3 Va. J.L. & Tech. 1 (Spring 1998) <http://vjolt.student.virginia.edu>
1522-1687 / © 1998 Virginia Journal of Law and Technology Association

VIRGINIA JOURNAL of LAW and TECHNOLOGY

UNIVERSITY OF VIRGINIA	SPRING 1998	3 VA. J.L. & TECH. 1

Anonymous Internet Communication and the First Amendment: A Crack in the Dam of National Sovereignty

by Michael H. Spencer[*]

I. Introduction

1. Anonymous discourse has been an integral part of English and American literary and social development. Notable examples of literary pseudonymity come from the works of Charles Dickens[1] (Boz) and Samuel L. Clemens[2] (Mark Twain). The intertwining of anonymous rhetoric and American social development is also evidenced by the pen of Publius[3] (James Madison and Alexander Hamilton) in the Federalist Papers and the observations of Junius,[4] a pre-Revolutionary War English pamphleteer whose identity still remains unknown. Such literary history serves as a backdrop for the Supreme Court's interpretation of the First Amendment of the Constitution and its applicability to anonymous communication.
2. With the history of anonymity serving as a precursory element to America’s political and social development, the Supreme Court began to shape the role of anonymity in First Amendment

jurisprudence. In justifying the role anonymous communication should play in developing American culture, the Court balanced the freedom to speak anonymously with the need for accountability. Such efforts, through time, have proven effective in defining the constitutional boundaries of anonymous communication.

3. Today, the Court's supreme authority in interpreting the constitutional parameters of anonymous communication may begin to waiver. The advent of anonymous internet communication coupled with the difficulty in tracing the authors of anonymous internet works may render the Court's decisions on such issues mere dead letters because of the inability to enforce the Court's holdings. Due to the global scope of internet communication, Congress' ability to pass enforceable legislation is also questionable. Therefore, the Constitution's supremacy and permanency in governing anonymous communication becomes increasingly suspect.
4. This article will discuss the development of First Amendment law as it relates to anonymous communication and whether the Constitution can adequately govern the coupling of anonymity and internet communication.

II. An Overview of the First Amendment and Anonymity.

5. The Court has applied the First Amendment, in varying degrees, to many forms of communication ranging from actual oral communication to print media. In the realm of anonymous communication, the Court has taken the view that the right to speak anonymously is protected under the First Amendment guarantee. This right, however, is not absolute.
6. In *Lewis Publishing Co. v. Morgan*,[5] the Court determined the validity of a federal statute that required newspapers wanting second class postage to provide names and addresses of publishers, editors, business managers and owners to the Postmaster General.[6] Two publishers of newspapers in New York argued that "this legislation abridged the freedom of the press protected by the 1st [Amendment] . . . ."[7] Nonetheless, the Court upheld the provision relying on the fact that it did not prevent the newspapers from using the mail system but only prevented them from getting a privilege of the second class system.[8] The Court, in effect, narrowed the means by which newspaper publishers could disseminate their work without revealing those who controlled the content of the publication.
7. In subsequent years, the Court began to implicitly recognize a right to anonymity as shown in *Thomas v. Collins*.[9] In *Thomas*, the Court held that a Texas law requiring the disclosure of union members to the Secretary of State before soliciting new members did not coincide with the rights of free speech and assembly.[10] Though not specifically discussing the issue of anonymity, the Court tacitly recognized that a law revealing the members of the union may have a detrimental effect on the exercise of First Amendment rights. Cases such as *Thomas*, *Watkins v. United States*,[11] and *NAACP v. Alabama ex. rel. Patterson*,[12] revealed the Court's willingness to protect the anonymity of individuals in order to ensure their First Amendment right of association.
8. In *NAACP v. Alabama*, a contempt order was issued against the NAACP for refusing to produce membership lists in accordance with a court order.[13] The petitioner claimed that this order violated the freedom of speech and assembly rights guaranteed to the petitioner and its members

under the Constitution.[14] Additionally, the petitioner showed that past submissions of the organization's members resulted in economic reprisals and the manifestations of public hostility.[15]

