Journal of Technology Law & Policy

Volume 6 | Issue 2 Article 2

December 2001

The Time Has Come for Limited Liability for Operators of True Anonymity Remailers in Cyberspace: An Examination of the Possibilities and Perils

George F. du Pont

THE TIME HAS COME FOR LIMITED LIABILITY FOR OPERATORS OF TRUE ANONYMITY REMAILERS IN CYBERSPACE: AN EXAMINATION OF THE POSSIBILITIES AND PERILS

George F. du Pont[*]

I. INTRODUCTION 176

II. ANONYMITY 180
A. *Anonymity Outside Cyberspace* 182
B. *Anonymity Today* 184
1. Abuse of Anonymity 184
2. Response to Abuses 185
C. *A Constitutional Question* 186
1. Attorney General Report 187
2. *ACLU v. Miller* 187
3. Decency Regulation 188
4. Supreme Court Stance on Cyberspace Anonymity 189
D. *Scholarly Opinions* 189

III. ANONYMITY REMAILERS 191
A. *Early Remailers* 194
B. *Remailers Evolve* 195
C. *Advanced Remailers Today* 198

IV. REMAILERS EVOLUTION HITS A WALL 199

V. THE EVOLUTION MUST CONTINUE: MY PROPOSAL FOR OFFERING 201

VI. EXAMINATION OF MY PROPOSAL 207
A. *Government Chip Proposal* 212
B. *Forced User-Log Proposal* 212
C. *One-World Government Proposal* 213
D. *No Satisfactory Fix-All Response Exists* 214

VII. CONCLUSION 215

---

* J.D., Northwestern Univ. Sch. of Law, May, 2001; A.B., Brown Univ., 1997; This Article is dedicated to Professor Stephen B. Presser, the Raoul Berger Professor of Legal History, Northwestern Univ. Sch. of Law, for his keen editorial guidance. The author is an Associate of Latham & Watkins in N.Y. City, N.Y. For further information, please contact the author by email: email@georgedupont.com.

I. INTRODUCTION

There is a new twist in anonymous communication. The advent of cyberspace enables anyone with basic reading and reasoning skills to send thousands of anonymous messages with relatively little effort. Although text-based electronic anonymous messages are not the only way to communicate anonymously,[1] they are far simpler than the alternatives. Sending truly anonymous messages in the physical world has always been an expensive art; the sender must keep the message devoid of all incriminating finger prints, telltale hairs or fibers, and other physical detritus that could betray their identity. Furthermore, the message must be sent from a location that cannot be traced back to the sender, and must consist of materials that cannot be traced through the manufacturer or by region. As O. J. Simpson would likely attest, anonymous phone calls on cell phones should be discouraged, especially when driving. Signals from O. J.'s phone passed through the nearest cells to the police as he drove down the highway after his wife's murder, leaving behind a digital dotted line resulting in a media spectacle highway chase.[2]

However, times have changed. Due to advances in technology and the emergence of cyberspace, personal identities and physical locations are far more easily cloaked in anonymity and pseudo-anonymity than ever before. Although the technology that enables people to send anonymous messages is still not as user-friendly,[3] vast improvements have been made since the inception of cyberspace.

Anonymity can be seen as both a good thing and a bad thing for society. Anonymity can be a benefit to society: systems of truly anonymous communication, when used legally, provide a socially valuable service. Indeed, anonymous political speech is considered to be a guaranteed right and a cornerstone of American democracy. Anonymity also has non-political, yet socially valuable, applications as well: for example, it is useful when you "[k]now something dangerous about your local nuclear power plant but don't want to risk getting run off the road by hired thugs."[4] On the other hand, when used illegally, anonymous communication can become

---

1. *See* Bruce P. Smith, *Cybersmearing and the Problem of Anonymous Online Speech*, 18 COMM. LAW. 3, 4 (2000).

2. *See* JONATHAN ROSENOER, CYBERLAW: THE LAW OF THE INTERNET 139 (1997) (citing *The Simpson Murder Case; Fugitive Relied On and Was Undone By Cellular Phone*, L.A. TIMES, June 19, 1994, at A11; *Police Like to Listen In: Crime, Cellular Phones Don't Mix*, S.F. CHRON., June 21, 1994, at A1).

3. A. Michael Froomkin, *Floor Control on the Information Ocean: Living With Anonymity, Digital Cash, and Distributed Databases*, 15 J.L. & COM. 395, 416 (1996).

