NEW MEXICO LAW REVIEW

Volume 32
Issue 1 *Frontiers of Law: The Internet and Cyberspace (Winter 2002)*

Winter 2002

Comment: Don't Shoot the Messenger: Limiting the Liability of Anonymous Remailer Operations

Robyn Wagner

COMMENT: DON'T SHOOT THE MESSENGER: LIMITING THE LIABILITY OF ANONYMOUS REMAILER OPERATORS

ROBYN WAGNER*

> I will close the remailer for the time being because the legal issues concerning the Internet in Finland are yet undefined. The legal protection of the users needs to be clarified. At the moment the privacy of Internet messages is judicially unclear...I have also personally been a target because of the remailer. Unjustified accusations affect both my job and my private life.
>
> Johan (Julf) Helsingius[1]

I. INTRODUCTION

Access to the Internet and other distributed networks has rapidly progressed from novelty to norm.[2] As laws can shape the course of technology, so too can technology shape the course of the law. In the next century, lawyers and policy makers will increasingly face the complexities arising out of this balance. It is essential, then, that both technical and legal limitations be thoroughly investigated and understood before approaching the regulation of new technology.

Cryptographic software[3] currently enables people to communicate with potentially impenetrable confidentiality.[4] Such software can also make truly anonymous speech possible.[5] Many of the implications arising from these abilities

---

* Class of 2002, University of New Mexico School of Law; registered to practice before the United States Patent and Trademark Office. The author wishes to thank Matthias Bauer at the University of Erlangen, Germany; Alex de Joode at the University of Amsterdam, The Netherlands; and Mike Shinn at Shinn Networks for each of their personal communications on remailer policy with the author. The author would also like to thank Professor Michael Froomkin at the University of Miami School of Law for helping the author to refine her copyright law analysis through several email discussions. The author may be reached at wagner_robyn@yahoo.com.

1. Press Release, Johan Helsingius, Johan Helsingius Closes His Internet Remailer (Aug. 30, 1996), *at* http://www.penet.fi/press-english.html.

2. As of August 2001, more than 166 million U.S. adults had access to the Internet. *See* NUA Ltd., *How Many Online? U.S. & Canada, at* http://www.nua.ie/surveys/how_many_online/n_america.html. Over 513 million had access worldwide. *See* NUA Ltd., *How Many Online? Worldwide, at* http://www.nua.ie/surveys/how_many_online/world.html.

3. *See, e.g.*, the "Pretty Good Privacy" program, which can be obtained from http://www.pgpi.com.

4. Much of this software implements "public key" cryptography. In such a system, each user creates a private key, which is kept in secret, and a public key, which is published. Messages encrypted to the public key can be decrypted by the private key, and vice versa. In a properly implemented public key system, the world may use the public key to encrypt messages that only the private key owner can read. A strong public key system enables users to establish a secure line of communication with anyone who is capable of using the algorithm. Generally, this is anyone possessing compatible decryption software. For a full description of public key cryptography, see Whitfield Diffie & Martin E. Hellman, *New Directions in Cryptography*, IT-22 IEEE TRANSACTIONS INFO. THEORY 644 (1976); Ralph C. Merkle, *Secure Communication over Insecure Channels*, COMM. ACM, Apr. 1978, at 294; BRUCE SCHNEIER, APPLIED CRYPTOGRAPHY 29 (1994); Whitfield Diffie, *The First Ten Years of Public-Key Cryptography*, 76 PROC. IEEE 560 (1988).

5. The term "anonymity" frequently takes on one of two meanings in the context of online communications. *See* Mike Godwin, *Who Was That Masked Man?*, INTERNET WORLD, Jan. 1995, at 22. "Apparent" anonymity is actually a form of pseudonymity, offering computer users the opportunity to use names other than their own for purposes of electronic chat discussions or electronic mail. Such "anonymity" is merely apparent because these assumed names are tied to a user's real name as registered with his Internet Service Provider. Such "anonymity," though used by virtually every member of computer networks like America Online, is particularly prized by celebrities who wish to interact online. *Cf.* John E. Bradley, *Mr. Lonelyhearts*, SPORTS ILLUSTRATED, Jan. 15, 1996, at 80, 83 (describing Dallas Cowboys' quarterback Troy Aikman's use of America Online). True or "perfect" anonymity is provided by anonymous remailers and thus is the focus of this Comment. "In this case, there may be no person or entity that can be relied on to know the identity of the originator of the postings." Godwin, *supra*, at 22.

are just now reaching society. Can a truly anonymous party be investigated or prosecuted? Who should be held liable when trade secrets are leaked anonymously via message boards or mailing lists? The obvious answer may be to prohibit truly anonymous speech, or at least to limit its efficacy. Legislation to restrict or prohibit anonymous speech has been passed[6] and continues to be introduced both in state legislatures and in Congress.[7] Such measures may be myopic, however, for a number of reasons. There are many legal, legitimate reasons for which a person may wish to conceal his electronic identity. Moreover, in a burgeoning digital society, any attempted government regulation of technology that offers transactional freedom should be viewed with a wary eye.

The situation is confounded further by the global reach inherent in distributed networks. A government's ability to police its electronic borders is eroded by pockets of data that lie outside its physical boundaries and by interconnection with foreign networks that may be governed by different rules. As long as anonymous communication tools remain available in other countries—indeed, so long as one website, hosted anywhere in the world, offers access to anonymous communication—there is very little that a single country can do to prevent access. If every nation connected to the Internet prevented its own citizens from providing these tools to others, either independently, or as a concerted effort, certainly anonymous electronic communication could be made more difficult and risky. Whether such a plan would be constitutional in the United States is debatable. Moreover, it is highly unlikely that the other industrialized nations, much less every country in the world, would agree to such a policy. As long as even a single nation with extensive Internet connections offers anonymous communication, all persons connected to the Internet will continue to have access.[8]

Furthermore, as encryption usage becomes increasingly ubiquitous, governments can no longer realistically monitor their citizens' communications.[9] Thus, governments have two options: they may either legislate against cryptographic use, or they may embrace it. Each path has profound ramifications on how an information society will develop.

Anonymity is vitally important to free speech and privacy. Thus, a discussion of anonymity on the Internet is simultaneously a discussion of the degree of political freedom that modern society will tolerate or foster.[10] Proposals to regulate Internet anonymity in the United States face two major hurdles: the Constitution and technical constraints inherent in a globally connected network. At present, a

---

6. *See* 1995 Pa. Laws 8 (amending 18 PA. CONS. STAT. § 910(a)(1)).

7. Proposed federal legislation sought to prohibit any anonymous electronic message intended to "annoy, abuse, threaten, or harass any person...who receives the communication." S. 314, 104th Cong. § 2(a)(1)(B) (1995). A similar proposal was introduced in Connecticut. *See* Lawrence Lessig, *The Path of Cyberlaw*, 104 YALE L.J. 1743, 1750 n.20 (1995).

8. *See generally* A. Michael Froomkin, *Flood Control on the Information Ocean: Living with Anonymity, Digital Cash, and Distributed Databases*, 15 J.L. & COM. 395, 400 & 443-49 (1996) [hereinafter *Flood Control*].

9. *See generally* A. Michael Froomkin, *The Metaphor Is the Key: Cryptography, the Clipper Chip, and the Constitution*, 143 U. PA. L. REV. 709 (1995).

10. *See* Joel R. Reidenberg, *Setting Standards for Fair Information Practice in the U.S. Private Sector*, 80 IOWA L. REV. 497, 500-01 (1995) ("In democratic society, information standards reflect specific conceptions of governance...For private interactions and the relationship between citizens, both law and practice set the balance between dignity and free flows of information.").

substantial portion of true Internet anonymity relies on a handful of unpaid volunteers—anonymous remailer operators—and the systems they operate. If governments began prohibiting, restricting, or merely regulating their activities, anonymity's availability on the Internet could be reduced substantially. This Comment seeks to explain why the current legal environment supports minimal liability for remailer operators and to suggest why this is the only reasonable course upon which to continue.

Section II of this Comment provides background on the topic, including: a brief history of anonymity in America and American jurisprudence (section II.A.), a description of how the Internet facilitates anonymous communication and how remailers work (section II.B.), and why people use anonymous remailers (section II.C.). Section III discusses the difficulties in bringing legal actions against anonymous parties. The remainder of the article addresses the liability of remailer operators in different contexts including civil liability for copyright infringement (section IV.A.1.) and defamation (section IV.A.5.), criminal liability (section IV.B.), state regulation attempts (section V), and federal regulation attempts (section VI).

II. BACKGROUND

A. *Anonymity in the "Real" World*

Anonymity can be a tool of both benevolent and malevolent uses.[11] This was true long before the advent of modern computing, and the framework for the anonymity debate appears easily demarked. Some suggest that anonymity's contributions to free discourse outweigh any harm that it may cause, or, that the alternatives—a ban on or censorship of anonymous speech—are more destructive of a free society than any such harms.[12] As the Supreme Court has noted, "It is plain that anonymity has sometimes been assumed for the most constructive purposes."[13] Others suggest that the inherent lack of accountability in truly anonymous communications presents a

---

11. This is true of a wide variety of technologies. As Scott Charney and Ken Alexander note,
> history teaches that criminals will frequently abuse new technologies to benefit themselves or injure others. Automobiles are an apt example. Designed to provide transportation for law-abiding individuals, the automobile soon became a target (*e.g.*, car theft, car-jacking), a tool (*e.g.*, the getaway car in a bank robbery), and a weapon (*e.g.*, hit-and-run). Clearly, computers are following the same route.

Scott Charney & Ken Alexander, *Computer Crime*, 45 EMORY L.J. 931, 934 (1996).

12. One author suggests that
> [t]here are numerous situations in which anonymity seems entirely appropriate and even desirable. Psychologists and sociologists point out that people benefit from being able to assume different personae. It is therefore natural that individuals use electronic communication to disguise themselves,....The media often cite "a prominent source" who does not wish to be identified, and pseudonymous authors have long been with us, sometimes in the past to prevent disclosure that the writer was female for fear her work would not be published were her gender known....Anonymity has also been protected in cases in which actual retaliation or harm may ensue if the source of the writing is known, as in the case of whistle-blowers or political dissidents under authoritarian regimes.

Ann Wells Branscomb, *Anonymity, Autonomy, and Accountability: Challenges to the First Amendment in Cyberspace*, 104 YALE L.J. 1639, 1642 (1995).

13. Talley v. California, 362 U.S. 60, 65 (1960).

way for criminals to remain safely above and outside the law's reach—and suggest at least some forms of anonymity should be regulated or outrightly banned.[14]

1. Cases for Anonymity

American anonymous rhetoric boasts and benefits from a rich history of use dating to the founding days of the United States. During these early days, anonymity of speakers produced what many would agree was a desirable outcome.

The Federalist Papers[15] are perhaps the finest example of how anonymous rhetoric has benefited American social development. Authored by "Publius,"[16] the work may never have been published or distributed had the authors been forced to reveal their true identities. Similarly, the pre-Revolutionary War "Letters of Junius" pseudononymously espoused a wealth of constitutional rhetoric during the years 1767–1772, including sentiment that ultimately influenced the content of the Bill of Rights.[17] Junius's true identity remains unknown today.[18]

For centuries, anonymity has also been employed positively for more mundane purposes. In his autobiography, Benjamin Franklin recounted how he employed anonymity not to found a republic but to be printed in his brother's newspaper:

> My Brother had in 1720 or 21, begun to print a Newspaper....[A]fter having work'd in composing the Types & printing off the Sheets I was employ'd to carry the Papers thro' the Streets to the Customers.– He had some ingenious Men among his Friends who amus'd themselves by writing little Pieces for this Paper, which gain'd it Credit, & made it more in Demand; and these Gentlemen often visited us.—Hearing their Conversations, and their Accounts of the Approbation their Papers were receiv'd with, I was excited to try my Hand among them. But being still a Boy, & suspecting that my Brother would object to printing any Thing of mine in his Paper if he knew it to be mine, I contriv'd to disguise my Hand, & writing an anonymous Paper I put it in at Night under the Door of the Printing House. It was found in the Morning & communicated to his Writing Friends when they call'd in as Usual. They read it, commented on it in my Hearing, and I had the exquisite Pleasure, of finding it met with their Approbation, and that in their different Guesses at the Author none were named but Men of some Character among us for Learning & Ingenuity.

---

14. *See generally* David G. Post, *Pooling Intellectual Capital: Thoughts on Anonymity, Pseudonymity, and Limited Liability in Cyberspace*, 1996 U. CHI. LEGAL F. 139.

15. THE FEDERALIST PAPERS (Clinton Rossiter ed., 1961).

16. The collective pseudonym of James Madison, Alexander Hamilton, and John Jay. *See* McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 343 n.6 (1995).

17. For example, in 1772, Junius wrote, "The liberty of the press is the palladium of all the civil, political and religious rights of an Englishman...." JOSEPH STORY, *Document 33 in* COMMENTARIES ON THE CONSTITUTION OF THE UNITED STATES (1833), *available at* http://presspubs.uchicago.edu/founders/documents/amendI_speechs33.html.

18. *McIntyre*, 514 U.S. at 343 n.6 (citations omitted). The Anti-Federalists also tended to publish under pseudonyms, as *McIntyre* notes,

> prominent among [Anti-Federalist pseudonyms] were "Cato," believed to be New York Governor George Clinton; "Centinel," probably Samuel Bryan...; "The Federal Farmer," who may have been Richard Henry Lee, a Virginia member of the Continental Congress and a signer of the Declaration of Independence; and "Brutus," who may have been Robert Yates, a New York Supreme Court Justice who walked out of the Constitutional Convention.

Id. (citations omitted).

A form of anonymity—substituting a number for a name—is employed by this law journal when assessing the writing skills of prospective journal members. Indeed, this technique of "blinding" academic submissions is similarly employed by law schools around the country during examinations. Moreover, authors in general have a history of adopting pseudonyms,[19] for varying reasons.

American jurisprudence also supports the use of anonymity. Throughout the course of this country's history, the Supreme Court has affirmed the benefits inherent in anonymity—particularly among dissidents.[20] In *NAACP v. Alabama ex. rel. Patterson*,[21] for example, the Supreme Court held that the right of anonymous association was protected by the guarantee of free speech in the Constitution, and that a state had no power to compel a local chapter of the NAACP to disclose a list of the names of its members. Of great concern, had the state prevailed, was that bigots might harm the NAACP members had the disclosure of their identities been made. As explained by the Court, "It is hardly a novel perception that compelled disclosure of affiliation with groups engaged in advocacy may constitute...restraint on freedom of association...."[22]

A more recent case, *McIntyre v. Ohio Elections Commission*,[23] illustrates both the importance of anonymity and the unique legal problems it presents. *McIntyre* was centered on the actions of Mrs. McIntyre, who distributed leaflets at a public meeting at the Blendon Middle School in Westerville, Ohio, expressing opposition to a proposed school tax levy. Some of the leaflets identified her as the author; others merely indicated that the leaflets expressed the views of "Concerned Parents and Taxpayers."[24] Mrs. McIntyre subsequently was fined for her actions by the Ohio Elections Committee for violating a statute that provided

> [n]o person shall write, print, post, or distribute, or cause to be written, printed, posted, or distributed, a notice, placard, dodger, advertisement, sample ballot, or any other form of general publication which is designed to...promote the adoption or defeat of any issue...through flyers, handbills, or other nonperiodical printed matter, unless there appears on such form of publication in a conspicuous place or is contained within said statement the name and residence or business

19. *E.g.*, Mark Twain (Samuel Langhorne Clemens), O. Henry (William Sydney Porter), Voltaire (Francois Marie Arouet), George Eliot (Mary Ann Evans), and Charles Dickens (sometimes writing as "Boz").

20. *See, e.g.*, Brown v. Socialist Workers' 74 Campaign Comm., 459 U.S. 87, 91 (1982) (holding that the "Constitution protects against the compelled disclosure of political associations"); Hynes v. Mayor of Oradell, 425 U.S. 610, 623-28 (1976) (Brennan, J., concurring in part) (asserting disclosure requirements put an impermissible burden on political expression); Shelton v. Tucker, 364 U.S. 479, 485-87 (1960) (holding invalid a statute compelling teachers to disclose associational ties because it deprived them of free association rights); Talley v. California, 362 U.S. 60, 64-65 (1960) (voiding an ordinance compelling the public identification of group members); Bates v. City of Little Rock, 361 U.S. 516, 522-24 (1960) (holding, on free assembly grounds, that the NAACP did not have to disclose its membership lists); Joint Anti-Fascist Refugee Comm. v. McGrath, 341 U.S. 123, 145 (1951) (Black, J., concurring) (expressing the fear that dominant groups might suppress unorthodox minorities if allowed to compel disclosure of associational ties).

21. 357 U.S. 449 (1958).

22. *Id.* at 462.

23. 514 U.S. 334 (1995).