9. The Court stated that in order to force the production of the membership lists, the government's interest must be compelling.[16] The government did not survive this heightened scrutiny, since the membership lists were not essential to the government's purpose.[17] Due to the government's failure to meet its burden, the Court upheld the petitioner's right to maintain the anonymity of its members.[18] In subsequent years, the Court took this qualified right to anonymity and expanded it to encompass certain forms of anonymous speech.
10. In *Talley v. California*,[19] the Court addressed the prosecution of Manuel D. Talley for the distribution of anonymous handbills advocating the boycott of local merchants.[20] Mr. Talley's actions violated a city ordinance that prohibited the distribution of handbills without the names of those who prepared, distributed or sponsored them.[21]
11. Justice Black, in writing for the majority, held that the ordinance was an unconstitutional abridgment of the freedom of expression.[22] In reaching this conclusion, Justice Black analyzed the government's position that this ordinance helped identify those responsible for fraud, false advertisements or libel.[23] The Court found that the ordinance was not so limited but barred all handbills, thereby restricting an individual's freedom to speak anonymously.[24] Furthermore, the Court noted that in certain instances, groups were only able to either criticize oppressive practices anonymously or not at all.[25] The Court, in weighing governmental versus individual interests, acknowledged a need to preserve anonymity in this type of political speech.[26] As a result, the Court struck down the provision as being in violation of the freedom of expression.[27] Still, subsequent interpretations of *Talley* showed that this decision did not viscerate the uncertainty as to the scope of anonymous expression.[28] Subsequent courts differed on the scope as to whether or not the decision of the *Talley* Court meant that a party must show a threat in order for anonymous discourse to receive First Amendment protection.[29]
12. In an attempt to further explain this area of law, the Court granted certiorari in *Buckley v. Valeo*.[30] In applying the same exacting scrutiny established in *NAACP v. Alabama*, the Court implicitly recognized a general First Amendment protection to anonymity apart from the showing of threats or reprisals.[31] However, the Court also stated that this First Amendment freedom is not absolute and that the government has the opportunity to make a showing that tips the scales in favor of disclosure.[32] Even with this strict scrutiny test, the government was able to show that its disclosure interests outweighed the right to anonymity.[33]
13. More recently, in *McIntyre v. Ohio Elections Commission*,[34] the Court heard arguments on the applicability of the First Amendment to an individual's distribution of anonymous political literature. In *McIntyre*, a pamphleteer challenged a fine imposed by an election commission for distributing anonymous leaflets opposing a school tax.[35] The Ohio Elections Commission argued that this prohibition prevented the dissemination of untruths.[36] In rejecting this argument, the Court stated that the "Ohio statute . . . contains no language limiting its application to fraudulent, false, or libelous statements . . . ."[37] The Court went on to say that "[t]he simple

interest in providing voters with additional relevant information does not justify a state requirement that a writer make statements or disclosures she would otherwise omit."[38] Simply put, Ohio's prohibition of anonymous leaflets "plainly is not its principle weapon against fraud."[39] Accordingly, the Court viewed the Commission's position as unjustifiable.[40]

14. The Court, in using this balancing test, attempts to strike a balance between governmental interests and constitutionally protected anonymous communication. Though theoretically viable, this test poses problems when applied to anonymous internet communication. Due to the vastness of internet communication which has no jurisdictional boundaries or actual geographic space, a court's rulings may lack enforceability.[41]
15. Many believe that the global scope of internet communication makes the Constitution nothing more than a local ordinance.[42] Internet communication, in effect, "mocks legal jurisdiction, defies its effectiveness, and challenges its capacity to keep pace with the range and complexity of the problems presenting."[43] Accordingly, Congress faces a very difficult challenge in governing this mode of communication.[44]

III. Defamation and Anonymous Communication

16. The law of defamation compensates parties for injuries to reputation.[45] As a result of such laws, many individuals curb their speech in order to avoid the possible legal consequences of their actions. The result is a rising tension between the First Amendment's freedom of speech and the law of defamation. Initially, there were no constitutional limitations on private actions of libel or slander. In 1964, this began to change in *New York Times Co. v. Sullivan*.[46]
17. In *Sullivan*, a libel suit was filed against *The New York Times* for placing an advertisement raising funds for civil rights advocates.[47] In this advertisement, some of the statements about Montgomery, Alabama police were exaggerated or incorrect.[48] The Commissioner of Public Affairs for the City of Montgomery filed a libel suit alleging that the advertisement's statements implicated misconduct on his part.[49] A jury found for the Commissioner and awarded damages of $500,000.[50] The Alabama Supreme Court affirmed the verdict**.** When the matter reached the Unites States Supreme Court, the Court stated that contrary to the argument that libel falls outside the Constitution, "libel can claim no talismanic immunity from constitutional limitations."[51] Consequently, the Court held that the Constitution prohibits a public official from recovering damages for defamation relating to official conduct unless it is proven to have been made with "actual malice."[52]
18. This ruling, created a distinction between the level of proof necessary to prove defamation for public officials versus private parties. This distinction was made evident in *Gertz v. Robert Welch, Inc.*,[53] in which Justice Powell's majority opinion stated that the "actual malice" standard applies only to public officials and public figures.[54] Justice Powell stated specifically that "[t]hose who, by reason of the notoriety of their achievements or the vigor and success with which they seek the public's attention are properly classed as public figures . . . ."[55] They, along with those who hold governmental office, may recover with clear and convincing proof that the