4. *See* WALLACE WANG, STEAL THIS COMPUTER BOOK 80 (1998).

a dangerous sword wielded by an invisible foe; government officials often express concern that anonymous communication systems in cyberspace thwart the efforts of law enforcement.[5] There are countless illegal uses of anonymity in cyberspace. For example, "[c]yberpredators often cruise the Internet in search of lonely, curious or trusting young people."[6] Illegal civil activities abound as well: "[T]he Internet has enabled individuals easily to widely disseminate misappropriated trade secret information. Once posted on the Internet, it is difficult if not impossible to put the genie back in the bottle."[7] Despite these concerns, true anonymity itself is merely a catalyst for speech: "[I]f anonymity encourages unwanted speech, it may also encourage wanted speech."[8]

When combined with the historical protections of political speech, the modern pros and cons of anonymity raise a constitutional question: if people acting anonymously in cyberspace cannot be held accountable for their words, what type of protection should their speech have? Despite the fact that truly anonymous and pseudo-anonymous communication has been popular for hundreds of years, and although the First Amendment protects freedom of speech, people are not guaranteed the right to say *anything* without accountability. Accordingly, there have been several governmental attempts to ban or curtail anonymous communication, in and outside of cyberspace. For example, in 1996 the state of Georgia attempted to ban cyberspace anonymity, and a section of the Federal Communications Decency Act also attempted to bar citizens from communicating anonymously in cyberspace. Both measures failed, as have other attempts. The United States Supreme Court has yet to rule on a narrowly tailored statute restricting cyberspace anonymity, but due to the unique and influential attributes of cyberspace, the opportunity may very well present itself shortly.

Apart from banning cyberspace anonymity entirely, many critics of true anonymity[9] believe that there is not enough liability for operators of anonymity systems. Their reasoning, in short, is that providing the masses with easy access to anonymity is the same as "[a]ccording an anonymous

---

5. *See* Seth R. Lesser, *Privacy Law in The Internet Era: New Developments and Directions*, 607 PLI/PAT 141, 148 (2000).

6. Lizette Alvarez, *House Passes Bill to Crack Down on Pedophiles Exploiting Internet*, N.Y. TIMES, June 12, 1998, at A16 (quoting Rep. Bill McCollum).

7. Robert C. Welch & Elia Weinbach, *Protection of Trade Secrets And Confidential Business Information in the Internet Age: A Brief Overview*, 1166 PLI/CORP 225, 233 (2000).

8. Lee Tien, *Who's Afraid of Anonymous Speech? McIntyre and the Internet*, 75 OR. L. REV. 117, 144 (1996).

9. *See infra*, § II.D; *see also* Marie M. Stockton, *Protecting Copyright in Cyberspace: Holding Anonymous Remailer Services Contributorily Liable for Infringement*, 14 T.M. COOLEY L. REV. 317, 321 (1997).

user complete immunity from prosecution."[10] Thus, these critics argue that, if a person enables an illegal and untraceable communication, then that person should be held liable for the result of the communication.

Most anonymous messages transmitted in cyberspace are now sent through computers called "remailers," which strip the sender's address and forward the message to the recipient. Remailers operate all over the world, and are very inexpensive to create. The individuals who operate the remailers (the "remailer operators"), are fierce advocates of free speech, and most provide their services for free. Unfortunately, these services are sometimes abused by people who send illegal or harmful messages. Because the message recipients cannot identify the true sender of the message, they often resort to attacking the remailer operator who has acted as a middle man. Even with no legal ground to stand on, an angry recipient of an anonymous message can strong-arm most remailers out of business.

The obvious result is that operators of true anonymity remailers often shut down their services at the first sign of trouble, due to the liability stemming from occasional user abuse of the system. This, in turn, creates an atmosphere that lacks consistent, reliable anonymity systems available at any given time for average citizens in legitimate need of anonymity. A lack of reliable anonymity systems goes against the interests of the general public.[11] Because of the social value of anonymity, true anonymity systems that afford operators limited liability and are directed for use by the general public should be encouraged.