24. *Id.* at 337.

> address of the chairman, treasurer, or secretary of the organization issuing the same, or the person who issues, makes, or is responsible therefore.[25]

The Court stated the issue in the case as "whether an Ohio statute that prohibits the distribution of anonymous campaign literature is a 'law...abridging the freedom of speech' within the meaning of the First Amendment."[26] Throughout its opinion, the Court eloquently referenced the "important role in the progress of mankind" that anonymous literature in all forms has played:[27]

> Anonymity...provides a way for a writer who may be personally unpopular to ensure that readers will not prejudice her message simply because they do not like its proponent. Thus, even in the field of political rhetoric, where the identity of the speaker is an important component of many attempts to persuade, the most effective advocates have sometimes opted for anonymity. [There is] a respected tradition of anonymity in the advocacy of political causes. This tradition is perhaps best exemplified by the secret ballot, the hard-won right to vote one's conscience without fear of retaliation.[28]

The Court concluded,

> Under our Constitution, anonymous pamphleteering is not a pernicious, fraudulent practice, but an honorable tradition of advocacy and of dissent. Anonymity is a shield from the tyranny of the majority. It thus exemplifies the purpose behind the Bill of Rights, and of the First Amendment in particular: to protect unpopular individuals from retaliation—and their ideas from suppression—at the hand of an intolerant society. The right to remain anonymous may be abused when it shields fraudulent conduct. But political speech by its nature will sometimes have unpalatable consequences, and, in general, our society accords greater weight to the value of free speech than to the dangers of its misuse. Ohio has not shown that its interest in preventing the misuse of anonymous election-related speech justifies a prohibition on all uses of that speech.[29]

"Anonymity" appears at issue in a strange sense in *McIntyre*. The Ohio Statute did indeed "prohibit the distribution of anonymous campaign literature."[30] Mrs. McIntyre's actions, however, were not anonymous at all. She attended a meeting and, acting in a fashion that ensured that her identity was evident to all, distributed campaign literature without her identification on the literature itself. Upon reflection, there appear to be two elements to the offense with which Mrs. McIntyre was charged: (1) anonymous communication via "a notice, placard, dodger, advertisement, sample ballot, or any other form of general publication which is designed to...promote the adoption or defeat of any issue";[31] and (2) a non-anonymous action sufficient to allow her to be identified and charged. Both

---

25. *Id.* at 338 n.3 (citing OHIO REV. CODE ANN. § 53599.09(A)).
26. *Id.* at 336.
27. *Id.* at 341 (quoting Talley v. California, 362 U.S. 60, 64 (1960)).
28. *Id.* at 342-43 (internal quotations and footnotes omitted).
29. *Id.* at 357 (citations omitted).
30. *Id.* at 338 n.3 (citing OHIO REV. CODE ANN. § 53599.09(A)).
31. *Id.*

elements were required, but only the first was prohibited by the Ohio legislature. The second element was more a consequence of a general truth that rules can only be enforced by identifying a party against whom to proceed. Yet, it is this second element that is responsible for much of the damage that anonymity potentially can cause.

2. "Cases" Against

Justice Scalia summed up the case against anonymity in his dissent in *McIntyre*[32] when he stated, "It facilitates wrong by eliminating accountability, which is ordinarily the very purpose of the anonymity."[33]

Conspiracy, hate speech, libel, disclosure of trade secrets, and other forms of illegal and immoral activity can be furthered easily by anonymous communication. Some of these communications may possess clues to identify their author.[34] Many communications, however, present stark law enforcement problems, particularly in the realms of libel and intellectual property law.[35]

Signed defamatory messages may carry more credibility than unsigned (anonymous) ones, and may thus be more damaging. Nevertheless, anonymous defamatory messages are not necessarily harmless. As Michael Froomkin has suggested, "Most people would probably be upset to discover a series of unsigned posters accusing them of pedophilia tacked to trees or lampposts in their neighborhood."[36] Similarly, a victim of anonymous libel is unlikely to be appeased by assertions that the anonymous attacker lacks credibility.[37] As Sissela Bok has argued, a society in which "everyone can keep secrets impenetrable at will," whether they be "innocuous...[or] lethal plans,...would force us to disregard the legitimate claims of those persons who might be injured, betrayed, or ignored as the result of secrets inappropriately kept."[38]

Aside from providing a tool for criminals, anonymity also is denounced frequently for limiting access to truth. Ironically put forth in an anonymously authored article,[39] the argument is that "disclosure advances the search for truth,"[40] because anonymous propaganda "makes it more difficult to identify the self interest or bias underlying the argument."[41] Justice Black, a noted First Amendment absolutist, shared this viewpoint. He believed mandatory identity disclosure would enhance the freedom of speech, and that Congress should require the disclosure of foreign agents "so that hearers and readers may not be deceived by the belief that

---

32. 514 U.S. 334 (1995).

33. *Id.* at 385 (Scalia, J. dissenting).

34. For example, disclosure of a trade secret may limit the pool of potential authors to the group of people with access to the secret. If this number is sufficiently small, the author may be found.

35. *See Flood Control*, *supra* note 8, at 402.

36. *Id.* at 404.

37. *See, e.g.*, New York v. Duryea, 351 N.Y.S.2d 978, 996 (1974) (arguing that people generally discount, to a certain extent, the veracity of anonymous writing).

38. SISSELA BOK, SECRETS: ON THE ETHICS OF CONCEALMENT AND REVELATION 16, 28 (1984).

39. Note, *The Constitutional Right to Anonymity: Free Speech, Disclosure and the Devil*, 70 YALE L.J. 1084 (1961).

40. *Id.* at 1109.

41. *Id.* at 1111.

the information comes from a disinterested source. Such legislation implements rather than detracts from the prized freedoms guaranteed by the First Amendment."[42]

The potential damage to society's ability to confront and remedy legitimate claims is, perhaps, anonymity's most compelling detractor. In addition to the above-noted commentators, the argument has popular resonance, as illustrated in a *Wall Street Journal* column critiquing the growth of anonymous communication on the Internet.[43] Such sentiment was expressed similarly by a more moderate writer, acknowledging that while anonymity has its merits, "[p]ermitting anonymity for the purpose of removing any vestige of accountability for abusive behavior...is not likely to be tolerated in the Networld."[44]

B. How the Internet Facilitates Anonymous Communication

Any digital communication can theoretically be made anonymous. "Anonymizing" web proxies,[45] for example, permits users to browse the World Wide Web without revealing to observers the pages they have visited.[46] Anonymous remailers exclusively handle electronic mail, and with it, posts to mailing lists, bulletin boards, and Usenet groups.[47] And, though the workings of remailer technology may appear opaque, use of one of several user-friendly software programs[48] or a simple web page[49] permits anyone with access to the Internet, and the requisite inclination, to send secure, anonymous email.

Tangible anonymous messages require that an author go to great pains to avoid connecting himself with his publication. This is especially so in an era where modern forensic techniques can easily lift fingerprints off a document and DNA from the saliva on an envelope. Digital messages, in contrast, bear only the identifying marks added by the sender or by intermediate relay systems used in the course of that message's delivery.[50] Thus, without those marks, and absent internal

---

42. Viereck v. United States, 318 U.S. 236, 251 (1943) (Black, J., dissenting).

43. *See* Walter S. Mossberg, *Accountability Is Key to Democracy in the On-Line World*, WALL ST. J., Jan 26, 1995, at B1.

44. Branscomb, *supra* note 12, at 1675; *cf.* George P. Long, III, Comment, *Who Are You?: Identity and Anonymity in Cyberspace*, 55 U. PITT. L. REV. 1177, 1205 (1994) ("[I]f law enforcement authorities are precluded from obtaining the identities of anonymous users, illegal activities will proliferate.").

45. *See, e.g.*, the service Orangatango, *at* http://www.orangatango.com.

46. Orangatano, for example, allows subscribers to connect securely from their personal Web browsers to the Orangatango server via an encrypted session. Users request specific Web pages, such as http://www.cnn.com, which Orangatano retrieves, forwarding the content back to the user over the encrypted channel. Web proxies that operate like Orangatano are useful for preventing "local" spying—i.e., if a user is "surfing" from work, the user's boss and network administrator are unlikely to defeat the protection provided by Orangatango. However, nothing prevents Orangatango from keeping logs on its users. Thus, while Orangatango may be useful for employees wishing to check stock quotes without being caught by their bosses, Orangatango does not offer true anonymity—law enforcement officials, for example, could likely subpoena Orangatango for information on specific users with minimum effort.

47. Posting to Usenet is accomplished by a service called a mail2news gateway. For general information on the development of Usenet, see JENNY FRISTRUP, USENET: NETNEWS FOR EVERYONE, 10-21 (1994).

48. *See, e.g.*, http://www.skuz.net/potatoware.html.

49. *See, e.g.*, http://www.gilc.org/speech/anonymous/remailer.html.

50. A standard email message contains "headers" before the body of the message. These typically include fields such as "From" and "To." Also typically found in the headers of a message is a listing of the route the message took to reach its final destination. This might be analogized to a postal letter bearing several postmarks showing its transit through different post offices.

clues in the message itself,[51] there is nothing inherent in the message that can reveal the sender's identity.

While the operation and security of anonymous remailers vary, they share one feature in common: they strip away the identifying information at the top of the message and forward it on with a new header attached.[52] Were this all that remailers did, however, little security would be gained, particularly against a powerful adversary.[53] Just as a facially anonymous letter mailed at the post office may be laden with clues for a forensic detective, as discussed below, so too may the author of an insecurely "anonymized" message be subject to discovery.[54]

An understanding of the different degrees of anonymity offered by different types of remailers is essential to making any informed policy decisions related to their operation. Thus, the next section will address the levels of security offered by the use of increasingly sophisticated methods of anonymity. As a continuing example, suppose that a fictional person named Alice wishes to send a message to Bob.

1. Free Web-Based Email Services

People frequently sign up for accounts from sites such as Hotmail[55] that offer free email services, even when they already have a valid email address with another, often paid, service provider. There are many reasons for this, including remote accessibility and address permanence. Hotmail accounts are frequently opened because people wish to add a layer of obfuscation to their messages. They may be purchasing items from online stores and wish to avoid marketing spam.[56] They may likewise wish to prevent a connection between a work or school address and their personal interests. Many people believe that services such as Hotmail are wholly unconnected to their real identities. This is *not* the case.

Suppose Alice works with Bob and every day Bob's bad parking renders an adjacent parking spot unusable. If Alice wishes to curb Bob's behavior, she may leave an unsigned note under the windshield wiper of his car. If Bob disregards her note and continues to park badly, Alice may wish to complain in a more forceful manner. If Bob does not take well to criticism, or if Bob is Alice's boss, she may have good reason to wish to conceal her identity.

---

51. *E.g.*, "Hi Jim, this is Fred."

52. A list of remailers and their features, as well as current information about their operation and recent performance statistics, can be found at the Web page for the Shinn Anonymous Remailer, at http://mixmaster.shinn.net.

53. This Comment borrows frequently from common cryptographic nomenclature. "Adversary" here and throughout this article refers to a person who wishes or attempts to access the contents of communication without permission from the communicants, for whatever reason, benign or malicious.

54. Some services appear to function as truly anonymous remailers, but are intentionally insecure. FakeMail, formerly at http://www.netcreations.com, allowed users to send messages (seemingly) from assorted real and fictitious dignitaries; however, it also inserted information into the detailed headers (discussed at more length below) allowing a user to reveal the origin of the message.

55. http://www.hotmail.com.

56. Spam is flooding the Internet with many copies of the same message, in an attempt to force the message on people who would not otherwise choose to receive it. Most spam is commercial advertising, often for dubious products, get-rich-quick schemes, or quasi-legal services. Spam costs the sender very little to send—most of the costs are paid for by the recipient or the carriers rather than by the sender.

Scott Hazen Mueller, *What Is Spam?*, *at* http://spam.abuse.net/whatisspam.html.

One morning, when Bob has rendered *three* spots unusable, Alice is sufficiently annoyed that she opens an account with Hotmail called parkingnarq@hotmail.com. Using this account, Alice sends mail to everyone in the office that might look as follows:

> To: Alice@company.com, Bob@company.com, Steve@company.com, Ted@company.com[57]
> From: parkingnarq@hotmail.com
> Date: 10:00AM, July 15, 2001
> Subject: Bob can't park.
> Once again, Bob has demonstrated his skill in parking this morning by consuming THREE parking spots. Way to go, Bob!

By sending the message, Alice may have a good chance of "shaming" Bob into changing his behavior. But how well has Alice protected her identity? Not at all against an adversary of even minimal sophistication. There are four visible "headers" in the above message: To, From, Date, and Subject. There are also several "hidden" headers containing information such as the path that the message took to get from hotmail.com to company.com. These headers can be viewed with nearly any client software, usually with as little effort as a mouse click or a few keystrokes. Hotmail inserts an additional header into all outgoing mail titled "X-Originating-IP." In parkingnarq's message, the header might read: "X-Originating-IP: [129.24.1.2]." If Alice's work computer is connected directly to the Internet, the IP address 129.24.1.2 is in all likelihood the IP address of Alice's machine, and parkingnarq's message is thus directly traceable to Alice.[58]

The whole of Alice's anonymity rests on the collective inability of everyone receiving the message to know to examine the message's full headers. While the repercussions of Alice's actions may be minimal in this example even if she is discovered, use of Hotmail to "anonymize" more sensitive information is a *very* bad idea.[59] To increase her security, Alice needs assurance that the headers of her email message will not betray her. Enter the "remailer."

---

57. If parkingnarq sent the message to everyone in the company but Alice, it would be fairly reasonable to assume that Alice authored the message.

58. If Alice's computer is behind a firewall, more steps will be needed to trace the message back to Alice, but these steps are still easily within the reach of anyone at Alice's company with access to server logs. Alice may also add a level of obfuscation to this scenario by making use of an anonymizing Web proxy, but that is discussed in more detail *supra* note 46.

59. Unfortunately, most people seem unaware of the limited anonymity offered by services such as Hotmail. For example, Alcoholics Anonymous offers an AA member mailing list, which terms of use statement reads,

> MEETING@recovery.org private email lists—As a result of this letter, RECOVERY.ORG is supporting private email discussion lists, for AAs to talk to one another. Not a "meeting," per se, just communication. This list will be hand-maintained but NOT moderated, rather than allowing subscriptions through a list management tool, in order to try to keep the unwanted spam to a minimum. Note that your email communications will NOT be anonymous, except to whatever degree your email address already protects your identity. You may want to use a free hotmail.com or yahoo.com address for your list postings, if personal anonymity is an issue to you.

http://www.recovery.org/aa. Though participants are warned that their identities could be compromised by posting to the list, the suggestion to use a Hotmail account for purposes of anonymity is troubling.

2. "Penet"—An Early Remailer

By far the best-known and most widely-used remailer was anon.penet.fi, or Penet,[60] run by Julf Helsingius out of Finland from 1992 through 1996.[61] In its lifetime, Penet was home to over half a million users[62] and accounted for almost five percent of all Usenet postings.[63] Penet was not an anonymous remailer. It was a pseudononymous remailer and worked as follows:[64] Suppose Alice wanted to post a message to Usenet without revealing her real email address, alice@somewhere.com. Alice could email her message to Penet, along with instructions specifying to which group she wanted the note posted. Penet would then post the message to Usenet, replacing Alice's real email address with something like anon123@anon.penet.fi. Penet maintained a list of "true" addresses and their corresponding aliases on Penet. This allowed people to reply to Alice without knowing her real address. Thus, mail sent to anon123@anon.penet.fi would be forwarded by the remailer to alice@somewhere.com.

The Penet system was both free and relatively simple to use. No special software was required, and users could gain the ability to send messages through Penet almost immediately after registering. Penet's location outside U.S. jurisdiction added to its popularity.

Helsingius spent approximately one thousand dollars per month running the system for what he described as humanitarian reasons.[65] Indeed, Penet was instrumental in enabling people to engage in discussion of a wide array of topics. Usenet newsgroups addressing highly sensitive or politically charged issues virtually owe their existence to Penet.[66] The remailer helped everyone from people recovering from sexual abuse, to human rights activists, to people with socially unpopular diseases looking for support, to "average Joes" who wanted to discuss everything from romance advice to erotic fetishes in public forums.[67]

Unfortunately, Penet had a rather glaring point of failure. Helsingius could readily determine the identity of his users by simply examining the records on his machine that mapped users' email addresses to their anonymous IDs. This flaw

---

60. http://www.penet.fi/.

61. See Press Release, Johan Helsingius, World-wide Internet Community Appalled Over the Scientology Seizure: Was the Child Porn Scandal Just a Cover? (Feb. 20, 1995) *at* http://www.eff.org/Censorship/SLAPP/Intprop_abuse/Scientology_cases/anon_server_compromised.announce; Johan Helsingius, Johan Helsingius Closes His Internet Remailer, *supra* note 1.