defamatory remarks were made with knowledge of their falsity or reckless disregard for the truth.[56]

19. The Court went on to hold that the appropriate standard for defamation of private individuals may be determined by the states themselves.[57] States, however, in matters of public concern, cannot impose punitive damages absent "actual malice."[58] Therefore, absent "actual malice," the injured party can only be compensated for actual injuries including out-of-pocket loss, injury to reputation, standing in the community, personal humiliation, mental anguish and suffering.[59] These defined boundaries have been blurred by subsequent Supreme Court decisions.
20. In *Dun & Bradstreet, Inc. v. Greenmoss Builders, Inc.*,[60] the Court faced the question of the applicability of the *Gertz* rule to private parties when false and defamatory statements do not involve matters of public concern.[61] Justice Powell's opinion held that in speech involving no matters of public concern, an award of presumed and punitive damages may still be appropriate even absent a showing of "actual malice."[62] Joined by only two other justices, Justice Powell's opinion created greater confusion as to the applicable standard of review.
21. Justice O'Conner, writing for the majority in *Philadelphia Newspapers, Inc. v. Hepps*,[63] helped alleviate some of this confusion by stating that the necessary questions to be asked in this situation are whether the plaintiff is a public figure, and whether the speech in question is a matter of public concern.[64] If there is an affirmative answer to these two questions, then the plaintiff must show falsity and "actual malice."[65] If the plaintiff is not a public figure, but there is a matter of public concern, then the plaintiff must at least prove negligence and falsity to recover actual damages.[66] If the plaintiff is not a public figure and the speech in question is not a mater of public concern, then the Constitution does not necessarily change the common law landscape.[67]
22. In applying defamation law to anonymous communication, it must be noted that in the context of protection of confidential sources, the Court explicitly held in *Branzburg v. Hayes*,[68] that the First Amendment does not give newsmen any special immunity from revealing their sources.[69] It then becomes axiomatic that the anonymous source of possible defamatory statements may be ascertained by injured parties. This safeguard alleviates some concern as to obtaining the identity of the source of anonymous statements. Such a safeguard, however, dissipates when applied to internet communication.
23. Though the United States Supreme Court invalidated certain provisions of the Communications Decency Act of 1996 in *Reno v. ACLU*,[70] other important provisions remain. One such provision removes publisher liability on the part of providers[71] who provide users a medium from which to post information on the internet.[72]

Section 230 of the Communications Decency Act:

[b]y its plain language, . . . creates a federal immunity to any cause of action that would make service providers liable for information originating with a third-party user of the service. . . . Thus, lawsuits seeking to hold a service provider liable for its exercise of a publisher's traditional editorial functions -- such as deciding whether to publish, withdraw, postpone or alter content --

are barred.[73]

As a result, an injured party can only seek out the individual who actually posted the defamatory message and not the provider of the system. This end result seems equitable since the actual creator of the message is held accountable. The fairness of this result is obfuscated when a message is posted via an anonymous remailer.[74] In that regard, it becomes even more difficult for an injured party to ascertain the identity of the creator of an allegedly defamatory message.[75]

