*. at 1062.

336 *Id*. at 1064.

337 *Id*. at 1062.

338 *Id*.

339 *Planned Parenthood*, 290 F.3d at 1062. "[The Freedom of Access to Clinics Act] gives aggrieved persons a right of action against whoever by 'threat of force . . . intentionally . . . intimidates . . . any person because that person is or has been . . . providing reproductive health services.'" *Id*. (quoting 18 U.S.C § 248 (a)(1), (c)(1)(A)).

340 *Id*. at 1063-64.

physicians' favor, including $108.5 million in punitive damages.[341] The district court also "enjoined ACLA from publishing the posters or providing other materials with the specific intent to threaten [the physicians]."[342] The court found that the defendants had "acted with specific intent and malice in a blatant and illegal communication of true threats to kill, assault or do bodily harm to each of the plaintiffs and with the specific intent to interfere with or intimidate the plaintiffs from engaging in legal medical practices and procedures."[343]

On appeal, the Ninth Circuit held that the web site constituted a true threat as defined under the Freedom of Access to Clinics Entrances Act and affirmed the ACLA's liability, but vacated the $108.5 million punitive damages award for the district court to determine whether it comported with due process.[344] Due to the Ninth Circuit's decision, the threat of further punitive damages awards has resulted in a number of providers unplugging the "Nuremberg Files" site and other anti-choice sites, including the "AbortionCams" web site, "which features thousands of photographs and videos of abortion clinic staff, patients and escorts."[345]

Spam e-mailers are continually engaging in cost-benefit analyses to determine whether a given activity is worth the price.[346] In the calculation of expected profits, the Internet wrongdoer will likely allow for possible refunds to those victims who object too vigorously, and will be perfectly content to bear the additional cost of litigation as the price for continuing an illicit business. "It stands to reason that the chances of deterring [people] are materially increased by subjecting [them] to the payment of punitive damages."[347]

3. Punishing Incendiary Flame Wars in Cyberspace

Punitive damages have begun to evolve as a social control against incendiary e-mail exchanges or web site postings. Consider the case of a 27-year-old British lawyer who received a

341 *Id*. at 1066 n.4.

342 *Id*. at 1063.

343 Planned Parenthood of Columbia/Williamette, Inc. v. Am. Coalition of Life Activists, 41 F. Supp. 2d 1130, 1154 (D. Or. 1999), *aff'd in part, rev'd in part*, 290 F.3d 1058 (9th Cir. 2002).

344 *Planned Parenthood*, 290 F.3d at 1063, 1086.

345 Frederick Clarkson, *New Version of Nuremberg Files Yanked Off Web*, *at* http://www.womensenews.org/article.cfm/dyn/aid/1627/context/archive (last visited Jan. 28, 2004). "The American Coalition of Life Activists subsequently folded, though most of its leaders remain active anti-choice militants." *Id*.

346 *See generally* GUIDO CALABRESI, THE COSTS OF ACCIDENTS: A LEGAL AND ECONOMIC ANALYSIS 68-69 (1970).

347 Walker v. Sheldon, 179 N.E.2d 497, 499 (N.Y. 1961).

spicy e-mail message at work from his girlfriend.[348] The tactless lawyer forwarded the e-mail to several others, "boasting, 'Now THAT'S a nice compliment from a lass, isn't it?'"[349] A week later, the firm's web site "crashed after receiving 70,000 hits in a single day."[350] The lawyer's careless e-mail caused him to be disciplined by his law firm and castigated in the court of public opinion. This case is an example of the types of e-mails that can cause a suit for punitive damages.

In *Mathis v. Cannon*,[351] the plaintiff filed a defamation claim against an Internet poster who accused him of being a thief and a crook in an online forum addressing concerns about a solid waste recovery facility.[352] The Internet-related postings were the result of impassioned debates over the expenditure of the county's resources for the ill-fated facility.[353] However, the plaintiff was barred from seeking punitive damages because he did not seek a retraction, which was a prerequisite to filing his defamation complaint.[354]

C. Protecting Individual Reputations in Cyberspace

Punitive damages are evolving to restrain abusive information-based torts in cyberspace. For example, a University of North Dakota physics professor filed a lawsuit against a former student who posted an article about him on the Internet.[355] The student accused the professor "of being a pedophile and having odd sexual habits."[356] The professor won his case and received a punitive damages award for the student's postings.[357]