But there is a fine line between permitting free anonymous speech in cyberspace and enabling illegal and harmful anonymous acts, such as child pornography. For this reason, I firmly believe that the need to catch anonymous abusers after their first offense is as high a priority as the need for limited liability for truly anonymous remailer operators. The crux of the problem is the fact that it is impossible to *guarantee* that all first-time anonymous abusers will be caught, as long as truly anonymous remailers exist. But the reality of the situation is that truly anonymous remailers will always exist, because they are inexpensive and simple to create. Furthermore, although these hidden remailers may be hard for the average person to find and use, criminals have an incentive to find them and figure them out.

Therefore, a compromise between the need for remailers and the need to catch criminals must be reached. Such a compromise must reflect a realistic, good faith attempt to catch first-time abusers, while at the same

---

10. George P. Long, III, Comment, *Who Are You?: Identity and Anonymity in Cyberspace*, 55 U. PITT. L. REV. 1177, 1205 (1994).

11. *But see infra*, § II.D (referring to Marie Stockton's argument for remailer operator liability).

time enabling truly anonymous, easily-accessible remailers to exist. At this point in the development of anonymity systems, "[i]nformation privacy is a social goal, not a technological one."[12] Therefore, the encouragement of limited liability for operators must come from law-making bodies, such as Congress and courts. Pamela Samuelson eloquently stated that "[t]o achieve information privacy goals will require social innovations, including the formation of new norms and perhaps new legal rules to establish boundary lines between acceptable and unacceptable uses of personal data."[13]

These new legal rules that Samuelson speaks of can be developed through the evolution of basic principles of corporate law. I propose the creation of a new corporate structure for remailers, and I further propose that the United States government provide remailer operators with a safe harbor in which to operate. This proposal will result in limited liability for remailer operators, and will fundamentally alter the relationship between remailers and governments, and remailers and average citizens in legitimate need of anonymity. Because the privilege of limited liability in my proposal hinges upon cooperation and not upon forcing truly anonymous remailers to become pseudo-anonymous, remailer operators should be willing to coordinate their efforts, band together with the government, and help track down anonymous abusers.

The current remailer situation is relatively chaotic. Critics attempt to seek out and destroy the few remaining remailers, which only drives them further underground. Many scholarly proposals attempt to protect truly anonymous remailers by turning them into pseudo-anonymous remailers. My proposal will enable truly anonymous communication to flourish, while providing law enforcement with the powerful tool of operator cooperation that currently does not exist. The end result will promote free speech, and combat crime more effectively. Although it goes against the current status quo, I believe that my corporate structure/safe-harbor proposal is the best solution to the many problems of anonymity in cyberspace.

This Article will examine the success and failure of past and present boundary lines and advances in cyberspace anonymity systems, and will consider the future of non-remailer anonymity in cyberspace such as possible peer-based anonymity message alternatives like *Gnutella* and *Crowds*. Furthermore, this Article will propose a template for a new generation of cyberspace anonymity systems that provides continuous, free, unlimited true anonymity to the masses through remailers while shielding the operator from liability *and* enabling governments to track and catch anonymous abusers.

---

12. Pamela Samuelson, *Cyberspace and Privacy: A New Legal Paradigm? Privacy as Intellectual Property?*, 52 STAN. L. REV. 1125, 1169 (2000).

13. *Id.*

II. ANONYMITY

Anonymous or pseudo-anonymous text messages are not, of course, the only way to communicate anonymously. However, as one scholar on the subject succinctly points out,

> [T]hose who insist on speaking anonymously in public settings are aberrations: the terrorist in a balaclava; the racist hidden by a white hood; or the mob informant whose on-air identity is obscured by shadows. In turn, with the exception of certain authors, long-haul truckers, and graffiti artists, the use of pseudonyms in daily life [outside of cyberspace] is also relatively rare.[14]

Although anonymity can be broken down into several shades or categories,[15] essentially the two main forms of anonymity are "true anonymity" and "pseudo-anonymity." Therefore, and in part due to the text-only parameters set by the technology of anonymous remailers, this Article will focus on text-based, truly anonymous messages.

Perhaps due to the allure and promise of the term "anonymity," many Internet-users who are not technologically savvy sometimes confuse systems that provide true anonymity with systems that provide only pseudo-anonymity, to their detriment. This confusion can lead to serious problems, because people who think they are acting truly anonymously may say and do different things than people who realize that they are only acting pseudo-anonymously.