24. It can be said that since licenses are required for almost every endeavor, such a requirement should be made applicable to internet communication in order to prevent the avoidance of accountability. By preventing individuals from hiding behind anonymity, there can be an assurance of accountability.[76] Still, in another context, the Court has expressed the need for individuals to be able to remain anonymous.[77] The tension between accountability and anonymity has led some scholars to take the view that "[t]he very power of anonymity . . . [as] the plaintiff's own protection, for anonymous remarks will be greatly devalued precisely because they are anonymous and easy to make."[78] Here, it is argued that anonymity itself may prove to be a victim's best protection.
25. Nevertheless, such rhetoric does not protect a person who's name is falsely attached to an internet message. An example of the ramifications of pseudonymity is evident in *Zeran v. AOL, Inc.*.[79] In *Zeran*, Kenneth Zeran was subjected to unbearable harassment and death threats, due to an internet message falsely attributed to him.[80] By preventing provider liability, as the Fourth Circuit held in *Zeran*, an injured party has no recourse but to pursue the anonymous poster of a defamatory message. Due to the anonymity of the individual, the injured party must pursue the anonymous remailer provider. The pursuit of such a provider may lead to the divulgence of the author of the message if the provider is within the jurisdiction of the United States. Again, a serious concern arises when such a provider exists outside of United States jurisdiction. This form of communication creates an existence that so "[d]iffers from Terra Firma,"[81] that the laws of the United States may not be enough to govern effectively.

IV. How is Anonymous Internet Communication Achieved?

26. Anonymous internet communication can be achieved through an anonymous remailer which strips off the senders address and name.[82] One such remailer was created by Gilut Enterprises yet discontinued as a result of a lack of funding.[83] As a result of this void, Karl Kleinpaste, a Carnegie Mellon programmer, developed his own anonymous server.[84] This system, however, became so overwhelmed by abuses that he dismantled it until he could reinstate it with restrictions.[85] By doing so, another void was created. In 1992, Johan Helsinguis filled this void by creating another anonymous site: anon.penet.fi, based on the same programming created by Kleinpaste.[86] He offered it world-wide since the lawsuit-intensive climate in the United States

caused many local servers to shut down.[87] "By setting up anon.penet.fi in Finland, [he] hoped to create a more stable service."[88] Kleinpaste objected to this use and threatened to organize a net-terrorist group that would utilize a Usenet Death Penalty (UDP) against anonymous postings.[89] One user that took such action was Dr. Richard Depew, a professor of microbiology and immunology at Northeastern Ohio Universities College of Medicine. Dr. Depew created the Automated Retroactive Minimal Moderation system (ARMM), which automatically killed all anonymous files posted.[90] This attempt at vigilantism was short lived since many users objected to its indiscriminatory destruction of anonymous postings.[91] Still, anon.penet.fi became the most famous anonymous server, registering over 50,000 users as of January 1994.[92] Helsinguis' anonymous site enjoyed a relatively safe existence until the Church of Scientology demanded the identity of the author of certain anonymous postings.[93] As a result of their queries, the Finnish police raided Helsinguis' server and demanded that he produce the information they requested or turn over his server for their perusal.[94] Due to a subsequent order by a Finnish court, Mr. Helsinguis complied with the demand and produced the information thereby bringing the relative autonomy the internet has enjoyed into question. By August of 1996, Johan Helsingius, amid accusations of aiding child pornographers through his anonymous remailer, shut down his server.[95] Nevertheless, other anonymous remailers still exist and are consistently employed by internet users.[96]

27. Up to this point in time, anonymous communication has been dealt with by individual governments in their particular jurisdictions. Today, however, anonymous internet communication reaches beyond territorial boundaries and calls into question the sovereign authority of local governing bodies. It is therefore necessary to determine the means by which a world society is to curb abusive behavior on the internet.[97] Moreover, it first must be understood what role anonymity on the internet plays in today’s increasingly globalized society.

V. Internet Communication and the Role of Anonymity

28. Internet communication has been defined as a bodiless suite of digital communication in which a great number of users can reach one another as well as a great deal of information around the world.[98] It has also been construed as "[t]he aggregation of those transmission facilities and services that are able to communicate meaningfully among one another by means of the TCP-IP protocols."[99] In simpler phraseology, internet communication can be characterized as a communication between wordprocessors throughout the world in which individuals can exchange information, ideas and thoughts without leaving their terminal. However, many individuals desire to engage in this form of communication without exposing their identity.
29. To some anonymity is a means of freedom.[100] One such user stated that, "I am a teenage girl, often looked down upon harshly in the science and computer world. But on-line, I am just another user, and therefore, my ideas are not discriminated against, as I've seen happen in courses at school."[101] Advocates of anonymity also point to the case of Jake Baker, a twenty-year-old University of Michigan student who wrote very distasteful stories that were particularly offensive to the University and authorities.[102] Since he used his name and did not remain anonymous,

authorities were able to find and jail this 5-foot-6, 120 pound sophomore without bail.[103] They considered him a threat to society.[104] A federal judge released him even though "two of his judicial colleagues as well as the 6th Circuit Court of Appeals in Cincinnati, . . . had ruled that our streets would be safer without Baker walking them."[105]