62. *See* Johan Helsingius, Johan Helsingius Closes His Internet Remailer, *supra* note 1.

63. *See Allegations of Child Porn Close Email Operation*, BOSTON GLOBE, Aug. 31, 1996, at A2.

64. The following description is based on the author's knowledge of Penet's workings. For a copy of Helsingius's original Penet instructions and description, see http://www.unik.no/~robert/anon.penet.fi.html.

65. *See* Daniel Akst, *Postcard from Cyberspace: The Cutting Edge; The Helsinki Incident and the Right to Anonymity*, L.A. TIMES, Feb. 22, 1995, at D1.

66. A number of anonymous posting and reply services predate Penet and were created with an eye to permitting anonymous discourse in particularly volatile newsgroups. David Mack created anonymous posting and reply service around 1988 for use in the alt.sex.bondage group. The service at wizvax.methuen.ma.us, as well as that at n7kbt.rain.com, was predominantly used in alt.personals. *See* L. Detweiler, *The Anonymity FAQ*, *at* http://www.eff.org/Privacy/Anonymity/net_anonymity.faq. While these early services contributed greatly to the discourse in specific groups, it was not until the functions of remailing and posting were unified into a single service, Penet, that the explosion of anonymous messages hit Usenet. *Id.*

67. Dave Mandl, *Life after Penet: The Remailer Is Dead, Long Live the Remailer*, *at* http://www.wfmu.org/~davem/docs/penet.html.

ultimately caused him to close his remailer as the result of the following two legal attacks made on his system. On February 2, 1995, an American representative of the Church of Scientology contacted Helsingius, informing him that some information residing on an internal Scientology computer in California was stolen and had been made public via a Penet Usenet post.[68] The Church claimed that the information was classified as a "corporate secret." The Church reported this event as a burglary to the LAPD and FBI, and the representative of the Church asked Helsingius for the real identity of the individual that had posted the confidential information.[69] After Penet's operator made it clear that he would *not* reveal the personal information of his users, he was informed that Interpol was already in the process of sending an official request to the Finnish Police.[70]

On February 8, 1995, Helsingius was served with a search and seizure warrant on his home and on the Penet server, demanding the name of the anonymous user.[71] Helsingius managed to prevent confiscation of the server by copying the requested information onto a diskette.[72] However, Helsingius revealed to Finnish police that the anonymous ID belonged to an account at Caltech.[73] Armed with this information, the Scientologist lawyers sent private investigators to Caltech that same day, demanding personal information on that user's account.[74] The school refused to give the Church or its private investigators any information, but it did divulge the information to LAPD detectives who subsequently contacted the school.[75]

The second attack on Penet came in the spring of 1996 after the Church of Scientology sued Grady Ward for purportedly violating the Church's copyrights by posting several of its "Advanced Technology" documents on the web via anonymous remailers.[76] In the course of its lawsuit, the Church of Scientology again pressured the Finnish police for access to Penet's records, this time to determine whether or not Grady Ward ever used the remailer.[77] Finnish police, granting the Scientologists' requests, contacted Helsingius in June of 1996, demanding that he turn over the names of two more users.[78] Specifically, they sought the identities of users who had posted Scientology documents to Usenet in February and March of

---

68. Johan Helsingius, World-wide Internet Community Appalled Over the Scientology Seizure, *supra* note 61.

69. *Id.*

70. *Id.*

71. *Id.*

72. *See* Matti Huuhtanen, Associated Press (Feb. 28, 1995), *available at* http://www2.thecia.net/users/rnewman/scientology/anon/AB-orig.txt.

73. *See* Ron Newman, *The Church of Scientology vs. anon.penet.fi*, *at* http://www2.thecia.net/users/rnewman/scientology/anon/penet.html; Temporary Restraining Order, Religious Technology Center v. Ward, No. 96-20207 RMW (N.D. Cal. 1996), *available at* http://www2.thecia.net/users/rnewman/scientology/media/bj-3.28.96.

74. *See* posting of Rich Fagan, rich@cco.caltech.edu, to alt.religion.scientology (June 26, 1995), *at* http://www2.thecia.net/users/rnewman/scientology/anon/caltech-pi-visit.

75. *See id.*

76. *See* Newman, *supra* note 73; *Religious Technology Center*, *supra* note 73.

77. *See* Newman, *supra* note 73; *see also* http://www2.thecia.net/users/rnewman/scientology/grady/960615-henri.

78. *See* Newman, *supra* note 73.

that year.[79] Helsingius asked the appropriate Finnish court for a delay, which the court granted until August 22, 1996.[80]

At a hearing on August 22, 1996, the Helsinki District Court decided against Helsingius and ordered him to turn over the names.[81] In effect, the court ruled that email was not protected by standard Finnish privacy laws as were other communications, such as telephone calls.[82] Helsingius appealed the ruling, but closed Penet on August 30, 1996, fearing that if he lost the case he might be forced to compromise the identities of more users.[83] Helsingius was ultimately ordered to reveal the accounts by the Finnish Court of Appeals. He complied.[84] Ironically, both accounts at Penet were mapped to accounts at alpha.c2.org, a pseudonym server offering the potential for being very secure and able to resist the very kind of attack that resulted in the demise of Penet.[85] After all, some three years had passed since Helsingius opened Penet, and the technology had vastly improved in that time.

3. Modern Remailer Technology—Offering Untraceable Anonymity[86]

Modern remailers make use of two important features not offered by Penet. By implementing cryptographic tools widely available on the Internet,[87] and by routing, or "chaining" messages through a series of remailers, users can ensure three things vital to preserving the true anonymity of their messages.[88] First, none of the remailer operators will be able to read the text of the message, because it has been encrypted

---

79. *See id;* posting of Peik J. Strømsholm, pjs@UWasa.Fi, to alt.religion.scientology (June 14, 1996), *at* http://www2.thecia.net/users/rnewman/scientology/anon/penet-6.14.96 (translating a post to sfnet.keskustelu.laki by Kaj Malmberg, the Finnish officer in charge of investigating the Internet-related charges).

80. *See* Newman, *supra* note 73.

81. *See id.*

82. *See* email from Azeem Azhar, azeem@dial.pipex.com, to undisclosed recipients (Aug. 30, 1996), *at* http://www2.thecia.net/users/rnewman/scientology/anon/penet-8.22.96; Press Release, Johan Helsingius Gets Injunction in Scientology Case: Privacy Protection of Anonymous Messages Still Unclear (Sept. 23, 1996), *available at* http://www.penet.fi/injunc.html.

83. *See* Newman, *supra* note 73.

84. *See* posting of T. Byfield, tbyfield@panix.com, to nettime-l@Desk.nl , *<nettime> anon.penet.fi: case closed* (Mar. 30, 1998), at http://nettime.khm.de/nettime.w3archive/199803/msg00126.html.

85. *See id.* Helsingius revealed that an498608@anon.penet.fi mapped to veno@alpha.c2.org, and an545430 @anon.penet.fi mapped to Helen@alpha.c2.org. *Id.*

86. As this is a legal, not a scientific, publication, the explanations in this section are simplified. For an excellent, in-depth analysis of the security of the modern remailer network, see Lance Cottrell, *Mixmaster and Remailer Attacks, previously at* http://www.obscura.com/~loki/remailer/remailer-essay.html (on file with author).

87. Public key cryptography tools are popular and widely available on the Internet. Pretty Good Privacy (PGP) can be obtained from many sites online, including http://www.pgpi.com. For an in-depth description of the technical workings and colorful political history of PGP, see SIMSON GARFINKEL, PGP: PRETTY GOOD PRIVACY (1994).

88. Modern remailers also make available the possibility of untraceable pseudonymity. As explained by computer security consultant Hal Finney,

> nyms allow for continuity of identity to be maintained over a period of time. A person posting under a nym can develop an image and a reputation just like any other online personality. Most people we interact with online are just a name and an email address, plus whatever impression we have formed of them by what they say. The same thing can be true of nyms. Cryptography can also help maintain the continuity of the nym, by allowing the user to digitally sign messages under the name of the nym. The digital signature cannot be forged, nor can it be linked to the True Name of the user. But it makes sure that nobody can send a message pretending to be another person's nym.

Flood Control, supra note 8, at 423.

in a fashion that requires the cooperation of each operator in turn before the message can be read.[89] Second, neither the intended recipient, nor any of the remailer operators in the chain (other than the first remailer operator to receive the message) can identify the sender of the message without the cooperation of every prior operator. Finally, as a result of the first two assurances, it is impossible for the recipient of the message to connect the message to its sender without the cooperation of every single anonymous remailer operator in the chain. As referenced above, "cooperation" would most likely involve each remailer keeping a log of all data that flowed through it, as well as the willingness of each operator to share this information with the recipient. Many remailer operators refuse to keep logs as a matter of principle and practice, indicating that there is a strong likelihood that the necessary information does not exist. Moreover, even if logs were maintained by each remailer operator, if remailers are located in assorted countries, compelling all of the operators to disclose such logs could present a potentially insurmountable barrier.[90]

4. Modern Anonymous Remailer Operators

As explained above, very effective Internet anonymity requires only two things: cryptographic software and some supply of remailer operators. Cryptographic tools are readily obtainable.[91] Moreover, if the user properly uses that cryptographic software, the message is untraceably anonymous so long as a single anonymous remailer operator is honest.[92] Nevertheless, a major potential constraint on Internet anonymity is the supply of remailer operators. Remailers are currently operated in a few countries by a relatively small number of volunteers that can generally be measured in the low tens.[93]

The remailer operator's dilemma is simple. The last remailer operator in a chain has no reliable way of concealing the identity of the sending machine from the message's intended recipient. Furthermore, no remailer operator can control the content of the encrypted messages that flow through the remailer. Thus, the last remailer in a chain risks being identified by an unhappy recipient.[94] An identifiable person is a potential target for investigation, prosecution, or regulation. If anonymous remailer operators were held strictly liable for the content of the messages that flow through their systems, even though they were unable to discover the content of those encrypted messages, very few people would find running a remailer an acceptable risk. As discussed above, remailer operators have already been the subject of legal attacks, most notably instigated by officials of the Church

89. This can be visualized by use of the following (postal) analogy: Alice writes Bob's address on an envelope. Inside the envelope is another envelope, with instructions for Bob to mail the inner envelope to Charlie. Charlie receives the envelope, opens it, and finds a smaller envelope with instructions to send it to Dave, and so on, until the innermost message is eventually sent to its intended recipient. This real world example is imperfect, however, because nothing prevents Bob from opening all of the envelopes. Encryption, however, provides protection against this in the digital context. *See* Cottrell, *supra* note 86.

90. The expense of locating and hiring foreign counsel, as well as potential language difficulties, are examples of the problems inherent in obtaining logs from foreign remailer operators.

91. *See supra* note 87.

92. Here, "honest" is taken to mean that the operator does not keep logs and is not colluding with any other remailer operator.

93. For a current listing of all known operational remailers, visit http://mixmaster.shinn.net.

94. For example, the recipient of a death threat.

of Scientology.[95] As a result, operating a remailer is not a risk-free activity today. At some point, if the number of remailers becomes sufficiently small, it becomes technically (if not necessarily legally or politically) feasible for authorities to conduct traffic analysis[96] on each remailer, making deductions about who sent what to whom.

Remailer operators derive no financial benefit from the provision of their remailer services.[97] Indeed, most remailer operators are motivated by either an interest in having the service available for their own use, or by a deep-seated belief in the virtues of anonymity.[98] Ultimately, in the absence of a jurisdiction capable of offering a safe haven for remailers and their operators, a cornerstone of Internet anonymity currently relies on the patience and courage of hobbyists.[99]

C. *Why People Use Remailers*[100]

Few people wish to be remembered for every word they utter. Nevertheless, some reluctant speakers are deserving of encouragement. Corporate whistle-blowers and associates at law firms may well fear losing their jobs; victims of all manners of abuse may suffer harm if their identities are discovered; and those criticizing

---

95. *See supra* section II.B.2.

96. Traffic analysis in this context means the study of the "traffic," or data, entering and leaving each machine, including the number of messages sent or received in a given amount of time, the size of the message, and a number of other values.

97. An excerpt from a "Frequently Asked Questions" document reveals some of the reasons behind the choice not to charge a fee for such services: "Why are some remailers free...? In the beginning, all remailers were free to users....How could a remailer administrator charge people who wanted maximum privacy? How could administrators ask for a credit card number or take checks? Several years ago, there was no technical solution to these problems." Andre Bacard, *Frequently Asked Questions About Anonymous Remailers* (last updated February 2, 2001), *at* http://www.andrebacard.com/remail.html.

98. As Julf Helsingius has said, "It's important to be able to express certain views without everyone knowing who you are....Living in Finland, I got a pretty close view of how things were in the former Soviet Union. If you actually owned a photocopier or even a typewriter there you would have to register it and they would take samples of what your typewriter would put out so they could identify it later. That's something I find so appalling." Joshua Quittner, *Anonymously Yours: An Interview with Johan Helsingius*, WIRED, June 1994, at 50, 52 (quoting Helsingius).

99. Many remailer operators are willing to face such obstacles, however. As Alex de Joode, a remailer operator since 1994, has remarked,

> Free speech means a lot to me. You have to be able to say anything you want—even mindless drivel. Stupidity or racist heckling cannot be wiped out through censorship but rather by confronting the problem. Censorship simply isn't the way to go. I established Replay [an anonymous remailer] to prevent censorship from succeeding and it seems to work very well. I felt that I could contribute to making it very difficult for governments and businesses to trace people. By setting up a remailer I would make it very difficult for one country to put censorship in place, since the Internet is global every person with a modem can use my service and circumvent censorship legislation, this person can speak freely and should not fear retribution for speaking what is on his mind. I've had trouble with the Singapore government because someone there questioned the rulings of the President, but that is exactly why the remailer is there!

Sabine Helmers, *A Brief History of anon.penet.fi—The Legendary Anonymous Remailer*, *at* http://www.december.com/cmc/mag/1997/sep/helmers.html.

100. The author has used anonymous remailers since the early 1990s. In her July 28, 2000, presentation at Defcon, an annual hacker convention, the author explained her initial remailer use as follows: "Back then, it was usually to post to assorted newsgroups where, coincidentally, young teenage girls are under-represented. I posted anonymously for a number of reasons...you're more likely to be taken seriously in technical groups if you're not a 12-year-old girl." A VHS copy of this speech is on file with the author.

political movements, religions, or cults may likewise fear retaliation.[101] Human rights workers and others speaking out against repressive governments or advocating revolution may have the most to fear, however, given the budgets and force available to those governments they oppose.[102] Even in seemingly free countries such as this one, it can be unsafe to criticize the government at certain times and places.[103] Perhaps ironically, remailers can also be used in the place of telephone "crime stopping hotlines."[104] As discussed below, people in each of these situations have successfully used anonymous remailers to conceal their identities while expressing themselves.[105] Indeed, anonymous remailers were initially created to encourage and allow individuals to communicate who, without the guarantee of privacy, would not otherwise participate in certain beneficial discussions. "The capability was designed to encourage open discussions among victims of child abuse or AIDS and originally was used only in such groups."[106]

Having the right to free speech may work well in the case of verbal expression, but it may cease to have its intended purpose in the face of retaliation that may occur decades later.[107] As a method of communication, sending electronic mail can be as casual and timely as a telephone call; however, it can also be stored and accessed with exponentially greater ease than traditional letters or audio recordings of conversations. If the storage of that email is not protected, the message can be accessed by anyone with the time and ability to sift through the records of any of the systems that may have intercepted that message.[108] Posts made to mailing lists, message boards, or Usenet are particularly susceptible to this, and as data collection

---

101. *See* Johyn Byczkowski, *Abuses vs. Uses Stirs Anonymous Servers Controversy*, CINCINNATI ENQUIRER, June 12, 1994, at F10 (describing use of remailers for news groups such as alt.sexual.abuse.recovery and alt.personals); Joshua Quittner, *Requiem for a Go-Between*, TIME, Sept. 16, 1996, at 74; David Post, *Knock Knock, Who's There?*, AM. LAW., Dec. 1995, at 113.

102. *Cf.* Dirk Johnson, *Chinese in U.S. Lament Bush Victory*, N.Y. TIMES, Jan. 27, 1990, 1, at 10 (discussing the fears of Chinese students in the U.S. that participating in protests against the Beijing government could result in persecution and retaliation against their families and against themselves should they return to China).

103. *See, e.g.*, Gitlow v. New York, 268 U.S. 652 (1925) (upholding a conviction under a state criminal anarchy statute for advocating the violent overthrow of the government by printing and distributing 16,000 papers advocating Communism); Dennis v. United States, 341 U.S. 494 (1951) (upholding a conviction under the Treason, Sedition, & Subversive Activities Act (Smith Act), 18 U.S.C. §§ 10-11 (1946).