An excellent example of a highly misleading commercial system that promises true anonymity but in reality offers only pseudo-anonymity is the "VoiceFive.com FuturEsq" Internet research project,[16] directed towards law students. For a chance to win a thirty thousand dollar scholarship, law students can "passively participate" in ongoing Internet research. FuturEsq collects and aggregates data to "help companies understand how law students collectively surf, shop, and research on the Internet." Despite the fact that the research process is described as "completely confidential and anonymous," the company's system is anything but anonymous. The fact that FiveVoice.com claims "law students across the country are comfortable with our privacy principles" only goes to show that bodies of the general public that should know how to read fine print sometimes fail

---

14. *See* Smith, *supra* note 1, at 4.

15. Froomkin divides anonymity into four categories: traceable anonymity, untraceable anonymity, traceable pseudonymity, and untraceable pseudonymity. *See* Froomkin, *supra* note 3, at 417-22. These distinctions are not relevant for the scope of this Article.

16. *See* http://www.voicefive.com/futuresq/a/privacy.asp (last visited Sept. 25, 2001).

to do so. VoiceFive.com's "anonymous" privacy principles, as described in their own privacy statement, consist of the following:

> VoiceFive may monitor all the Internet behavior of your Household's registered computers. VoiceFive monitors both the normal web browsing you perform, and also the activity you may have through secure sessions, such as when filling a shopping basket or checking out from online shopping. VoiceFive's technology allows us to see the details of secure pages.
>
> . . . .
>
> . . . [T]he registration process has a step that configures your browser and computer so that your Household's Internet communications are routed through our high-performance network. The configuration process includes inserting a unique identifier into your browser that enables us to confidentially monitor your Household's Internet behavior.[17]

The bottom line is that VoiceFive.com collects reams of data regarding the daily habits of their users, and ties this data to the identities of the users. This interaction is not at all "anonymous," despite the fact that it is so labeled by VoiceFive.com. In an even greater departure from true anonymity, and despite their initial assurances to the contrary, VoiceFive.com does not keep users' personal information confidential:

> While we do not sell any personally identifiable member information, we may share personal identification information with third parties that help us deliver part of the VoiceFive service to you. This includes companies that administer the VoiceFive sweepstakes and individuals that you refer to us as part of the refer-a-friend program. When we do this, we establish controls and legal agreements that govern the use of that member information. These companies are obligated not to use the information for purposes other than to serve VoiceFive, and not to release the information, unless you have entered into a relationship with a specific company that would directly allow them to do so.
>
> . . . .

17. *Id.*

> . . . Our employees are obligated to abide by our internal security policies and procedures to further safeguard the information. *We take privacy protection very seriously.* All employees are made aware of our privacy statement and have agreed in writing to follow it.[18]

So only VoiceFive's employees, third party associates, and refer-a-friend targets know the confidential, anonymous identities of their clients. This fine print is typical of an Internet system that promises true anonymity on its main page, but in reality only provides pseudo-anonymity to its users.[19] This example helps illustrate the potential problems innocent users can encounter when they think they have true anonymity, and expresses why an easy-to-understand electronic system that actually provides true anonymity to the masses is a useful and much needed tool.

In *truly* anonymous communication, the author of the message is not known and cannot be discovered by anyone else. Conversely, the author of pseudo-anonymous communication is discoverable or perhaps known by others, but not generally by everyone. For example, if Alice sneaks up to Bob's house in the dead of night with no one watching, and leaves no trace of herself as she slips a fingerprint-free, unsigned message under Bob's door, that message may be truly anonymous.[20] However, if Alice signs the message with a pseudonym that only Bob recognizes, then the message is pseudo-anonymous. The same concepts apply to electronic anonymity in cyberspace: a message that arrives from a neutral remailing service,[21] stripped of all identifying marks except the contents of the message itself, is truly anonymous so long as its path cannot be traced back through the remailing service to the original sender. Use of cryptography can help cloak the sender's identity to any eyes that may read the message, but it is not strictly necessary to send an anonymous message.[22]

A. *Anonymity Outside Cyberspace*

Anonymous action is as old as the concept of identity. However, it is an age-old question as to how much legal protection "should be accorded to

---

18. Id.

19. The privacy statement for VoiceFive is an example of an agreement with such fine print. *See id.*

20. *See* Froomkin, *supra* note 3, at 418.

21. *See infra,* § III, Anonymity Remailers.