30. Other users explain their desire to discuss politics that cannot be freely discussed in large parts of the world.[106] Access to anonymity has led to the violation of many U.S. laws ranging from pornography to copyright infringement and slander. One company had a "rash of sexually suggestive -- and even obscene -- e-mail sent to several female employees."[107] As a result of such abuses, many politicians have sought to regulate this booming form of communication.[108] In response to such actions, the proponents of anonymity have sought the protection of the First Amendment.[109]
31. From a policy standpoint, anonymity could also prove to be beneficial to internet communication. For instance, it could protect against actual retaliation or harm that may come to an individual who reports wrongdoing on the part of a colleague or a superior.[110] Furthermore, one aerospace manufacturer encourages anonymous communication in order to gain insight to a broader range of ideas that may help the company.[111] It can help hide the identity of those who were abused and want to discuss these issues in certain newsgroups.[112] Anonymity has even been characterized as somewhat therapeutic.[113] Such freedom can also be adventurous since an individual can pretend to be anyone they choose.[114]
32. Due to such wide-ranging uses, it is unclear how the Court or Congress will deal with the promise and pitfalls of anonymous internet communication. As many internet users are not within the jurisdiction of the United States, internet regulation also faces a serious problem of enforceability.

VI. Is Regulating Internet Communication Feasible and Practical in Global Communication?

33. As previously discussed, the benefits of anonymous internet communication are coupled with just as many problems. One major concern is whether speech that is not constitutionally protected can be effectively regulated without resorting to multiple international accords?
34. Complex jurisdictional issues will develop in which service providers, subscribers and remailers exist in several independent jurisdictions outside of the United States. Such circumstances become problematic when a citizen of the United States is allegedly defamed by an anonymous internet message that can be accessed by any individual with the internet. Even if a United States District Court or a state court claims jurisdiction, can its decisions be enforced absent international law?[115] With the increase of non-domestic internet users, will it matter whether or not a United States court deems certain language protected by the First Amendment? This situation may force the government to prohibit the use of anonymous remailers located outside the United States or only allow its use with countries that have a reciprocal treaty of accessibility. Will such a decision create a feeling of an Orwellian existence?[116]
35. Some users may view this problem of regulation as evidence of the inappropriateness of one

country’s attempt to regulate the internet. If, however, U.S. law is rendered ineffective in governing this form of communication,[117] then what is there to prevent the government or any other entity from using its resources in aggressively engaging in computer "hacking" to gain access to the identities of anonymous users stored in a foreign server.

36. If the First Amendment protection is rendered virtually irrelevant in this international scenario, then what can control governmental actions on the internet? Consequently, no anonymous user will be able to hide behind the protective ambit of the First Amendment. All of these possibilities not only reveal the issues facing the First Amendment in global communications, they foreshadow the growth of international law at the expense of national sovereignty.

VII. Solutions to an International Problem

37. The use of international treaties to regulate anonymous internet communication would be a cumbersome process and difficult to maintain. Due to the vast number of countries and their cultural differences, the use of reciprocal treaties on this issue becomes an untenable proposition. The number of treaties required would be directly proportional to the number of countries with internet access. The fallibility of an international treaty solution in regulating anonymous internet communication is evident when applied to anonymously traded pornography.
38. In the United States, anyone under the age of 18 years is considered a minor and therefore, any material depicting these minors in a sexual act would be construed as illegal pornography.[118] In contrast, the Netherlands has a much more liberal view of pornography.[119] As a result, that which is illegal in the United States would be permissible in the Netherlands. When such pornography is then anonymously posted on the internet, it becomes readily available in the United States to any individual with internet access. This simple scenario circumvents Congress’ attempt to regulate the dissemination of this type of material.
39. A simpler solution would be an international governing body that would be represented by every nation which would, in turn, promulgate rules and regulations governing internet communication. As such, this body would have the ultimate authority in determining what acts on the internet are actionable. To deny the need for such an organization would, in effect, allow the festering of this growing international problem.
40. Some legal scholars propose theories that call for better international treaties in the form of extradition laws.[120] This scheme, however, will eventually be overwhelmed as more nations and therefore individuals gain internet access. The only other solution, as noted by Ms. Pollack, is an international one.[121] This international governing body is that solution.