Damages awarded in online defamation cases frequently involve head-on collisions with the First Amendment. The facts of *Griffis v. Luban*[358] exemplify the typical online defamation case, arising out of an incendiary exchange of e-mails and postings to a web site. In *Griffis*, a Minnesota resident was assessed damages in an Alabama court default judgment after being sued for posting Internet messages challenging the

348 Jeffrey Rosen, *In Lieu of Manners*, N.Y. TIMES, Feb. 4, 2001 (Magazine), at 46.
349 *Id*.
350 *Id*.
351 573 S.E.2d 376 (Ga. 2002).
352 *Id*. at 377, 379.
353 *Id*. at 378-79.
354 *Id*. at 386.
355 Carlson, *supra* note 35, at A33.
356 *Id*.
357 Wagner v. Miskin, 660 N.W.2d 593, 595-96 (N.D. 2003), *cert. denied*, 124 S. Ct. 1156 (2004).
358 646 N.W.2d 527 (Minn. 2002), *cert. denied*, 538 U.S. 906 (2003).

credentials of an Egyptologist.[359] The Minnesota resident posted on a web forum that the Alabama scholar had "obtain[ed] her degree from a 'box of Cracker Jacks.'"[360] The Alabama court entered a default judgment for $25,000 in money damages and an injunction to prevent future defamatory postings.[361] In an unpublished decision, a Minnesota Court of Appeal overturned the Alabama injunction as an invalid prior restraint in violation of the First Amendment.[362] The Minnesota Supreme Court ruled that the Alabama judgment was not entitled to full faith and credit because the Alabama court lacked personal jurisdiction.[363] The court ruled that the Alabama court's exercise of jurisdiction was in error because the postings by the plaintiff were not aimed at the Alabama forum.[364]

D. Expanded Consumer Protection Through Punitive Justice

Deterrence will only occur when the tortfeasors are held accountable for their conduct in cyberspace. Given the difficulty Internet consumers have in detecting, let alone pursuing, Internet fraudsters, the cost of wrongdoing must be steep enough to convince even the Internet mice not to repeat the conduct. Internet elephants must also be punished in excess of their profit in order to deter similar future behavior. Accordingly, effective deterrence cannot be achieved without at least the threat of uncapped punitive damages.

Punitive damages are necessary in cyberspace to punish and deter wrongful acts such as improper billing, excessive charges, and consumer chiseling. Suppose an ISP decides to skim $10 off each consumer's account over a two-year period. The provider can count on the likelihood that only a small fraction of consumers will detect the excessive charges. It is also likely that not every consumer who detects the skimming will successfully sue for her $10 charge. Limiting an Internet consumer to purely contractual remedies will result in under-deterrence. It is the unpredictability of tort law and the remedy of punitive damages that make the Internet seller or entrepreneur think twice before engaging in wrongful conduct that is profitable but a serious social problem to society. Predatory Internet sellers may perform a cost-benefit analysis deciding that it is profitable to cheat consumers where the probability of detection is low. Punitive

359 *Id*. at 530.

360 *Id*.

361 *Id*.

362 Griffis v. Luban, No. CX-01-1350, 2002 WL 338139, at *6 (Minn. Ct. App. Mar. 5, 2002).

363 *Griffis*, 646 N.W.2d at 537.

364 *Id*. at 536-37.

damages are a deterrent to a company because producers cannot balance the benefit of chiseling Internet users against the costs of detection with any certainty.

The cheating of countless consumers in cyberspace is comparable to the societal wrong described in *Walker v. Sheldon*,[365] where the New York Court of Appeals observed:

> [T]hose who deliberately and cooly [sic] engage in a far-flung fraudulent scheme, systematically conducted for profit, are very much more likely to pause and consider the consequences if they have to pay more than the actual loss suffered by an individual plaintiff. An occasional award of compensatory damages against such parties would have little deterrent effect. A judgment simply for compensatory damages would require the offender to do no more than return the money, which he had taken from the plaintiff. In the calculation of his expected profits, the wrongdoer is likely to allow for a certain amount of money, which will have to be returned to those victims who object too vigorously, and he will be perfectly content to bear the additional cost of litigation as the price for continuing his illicit business. It stands to reason that the chances of deterring him are materially increased by subjecting him to the payment of punitive damages.[366]

If the probability of detection is low, there is a greater potential that a spam e-mailer will send millions of unwanted e-mails. For the Internet merchant tempted to cheat consumers, he or she must not be able to coldly calculate the worst-case scenario of paying only what was owed in the first place. Wrongdoers must know that their financial existence may be threatened if they violate Internet business norms. In *Emery-Waterhouse Co. v. Rhode Island Hospital Trust National Bank*,[367] the First Circuit Court of Appeals portrayed the retention of money not belonging to a bank as conduct analogous to theft.[368] Accordingly, the First Circuit upheld a punitive damages award against the assignee.[369] There are analogous circumstances in this case when it comes to protecting consumers in cyberspace. The punishment of Internet defendants who intentionally or recklessly breach their obligation to treat consumers fairly sends a signal to the information industry. It is entirely appropriate that the states punish conduct that violates a recognized public interest and there is no lesser interest in cyberspace.