22. *See* SIMON SINGH, THE CODE BOOK: THE SCIENCE OF SECRECY FROM ANCIENT EGYPT TO QUANTUM CRYPTOGRAPHY (1999).

a person's thoughts, sentiments, and emotions."[23] Today, *McIntyre v. Ohio Elections Comm'n*[24] is the case that has come to stand as the backbone for modern First Amendment protection of true anonymity. In *McIntyre,* the Supreme Court ruled that Ohio's statutory prohibition against distribution of any anonymous campaign literature violated the First Amendment.[25]

In the United States, anonymous and pseudo-anonymous political speech have been popular for hundreds of years, and identity-cloaking authors have made rich contributions to the political discourse.[26] During the American Revolution it was common to use nicknames and codes when sending letters. In 1735, after publishing pseudo-anonymous essays, John Zenger was arrested for seditious libel, tried, and acquitted.[27] Thomas Paine's *Common Sense* was first published as written by "An Englishman," and even some authors of the Federalist Papers used anonymous names; as the famous footnote six from *McIntyre* states:

> That tradition [of true anonymity with respect to political speech] is most famously embodied in the Federalist Papers, authored by James Madison, Alexander Hamilton, and John Jay, but signed "Publius." Publius' opponents, the Anti-Federalists, also tended to publish under pseudonyms: prominent among them 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. A Forerunner of all of these writers was the pre-Revolutionary War English pamphleteer "Junius," whose true identity remains a mystery. The "Letters of Junius" were "widely reprinted in colonial newspapers and lent considerable support to the revolutionary cause."[28]

---

23. SAMUEL H. HOFSTADTER & GEORGE HOROWITZ, THE RIGHT OF PRIVACY 18 (1964) (referencing Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 196 (1890)).

24. 514 U.S. 334, 357 (1995).

25. *Id.*

26. Jonathan D. Wallace, *Nameless in Cyberspace; Anonymity on the Internet*, 54 CATO INST. BRIEFING PAPERS 2 (December 1999).

27. *See id.*

28. *McIntyre*, 514 U.S. at 343 n.6 (citations omitted).

When combined with the new technologies of cyberspace, this rich history of anonymous communication faces a revolutionary new set of challenges.[29]

B. *Anonymity Today*

The bold tradition of anonymous communication continues today in cyberspace, where sending anonymous messages has become very popular. Unlike Harvard and other schools that prevent unidentified people from utilizing their computer networks, Geoffrey Stone, Provost of the University of Chicago, opened the university's networks for anonymous use because he reasoned that "people should have the right to communicate at the university anonymously, because the First Amendment to the Constitution guarantees the same right vis-à-vis governments."[30] In 1999, many Kosovars and Serbs used anonymous cyberspace communication to send and receive political news without risking their lives; if governments had access to the true identities of these message senders, entire families would have been in grave danger.[31]

Furthermore, other users of anonymity, such as crime witnesses, novelists, on-line therapy group members and corporate whistle blowers are among the socially valued and constitutionally protected beneficiaries of truly anonymous communication. These users are considered necessary elements of society. In support of privacy of communications, Judge Posner argued that "there is no reason to believe that on average more false than true disparagements are made in private conversations, and the true are as likely to be suppressed by the prospect of publicity as the false."[32]

1. Abuse of Anonymity

Unfortunately, some people abuse public anonymity systems by engaging in criminal actions such as large-scale intellectual property theft, financial crimes, copyright infringement, cyberstalking threats, child pornography, and even terrorist instructions.[33] Cyberspace has enabled a new virtual frontier for computer crimes. In terms of dollars, and regardless of anonymity, "one estimate is that a crime committed with a handgun results in a theft of $1,900 on average, whereas a crime committed with a

---

29. *See* Jonathan I. Edelstein, Note, *Anonymity and International Law Enforcement in Cyberspace*, 7 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 231, 243 (1996).

30. LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE 26 (1999).

31. *See* BRUCE SCHNEIER, SECRETS & LIES, DIGITAL SECURITY IN A NETWORKED WORLD 64 (2000).