VIII. Conclusion

41. It is evident that the First Amendment is applicable to anonymous internet communication. Nevertheless, the growing scope of internet communication may overwhelm the Constitution’s usefulness in regulating it. Accordingly, an international solution is necessary in order to curb ongoing abuses of the internet. Only an international governing body would adequately serve this

purpose. The development of such a body will mean that the Constitution, the foundation of American sovereignty, may become secondary to international law with respect to internet communication.

Footnotes

[*]Michael H. Spencer, J.D., 1996, Washington and Lee Law School; 1995-96 Managing Editor of the *Capital Defense Journal*. Clerk to the Hon. Elizabeth V. Hallanan, U.S. District Court for the Southern District of West Virginia. Special thanks to Abraham Barker for his comments on the article.

[1] VIRGIL GRILLO, CHARLES DICKENS' SKETCHES BY BOZ: END IN THE BEGINNING (Boulder, Colo. Assoc. Univ. Press 1974).

[2] EVERETT EMERSON, THE AUTHENTIC MARK TWAIN: A LITERARY BIOGRAPHY OF SAMUEL L. CLEMENS (Univ. of Penn. Press 1984).

[3] ALBERT FURTWANGLER, THE AUTHORITY OF PUBLIUS; A READING OF THE FEDERALIST PAPERS (Cornell Univ. Press 1984).

[4] DEDICATION TO THE ENGLISH NATION, THE LETTERS OF JUNIUS (1769-1771), *reprinted in* FAMILIAR QUOTATIONS 1001 (J. Bartlett ed., 13th ed. 1955).

[5] 229 U.S. 288 (1913).

[6] *Id.* at 316.

[7] *Id.* at 297.

[8] *Id.* at 308, 310.

[9] 323 U.S. 516 (1945).

[10] *Id.*

[11] 354 U.S. 178 (1957) (prohibiting mandatory membership disclosure laws for political parties if such disclosures subject a member to reprisals).

[12] 357 U.S. 449 (1958).

[13] *Id.* at 451.

[14] *Id.* at 453.

[15] *Id.* at 462.

[16] *Id.* at 463.

[17] *Id.* at 466.

[18] *Id.* at 463-66.

[19] 362 U.S. 60 (1960).

[20] *Id.* at 61.

[21] *Id.* at 60-61.

[22] *Id.* at 64-65.

[23] *Id.* at 64.

[24] *Id.*

[25] *Id.* at 64-65.

[26] *Id.*

[27] *Id.*

[28] *Compare* United States v. Insco, 365 F. Supp. 1308 (M.D. Fla. 1973) (broad interpretation of *Talley*) *with* United States v. Scott, 195 F. Supp. 440 (D.N.D. 1961) (a narrow reading of the *Talley* decision).

[29] *Insco*, 365 F. Supp. at 1311.

[30] 424 U.S. 1 (1976).

[31] *Id.* at 64-65.

[32] *Id.* at 25.

[33] *Id.* at 68-74.

[34] 514 U.S. 334 (1995).

[35] *Id.*

[36] *Id.* at 343.

[37] *Id.*

[38] *Id.* at 348.

[39] *Id.* at 350.

[40] *Id.* at 351.

[41] Ian C. Ballon, *The Law of the Internet: Developing a Framework for Making New Law*, 482 PLI/PAT 9, 16 (1997).

[42] Anne Wells Branscomb, *Anonymity, Autonomy and Accountability: Challenges to the First Amendment in Cyberspaces*, 104 YALE L.J. 1639, 1646 (1995).

[43] Hon. Justice Michael Kirby, *Legal Aspects of Transborder Data Flows*, 11 COMPUTER/L.J. 233, 233 (1991).

[44] *See* Reno v. ACLU, 117 S. Ct. 2329 (1997); *See generally* Ballon, *supra* note 42, at 21-28 (outlining the legal difficulties in restricting the internet).

[45] 50 AM. JUR. 2D *Libel and Slander* § 375 (1995).

[46] 376 U.S. 254 (1964).

[47] *Id.* at 256.

[48] *Id.* at 258-59.

[49] *Id.*

[50] *Id.* at 256.

[51] *Id.* at 269.