365 179 N.E.2d 497 (N.Y. 1961).
366 *Id*. at 499.
367 757 F.2d 399 (1st Cir. 1985).
368 *Id*. at 408.
369 *Id*. at 401.

The awarding of punitive damages serves the additional purpose of limiting the defendant's ability to profit from its fraud by escaping detection and (private) prosecution. If a tortfeasor is "caught" only half the time he commits torts, then, when he or she is caught, the tortfeasor should be punished twice as heavily in order to make up for the times that he or she actually escaped punishment. As a result, the tortfeasor will be forced to consider the cost of being caught, not merely the odds of escaping, even if the tortfeasor is only held accountable for a small portion of his conduct.

Punitive damages also serve as a mechanism for ensuring that the "wrongdoer bears all the costs of its actions, and is thus appropriately deterred from causing harm, in those categories of cases in which compensatory damages alone result in systematic underassessment of costs, and hence in systematic underdeterrence."[370] The social cost of underdeterrence is that actors "will have an incentive to undertake activities whose social costs exceed their social benefits."[371] Online thieves are using a new technique called "phishing" to steal the identity and credit card numbers of consumers. As briefly mentioned earlier in this Article, phishing is the transmittal of e-mails, which appear to come from major corporations, to consumers.[372] The predator directs consumers to fraudulent web sites that mirror the companies' real sites and obtain bank account or credit card information from the consumers by asking them to verify or update their accounts.[373]

The punishment of intentional or reckless breaches of the obligation to treat Internet consumers fairly is a necessary signal to new industries. The strong arm of punitive damages is called into play to punish firms who play fast and loose with Internet users' money, data, identity, and right to privacy. Punitive damages are the only remedy that is tailored to punish and deter e-businesses from engaging in actions contrary to the public interest. The underlying public purpose is to teach fraudulent Internet companies that "tort does not pay."[374] Punitive damages encourage plaintiffs to act as "private attorneys general" and serve as an incentive to encourage a plaintiff to sue when there is widespread harm.[375]

---

370 Ciraolo v. City of New York, 216 F.3d 236, 243 (2d Cir. 2000) (Calabresi, J. concurring).

371 *Id*. (Calabresi, J. concurring).

372 James Covert, *Amazon Sues to Stop E-Mails That Use Its Name*, WALL ST. J., Aug. 27, 2003, at D4. *See supra* notes 11-13 and accompanying text.

373 *Id*.

374 Rookes v. Barnard, 1964 A.C. 1129, 1227 (H.L. 1964) (appeal taken from Eng.).

375 *See, e.g.*, Leslie E. John, Comment, *Formulating Standards for Awards of Punitive*

Deterrence cannot be achieved unless the costs of wrongful conduct are sufficient to induce fraudulent Internet wrongdoers and others tempted by ill-gotten gains not to repeat the conduct again. The awarding of punitive damages against Internet defendants will send a clear message to an e-business corporate headquarters or offshore haven that it is risky to defraud consumers. The ultimate goal of punitive damages is to punish by taking away the "ill gotten" gain, setting an example, and deterring future conduct of a like nature.

Punitive damages are an efficient remedy to punish and deter intentional and reckless torts in situations where "the probability of detection is very low and the probability of harm is very high."[376] Lowering the probability of enforcement implies that enforcement costs can be minimized. The lower that the probability of detection is, the fewer the resources devoted to enforcement need to be, and the fine can be set high enough so that the fine multiplied by the probability of its being imposed (the "expected fine") reaches the optimal level for deterrence.[377] A large punitive damages award is necessary to achieve optimal deterrence where the probability that any one Internet user will uncover wrongdoing is minimal.[378]

The Fifth Circuit in *Jackson v. Johns-Manville Sales Corp.*[379] stated that "punitive damages reward individuals who serve as 'private attorneys general' in bringing wrongdoers to account."[380] Private attorneys general provide a backup in situations in which government enforcement agencies fail to adequately protect the public. Fraud in the e-business executive suites will typically be more difficult and expensive to detect and prosecute than crime in the streets.