104. Charles Arthur, *Super Informant Highway Set Up on the Internet: Police Open Route for Anonymous Electronic Mail*, INDEPENDENT, May 13, 1995, at 7 (describing initiative by police force to encourage "anyone with information about crimes in the West Mercia (U.K.) area...to post electronic mail to the police" via anonymous remailer).

105. Abused as a child, an adult decides to share his story with a support group. A young woman who has tested postive for HIV discusses her feelings with others affected by the AIDS virus. After observing illegal activities at his company, a man debates the implications of "blowing the whistle" on his employer. A dissident in China publishes some of his banned writings. For privacy reasons, all four individuals wish to remain anonymous. These scenarios would not be unique in today's society, except that they are occurring daily over an extensive computer network known as the Internet.

George P. Long, III, *supra* note 44, at 1178.

106. William Bulkeley, *Censorship Fights Heat Up on Academic Networks*, WALL ST. J., May 24, 1993, at B1.

107. Judge James Rosenbaum, sitting on the U.S. District Court for the District of Minnesota, has proposed a "cyber statute of limitations" to address the "durability of computerized material." *In Defense of the Delete Key*, 3 GREEN BAG 2D 393, 395 (2000).

108. For example, at http://groups.google.com, one may search through a significant portion of the posts made to Usenet since March 29, 1995. *See* http://groups.google.com/advanced_group_search (formerly http://www.deja.com).

technology improves, it becomes increasingly likely that archives will be maintained and made searchable indefinitely.[109]

Ironically, it is anonymity that helps encourage participation in Usenet groups and mailing lists. Many people live in communities that are violently intolerant of their social, political, or religious views. They may use remailers to network with those more understanding of their situation. As one poster to alt.privacy.anon-server wrote,

> I consider myself to be a fairly good example of why anonymous remailers are needed on the Net. To be blunt, I am bisexual, a pervert and a witch. I also live in Alabama, where at least two of the three are illegal. In a worst-case scenario, I could lose my job, have my career ruined, face prosecution and possibly even have to deal with violence.[110]

Anonymous communication can also allow for the creation of digital personae, which may be liberating to some.[111] This ability to create such personae may enhance the quality of speech and debate available on the Internet. A communication that discloses no information on the author's identity—including age, race, sex, and national origin—means that the author must be judged solely on the content of his message. This makes stereotyping and bigotry extremely difficult, potentially encouraging parties to discuss the merits of ideas, rather than the prejudiced views of the speaker.[112]

Aside from psychological benefits that an anonymous poster may gain by finding a community outside his own, there may also be external benefits to a community as a whole. For example, public health is generally improved by wide dissemination of information concerning communicable diseases. Nevertheless, many people would be unwilling to inquire publicly about such information—particularly regarding socially stigmatizing diseases like alcoholism[113] or AIDS for fear of being identified as a potential sufferer.

It is not uncommon for prospective employers to perform searches on job applicants' email addresses to ascertain in which types of online participation they

---

109. *See id.* The "X-No-Archive: Yes" header is a frequently used directive to archiving programs/services, such as Deja News not to archive a copy of the message. People who use "X-No-Archive: Yes" want to reduce the risk of their articles being stored for future access. Nevertheless, this directive is simply a request to avoid archiving. It is not a guarantee that the message will not be recorded and stored on a server indefinitely. Indeed, the X-No-Archive Project, run by Jerry Terranson of Missouri Freenet, sought to capture all posts containing this directive and compile them into a searchable database on his website. The website no longer contains this information; however, a discussion of the matter can be found at http://www.shmoo.com/mail/cypherpunks/mar00/msg00062.shtml.

110. *Quoted in* Daniel Akst, *Postcard from Cyberspace: The Cutting Edge; The Helsinki Incident and the Right to Anonymity*, L.A. TIMES, Feb. 22, 1995, at D1.

111. For a discussion of such "digital personalities," see Curtis E.A. Karnow, *The Encrypted Self: Fleshing Out the Rights of Electronic Personalities*, 13 J. MARSHALL J. COMPUTER & INFO. L. 1 (1994).

112. For a glimpse at the potential ramifications of "blinded" speech in an "identity-conscious society and legal world," see Clark Freshman, *Were Patricia Williams and Ronald Dworkin Separated at Birth?*, 95 COLUM. L. REV. 1568, 1576-77 (1995) (book review); Christopher A. Ford, *Administering Identity: The Determination of "Race" in Race-Conscious Law*, 82 CAL. L. REV. 1231 (1994).

113. *See, e.g., The Importance of Anonymity, at* http://www.alcoholics-anonymous.org/english/E_FactFile/M-24_d9.html ("As the Fellowship of A.A. grew, the positive values of anonymity soon became apparent...[W]e know from experience that many problem drinkers might hesitate to turn to A.A. for help if they thought their problem might be discussed publicly, even inadvertently, by others.").

may have engaged.[114] Employers may even perform these sorts of searches on their current employees—to see if they are seeking other employment,[115] to see if they are expressing undesirable opinions about the company or its product, or to see if they are engaging in behavior that may be offensive to the employer.[116] Indeed, the ability to search Internet archives has resulted in a new kind of "absolute accountability"[117] allowing archive searchers to obtain lists of people who

> have used racist slurs in print, or who have a history of organizing for labor unions. Says [Ross] Stapleton, "It's increasingly easy for someone in an HR department to say—'Look, Joe here says that skydiving is cool. Do we want to carry him on the rolls considering that he might die? Jane here is in a lifestyle that the chairman might not find attractive. We might not want to put her forward for the public affairs spot.' I don't have any activities that I don't want to post about. If I did, I would be very cautious."[118]

Employees, understandably reluctant to suffer such close scrutiny of their personal lives, frequently opt to use anonymous remailers to engage in legal behavior that may nevertheless offend their employer. For example, a computer engineer may wish to share his expert opinion, "off the record," of how his product stacks up against the competition.

In light of legislation such as the Digital Millennium Copyright Act[119] and the potential for civil litigation under state trade secret laws,[120] many successful reverse

---

114. [P]ostings to the Internet's 33,000 news groups may fall off the edge of Usenet after a week or so, but they live on in databases such as Deja News and the Internet Archive....We can already see the outlines of this new world. When you apply for a job in the high-tech sector, there's a fair chance your prospective employer will use a search engine to scout out your online postings, from late-night musings to intemperate rants fired off to a political news group. Would an employer's decision be colored by information that has nothing to do with a candidate's job qualifications, such as your out-of-the-mainstream religious beliefs, sexual orientation, HIV status or personal habits? Absolutely, and without apology. After all, "character" counts, too.

Joseph D. Lasica, *Your Past Is Your Future, Web-Wise*, THE WASH. POST, Oct. 11, 1998, at C01.

115. For example, by looking on job-related websites, such as http://www.monster.com, or in Usenet groups under the jobs.* hierarchy.

116. In 1999 the *Boston Herald* published a story detailing the results of an in-depth investigation of Internet use by public employees and others using taxpayer-funded accounts. The *Herald* discovered an account belonging to MassEd.Net, a taxpayer-funded organization that subsidizes Internet access for schools, was being used "to promote a sex-and-wrestling Web site." Joseph Mallia, *Waste.com, Public Employees Using Internet for Sex, Drugs and Rock 'n' Roll*, BOSTON HERALD, May 12, 1999, at 1. It also found that an Internet user at the Secretary of State's office had sent 324 messages about TV shows, including the Simpsons; that students using their high school accounts traded advice on how to make and buy LSD and other hallucinogens; that an account registered to the Public Works department was used to buy and sell erotic Japanese cartoons; that an account registered to the state auditor's office was used to scalp sporting event tickets—in violation of state law. Much of the source material for the article came from searches of Deja.com, a Usenet archive.

117. SIMSON GARFINKEL, DATABASE NATION: THE DEATH OF PRIVACY IN THE 21ST CENTURY, 9, 87 (2000).

118. *Id.* (quoting Ross Stapleton).

119. Pub. L. No. 105-304 (1998).

120. *See* DVD Copy Control Ass'n, Inc. v. McLaughlin, No. CV 786804 (Cal. Super. Ct. 2000). At issue in *DVDCCA* is whether the defendants illegally revealed trade secrets by posting on their Web site's DeCSS, a tool for circumventing DVD copy protection. *Id.* Plaintiff argued that the reverse engineering required to author DeCSS was achieved through the misappropriation of trade secrets. Plaintiff further alleged that DeCSS was designed specifically to illegally pirate DVDs. *Id.* Defendants argued that Plaintiff was attempting to stifle free discussion about the issue by litigating against the people who posted the program rather than the people who created it. *Id.*

engineering[121] attempts are disclosed anonymously via remailers.[122] Thus, in at least some circumstances, remailers protect the legitimate disclosure of information against corporations who have made a habit of challenging all reverse engineering attempts of their products, hoping their competition will fold under the burden of litigation. Computer security information—exploits, bugs, and other similar forms of information—can also be disclosed this way.[123]

People also employ anonymous remailers to prevent "spammers"[124] and other unwanted persons from harvesting their real email addresses.[125] It is important to remember the ramifications of posting one's identity in a public forum, even a seemingly innocuous one.[126] People frequently post very benign messages via remailers for this very reason.[127]

Finally, as Patrick Ball, Deputy Director of the American Association for the Advancement of Science's Science and Human Rights program has said, "Encrypted and anonymous communication is very important for human rights activists, and for anyone who needs to denounce violations of human rights committed by repressive regimes."[128] In early 1999, the anonymous remailer network allowed ethnic

---

121. Reverse engineering is the process of recreating a design by analyzing a final product. Reverse engineering is common in both hardware and software. *See* http://whatis.techtarget.com/definition/0.289893 .sid9gc.507015.99.html.

122. The legality of specific reverse engineering attempts under these laws lies outside the scope of this Comment.

123. For example, on April 29, 2000, nobody@lobeda.jena.thur.de (an anonymous remailer account) posted the following message to bugtraq@securityfocus.com, a well-known computer security alert list:

> It's been alleged that this source code, once compiled, was used by persons unknown in the distributed denial of service (DDoS) attacks earlier this year. Obviously such a thing cannot be confirmed aside from through a process of targeted sites making an appropriate comparison between the traffic this software would generate and the traffic they actually received.
>
> The code was made available anonymously to us (ie [sic] we didn't write it and don't know who did) and is hereby made available anonymously to AusCERT, CERT, CIAC, Mr. David Dittrich (who carried out analyses on binary versions of the trinoo, tfn2k and stacheldracht DDoS tools around the 1999/2000 New Year period), as well as several other "full disclosure" mailing lists/forums. It's not known if this source code has seen the light of day prior to now, so your mileage will definitely vary.—Anon

See http://cert.uni-stuttgart.de/archive/bugtraq/2000/05/msg00006.html.

124. One who sends "spam," as defined *supra* note 56.

125. It is common practice on Usenet to modify one's email address by including the term "nospam" somewhere inside. For example, alice@somewhere.com might change her address to alice-nospam@somewhere.com or alice@somewhere.nospam.com. The theory is that a human wishing to reply to Alice's post will immediately recognize this clue to her true address (alice@somewhere.com), while an automated email address harvester will not. It is relatively trivial to program around this trick, but it illustrates many authors' desire to remain free of spam.

126. For a period of several months, for example, flight attendants posting to the Usenet group rec.travel.air had their personal and work email addresses copied down by an individual who subsequently posted defamatory remarks about them in other newsgroups. These posts were in the tradition of publishing a person's phone number on a bathroom wall with "For a good time, call" prepended. The lengthy series of posts may be obtained from http://groups.google.com by searching for "remailer" in "rec.travel.air."

127. For example, on October 21, 2000, nobody@noisebox.remailer.org (an anonymous remailer account) posted the following message to the group, alt.tv.simpsons: "What state do the simpsons live in? It seems like every time they're about to tell, something blocks it out or interrupts it. It's very frustrating!" See also a post made to alt.tv.er on October 21, 2000, also made by nobody@noisebox.remailer.org, stating, "Missed Thursday's episode. What happened?"

128. Press Release, Anonymizer.com, Anonymizer.com Launches Kosovo Privacy Project to Protect Online Communications in Yugoslavia and Kosovo (March 26, 1999), *at* http://www.tao.ca/wind/rre/0658.html.

Albanians to provide first-hand accounts of Serbian atrocities in Kosovo[129] without fear of retribution.[130] Similarly, remailers have often been used by victims of rape, domestic violence, and other sensitive or life-threatening settings to solicit advice.[131] As Julf Helsingius remarked, "[r]emailers have made it possible for people to discuss very sensitive matters, such as domestic violence, school bullying or human rights issues anonymously and confidentially on the Internet. The closing of [the] anon.penet.fi [remailer] will make it harder to discuss these matters."[132]

For all these lawful uses of remailer technology, there are also many reasons why criminals and perceived criminals may make use of remailers. For example, libel can effectively be made indelible by Internet dissemination. This is so because once it is introduced to the data stream, it may be reproduced and stored in any number of computers.[133]

Trade secrets are also vulnerable in light of anonymous electronic communication. On September 9, 1994, for example, an anonymous person mailed to the Cypherpunks mailing list a message containing what was purported to be the source code for RC4, a proprietary cryptographic algorithm owned by RSA Data Security, Inc.[134] More recently, On October 26, 1999, the source code for CSS authentication was also released via the anonymous remailer network.[135] Public posting, in most cases, tends to reduce the value of a trade secret, thus trade secret disclosure can be particularly damaging to the company that holds it.

Anonymous remailers have a notorious history of being used to disseminate copyrighted works, particularly via Usenet.[136] Many remailers have limits on

---

129. For a general explanation of Internet access during the Kosovo conflict and the role it played in disseminating both government propaganda and independent reports, see Dorothy E. Denning, *Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy, at* http://www.infowar.com/class_2/00/class2_020400b_j.shtml.

130. On March 26, 1999, Anonymizer.com launched the Kosovo Privacy Project to address the immediate concerns of Kosovars, Serbs, and others reporting on the situation in Kosovo. The project was conceived by Alex Fowler, public affairs director of the Electronic Frontier Foundation, after "seeing messages being posted on Web pages that are just as easy for me to read as they would be for Milosevic and his government agents." Press Release, Anonymizer.com, *supra* note 128.

131. For example, on September 21, 2000, nobody@dizum.com (a remailer account) posted a message to sci.psychology.psychotherapy containing the following:

> I need advice. I am aware of a psychologist-in-training who has three times threatened physical assault and has threatened to stalk me. He has also threatened illegal actions. Plus he has done libelous things and engaged in many posting activities that some of the leaders of this newsgroup would consider "sexual abuse."
>
> My question is: Should an individual like this be reported (with documentation) to the graduate school where he is doing his studies?...
>
> I need to know now. Please advise.

132. Helsingius, *supra* note 1.

133. *See* Francis Auburn, *Usenet News and the Law*, 1 WEB J. CURRENT LEGAL ISSUES (1995), *available at* http://webjcli.ncl.ac.uk/articles1/auburn1.html (discussing the failure of the Western Australia Supreme Court in Rindos v. Hardwick [No. 1994] (1994) to understand USENET and measure damages properly).

134. *See* http://cypherpunks.venona.com/date/1994/09/msg00304.html.

135. The October 1999 archive of the Linux Video and DVD Project (LiVid) mailing list was located at http://livid.on.openprojects.net/pipermail/livid-dev/1999-October but has subsequently been removed. An archived copy of this particular post is available at http://www.ccc.de/mirrors/cryptome.org/dvd-msgs.htm.

136. "The Secrets of Scientology" are regularly posted, anonymously, to the group, alt.religion.scientology. For example, on October 18, 2000, nobody@noisebox.remailer.org (an anonymous remailer account) posted a message, "How to Read a Meter on a Silent Subject," which was a copy of an internal document published by the Hubbard Communications Office.

message sizes that they will accept, thus very little dissemination of pirated music, movies, or software takes place via the remailer network. Nevertheless, textual works, including copies of Frank Herbert's "The Green Brain" and "The Eyes of Heisenberg" have been posted via anonymous remailer to Usenet where others may freely obtain copies of those copyrighted works.[137] Indeed, several of the Church of Scientology's secret doctrinal works are posted with such frequency to Usenet that the documents are effectively always accessible, even without resorting to archives. Finally, anonymous remailers are frequently accused of being used to distribute child pornography. While the incidence of this is very low, it remains possible for criminals to employ remailers to this effect. Remailers similarly provide an attractive avenue for sending death threats. Thus, for all their positive uses, remailers can and will be used for potentially actionable purposes, which raises the question of the legal implications of remailer technology.