[52] *Id.* at 279-80.

[53] 418 U.S. 323 (1974).

[54] *Id.* at 341.

[55] *Id.* at 342.

[56] *Id.*

[57] *Id.* at 347.

[58] *Id.* at 349-50.

[59] *Id.*

[60] 472 U.S. 749 (1985).

[61] *Id.* at 751.

[62] *Id.* at 763.

[63] 475 U.S. 767 (1986).

[64] *Id.* at 775.

[65] *Id.*

[66] *Id.*

[67] *Id.*

[68] 408 U.S. 665 (1972).

[69] *Id.*

[70] 117 S. Ct. 2329 (1997).

[71] Information Content Providers are defined as "any person or entity that is responsible, in whole or part for the creation or development of information provided through the Internet or any other interactive computer service." 47 U.S.C. § 230(e)(3) (1998).

[72] 47 U.S.C. § 230 (c)(1); *See, e.g.,* Zeran v. AOL, 129 F.3d 327, 330 (4th Cir. 1997).

[73] *Zeran,* 129 F.3d at 330.

[74] *See infra,* § IV.

[75] Branscomb, *supra* note 43, at 1679 n.10.

[76] *See* Hearing on S. 2030 Before the Subcommittee on Technology and the Law of the Senate Committee on the Judiciary, 101st Cong. 2d Sess. 265 (1990).

[77] *McIntyre*, 514 U.S. at 343.

[78] Trotter Hardy, *The Proper Legal Regimen for "Cyberspace"*, 55 U PITT. L. REV. 993, 1049 (1994).

[79] *Zeran,* 129 F.3d at 329-330.

[80] *Id.*

[81] Ballon, *supra* note 45.

[82] Keith Siver, *Good Samaritans in Cyberspace*, 23 RUTGERS COMPUTER AND TECH. L.J. 1, 42 n.173 (1997); David G. Post 1996 U. CHI. LEGAL F. 139, 169 n.5; Andre Bacard, *Anonymous Remailer FAQ* (updated Nov. 15, 1996) <http:www.well.com/user/abacard/remail.html>.

[83] L. Detweiler, *Anonymity on the Internet FAQ (1 of 4)* (last modified May 9,1993) <http:www.websteruniv.edu/~bumbaugh/net/anonfaq.html>.

[84] *Id.*

[85] *Id.* Abuses, in Kleinpaste's view, range from harassing e-mail postings, to child and adult pornography.

[86] *Id.*

[87] William Bulkeley, *Information Age: Censorship Fights Heat Up on Academic Networks*, WALL ST. J., May 24, 1993, at B1; Detweiler, *supra* note 84.

[88] *Id.*

[89] *Id.*

[90] Bulkeley, *supra* note 88; L. Detweiler, *Anonymity on the Internet FAQ (4 of 4)*, (1993), <www.websteruniv.edu/~bumbaugh/net/>. Dr. Depew even called it UDP for Usenet Depew Penalty.

[91] Bulkeley, *supra* note 88.

[92] Joshua Quittner, *Life in Cyberspace: Stamp Electronic Mail with Name?*, NEWSDAY, Jan. 4, 1994, at 53.

[93] Joshua Quittner, *Requiem for a Go-Between*, TIME, Sept. 16, 1996, at 74.

[94] Joshua Quittner, *Unmasked on the Net the Finns Raid a Computer that Ferries Anonymous Messages. Now Users Fear Their Secrets are at Risk*, NEWSDAY, Mar. 6, 1995, at 72.

[95] Amy Harmon, *Internet Figure Pulls Plug on His Anonymity Service Technology: Supporters say 'remailer' promoted free speech. Critics blame it for crime, pornography*, L.A. TIMES, August 31, 1996, at A1. *See also, British Newspaper Stands By Internet Child Porn Article*, NEWSBYTES, Sept. 6, 1996.

[96] *Lucent Technologies Offers Internet Anonymity*, P.C. WK, November 17, 1997, at 79. Several anonymous remailers are: alias@alias.cyberpass.net, remailer@replay.com, mix@squirrel.owl.de, mccain@notatla.demon.co.uk and tea@notatla.demon.co.uk.

[97] Noah Levine, *Establishing Legal Accountability for Anonymous Communication in Cyberspace*, 96 COLUM. L. REV. 1526 (1996), (Levine proposes the imposition of "liability on remailer administrators for the acts of their users only when the administrator has constructive knowledge of the user's illegal activites.") Such an idea has a sound foundation but in light of *Zeran* it seems that this argument may be lost.