Damages in the Borderland of Contract and Tort, 74 CAL. L. REV. 2033, 2051-52 (1986) (arguing that punitive damages are an incentive to sue where the plaintiff might not otherwise do so or when the defendant is unlikely to be prosecuted criminally). *See also* Susan Abramson, Note, *Crawling Out from Under* Boulder, 34 CASE W. RES. L. REV. 303, 337-38 (1984) (arguing that private damage remedy fulfills "private attorney general" functions). The policy behind attorney fee shifting is also justified on a "private attorney general" rationale. *See* Thomas D. Rowe, *The Legal Theory of Attorney Fee Shifting: A Critical Overview*, 1982 DUKE L.J. 651, 653 (1982) ("[T]he 'private attorney general' theory justifies a fee award on the basis of the public usefulness of advancing a particular type of claim.").

376 Thomas Koenig, *The Law Arises Out of Fact, Even for a "Poet Laureate,"* 28 SUFFOLK U. L. REV. 1021, 1033 n.47. *See generally* WILLIAM M. LANDES & RICHARD A. POSNER, THE ECONOMIC STRUCTURE OF TORT LAW 160-61 (1987).

377 *See generally* Gary S. Becker, *Crime and Punishment: An Economic Approach*, 76 J. POL. ECON. 169, 190-93 (1968).

378 *See* A. Mitchell Polinsky & Steven Shavell, *The Optimal Tradeoff Between the Probability and Magnitude of Fines*, 69 AM. ECON. REV. 880, 880-81 (1979).

379 781 F.2d 394 (5th Cir. 1986), *abrogation recognized by* Centennial Ins. Co. v. Ryder Truck Rental, Inc., 149 F.3d 378 (5th Cir. 1998).

380 *Id*. at 403.

IV. CONCLUSION

The remedy of punitive damages is particularly well-suited to assist consumers in unmasking deliberate, concealed economic harms, like those suffered by the victims of computer viruses, fraudulent Internet sales and services, and the routine invasions of privacy that compromise the identity of users.[381] Without exemplary damages, the predatory Internet wrongdoers run little probability of detection if they injure a large number of consumers in relatively minor ways such as through pop-up ads, spam e-mail, or hidden charges. A popular misconception contends that punitive damage awards have spun out of control, threatening big, vulnerable companies. This is simply not so. Punitive damages are appropriate where a cyberspace defendant has acted in reckless indifference of the rights of large groups of consumers with the calculated purpose of making illicit profits.[382]

Limiting a consumer cheated in a cyberspace transaction to purely contractual remedies will certainly result in diminished deterrence. Despite the theoretical promise of punitive damages for protecting consumers, the remedy is stillborn. Punitive damages are particularly needed to punish and deter conduct on the borderline between the law of torts and criminal law in cyberspace. Punitive damages are needed now more than ever by consumers to detect and punish fraudsters, predators, and other online criminals on the World Wide Web. In cyberspace, punitive damages have a potentially useful role of deterring reprehensible conduct that, although arguably rational from the standpoint of the particular Internet predator, has widespread social costs for consumers and for society. Internet wrongdoers must know they cannot estimate the cost of their misdeeds by coldly calculating the cost of paying compensatory damages. Internet con artists must know that their financial existence may be threatened by shortchanging Internet users, violating their privacy, or trading upon their identity.

381 *See* William M. Landes & Richard A. Posner, *New Light on Punitive Damages*, REGULATION, Sept.-Oct. 1986, at 33.

382 For example, punitive damages have been deemed appropriate against insurance companies that chisel small amounts from their policyholders. *See, e.g.*, Hawkins v. Allstate Ins. Co., 733 P.2d 1073, 1085 (Ariz. 1987).

APPENDIX

Research Methods for Study of Punitive Damages in Cyberspace

The term "Internet" appeared in 1,559 state and federal opinions issued in 2002 but only a small percentage of these cases appear in the sample because the role of the Internet was only incidental in most of this litigation.[383] This study examined all Internet-related cases in which there was an equitable or legal remedy during the years 1992-2002.