32. Tien, *supra* note 8, at 144 (citing RICHARD A. POSNER, THE ECONOMICS OF JUSTICE 173 (1981)).

33. *See* Edelstein, *supra* note 29, at 250-51.

computer results in a theft of $450,000 on average."[34] Anonymous hackers routinely target, enter and deface or steal from the computers of the *New York Times*, The White House, Senate, and FBI.[35] Lawsuits and legal actions abound; disgruntled employees and "pissed-off investors" who attempt to act anonymously are "increasingly likely to be sued for libel by image-conscious companies."[36] Even the Federal Security Service, formerly the K.G.B., has recently revived the cold-war tactic of relying upon anonymous accusations against Russian citizens.[37] "Federal law enforcement estimates indicate that more than $10 billion in [electronic] data is stolen annually in the United States,"[38] and anonymity plays a role in enabling the perpetrators.

These abuses of anonymity will continue, despite scholarly proposals that advocate "provisions [that] would deter harmful anonymous acts by putting the perpetrators on notice that they will be more easily identified in the future."[39] People who want to commit "harmful anonymous acts" will commit them regardless of the deterrents proposed. Furthermore, as will be discussed at length below, outright prevention of anonymous communication is technologically impossible. One scholar's assertion that "[b]y preventing individuals from hiding behind anonymity, there can be an assurance of accountability" fails to recognize this fact.[40]

2. Response to Abuses

In response to abuses of cyberspace anonymity, both the U.S. Federal Government as well as some state governments have addressed, to various degrees, the unique issues related to anonymity in cyberspace. Furthermore, the popular media and scholarly literature have embraced the topic, and discussions concerning the implications of widespread cyberspace anonymity have become commonplace.[41]

---

34. Stockton, *supra* note 9, at 319 n.12 (citing *Companies Resist High-Technology Theft*, RISK MGMT., Apr. 1, 1995, at 14, 1995 WL 12528346).

35. WINN SCHWARTAU, CYBERSHOCK: SURVIVING HACKERS, PHREAKERS, IDENTITY THIEVES, INTERNET TERRORISTS AND WEAPONS OF MASS DISRUPTION 155 (2000).

36. Alicia Ault, *"Fire" In A Crowded Chat Room*, WIRED MAG., Apr. 2001, at 66.

37. Michael Wines, *Reviving a Tactic, K.G.B. Heir Acts on Anonymous Accusations*, N.Y. TIMES, Feb. 15, 2001, at A5.

38. Edelstein, *supra* note 29, at 251 (citing Clinton Wilder & Bob Violino, *Online Theft: Trade in Black-Market Data is a Growing Problem for both Business and the Law*, INFO. WK., Aug. 28, 1995, at 30).

39. Noah Levine, *Establishing Legal Accountability for Anonymous Communication in Cyberspace*, 96 COLUM. L. REV. 1526, 1528 (1996).

40. Michael H. Spencer, *Anonymous Internet Communication and the First Amendment: A Crack in the Damn of National Sovereignty*, 3 VA. J.L. & TECH. 1, 24 (1998).

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

There are two distinct approaches that critics can take when they address the abuse of anonymity in cyberspace: the technological side, and the legal side. Some commentators believe that the technological side of the debate is the most important battle between free speech advocates and anti-anonymity crusaders. A technological battle involves "the ability of remailers to strip messages of their identifying information, of Internet consultants to mine sites for content and electronic footprints, and of encryption specialists and code breakers."[42] As will be discussed in greater detail later in this Article, I believe that the technological side of the remailer battle has already been fought, breakthroughs and limitations have been acknowledged by both sides, and the evolution of remailer theory and practice has hit a brick wall. As it now stands, technological innovations and remailer war tactics only go as far as the remailer operator's stamina in the face of a legal challenge. In short, the technological battle is over.

Meanwhile, the legal side of the debate rages on. It remains an open legal question exactly what forms of anonymous communication the U.S. Constitution protects, although it is generally agreed upon that the government cannot directly ban all forms of anonymous communications.[43] As a general rule, it can be inferred that the "First Amendment prevents the outlawing of true anonymity, although it only prevents governmental interference with anonymous messages."[44] The theory behind this reasoning is that access to methods of anonymous communication is vital for promoting and protecting socially important forms of free speech.

C. *A Constitutional Question*[45]

The First Amendment to the U.S. Constitution reads in part that "Congress shall make no law... abridging the freedom of speech, or of the press."[46] The Amendment "was designed to prevent the majority, through acts of Congress, from silencing those who would express unpopular or unconventional views."[47] The Amendment's purpose is to encourage formation of public forums "into which messages may be inserted without

---

42. Smith, *supra* note 1, at 9.

43. *See generally* George F. du Pont, Comment, *The Criminalization of True Anonymity in Cyberspace*, 7 MICH. TELECOMM. & TECH. L. REV. (2000-01), *available at* http://www.law.umich.edu/mttlr/volseven/duPont.html (last visited Sept. 25, 2001).