[98] Branscomb, *supra* note 43, at 1639 n.5.

[99] E-Mail from Lewis M. Branscomb, Prof. Emeritus of Science and Tech Policy, Harvard University, former Chief Scientist of IBM and Director of the Project on the National Information Infrastructure, John F. Kennedy School of Government.

[100] *Computers in the '90s; Anonymity Viewed as Freedom*, NEWSDAY, Jan. 25, 1994, at 57.

[101] *Id.*

[102] Megan Garvey, *Crossing the Line on the Info Highway; He Put His Ugly Fantasy on the Internet. Then He Ran Smack Into Reality*, WASH. POST, Mar. 11, 1995, at H01.

[103] *Id.*

[104] *Id.*

[105] *Id.*

[106] Joshua Quittner, *Life in Cyberspace; Stamp Electronic Mail With Name?* NEWSDAY, Jan. 4, 1994, at 53.

[107] Michael Schrage, *Does the Mail Animal Need Electronic Anonymity?* WASH. POST, Apr. 1, 1994, at F2.

[108] Senator Jim Exon of Nebraska reintroduced a Communications Decency Act which regulates computer use by providing that those who "transmit or otherwise make available obscene, lewd, indecent, filthy or harassing communications could be liable for a fine or imprisonment." *Letters to the Editor - We Can't Allow Smut on the Internet*, WASH. POST, Mar. 9, 1995, at A20. Republican Speaker of the House, Newt Gingrich, has come out against tough restrictions on the Internet. *Networkings - High-Tech Group Flees D.C. in Cyberspace's Time of Need*. WASH. POST, July 10, 1995, at F19.

[109] *See* Reno v. ACLU, 117 S. Ct. 2329 (1997).

[110] Branscomb, *supra* note 43, at 1642.

[111] Schrage, *supra* note 108, at F2.

[112] Such a discussion group is alt.abuse.recovery

[113] Douglas Birch, *Just A Little Too Tangled Up in the Internet*, L.A. TIMES, Sept. 5, 1994, at E3.

[114] *Computers in the '90s*, *supra* note 101, at 57.

[115] In cases involving internet postings made by individuals in one state who were subjected them to liability in another jurisdiction. *See e.g.*, Compuserve, Inc. v. Patterson, 89 F.3d 1257 (6th Cir. 1996) (internet subscriber purposefully availed himself to benefits of doing business in service's home state, therefore, the exercise of jurisdiction was reasonable); American Network, Inc. v. Access America/Connect Atlanta, Inc., 975 F. Supp. 494 (S.D.N.Y. 1997) (internet service provider in New York brought a trademark infringement action against Georgia provider; New York District Court held that Georgia provider was subject to personal jurisdiction in New York); Telco Communication v. An Apple a Day, 977 F. Supp. 404 (E.D.Va. 1997) (defendants were subject to personal jurisdiction in Virginia for posting allegedly defamatory press releases regarding plaintiff on passive internet site); *Compare* Bensusan Restaurant Corp. v. King, 126 F.3d 25 (2d Cir. 1997) (action dismissed for lack of personal jurisdiction in dispute over a web site created by a Missouri jazz club).

[116] Companies currently monitor employees which creates "Big Brother overtones." Tom Henderson, *Test Drive: Internet Monitors*, NETWORK MAG., Nov. 1, 1997.

[117] *See* Scott M. Montpas, *Gambling On-Line: For a Hundred Dollars I Bet You Government Regulation Will Not Stop the Newest Form of Gambling*, 22 U. DAYTON L. REV. 163, 182 (1996); Phillip Palmer McGuican, *Stakes are High in Battle to Bar Internet Gambling*, NAT'L. L.J., November 3, 1997, at B8.

[118] 18 U.S.C. §§ 2252, 2256 (1998).

[119] *See* John T. Soma, *Transnational Extradition for Computer Crimes: Are New Treaties and Laws Needed?*, 34 HARV. J. ON LEGIS. 317, 340 (1997).

[120] *Id.* at 358-68.

[121] *See* Robyn Forman Pollack, *Creating the Standard of a Global Community: Regulating Pornography on the Internet--An International Concern*, 10 TEMP. INT'L & COMP. L.J. 467, 490 (1996).