Since no international, federal, or state agency systematically collects data on Internet-related cases, all available published and unpublished data sources were searched. The following sources were exhaustively examined: (1) trial verdict reporters;[384] (2) LEXIS and WESTLAW's federal and state databases and news services;[385] (3) cyberspace research libraries of law firms;[386] (4) national, regional, and local verdict reporters;[387] (5) reports of domain name disputes;[388] (6)

383 For example, in Kootenai Tribe of Idaho v. Veneman, 313 F.3d 1094 (9th Cir. 2002), the court reviewed the United States Forest Service's "Roadless Area Conservation Rule." *Id*. at 1104. The court's reference to the Forest Service's posting of the rule on its web site is not sufficient to qualify the case for the study of cyberspace litigation. *Id*. at 1119.

384 The combined jury verdicts and settlements database of LEXIS reports verdicts from Alaska, Alabama, Arizona, Arkansas, California, Connecticut, District of Columbia, Florida, Georgia, Idaho, Indiana, Kentucky Louisiana, Maine, Maryland, Massachusetts, New Jersey, New York, Ohio, Oregon, Pennsylvania, Rhode Island, Tennessee, Texas, Utah and Vermont. Most state verdict reporters cover the entire period of this study (1992-2002). In addition, I examined the National Jury Verdict Review & Analysis, and the Combined Jury Verdicts and Settlements sources.

385 I examined all federal district court decisions, federal appellate decisions, and state appellate decisions reported in WESTLAW and LEXIS. Searches were conducted for internet-related cases using the following searches: (1) hlead (internet or e-mail or web or world wide web or worldwide web) and damages or injunction; (2) internet or website or web site or world wide web or www and damage or award or injunct! and date aft 1992; (3) atleast3 (Internet or cyberspace or world wide web or e-mail) and verdict or judgment and date aft 1992.

386 I searched the 300-plus Internet law cases published in the Phillips Nizer Internet Law Library. Martin H. Samson, *Internet Library of Law and Court Decisions*, *at* http://www.phillipsnizer.com/internetlib.htm (last visited Feb. 15, 2004). The Seattle law firm of Perkins, Coie publishes the *Internet Case Digest*, which is an online "compilation of cases designed to bookmark, collate and monitor important developments in Internet law, including cases that have significant implications for Internet legal issues even if they are not directly related to the Internet. The Digest includes both filed and decided cases to capture the most recent developments as well as new judicial precedents." *Internet Case Digest*, *at* http://www.perkinscoie.com/casedigest/default.cfm (last visited Feb. 15, 2004). The Finnegan, Henderson, Farabow, Garrett & Dunner, LLP web site was an important resource because of its exhaustive collection of Internet-related trademark cases. *Internet Trademark Case Summaries*, http://www.finnegan.com/publications/index.cfm?info=trademark (last visited Feb. 19, 2004).

387 In WESTLAW, I reviewed the Combined Jury Verdicts and Settlements, which included: (1) Association of Trial Lawyers of America ("ATLA"); (2) California Jury Verdicts and Judgments; (3) Florida Jury Verdict Reporter; (4) Jury Verdict and

individual cyberspace cases reported on law firm web sites;[389] (7) law school research centers;[390] (8) American Law Reports ("ALR") annotations;[391] (9) all Internet-related Mealey publications;[392] (10) e-commerce law secondary sources;[393] (11) Internet treatises;[394] (12) legal news services;[395] (13) Security and Exchange Commission ("SEC") filings;[396] and (14) general news[397]

Settlement Summaries; and (5) Verdict Settlements. All of these sources had complete data for the years studied.

388 I searched the combined domain name disputes and decisions but did not include cases channeled to the Uniform Dispute Resolution Procedures ("UDRP") developed by World Intellectual Property Organization ("WIPO"). Since the end of 1999, most domain name disputes have been decided by one or three person alternate dispute resolution panels rather than by the federal courts. As part of the process of registering a domain name, the registrant agrees to submit complaints filed by third parties to alternative dispute resolution panels. These proceedings are quick, inexpensive, and adjudicate domain name disputes between litigants in different countries. Panels have the limited power of ordering the transfer or cancellation of domain names and cannot award damages, attorney's fees, or costs. Unlike court cases, the UDRP are informal, non-appealable, and stare decisis is not followed. The sample of domain name cases is limited to those filed in federal court under the Federal Dilution Act of 1995 and the Anti-Cybersquatting Act of 1998.

389 Law firms frequently report individual "victories" in their web site marketing materials. A number of law firms compile cyberlaw verdicts won by other firms.

390 The UCLA Online Institute for Cyberspace Law and Policy compiles the leading Internet law cases by year. *The UCLA Online Institute for Cyberspace Law and Policy*, *at* http://www.gseis.ucla.edu/iclp/hp.html (last visited Feb. 15, 2004). The Berkman Center for Internet & Society at Harvard Law School was also searched. *The Berkman Center for Internet & Society*, *at* http://cyber.law.harvard.edu/home (last visited Feb. 15, 2004).