III. LITIGATION NIGHTMARES: HUNTING AN ANONYMOUS PARTY

In the vast majority of traditional litigation, actions are brought against named defendants. How does one serve process on fido123@hotmail.com? What about nobody@remailer.org? Worse, how does one serve process on someone@xs4all.nl, who is ostensibly in the Netherlands, but may just as easily live in Libya?[138,139]

Beginning on March 25, 1998, a group of "anonymous" participants posted information about Raytheon to a Yahoo! Message Board dedicated to topics concerning Raytheon that the Massachusetts electronics firm claimed contained company secrets.[140] Assuming such names as RAYINSIDER, DITCHRAYTHEON, and RSCDeepthroat, the messages contained information "mostly about manpower projections and financial issues."[141] In February 1999, Raytheon filed suit against those employees as "John Does 1–21" for breach of employment agreements and misappropriation of trade secrets.[142] Raytheon's lawyers then traced the posters from Yahoo! to accounts at AOL, Microsoft, and other ISPs, from which they subpoenaed the identities of the John Does.[143] After obtaining the names of the posters, Raytheon

137. "The Green Brain" was posted to alt.fan.dune on July 14, 2001, by nobody@remailer.privacy.at and can be found at http://groups.google.com. "The Eyes of Heisenberg" was similarly posted on July 9, 2001, by remailer@remailer.xganon.com.

138. Registry of .com subdomains is not limited to the United States. Many foreign top-level domains similarly sell subdomains outside their country. The Kingdom of Tonga, for example, was one of the first top-level domains to offer subdomains under .to to outsiders. *See* http://www.tonic.to.

139. Personal jurisdictional issues may arise particularly when a John Doe is located outside the United States; however, this topic lies outside the scope of this Comment.

140. In fact, many of the messages posted in the forum were inaccurate or already publicly known. For example, "h12345678" posted a message on April 30, 1998, claiming "Raytheon win Missle-defense [sic] contract. Good news will be announce(d) tomorrow," when the contract was actually awarded to a competitor the next day. Another message, posted by "Rayman-mass" on October 21, 1998, stated that the company sold one of its units to DRS Technologies for $45 million. That deal had already been made public by Raytheon at the time of the post.

141. *Raytheon Sues 21 People over Sharing of Company Secrets Online*, Associated Press, March 5, 1999.

142. Raytheon Co. v. John Does 1–21, No. 99-816 (Super. Ct. Middlesex Cty., Mass. filed Feb. 1, 1999).

143. Under Massachusetts law, such discovery is permissible to obtain "testimony or documents or other things in an action pending" there. MASS. GEN. LAWS ANN. ch. 223A § 10(a) (West 2000). Other states and the Federal Rules of Civil Procedure have similar provisions. FED. R. CIV. P. 45.

dropped the suit,[144] later reporting that seventeen of the workers had entered "corporate counseling" and four had quit.[145]

What began as a handful of John Doe suits in the summer of 1998 mushroomed into a barrage of such suits by 1999.[146] For example, in May of 1999, Xircom, Inc., sought the identity of a Yahoo! user named "A_View_From_Within" who, purporting to be a company engineer, alleged that Xircom was poorly managed, losing talented staff, and manufacturing faulty products.[147] In November of 1999, Fruit of the Loom subpoenaed the identities of two Yahoo! handles who disparaged lobbying efforts by the company for a bill that would allow Fruit of the Loom to import certain items duty-free.[148] As David Sobel, general counsel at the Electronic Privacy Information Center has said, "The word is clearly out among in-house corporate counsel that this is the way to deal with the problem of online criticism."[149]

This use of the subpoena power is certainly not limited to corporate counsel. Individuals have also sought to serve subpoenas on ISPs for subscriber identities. After suffering a half-year campaign of "anonymous" electronic messages accusing him of covering up sexual assault, administrative failures, and using students to spy on faculty, the principal of Paramus Catholic High School in New Jersey filed suit against John Doe and sought to serve subpoenas on AOL and Hotmail, the services from which the postings originated.[150] A Denver lawyer likewise subpoenaed AOL for the identity of a person who filled the colobuffs.com website[151] with "anonymous" obscenities.[152]

Many ISPs have policies in place to protect the identity of their subscribers. Nevertheless, these policies do not contravene valid court orders, warrants, or subpoenas.[153] But what happens when an ISP is unable to divulge the identity of a subscriber? An aggrieved party may wish to sue the ISP directly, particularly if the ISP has deep pockets. The remainder of this Comment will address some of the ways an anonymous remailer might become the target of a lawsuit, and why neither policy nor the law support such suits.

---

144. Raytheon Co. v. John Does 1–21, No. 99-816 (Super Ct. Middlesex Cty., Mass. dismissed May 20, 1999).

145. *Raytheon Drops Internet Chat Suit*, Associated Press, May 24, 1999. The Raytheon incident raises serious questions about the potential for abuse of the discovery process. For a brief examination of the due process concerns involved in John Doe litigation, see David L. Sobel, *The Process that "John Doe" Is Due: Addressing the Legal Challenge to Internet Anonymity*, 5 VA. J.L. & TECH. 3 (2000).

146. Bruce P. Keller & Peter Johnson, *Online Anonymity: Who Is John Doe?*, ELECTRONIC COMMERCE & LAW REPORT, Volume 5 Number 3, January 19, 2000, at 70.

147. Xircom, Inc. v. John Doe, aka, "A_View_from_Within," No. Civ. 188724 (Cal. Super Ct. Ventura Cty. filed May 1999).

148. Elinor Abreu, *EPIC Blasts Yahoo for Identifying Posters*, THE INDUSTRY STANDARD, Nov. 10, 1999.

149. *Id.*

150. Vail v. Doe, No. 99-654(WHW) (D.N.J. filed Feb. 16, 1999); Steve Strunsku, *Suit Is Trying to Unmask a Principal's Accuser*, N.Y. TIMES, Feb. 28, 1999, at 6.

151. Ted Smith established the site to support the "Buffs," the University of Colorado football team.

152. Sue Lindsay, *Court Tells AOL to ID "John Doe,"* ROCKY MOUNTAIN NEWS, Dec. 23, 1998, at 21A.

153. For example, AOL "will not give out information that would link your screen names with your actual name..." with two exceptions: "We will release specific information about your account only to comply with valid legal process such as a search warrant, subpoena or court order, or in special cases such as a physical threat to you or others." AOL Privacy Policy, *at* http://legal.web.aol.com/policy/aolpol/privpol.html (last visited Nov. 1, 2001).

IV. REMAILER OPERATOR LIABILITY

Caselaw most closely addressing potential liabilities of anonymous remailer operators offers effectively no guidance to operators because it is complex and not specifically focused on the unique situation of the remailer operator. Nevertheless, several decisions address the liability of computer network and electronic bulletin board operators for legal violations that occur as the result of users of those online services. Because the operator of a computer network or electronic bulletin board is an actor once removed from the person directly responsible for the infraction of the relevant law, these cases may analogize in some fashion to the anonymous remailer operator who is in a similar situation. Moreover, recent laws addressing Internet Service Provider liability may also prove relevant.

A. Civil Liability

There are a number of theories under which an anonymous remailer operator might be sued. Copyright violations and defamation actions will be discussed primarily because they constitute the most prevalent abuses of remailer technology.[154]

1. Copyright Infringement

The Internet provides a means of inexpensive, accurate, and prompt distribution of digital information such that effectively anyone with access to an ordinary personal computer and a connection to the Internet can send or receive text, sound, images, software, and data with minimal effort. Access to the Internet can thus present an impressive challenge to laws that govern the dissemination and duplication of information.[155] A person with access to digital copyrighted material can duplicate, disseminate, and possibly even adapt such work. Commercial proprietors, or "content providers" of copyrighted works thus may view the Internet as a significant threat to their economic interests, particularly when each duplication of a work can arguably represent a copyright infringement.[156] Indeed, "[i]t has been estimated that tens of billions of dollars of revenue are lost each year to copyright infringements on the Internet."[157]

If a person makes a digital copy of a book available online, by posting a copy to Usenet, for example, providers arguably lose their ability to sell paper copies of that book to anyone who downloads the book. A single copyright infringement in this manner can easily translate into arguably hundreds or thousands of lost sales.[158]

Copyright laws reserve the right to distribute or reproduce copyrighted material to the copyright holder.[159] Thus, an argument can be made that under a theory of

---

154. The author hopes to publish further research on alternate liabilities at a later date.

155. *See* 17 U.S.C. § 106 (Supp. IV 1998).

156. *See* 17 U.S.C. § 106(4)-(6) (Supp. IV 1998) (granting the exclusive right to reproduce and distribute the copyrighted work to the copyright holder).

157. Marc S. Friedman et al., *Infojacking: Crimes on the Information Superhighway*, 40 N.J. L.J. 658, 658 (1995).

158. *See, e.g.*, Marobie-FL, Inc. v. National Ass'n of Fire Equip. Distribs., 983 F. Supp. 1167, 1171 (N.D. Ill. 1997).

159. 17 U.S.C. § 106 (reserving the rights of distribution and reproduction to the copyright owner). The theory

enterprise liability, anonymous remailer operators may be held liable for copyright violations committed by their users.[160] The argument follows that because the risk of copyright infringement is a natural byproduct of Internet service, anyone offering such service should internalize losses resulting from the risk of copyright infringement as a cost of doing business. Remailer operators would then be encouraged to deter copyright infringement and/or raise compensation for copyright infringements that would occur by spreading costs among many users.[161]

General liability can also be plausibly found under two copyright doctrines.[162] First, remailer operators may be directly liable for infringing acts of users because operators likely own the equipment that copy, store, and transmit copies of copyrighted material. Second, operators may be contributorily liable by knowingly providing Internet service to a user committing copyright infringement.

In 1998, Congress addressed the ambiguities of Internet service provider (ISP) liability for copyright infringement in the Digital Millennium Copyright Act (DMCA).[163] Instead of definitively answering the question of such liability, however, Congress left the underlying copyright law relatively untouched, incorporating a knotty set of "safe harbor" procedures that protect ISPs from liability so long as they adopt "good citizenship" policies. Under the DMCA, an ISP who removes allegedly infringing material from the Internet and terminates the account of that alleged infringer is "safe." Thus, under the current regime, an ISP *may* be liable for the behavior of its users, but may escape that liability by cooperating with parties alleging copyright infringement. However, because the DMCA deliberately avoids altering the underlying caselaw, and because an argument may be made that remailers and their operators do not likely fall under the ambit of the DMCA's statutory definition of an "ISP," an exploration of liability in the absence of the DMCA is important. Moreover, the DMCA's requirements and limitations on ISP liability are somewhat complicated. Situations thus may arise in which the DMCA's "safe harbor" provisions might not apply, even if remailers and their operators were covered by the statute. The following sections, therefore, address standard copyright doctrines under which a remailer operator might be liable for copyright infringement.

---

of enterprise liability holds that enterprise-creating risk should bear the burden of that risk as a cost of doing business. *See generally* George L. Priest, *The Invention of Enterprise Liability: A Critical History of the Intellectual Foundations of Modern Tort Law*, 14 J. LEGAL STUD. 461 (1985).

160. 17 U.S.C. § 501(a) (providing that violation of a copyright holder's exclusive rights constitutes copyright infringement). Though the copyright code reserves the rights of distribution and reproduction to copyright holders, those rights are limited by doctrines such as "fair use" and the "expression/idea dichotomy." Thus, a user "may" and not "shall" be liable for distributing or reproducing copyrighted material as tempered by the above limits. Many unauthorized uses of copyrighted material are legal. *See, e.g., id.* § 107 (excluding fair use from copyright infringement); *id.* § 102(b) (prohibiting copyright protection for ideas).

161. As it applies to Internet Service Providers, one prominent supporter of this type of liability has been a working group operated under President Clinton's Information Infrastructure Taskforce. *See* WORKING GROUP ON INTELLECTUAL PROPERTY RIGHTS, INFORMATION INFRASTRUCTURE TASKFORCE, INTELLECTUAL PROPERTY AND THE NATIONAL INFORMATION INFRASTRUCTURE at 1-6, 117-18 (1995) (hereinafter WORKING GROUP) (describing the Working Group's advocating ISP liability due to ISPs unique ability to spread costs among their users).

162. Vicarious liability is not applicable here because remailer operators derive no financial benefit from running an anonymous remailer.

163. 17 U.S.C. §§ 1201-1332 (Supp. IV 1998).

a. Strict Liability/Direct Infringement

A court might hold a remailer operator directly liable for copyright infringing behavior committed by one of its users simply because that operator provides some basic Internet services to that user. This theory is at least mildly plausible because remailer operators routinely and automatically reproduce and deliver copyrighted material when so requested by a subscriber. Each time a person uses a remailer to transmit a message, whether it is a copy of *Dune*, a photograph of Britney Spears, or a poem written by the message's author, the remailer duplicates the supplied material, sending copies through the Internet to the intended party. The remailer is necessarily an integral part in the transaction, because it receives copies of copyrighted material and forwards that material on to the intended recipient, either directly, or via another remailer. Each of these activities arguably infringes on the copyright holder's exclusive rights of distribution and reproduction. To date, however, this theory is only supported by *Playboy Enterprises, Inc. v. Frena.*[164] Indeed, in subsequent cases and commentary, the theory is discredited.

The defendant in *Frena* operated a bulletin board service (BBS) where subscribers connected via modem and could browse through and download material—mainly photographs—from the BBS for a fee.[165] Frena's subscribers could similarly upload material.[166] Copyrights on a number of the photographs contained on Frena's BBS were owned by Playboy. In part, Playboy sued Frena and made a successful motion for summary judgment on a claim of copyright infringement.[167] Frena argued that he had not personally uploaded any of the Playboy photographs to the BBS and further claimed to have removed any copyrighted material from the BBS as he became aware of it. The court specifically rejected this theory, holding that the BBS's automatic storage, copying, and distribution of the copyrighted images infringed on Playboy's exclusive rights.[168] In the court's words, "It does not matter that Defendant Frena may have been unaware of the copyright infringement. Intent to infringe is not needed to find copyright infringement. Intent or knowledge is not an element of infringement, and thus even an innocent infringer is liable for infringement...."[169]

Thus, if Frena were liable simply for passively accepting uploads from subscribers and for passively sending copies of those uploads to other subscribers, it is but a small step to move to a general rule in which anonymous remailer operators could be directly liable for copyright infringements caused by user instructions. Such a rule is highly problematic. While neither intent nor knowledge is an element of a claim for copyright infringement,[170] the irrelevance of intent or knowledge suggests a virtually unlimited scope of liability for a remailer operator

164. 839 F. Supp. 1552 (M.D. Fla. 1993).
165. *Id.* at 1554.
166. *Id.*
167. *Id.*
168. *Id.* at 1556-57.
169. *Id.* at 1559.
170. *See* Buck v. Jewell-La Salle Realty Co., 283 U.S. 191, 198-99 (U.S. 1931); Shapiro, Bernstein & Co. v. H. L. Green Co., 316 F.2d 304, 308 (2d Cir. 1964) (discussing strict liability in copyright); Singer v. Citibank N.A., No. 91 Civ. 4453, 1993 WL 177801 at *5 (S.D.N.Y. May 21, 1993) (noting that copyright infringement is a tort that generally does not require scienter).

who reproduces or distributes a copyrighted material, even when conducted as the passive result of executing user commands. As stated previously, when a user transmits an email message or makes a Usenet posting, that message may travel through several machines while en route to its intended recipient. If *Frena* were broadly applied, the owners of each of these machines would be directly liable for copyright infringement because they, like the primary infringer, "duplicated" and "sent" copyrighted material at the request of a third party.

Several courts have found the result in *Frena* extreme and have refused to follow its holding. For example, in *Religious Technology Center v. Netcom On-Line Communication Services, Inc.*,[171] the Northern District of California heard a direct liability claim against Netcom, an ISP, for duplicating and disseminating postings made to the Internet by Dennis Erlich, a user of a BBS.[172] The court specifically examined and rejected the approach in *Frena*, stating,

> Plaintiffs' theory would create many separate acts of infringement and, carried to its natural extreme, would lead to unreasonable liability....[P]laintiffs' theory further implicates a Usenet server that carries Erlich's message to other servers regardless of whether that server acts without any human intervention beyond the initial setting up of the system. It would also result in liability for every single Usenet server in the worldwide link of computers transmitting Erlich's message to every other computer. These parties, who are liable under plaintiffs' theory, do no more than operate or implement a system that is essential if Usenet messages are to be widely distributed. There is no need to construe the [Copyright] Act to make all of these parties infringers. Although copyright is a strict liability statute, there should still be some element of volition or causation which is lacking where a defendant's system is merely used to create a copy for a third party.[173]

The *Netcom* dismissal of *Frena* has been supported in subsequent cases,[174] and commentators have similarly supported *Netcom*'s reasoning.[175] Thus, while *Frena* has not been directly overruled, it is difficult to support a claim that an anonymous remailer operator could or should be held directly liable in copyright for providing service to infringing users.

b. Contributory Infringement

As mentioned above, in *Netcom*, a claim of copyright infringement was brought by the holders of the copyrights in the works of L. Ron Hubbard, the deceased founder of the Church of Scientology.[176] Defendant Dennis Erlich was a former

---

171. 907 F. Supp. 1361 (N.D. Cal. 1995).

172. *Id.* at 1365-67.

173. *Id.* at 1369-70.

174. *See* Marobie-FL, Inc. v. National Ass'n of Fire Equip. Distribs., 983 F. Supp. 1167, 1178 (N.D. Ill. 1997) (following *Netcom*); Sega Enters. v. MAPHIA, 948 F. Supp. 923, 931-32 n.5 (N.D. Cal. 1996) (following *Netcom* and explicitly negating any implication that a prior opinion in the same case established direct liability for infringement).

175. *See* 3 MELVILLE B. NIMMER & DAVID NIMMER, NIMMER ON COPYRIGHT § 12.04 [A][3][e], at 12-98 (1999); Bruce W. Sanford & Michael J. Lorenger, *Teaching an Old Dog New Tricks: The First Amendment in an Online World*, 28 CONN. L. REV. 1137, 1164 (1996) (describing the "tortured reasoning" of *Frena*).

176. 907 F. Supp. at 1371 and n.17.

Church minister and vocal critic of the Church. Erlich posted significant portions of copyrighted church doctrines in the Usenet group "alt.religion.scientology" as part of his critiques of the Church.[177] In addition to Erlich, the Church named as defendants Tom Klemesrud, the owner of support.com, the local computer bulletin board through which Erlich gained Internet access, and Netcom, another computer network that served as the connection between support.com and the Internet.[178] The court declined the plaintiffs' motion for a preliminary injunction against Klemesrud and Netcom, distinguishing between an actor who initiates a process that infringes a copyright and an actor who makes incidental copies automatically as part of the process of operating a computer network.[179] Though the court acknowledged the Copyright Act's strict liability nature,[180] it refused to interpret the statute in such a manner because unreasonable consequences would follow:

> Plaintiff's theory [of direct infringement] would create many separate acts of infringement and, carried to its natural extreme, would lead to unreasonable liability....It would also result in liability for every single Usenet server in the worldwide link of computers transmitting Erlich's message to every other computer....There is no need to construe the Act to make all of these parties infringers. Although copyright is a strict liability statute, there should still be some element of volition or causation which is lacking where a defendant's system is merely used to create a copy by a third party.[181]

As discussed above, the court in *Netcom* attacked *Frena* directly. The court reasoned that *Frena* was inadequate because only the original composer of an infringing message causes the infringement, whereas the network's actions are "automatic and indiscriminate."[182] The court also distinguished the facts of *Netcom* from *Frena*, noting that the *Frena* bulletin board operator maintained an archive of files for users and therefore arguably could have supplied a product.[183] The court stated,

> It would be especially inappropriate to hold liable a service that acts more like a conduit, in other words, one that does not itself keep an archive of files for more than a short duration. Finding such a service liable would involve an unreasonably broad construction of public distribution and display rights. No

177. *See Netcom*, 907 F. Supp. at 1365-66.

178. Both Klemesrud and Netcom ultimately settled. Klemesrud settled with the Church by agreeing to pay it $50,000 without an admission of liability. *See Internet Copyright Case Settled*, L.A. TIMES, Aug 23, 1996, at D2. Netcom established "a new protocol for handling such disagreements, including a system for removing suspect materials while it investigates whether a copyright violation has occurred." *Netcom, Scientologists Settle Suit over Internet Postings*, L.A. TIMES, Aug. 6, 1996, at D2.

179. *See Netcom*, 907 F. Supp. at 1368-69.

180. *See id.*, 907 F. Supp. at 1367 and n.10.

181. *Id.* at 1369-70. The court made a statement particularly relevant to anonymous remailers as "forwarders" of previously composed messages: "Every Usenet server has a role in the distribution, so plaintiffs' argument would create unreasonable liability. Where the BBS merely stores and passes along all messages sent by its subscribers and others, the BBS should not be seen as causing these works to be publicly distributed or displayed." *Id.* at 1372.

182. *Id.*

183. *See id.*

> purpose would be served by holding liable those who have no ability to control the information to which their subscribers have access....[184]

The *Netcom* decision thus advocates a copyright infringement theory limiting strict liability to the party initiating the process of copyright infringement—the author of the original message.

After rejecting the application of the strict liability theory to computer network operators, the court applied the theory of contributory copyright infringement. The contributory infringement theory fulfilled the court's test for the "element of volition or causation"[185] previously discussed in the opinion as the limited need to prevent the extension of unreasonable, worldwide liability.[186] Thus, whether Netcom could be held liable for the infringing acts of Erlich depended on whether Netcom's actions and status met the criteria for contributory copyright infringement: knowledge of, and material contribution to, the infringing act.[187] The court held that a service that "allows for the automatic distribution of all Usenet postings" and yet "does not completely relinquish control over how its system is used," meets the material contribution requirement.[188] Accordingly, the most important question of fact remaining was whether Netcom acquired knowledge of Erlich's copyright infringement with sufficient time to remedy the situation.[189] The court commented, "If plaintiffs can prove the knowledge element, Netcom will be liable for contributory infringement...."[190] Thus, the rule emerging from *Netcom* appears to be that a computer network operator is liable for copyright infringement caused by a user if, and only if, the operator has knowledge of the infringing use before it is too late to remedy that infringement.[191]

The anonymous remailer has the same features of automatic distribution and maintenance of some control by the administrator that the *Netcom* court found to be attributes sufficient to meet the material contribution requirement. Thus, under a *Netcom* contributory copyright infringement framework, the liability of remailer operators turns on their knowledge of users' infringing use. The operator of a modern remailer, however, cannot possibly have advance knowledge of a user's infringement. Due to the strong cryptography designed into the system, the operator has no way of knowing the content, much less whether or not that content infringes a copyright. Accordingly, any notification would be insufficient to allow the operator to "reasonably verify a claim of infringement."[192] Moreover, even if the message were sent in the clear, and every message were reviewed by the operator,

---

184. *Id.*

185. *Id.* at 1370.

186. *See id.* at 1372-73. Knowledge was precisely the limiting factor envisioned by the court as evidenced in the conclusion to its discussion of the direct infringement claim: "Because the court cannot see any meaningful distinction (without regard to knowledge) between what Netcom did and what every other Usenet server does, the court finds that Netcom cannot be held liable for direct infringement." *Id.* at 1373.

187. *See* Gershwin Publ'g Corp. v. Columbia Artists Management, Inc., 443 F.2d 1159, 1162 (2d Cir. 1971).

188. *Netcom*, 907 F. Supp. at 1375.

189. *See id.* at 1374.

190. *Id.*

191. The rule assumes that while most computer networks automatically create copies of messages posted to them, those operators still maintain some degree of control over those networks.

192. *Netcom*, 907 F. Supp. at 1374.

the remailer operator has no way of identifying or distinguishing individual users and thus no meaningful way of knowing whether or not the material infringes a copyright.[193]

c. The DMCA Confounds the Matter

Title II of the DMCA,[194] codified at section 512 of the Copyright Act, is Congress's response to the issue of ISP liability for subscriber infringement. The DMCA is cumbersome, disorganized, and flawed. Specifically, by leaving the underlying caselaw of ISP liability untouched, a complicated liability scheme was devised that has the effect of encouraging ISPs to remove alleged copyright infringements from the Internet. The possibility that courts will impose broad ISP liability is left open by the DMCA's failure to clarify the underlying law. Moreover, the peculiar nature of anonymous remailers leaves open the question of whether Title II of the DMCA is applicable to anonymous remailer operators at all.

The DMCA insulates ISPs from liability so long as they comply with certain statutory requirements designed to facilitate content providers' efforts to protect their copyrighted material.[195] The DMCA defines a "service provider" as "an entity offering the transmission, routing, or providing of connections for digital online communications, between or among points specified by a user, of material of the user's choosing, without modification to the content of the material as sent or received."[196] Based on such a definition, anonymous remailer operators and their systems appear to be service providers. A remailer operator constitutes an entity offering both "transmission" and "routing" of "digital online communications" by sending electronic messages from users between remailers and to final recipients as directed by the users.[197]

Congress plainly did not intend to address anonymous remailers as "service providers" under the DMCA, however. Section 512(a) insulates ISPs against liability for "transitory digital network communications" so long as five requirements are met. The first four requirements focus largely on the "automated" nature of the ISP's role in the transmission of infringing material. The final provision does as well, but its wording is troublesome when applied to an anonymous remailer. That provision requires that "the material is transmitted through the system or network without modification of its content."[198]

Adding or removing the headers of an encrypted message arguably does not alter the content of the message. This is similar to adding or removing the return address from the outside of an envelope. The content of a letter within the envelope remains unaltered. It is more difficult, however, to argue that the decryption of content that takes place at each link in the remailer chain does not alter "content," particularly

---

193. The court listed the following reasons why an operator would be unable to reasonably verify an infringement claim: "a possible fair use defense, the lack of copyright notices on the copies, or the copyright holder's failure to provide the documentation to show that there is a likely infringment...." *Id.*

194. 17 U.S.C. § 512 (Supp. IV 1998).

195. *See id.* §§ 512(a)-(d), (f), (g), (i).

196. *Id.* § 512(k)(1)(A).

197. Whether or not the remailing process constitutes "modification to the content of the material as sent or received" presents an intriguing question addressed in the main text of this Comment.

198. 17 U.S.C. § 512(a)(5).

in the final hop. It is arguable that the original message drafted by the remailer user and the final message as received by the intended recipient are the same. This would equate the remailing process to data encoding, whereby content in one format may be "translated" into another format.[199] Navigating down this maze leads only to more sharp corners, however.[200]

To qualify for immunity from infringement liability under the DMCA, 17 USC § 512(i)(1) outlines "conditions for eligibility" where the ISP,

> (A) has adopted and reasonably implemented, and informs subscribers and account holders of the service provider's system or network of, a policy that prόvides for the termination in appropriate circumstances of subscribers and account holders of the service provider's system or network who are repeat infringers; and
> (B) accommodates and does not interfere with standard technical measures.

Ignoring the question of what "appropriate circumstances" might entail, it is important to note that the statute no longer references "users," but the more strict terms of "subscribers" and "account holders." The section defines "standard technical measures" but does not describe "subscribers" or "account holders." An anonymous remailer has neither "subscribers" nor "account holders." Both terms seem to indicate identifiability, or at least distinction, between the assorted users of the system. Moreover, the term "subscribers" appears to imply some form of monetary compensation in exchange for services, again, not applicable to anonymous remailer operators.

Finally, some of the remedies set forth in 17 U.S.C. § 512(j)(1) represent problems similar to those in Section 512(i)(1). Specifically, under Section (j)(1)(A)(ii), a court may grant injunctive relief "with respect to a service provider" by "restraining the service provider from providing access to a subscriber or account holder of the service provider's system or network who is engaging in infringing activity and is identified in the order, by terminating the accounts of the subscriber or account holder that are specified in that order." This subsection is rendered meaningless in the face of a service in which a single "account" (nobody@remailer.somewhere.com) is shared by an unidentifiable number of anonymous users.[201] Most importantly, of course, this provision requires identification of the "account holder," which is impossible for a number of reasons.[202] In short, attempting to apply Title II of the DMCA to anonymous

---

199. An example of data translation is authoring a letter using only lowercase letters, then "encoding" the letter entirely in capital letters, leaving the content unchanged.

200. Suppose Alice writes a message containing the text of a copyrighted poem and prepares it for remailing by creating a nested, encrypted version of that message. Is Alice's "content" the plaintext message, or is it instead the nested, encrypted version? The first remailer only sees the nested, encrypted version. Each remailer necessarily must modify the message body in order to properly process and send on the message. But somewhere down the chain, the nested, encrypted version is ultimately turned back into the original, copyrighted poem, otherwise a remailer operator could not observe the infringement. How can one reconcile with the statute an automated process that relies on content modification in the "passive" transmission of that data?

201. The situation is further confounded when one considers that some anonymous remailers have web-based "frontends." At http://mixmaster.shinn.net, for example, one may obtain a list of frontends that allows users to paste their messages into a web form, which will then be processed through the underlying remailer.

202. This includes both the fact that an undetermined number of users make use of a remailer and that the

remailer operators is futile. Thus, in recognition of this futility, this Comment suggests that any potential copyright infringement actions brought against anonymous remailer operators be governed by caselaw as exemplified in *Netcom*.

2. Defamation

As with copyright liability, a remailer operator's liability for defamatory acts of users is murky. Also parallel to the field of copyright, analysis under both caselaw and federal statute proves necessary due, inter alia, to the questionability of a remailer's status as an ISP.

Though parties are not in a position to physically harm one another, electronic communications can amount to "fighting words" nevertheless. This behavior, known as "flaming," can rapidly deteriorate into statements that can easily be disseminated widely across the network. Flaming is particularly prevalent in Usenet and other communal settings. Not limited to character statements, negative product reviews, and unfavorable comments about a company's performance or management can also be made online.

The relevant cases have yielded a mixed message for defendants: one network incurred liability, while the other escaped. The crucial distinction here, however, was whether the court viewed the computer network as a publisher or a distributor of the defamatory material, for the standards of liability between the two differ.[203] If a court finds a defamation defendant to be a distributor or otherwise in the role of a bookseller, then the First Amendment precludes liability without the ISP's knowledge of the underlying defamatory nature of the material.[204] If, however, a court finds a party to be akin to a publisher, First Amendment concerns become significantly less important, thus the party may be held liable despite lack of knowledge of the defamatory character of the material. The precise distinction between publisher and distributor proves important.

a. Distributor

In *Cubby, Inc. v. CompuServe Inc.*,[205] the plaintiff ran a bulletin board service on CompuServe's Journalism Forum called "Skuttlebutt." When a rival bulletin board

---

identities of those people is necessarily unknown.

203. The difference stems from Smith v. California, 361 U.S. 147 (1959). There, the Supreme Court considered the application of a criminal statute that prohibited the possession of obscene materials by booksellers, regardless of whether they knew the contents of the obscene book. *See id.* at 149. The Court concluded that the lack of a scienter element in the statute "imposed a restriction upon the distribution of constitutionally protected as well as obscene literature," and held the statute unconstitutional. *Id.* at 153. The court further found that

> [i]f the contents of bookshops and periodical stands were restricted to material of which their proprietors had made an inspection, they might be depleted indeed. The bookseller's limitation in the amount of reading material which he could familiarize himself, and his timidity in the face of his absolute criminal liability, thus would tend to restrict the public's access to forms of the printed word which the State could not constitutionally suppress directly.

Id. at 153-54.

204. *See, e.g.*, Cubby, Inc. v. Compuserve Inc., 776 F. Supp. 135, 139 (S.D.N.Y. 1991) (stating that "[t]he requirement that a distributor must have knowledge of the contents of a publication before liability can be imposed for distributing that publication is deeply rooted in the First Amendment...").

205. 776 F. Supp. 135 (S.D.N.Y. 1991).

derided it as a "start-up scam," Skuttlebutt sued CompuServe for libel.[206] The central issue in the case was whether CompuServe was a publisher or distributor of the defamatory material, because it could be subject to liability only if it were viewed as the former. Under New York law, a party considered equivalent to a distributor may be subject to liability only if the party knew or had reason to know of the defamatory material.[207] The district court, citing *Smith v. California*,[208] explained that the standard for defamation liability was rooted in the First Amendment because strict liability for defamatory messages would restrict free expression in an unconstitutional manner. Next, the court found that factors such as CompuServe's lack of editorial control over the contents of the publications it carried on its server, as well as the impracticability of examining every publication for potentially defamatory statements favored a ruling that CompuServe was the "functional equivalent of a more traditional news vendor."[209] The court then invoked the standard of liability applicable to the traditional news distributor or bookseller, defining the legal standard of liability for computer network operators like CompuServe as "whether it knew or had reason to know of the allegedly defamatory...statements."[210] Because the complaint did not allege that CompuServe knew or had reason to know of the false and defamatory statements made about the plaintiffs, the court granted CompuServe's motion for summary judgment.[211]

b. Publisher

Stratton Oakmont, Inc. v. Prodigy Services Co.[212] addressed the liability of an online service provider who purported to exercise editorial power over its subscribers. In that case, postings accusing a securities firm of fraudulent and criminal acts were made in a Prodigy bulletin board forum.[213] Though the New York state court found that "[c]omputer bulletin boards should generally be regarded in the same context as book stores, libraries and network affiliates," it held Prodigy to be the equivalent of a publisher and therefore subject to strict liability for the defamatory statements.[214] The court distinguished *Cubby* in two ways. First, unlike CompuServe, Prodigy "held itself out to the public and its members as controlling the content of its computer bulletin boards."[215] Second, Prodigy used both software screening and human control to fulfill its promise to regulate the content of its electronic bulletin boards.[216] These two factors suggested to the court that Prodigy

206. *See id.* at 138.
207. *See id.* at 139.
208. 361 U.S. at 147.
209. *Cubby*, 776 F. Supp. at 140.
210. *Id.* at 141.
211. *See id.*
212. 23 Media L. Rep. (BNA) 1794 (N.Y. Sup. Ct. May 25, 1995).
213. *See id.* at 1795.
214. *Id.* at 1798.
215. *Id.* at 1797. In fact, Prodigy described its service and content guidelines by an analogy to a newspaper: "Certainly no responsible newspaper does less when it chooses the type of advertising it publishes, the letters it prints, the degree of nudity and unsupported gossip its editors tolerate." *Id.* at 1795.
216. Prodigy software screened all postings for offensive language. *See id.* at 1796. Prodigy also employed a human "Board Leader," charged with the task of enforcing content guidelines by way of a manual emergency delete power. *See id.*

exercised editorial control over its service and thus, for purposes of the plaintiff's claims, Prodigy was a publisher. The court was unmoved by the fact that many of Prodigy's editorial decisions did not occur until after a complaint was received. The court found that the response to complaints of defamatory material constituted editorial control sufficient to incur liability as a publisher.[217]

c. Communications Decency Act of 1996

Congress resolved the opposing rules of *Cubby* and *Stratton Oakmont* by granting ISPs limited statutory immunity from liability for third party-created content. Under 47 U.S.C. § 230, "[n]o provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider."[218] Though the statute clearly seeks to protect a traditional ISP such as Prodigy, whether the statute applies to anonymous remailers requires further analysis.