391 An online database of all Internet-related annotations in American Law Reports ("ALR") was extensively searched.

392 My content analysis of reported cases focused upon Cyber Tech & E-Commerce: Mealey's Litigation Report, Emerging Insurance Disputes: Mealey's Litigation Report, Intellectual Property: Mealey's Litigation Report, Litigation: Mealey's Combined Reports, Patents: Mealey's Litigation Report, and Trademarks: Mealey's Litigation Report.

393 I searched the commercial law, computer law, and e-commerce secondary literature. I conducted searches of Matthew Bender's UCC Reporter and Digest as well as the following Bender treatises: E-Commerce and Communications: Transactions in Digital Information, Nimmer on Copyright, Gilson on Trademark Protection & Practice, Intellectual Property Counseling and Litigation, Computer Contracts, Computer Law, and Law of the Internet.

394 During the period of the study, I updated four editions of the *E-Business Legal Handbook* (2003). All of the cases uncovered in each year's edition were included in the research universe. Other treatises searched were: Julian S. Millstein et. al., DOING BUSINESS ON THE INTERNET (2002); Kevin J. Connolly, LAW OF INTERNET OF SECURITY & PRIVACY (2002); Ian Ballon, E-COMMERCE & INTERNET LAW (2001).

395 The principal source here was the LEXIS library of legal news newsletters and publications. However, I also surveyed the general news databases as well as the combined news databases from the states compiled by WESTLAW. WESTLAW includes all Dow Jones magazines, newspapers, and wires, as well as other magazine databases. Both services have extensive libraries of newswires and news services providing additional information on case developments.

396 Corporate annual reports to shareholders were examined on LEXIS's FEDSEC database, as well as the SEC Edgar databases. Companies are required to disclose pending or settlement cases that may affect stock prices. LEXIS has complete SEC filings and exhibits in its online database.

397 Newspapers and popular magazines were analyzed on many LEXIS and WESTLAW databases.

and information services.[398] The sample excludes all criminal cases as well as dispositions for convicted offenders who are challenging the constitutionality of Internet postings of their criminal records and personal information.[399] The sample excluded Internet-related small claims actions because there is no reliable reporting service.[400] The sample does not include discovery orders to produce computer tapes or other information. The dataset does not include disputes decided under alternative dispute resolution such as the Uniform Domain Name Resolution Policy.

Furthermore, the sample does not include criminal prosecutions, regulatory actions brought by governmental units, or bankruptcies. Regulatory, criminal, and dot-com insolvency involves the government as the adjudicator of rights. These public law subjects are sharply different than private litigation, so they will be examined in a separate article.[401] The focus of this Article is on the role of private litigants in Internet litigation. Foreign litigants are included only to the extent that actions are tried in U.S. state and federal courts.

398 I systematically searched the extensive collection of computer law and cyberlaw publications on LEXIS and WESTLAW. Sources include: all Andrew Publications Newsletters on Internet-related topics, Computer Law Newsletters, Leader Publications Newsletters, and the published outlines of the Practicing Law Institute.

399 This Article focuses on civil litigation rather than criminal or quasi-criminal cyberspace cases where the plaintiff was a governmental agency or prosecutor.

400 In the state of Washington, there are newspaper reports of small claims courts ordering commercial e-mailers to compensate consumers. However, the complete absence of written opinions or other records makes it impossible to determine what role these informal tribunals play in the overall picture.

401 The research includes a content analysis of every FTC litigation report and SEC litigation release from 1995 to 2003. The FTC asserts broad investigative and law enforcement authority to police Internet fraud. The FTC uncovers many of its cases by enlisting volunteers to surf web sites in order to uncover get rich schemes, false advertising, miracle cures, privacy infractions, online pyramid schemes, credit card billing schemes, and other deceptive sales practices. Most FTC actions are based on the Commission's broad enforcement authority to restrain "unfair or deceptive acts or practices in or affecting commerce." 15 U.S.C. § 45(a)(1) (2003). Similarly, the SEC has been active in extending federal securities law to the enforcement of predatory, anti-fraud and anti-competitive practices in cyberspace. SEC actions may be brought for insider trading, pyramid schemes, fraudulent investment opportunities, and false and misleading information about securities and the companies that issue them. *U.S. Securities and Exchange Commission*, http://www.sec.gov (last visited Feb. 15, 2003).