The term "interactive computer service" may or may not apply to anonymous remailers. The statutory definition explains that

> "interactive computer service" means any information service, system, or access software provider that provides or enables computer access by multiple users to a computer server, including specifically a service or system that provides access to the Internet and such systems operated or services offered by libraries or educational institutions.[219]

Certainly the services offered by a provider such as Prodigy and an anonymous remailer are different. Through the use of a system such as Prodigy, an individual user may gain access to and view information. A remailer, however, provides or enables access only in the sense that an individual user will use the remailer to facilitate transmission of a communication. The remailer user does not access or view any information via the remailer. Thus, it is possible that the statute does not apply to anonymous remailers, meaning that the publisher/distributor determination in *Cubby* and *Stratton Oakmont* would remain relevant. Modern remailer technology does not allow a remailer operator to take editorial control of messages flowing through the remailer. Because the messages are encrypted, the operator cannot review or screen the messages for content, even if the operator so desires. Thus, it appears that under *Cubby* and *Stratton Oakmont*, a remailer operator cannot be held liable for defaming acts committed by users.

Interpretation of the statute could also favor inclusion of a remailer as a service provider, however. Certainly, the remailer enables "access by multiple users to a computer server," in the sense that multiple users may use a remailer to transmit messages to Usenet. If the statute were interpreted to apply to remailers generally, though, the extent of protection offered by the statute remains unclear. The provision is found in a section entitled, "Online Family Empowerment,"[220] and one of the main purposes of the statute is "to remove disincentives for the development

217. *See id.* at 1797.
218. 47 U.S.C. § 230(c)(1) (1998 Supp. IV).
219. *Id.* at § 230(f)(2).
220. *Id.* at § 230.

and utilization of blocking and filtering technologies that empower parents to restrict their children's access to objectionable or inappropriate online material."[221] Thus, the primary harm sought to be remedied by the statute appears to have been *Stratton Oakmont*'s effect of discouraging efforts by network operators like Prodigy to filter out material objectionable or inappropriate for children. The statute does not, however, appear concerned with a similar harm resulting from defamatory materials,[222] thereby making examination of the general rule in *Cubby* and *Stratton Oakmont* necessary.

Ultimately, the *Cubby* and *Stratton Oakmont* decisions suggest a list of factors that might be used by a future court in making a determination of whether a remailer constitutes a distributor or publisher for purposes of assessing liability for defamation: (1) the degree of editorial control exercised by the network, (2) the degree of editorial control advertised by the network, and (3) the practicality of examining the contents of messages on the network. As discussed above, modern remailers prevent content examination by operators, and thus remailers appear to fall squarely into the distributor category.

B. Criminal Liability

Criminal threats, harassing, stalking, extortion, and hate speech could all potentially be conducted via an anonymous remailer. Indeed, the number of crimes that can potentially be committed via a remailer is sufficiently large that it exceeds the scope of this Comment. Of the legal problems associated with the Internet, however, criminal acts involving the transmission of obscene materials have generated the most public attention.[223] Thus, this section will focus on federal criminal provisions involving the receipt, possession, sale, and distribution of child pornography as an example of potential criminal liability.[224]

There appears to be very little evidence of child pornographers employing anonymous remailers in their trade. Nevertheless, such a use of remailer technology is possible and has been sufficiently popular in the media[225] to warrant discussion.

---

221. *Id.* at § 230(b)(4).

222. The relevant legislative history states,

> One of the specific purposes of this section is to overrule Stratton-Oakmont v. Prodigy and any other similar decisions which have treated such providers and users as publishers or speakers of content that is not their own because they have restricted access to objectionable material. The conferees believe that such decisions create serious obstacles to the important federal policy of empowering parents to determine the content of communications their children receive through interactive computer services.

H.R. CONF. REP. NO. 104-458, at 194 (1996), reprinted in 1996 U.S.C.C.A.N. 124, 208.

223. *See, e.g., Cyberporn Hearings Begin in Senate*, OMAHA WORLD-HERALD, July 25, 1995, at 5 (discussing the rise of child pornography trafficking on computer networks); Jared Sandberg & Glen R. Simpson, *FBI Crackdown on Computer Child Pornography Opens Hornet's Nest, Stinging America Online*, WALL ST. J., Sept. 15, 1995, at A16 (describing crackdown on online child pornography).

224. *See, e.g.*, 18 U.S.C. § 2252 (1994) (provision on "[c]ertain activities relating to material involving the sexual exploitation of minors").

225. *See, e.g.*, Charles Arthur, *Pornographers on Internet Skilled at Covering Tracks: Network Impossible to Censor*, INDEPENDENT, July 27, 1995, at 3 (discussing the "enormously difficult task" of tracking down pedophiles who "can use 'anonymous remailers'—computers which receive messages and strip off the details of their sender, before forwarding it elsewhere on the network"); Helen Nowicka, *Innovations: Vice Squad Cleans Up the Superhighway*, DAILY TELEGRAPH, June 27, 1995, at 16 (describing discovery by West Midlands vice unit that

Section 2252 of 18 U.S.C. provides for the punishment of one who "knowingly transports or ships in interstate or foreign commerce by any means including by computer" the materials defined therein to constitute child pornography.[226] Similarly, Section 2252 also criminalizes the acts of one who "knowingly receives, or distributes...by any means including by computer" any visual image of child pornography that has traveled in the channels of interstate or foreign commerce; or "knowingly reproduces...by any means including by computer" such a visual image for distribution in the channels of interstate or foreign commerce.[227] Thus, provided that the original sender "knows" that he or she has transported, shipped, distributed, or reproduced an illegal image by sending it to a remailer, that person is criminally liable under the statute.[228]

Criminal liability for the remailer operator, however, depends on whether "knowingly" is read to apply beyond the enumerated action verbs of the statute—transports, ships, receives, distributes, or reproduces. Certainly, the remailer operator knows that the remailer receives, distributes, and reproduces all messages sent to it by a user. Thus, if the statute were interpreted to require knowledge only of the act of transmission, or of receipt or reproduction, a remailer operator would be criminally liable under Section 2252. Because messages sent through anonymous remailers are encrypted, however, remailer operators should never know the contents of the messages sent through their remailers.

This general knowledge requirement was at issue in *United States v. X-Citement Video, Inc.*[229] In that case, respondent, the owner and operator of X-Citement Video, Inc., argued that Section 2252 lacked a requirement of knowledge of performers' ages and was thus facially unconstitutional under the First Amendment. The Court found limiting "knowingly" to only the relevant statutory verbs would, in some applications, "produce results that were not merely odd, but positively absurd."[230] Moreover, the court stated that criminal statutes are interpreted "to include broadly applicable scienter requirements,"[231] and that the legislative history indicated that the term "knowingly" should apply to the "requirement that the depiction be of sexually explicit conduct."[232] Taking these factors together with its pronouncement that the statute should be interpreted so as to avoid constitutional doubts,[233] the Court held that "the term 'knowingly' in Section 2252 extends both to the sexually

---

"(c)hild pornographers conceal their actions by sending encrypted images, or having their electronic address removed by an anonymous remailer"); Peter H. Lewis, *Despite a New Plan For Cooling It Off, Cybersex Stays Hot*, N.Y. TIMES, Mar. 26, 1995, at 34 (describing the difficulties of tracking down traffickers in pornographic material on the Internet because users can "easily route their messages through so-called anonymous remailers who hide their identities").

226. 18 U.S.C. § 2252(a)(1). Section 2252 does not invoke the term "child pornography." It instead prohibits acts such as transporting and shipping "visual depiction[s], if—(A) the producing of such visual depiction involves the use of a minor engaging in sexually explicit conduct; and (B) such visual depiction is of such conduct." *Id.* This language is repeated throughout the statute. *See id.* § 2252(a)(2), (3)(B), (4)(B).

227. *Id.* § 2252(a)(2).

228. The original sender may also be liable under the later subsections of Section 2252, which criminalizes the intent to sell or possess three or more types of media containing such visual images. *See id.* § 2252(a)(3)(4).

229. 513 U.S. 64 (1994).

230. *Id.* at 69.

231. *Id.* at 70.

232. *Id.* at 77.

233. *See id.* at 78.

explicit nature of the material and to the age of the performers."[234] As interpreted in X-Citement Video, then, Section 2252 would not apply to modern remailer operators who do not possess knowledge of the contents of messages that pass through their systems—including the ages of performers in any sexually explicit material potentially contained therein.

As stated above, virtually all of the crimes that could potentially be committed via an anonymous remailer would require some degree of knowledge on the part of the operator before inculpating that operator. Thus, under current caselaw, criminal charges directed at an operator of a modern remailer for the acts of users appears misplaced. This leaves open a wide question of how to prosecute crimes perpetrated by remailer users.

V. FIGHTING ANONYMITY AT THE STATE LEVEL

Proposals to regulate Internet content within the United States face several formidable hurdles including the Constitution, technical constraints, and a strong and diverse public opposition. On the Internet, a law prohibiting anonymous speech is not only of dubious constitutionality; it verges on incoherence. If a state seriously contemplates prohibiting such communications, something other than a law prohibiting "anonymous communication" is required. This is so because perfect anonymity fatally challenges the enforceability of any laws prohibiting perfect anonymity.[235]

Nevertheless, worry over the potential for inexpensive, ubiquitous access to means of avoiding accountability for one's speech has led to increasing attempts to regulate anonymous communication. For example, in 1995, Pennsylvania enacted a statute making it illegal to possess, program, or use any device that could be used to "conceal or to assist another to conceal...the origin or destination of any telecommunication."[236]

In 1996, the legislature of the state of Georgia passed, by an overwhelming margin, a statute specifically aimed at combating anonymity online.[237] The Georgia law provided that it was illegal for any person "knowingly to transmit any data through a computer network...if such data uses any individual name, trade name, registered trademark, logo, legal or official seal, or copyrighted symbol to falsely identify the person, organization, or representative transmitting such data."[238] The bill's supporters argued that it had "nothing to do with censorship of information on the Net. It has to do with the identification of people who have the information."[239]

---

234. *Id.*

235. The decentralized architecture of distributed networks and the difficulties of applying physically based notions of personal jurisdiction in an environment in which physical boundaries are difficult, if not impossible, to identify, make direct enforcement of legal rules against individual violators more difficult once the means to accomplish such violations is widely disseminated.

236. *See* S. Res. 655, 179th Gen. Assem., 1995-96 Reg. Sess. (Pa. 1995) (amending 18 PA. CONS. STAT. § 910(a)(1)).

237. Act No. 1029, 1996 Ga. Laws 1505-06, codified at GA. CODE ANN. § 16-9-93.1 (1996).

238. GA. CODE ANN. § 16-9-93.1(a).

239. *See* Michael E. Kannell, *The AJC's Daily Online Guide: Bill Aims to Protect Logos, Trademarks*, ATLANTA J. & CONST., Mar. 19, 1996, at C3.

When challenged in federal court by the ACLU and twelve other organizations and individuals,[240] Georgia insisted that the legislation did not impose unconstitutional content-based restrictions on the right to communicate anonymously.[241] Instead, the state claimed that the legislation forbade only "fraudulent transmissions or the appropriation of the identity of another person or entity for some improper purpose."[242] Indeed, the bill's sponsor claimed that the legislation was not intended to apply to "fictitious or pen names or anonymous communications on the Internet."[243] The plaintiffs asserted an impressive number of pro-anonymity arguments against the law,[244] including arguments that the Georgia law violated the federal Commerce Clause.[245] This argument was based on four points. First, the plaintiffs explained that the Georgia law permitted prosecutions in any Georgia county where prohibited communications originated, were received, or simply passed through.[246] Therefore, the law applied to communications as diverse as chat rooms, discussion groups, and bulletin boards originating anywhere in the world, simply because they could be accessed in Georgia.[247] Second, provided that the message was relayed through an in-state computer, the law applied to communications between people entirely outside Georgia's borders.[248] Third, because the Internet generally lacks geographic markers that allow users to know when they access a website hosted in Georgia, the law potentially affected every World Wide Web user regardless of location.[249] Finally, because no publisher could prevent Georgia users from accessing particular web sites,[250] every publisher, regardless of location, would be required to comply with Georgia law.[251] Thus, the plaintiffs argued that the restrictions imposed by the Georgia law constituted a direct regulation of interstate commerce and were per se violations of the Commerce Clause.[252] The plaintiffs argued an alternative Commerce Clause violation by suggesting that the law burdened interstate commerce in excess of any local benefit.[253] Plaintiffs explained that under *Pike v. Bruce Church, Inc.*, Georgia had no legitimate interest in regulating Internet communications outside the state.[254] Moreover, plaintiffs asserted that if each of the states were permitted to regulate the Internet in the manner that Georgia had attempted, the result would cause "just the

240. *See* Art Kramer, *Courts Overturn Internet Laws in Georgia, New York*, ATLANTA J. & CONST., June 21, 1997, at C4.

241. *See* ACLU of Ga. v. Miller, 977 F. Supp. 1228, 1231 (N.D. Ga. 1997).

242. *Id.*

243. Brief in Opposition to Plaintiffs' Motion for Preliminary Injunction, ACLU of Ga. v. Miller, 977 F. Supp. 1228 (N.D. Ga. 1997) (No. Civ.A.1: 96 V2475MHS).

244. For a thorough treatment of these arguments, see Donald J. Karl, *State Regulation of Anonymous Internet Use after ACLU of Georgia v. Miller*, 30 ARIZ. ST. L.J. 513, 518-21 (1998).

245. *See* Brief in Support of Motion for Preliminary Injunction at 1, ACLU of Ga. v. Miller, 977 F. Supp. 1228 (N.D. Ga. 1997)(No. CIV.A.1:96CV2475MHS), *available at* http://www.aclu.org/issues/cyber/censor/GABRIEF.html [hereinafter Plaintiffs' Supporting Brief].

246. *See* Plaintiffs' Supporting Brief, at 12-13.

247. *See id.* at 13.

248. *See id.*

249. *See id.*

250. *See id.*

251. *See id.*

252. *See id.*

253. *See id.*

254. *See id.*

kind of competing and interlocking local economic regulation that the Commerce Clause was meant to preclude."[255]

Finding the statute overbroad, the district court enjoined the enforcement of section 16-9-93.1 on August 7, 1997.[256] Stating that the plaintiffs had "demonstrated a substantial threat of irreparable injury...[due to] self-censorship,"[257] the federal court found that the plaintiffs were likely to prevail on their First Amendment claims[258] and did not address the Commerce Clause challenge. A federal court in New York, however, subsequently addressed state Internet regulation under the Commerce Clause,[259] raising issues closely parallel to those in *Miller*.

The New York legislature criminalized intentionally communicating with a minor over a computer network and transferring to the minor any communication that "in whole or in part, depicts actual or simulated nudity, sexual conduct or sado-masochistic abuse, and which is harmful to minors."[260] Like the plaintiffs in *Miller*, the plaintiffs in *Pataki* complained that the New York statute unconstitutionally infringed on their First Amendment rights and that it violated the Commerce Clause.[261] The New York federal court followed a course opposite that in *Miller*, striking down the statute under the Commerce Clause, failing to reach the First Amendment questions.[262] As a prelude to its analysis of the Commerce Clause, the federal district court described the nature of the Internet in detail[263] as a decentralized network, with vast quantities of "people, institutions, corporations, and governments all across the world" linked together.[264] Moreover, despite the "inventiveness that has made this complex of resources available to just about anyone," the court explained that the Internet is subject to "traditional legal principles" that are adaptable for use online.[265] In the court's view, the Internet fits "easily within the parameters of interests traditionally protected by the Commerce Clause."[266] Applying three principles of Commerce Clause jurisprudence, the court ultimately found New York's attempted Internet regulation unconstitutional.[267] The final principle, that an Internet user must "self-censor or risk prosecution, a Hobson's choice that imposes an unreasonable restriction on interstate commerce,"[268] is potentially the most important to future state Internet regulation, including regulation of anonymous remailers.

---

255. *Id.*
256. *See Miller*, 977 F. Supp. at 1235.
257. *Id.*
258. *See id.* at 1232.
259. *See* American Libraries Ass'n v. Pataki, 969 F. Supp. 160 (S.D.N.Y. 1997).
260. *Id.* at 163.
261. *See id.* at 161.
262. *See id.* at 183.
263. *See id.* at 164-67.
264. *Id.* at 164.
265. *Id.* at 167.
266. *Id.*
267. *See id.* 183-84.
268. *Id.* (quoting Allen B. DuMont Labs, Inc. v. Carroll, 86 F. Supp. 813, 816 (1949)).

The Commerce Clause was written by the Framers to prevent individual states from overreaching their authority, thereby jeopardizing the nation's growth by crippling the national communications and trade infrastructure.[269]

> The Commerce Clause is more than an affirmative grant of power to Congress. As long ago as 1824, Justice Johnson in his concurring opinion in *Gibbons v. Ogden*, recognized that the Commerce Clause has a negative sweep as well. In what commentators have come to term its negative or "dormant" aspect, the Commerce Clause restricts the individual states' interference with the flow of interstate commerce....[C]ourts have long held that state regulation of those aspects of commerce that by their unique nature demand cohesive national treatment is offensive to the Commerce Clause.[270]

The Internet is a crucial part of the national communications infrastructure. Internet regulation thus requires cooperation on a national, if not global scale to be effective.[271] Were individual states permitted to regulate the Internet, "uncoordinated state regulation" would hamper further Internet development that depends on predictable results of Internet use.[272]

The Internet is no different in New York than it is in Georgia or New Mexico. Thus, it is the Internet's prominence in the national communications and trade infrastructure that ultimately forecloses state regulation of anonymous remailers under the Commerce Clause.

VI. FEDERAL "SOLUTIONS"

At the opening of Senate hearings on "Mayhem Manuals and the Internet," Senator Arlen Specter remarked,

> Among those who communicate on the Internet are purveyors of hate and violence. Among the full text offerings on the Internet are detailed instruction books describing how to manufacture a bomb...Anyone with access to the Internet can obtain this recipe for disaster, even a 10-year-old child who can find a glass container and some gasoline...There are also electronic mail discussion groups where information on bomb making can be traded anonymously. One disgusting example is this anonymous message posted on an Internet electronic bulletin board shortly after the Oklahoma City bombing: "Are you interested in receiving information detailing the components and materials needed to construct a bomb identical to the one used in Oklahoma[?]" The information specifically details the construction, deployment, and detonation of high-powered explosives....The individual who posted this message, who cowers in anonymity, deserves condemnation for using the Internet to suggest how the Oklahoma City bombing "could have been better." This is just one of many other examples....Among the issues before us are the extent of such usage of the Internet and whether anything can or should be done to curb it."[273]

---

269. *See id.* at 169.
270. *Id.* (citations omitted).
271. *Id.* at 181.
272. *Id.* at 183.
273. *Hearings on "Mayhem Manuals and the Internet" before the Subcommittee on Terrorism, Technology and Government Information of the Senate Judiciary Committee*, 1995 WL 311682 (FDCH) (May 11, 1995)

The Supreme Court has not yet had the opportunity to consider a narrowly tailored statute restricting Internet anonymity.[274] Nevertheless, as Senator Specter's remarks illustrate, the Court may be presented with an anonymity-based question in the near future. The direction in which such a ruling might lean may be divined from the Court's opinion in *Reno v. ACLU*,[275] striking down portions of the Communications Decency Act (CDA). In that case, the Court noted that the Internet constitutes "a unique and wholly new medium of worldwide human communication...located in no particular geographical location but available to anyone, anywhere in the world."[276] It further noted that the Internet "can hardly be considered a 'scarce' expressive commodity" because it provides "relatively unlimited, low-cost capacity for communication of all kinds."[277] This was relevant because "scarce" commodities, such as radio and television frequencies, have limited bandwidth[278] and are subject to strict government regulation. The proponents of the CDA claimed that the law would protect children while promoting cyberspace expansion.[279] The Court disagreed. It found that the CDA "lack[ed] the precision that the First Amendment requires when a statute regulates the content of speech," and therefore acted as a hindrance on the desired expansion of Internet communication.[280] The Court noted that "[a]s a matter of constitutional tradition, in the absence of evidence to the contrary, we presume that governmental regulation of the content of speech is more likely to interfere with the free exchange of ideas than to encourage it."[281]

Based on the Supreme Court's current sentiment, a ban on Internet anonymity, of the sort required to prohibit use of modern remailers, will likely fail. This is probable because such a law could not be sufficiently narrowly tailored, focused on specific problem areas, or non-detrimental to the expansion of the medium, as discussed at greater length in section VI.C. Short of such a ruling, however, a further examination of regulatory proposals is necessary.

A. Regulatory Control

The harms attendant on anonymous speech are often more easily recognized and more impressive[282] than the often subtle benefits that it may produce. In *McIntyre*, Justice Ginsburg left open the possibility that the Ohio disclosure requirement might be constitutionally permissible in a different context:

> The Court's decision finds unnecessary, overintrusive, and inconsistent with American ideals the State's imposition of a fine on an individual leafleteer who,

---

(statement of Senator Arlen Specter).

274. *See* Karl, *supra* note 244, at 533.

275. 521 U.S. 844 (1997).

276. *Id.* at 850-51.

277. *Id.* at 870.

278. *Cf.* NICHOLAS NEGROPONTE, BEING DIGITAL 4, 23-24 (1995).

279. *Reno*, 521 U.S. at 885.

280. *Id.* at 874.

281. *Id.* at 885.

282. It is not difficult to foresee a day when law enforcement authorities will report that a serious crime has been planned by means of anonymous electronic communication. It is further not difficult to imagine the popular press reacting with horror, intensifying calls for prohibition of this mode of communication.

> within her local community, spoke her mind, but sometimes not her name. We do not thereby hold that the State may not in other, larger circumstances require the speaker to disclose its interest by disclosing its identity.[283]

One could argue that the Internet constitutes one of those "larger circumstances." That is, the harms flowing from the easy availability of truly anonymous speech on distributed networks—the ability to freely disclose trade secrets, terrorist plots, or child pornography without fear of law enforcement intrusion—have increased so substantially that they are precisely equal to the benefits flowing from that speech.

As a general matter, information about the identity of the author of an email message does not appear to be protected under U.S. law. While the Electronic Communications Privacy Act[284] prohibits (with certain exceptions) the disclosure of "the contents of any...electronic communication,"[285] the statute does not similarly protect the name or address of the originator of the message. Accordingly, it does not appear that third-party system operators or administrators have a statutory duty to disclose, or to refrain from disclosing, such information.

Some propose that the most effective way of controlling anonymous remailers is to require remailer operators to keep records of sender identities.[286] Such a system might include an "incentive" whereby the remailer operator would be guaranteed "protection from civil and criminal liability when the administrator (1) has acted in good faith, and (2) voluntarily discloses to the authorities the identity of a user engaging in illegal activities."[287] This sort of proposal will not work for a number of reasons.

First, a necessary byproduct of such a proposal is the criminalization of running a remailer without maintaining logs. Such proposals neglect to address the strong cryptography underlying the modern remailer network. As implemented, law enforcement may be presented copies of all data passing through a network and still be unable to recover the identity of users.[288] Short of mandated key escrow, or an outright ban on strong cryptography,[289] any logging system will fail. There are numerous technical implications of requiring a system administrator to maintain

---

283. *McIntyre*, 514 U.S. at 358 (Ginsburg, J., concurring).

284. 18 U.S.C. §§ 2510-2521(1994).

285. 18 U.S.C. §§ 2511(c), 2511(e)(i).

286. *See* Noah Levine, Note, *Establishing Legal Accountability for Anonymous Communication in Cyberspace*, 96 COLUM. L. REV., 1526, 1561 (1996).

287. *Id.* at 1563.

288. This is by design. The modern remailer network was constructed to withstand attacks by the most powerful of adversaries, an organization such as the National Security Agency, which is assumed to have the capabilities of recording all traffic on the Internet.

289. The FBI is constantly lobbying for so-called key-recovery features that could give them access to a person's private key to unlock their encrypted data. Law enforcement and powerful intellectual property owners—such as the record and music industries—don't want Net users to be completely anonymous because obviously, that makes them harder to bust if they are suspected of trafficking pirated material or committing other Net-based crimes.

Courtney Macavinta, *New Product Guarantees Online Anonymity*, CNET News.com (December 13, 2000), *at* http://www.cnet.com. For a thorough treatment of the legal issues of key recovery, see Phillip R. Reitinger, *Compelled Production of Plaintext and Keys*, 1996 U. CHI. LEGAL F. 171 (1996).

logs.[290] Moreover, there is little legal basis for supporting such a log-maintaining requirement.[291]

Second, issues of international concern are presented by any legal solution to Internet-related problems due to the borderless nature of distributed networks. Offshore remailers located outside the jurisdiction of United States courts will ultimately remain open for American use in the face of American regulation. Though a change in the legal treatment of remailers in the United States might have an effect on the "accepted behavior" of foreign remailers, not all jurisdictions look to the United States for guidance. Indeed, such an assertion would be both naive and presumptuous.

Finally, the classic adage, "when guns are outlawed, only outlaws will have guns," is apropos. The first cypherpunk remailer was written in a weekend by a single individual.[292] Criminals who wish to communicate anonymously will find ways to do so regardless of legislation. Thus, claims that shooting the messenger—banning the public anonymous remailer—will prevent criminals from cloaking themselves in anonymity are absurd.

B. Strict Liability Proposals

The areas of law most likely to touch upon remailer administration, if they require an element of scienter at all, generally require knowledge of the user's underlying illegal act before assessing liability—whether civil or criminal—against the operator. This knowledge requirement appears essential for a number of reasons, including First Amendment concerns.[293] Thus, suggestions that remailer operators be held to a strict liability standard appear fatally flawed.

C. Outright Bans

Some view outright statutory prohibition as the only possible solution.[294] After concluding that a strict liability regulation regime would be inappropriate for a

---

290. *See* Kevin DiGregory, *Fighting Cybercrime—What Are the Challenges Facing Europe?*, Remarks at the Meeting of the European Parliament (September 19, 2000); *see also* Paul Meller, *ISPs Join to Cry Foul Over Pending European Cybercrime Rules*, INFOWORLD, vol. 23, issue 13, Mar. 26, 2001.

291. Though there are a number of federal regulations requiring record keeping, analogizing such requirements to mandated remailer logs presupposes that the remailer operator has any means of accessing the required information. *See, e.g.*, 7 U.S.C. § 2140 (1994) (requiring record keeping concerning the "purchase, sale, transportation, identification, and previous ownership of animals" for "dealers, exhibitors, research facilities, intermediate handlers, and carriers"); 15 U.S.C. § 5409 (1994) (requiring record keeping by manufacturers, importers, private label distributors, persons who make significant alterations, and labs performing inspections and testing of fasteners); 19 U.S.C. § 1508 (1994) (requiring record keeping of owners, importers, consignees, importers of record, entry filers, or other parties engaged in similar customs activities).

292. As explained by one of the founders of "Cypherpunks," a collection of cryptography enthusiasts,

> The Cypherpunk—and Julf/Kleinpaste—style remailers were both written very quickly, in just days—Eric Hughes wrote the first Cypherpunks remailer in a weekend, and he spent the first day of that weekend learning enough Perl to do the job. Karl Kleinpaste wrote the code that eventually turned into Julf's remailer (added to since, of course) in a similarly short time:—"My original anon server, for godiva.nectar.cs.cmu.edu 2 years ago, was written in a few hours one bored afternoon. It wasn't as featureful as it ended up being, but it was 'complete' for its initial goals, and bug-free." [Karl_Kleinpaste@cs.cmu.edu, alt privacy.anon-server, 1994-09-01].

Tim May, *Cyphernomicon 2.4*, *at* http://www2.pro-ns.net/~crypto/cyphernomicon.html.

293. The impracticality of a liability rule without a scienter requirement is also important to note.

294. *See, e.g.*, I. Trotter Hardy, *The Proper Legal Regime for "Cyberspace,"* 55 U. PITT. L. REV. 993 (1994).

number of reasons, Professor Hardy reluctantly argues that an absolute prohibition is "the only effective deterrent."[295] Given the global diversity of remailers, Hardy also acknowledges the need for some form of international cooperation to make the prohibition effective.[296]

Such proposals are troublesome for a number of reasons. First, not all anonymous remailer use is criminal. As discussed above numerous times, remailers provide critical social benefits. Second, a prohibition of anonymity drafted so broadly as a complete ban on the use of anonymous remailers would surely be constitutionally defective. The Supreme Court reaffirmed that anonymity is protected under the First Amendment in *McIntyre*.[297] The case only addressed political speech,[298] though, and did not hold that all prohibitions of anonymous political speech would be constitutionally invalid.[299] Therefore, the ruling in *McIntyre* would not necessarily preclude a prohibition of anonymous remailers.[300]

D. Constructive Knowledge Proposals

Noah Levine suggests that "[a] better approach is to subject the remailer administrator to liability for the illegal acts of...users when the administrator has constructive knowledge of the underlying illegal uses."[301] He defines constructive knowledge in this context as "reason to believe that a specific individual is using the remailer for an illegal purpose."[302] He suggests that in circumstances where operators are "notified by another party (*e.g.*, a victim) of past improper use by one of the remailer's users...[those] remailer administrators should either monitor future messages sent by the same user, or deny that individual the use of the remailer altogether."[303] Such a suggestion ignores the underlying technological barriers to implementing such a scheme. A remailer operator incapable of monitoring messages and their sources is incapable of denying access to specific users.

VII. CONCLUSION

The proliferation of strong cryptography and anonymous remailers enables truly anonymous communication to flourish to a degree never before experienced. The result is that both laudable and criminal acts may be perpetrated through such remailers, and both will grow as the influence of the Internet increases in society. To address the looming concern of anonymous criminals, legislatures and authorities

---

295. *Id.* at 1051. Hardy admits his reluctance in proffering such a statement: "This is, in terms of the various levels of behavioral regulation discussed in this article, a rather drastic solution, but the sharp externalities and the problems of identifying the BBS origins of anonymous messages suggest that this will prove to be the only recourse." *Id.*

296. *See id.*

297. *McIntyre*, 514 U.S. at 357.

298. *See id.* at 346.

299. *See id.* at 352 (arguing, inter alia, that the Ohio prohibition "encompâsse[d] documents that are not even arguably false or misleading"). The same overbreadth of concern could be present in the case of an absolute prohibition of anonymous remailers.

300. For a detailed treatment of the applicability of the Supreme Court's anonymity jurisprudence to the problem of anonymous remailers, see *Flood Control*, *supra* note 8, at 427.

301. Levine *supra* note 286, at 1559.

302. *Id.*

303. *Id.*

are throwing increasing amounts of time, energy, and money at computer crime.[304] Such efforts neglect to account for the true nature of the underlying technologies, as well as the severe policy implications of attempting to corral those technologies by force of law. The availability of anonymous remailers is essential for society to maintain and reap the benefits of anonymous speech in the electronic world. Accordingly, the liability placed on those who operate remailers for acts committed by users must be minimized, a proposition dictated by policy, law, and common sense.

304. "Growing concern over the increased threat of cyber crime has prompted the Justice Department to request another $37 million next year on top of the estimated $100 million already being spent to combat increasingly sophisticated computer criminals." *Justice Department Wants More Funds to Fight Cyber Crime*, CNN.com (Feb. 9, 2000), *at* http://www.cnn.com/2000/US/02109/cyber.crime.money/index.html. Yet, Troy Wolverton and Greg Sandoval, staff writers for CNET News.com, say that "although crime might pay, combating it usually doesn't" because "[m]ost online fraud cases involve amounts small enough that authorities often won't investigate." They explain that "[l]aw enforcement officials have been scrambling to catch up with these kinds of criminals—hobbled by insufficient resources and a flurry of trained investigators leaving for the private sector." Wolverton & Sandoval, *Net Crime Poses Challenge to Authorities*, CNET News.com (Oct. 12, 1999), *at* http://news.cnet.com/news/0-3834-200-850601.html. The president of the Florida Association of Computer Crime Investigators agreed, stating, "Unfortunately I don't think that you're going to see law enforcement catch up with the curve. In many ways, it's easier to commit crimes in cyberspace than the real world." *Id.*