44. Anne Wells Branscomb, *Anonymity, Autonomy, and Accountability: Challenges to the First Amendment in Cyberspaces*, 104 YALE L.J. 1639, 1641 (1995).

45. Much of the constitutional analysis contained in this section is adapted from my earlier published short article entitled *The Criminalization of True Anonymity in Cyberspace*. *See supra* note 43. For a more in-depth constitutional analysis of anonymity in cyberspace, please refer to this work.

46. U.S. CONST. amend. I.

47. ACLU v. Reno, 31 F. Supp. 2d 473, 476 (E.D. Pa. 1999).

censorship."[48] Although most courts and commentators agree that protecting freedom of speech is important to foster the marketplace of ideas,[49] practitioners also recognize that the First Amendment does allow some regulation that may limit free speech. In other words, the Amendment does not guarantee individuals freedom of speech without accountability in all cases.

Historically, legislative attempts to ban anonymous communication has met with varying degrees of success. Anti-anonymity legislation targeted at cyberspace has been particularly unsuccessful, due to the general First Amendment protections on free speech. Legislators and government officials ignorant of the day-to-day fundamentals of the Internet too often overreact to perceived cyber threats stemming from the unique and still undefined long-term nature of cyberspace. As a result, several recent anti-anonymity statutes have failed. Meanwhile, government reports addressing anonymity and the threats it poses have yet to provide concrete solutions to these problems.

1. Attorney General Report

Opponents of limited liability for remailer operators support the Attorney General's August 1999 report on cyberstalking, because it recognized several possible dangers stemming from true anonymity.[50] The report went so far as to recommend that state legislatures create statutes addressing the problems of true anonymity, but it failed to offer specifics regarding exactly how to word such a statute.[51] In the end, the report recommended that federal law be "amended to make it easier to track down stalkers and other criminals in cyberspace while maintaining safeguards for privacy," but its specific prescription included only an amendment to the Cable Communications Policy Act of 1984 and failed to propose large-scale legislative solutions.[52]

2. *ACLU v. Miller*

Perhaps this failure to provide new legislative solutions is due to lack of success of past attempts. For example, in 1996 the Georgia State legislature

---

48. Branscomb, *supra* note 44, at 1676.

49. *ACLU*, 31 F. Supp. 2d at 476.

50. *See 1999 Report on Cyberstalking: A New Challenge for Law Enforcement and Industry, A Report from the Attorney General to the Vice President*, (Aug. 1999), *available at* http://www.usdoj.gov/criminal/cybercrime/cyberstalking.htm (last visited Sept. 25, 2001).

51. *See id.* (stating "[c]are must be taken in drafting cyberstalking statutes to ensure that they are not so broad that they risk chilling constitutionally protected speech, such as political protest and other legitimate conduct").

52. *Id.*

passed by an overwhelming margin a statute specifically aimed at combating anonymity in cyberspace[53] The Georgia law made it illegal for any person to knowingly transmit data through a computer network if that data used individual names to falsely identify the person or entity sending the data.[54] Although Georgia claimed that the legislation prohibited only "fraudulent transmissions or the appropriation of the identity of another person or entity for some improper purpose,"[55] the District Court of Georgia found the statute was "over-broad and threatened irreparable harm to the plaintiffs from continued self-censorship."[56] The statute was overturned.

3. Decency Regulation

A similar federal statute met the same fate as the Georgia statute. This statute, under Title V of the Telecommunications Act of 1996 is known as the "Communications Decency Act of 1996."[57] The purported goal of the law was "to regulate the access of minors to 'indecent' and 'patently offensive' speech" in cyberspace.[58] Because "[a] child with minimal knowledge of a computer, the ability to operate a browser, and the skill to type a few simple words [such as 'dollhouse' or 'toys'] may be able to access sexual images and content over the World Wide Web,"[59] the Communications Decency Act required people transmitting any content in cyberspace to verify the age and identity of all potential recipients of "indecent" material.[60] Opponents of the law claimed that the Act violated the First Amendment guarantee of freedom of speech, because it "would have destroyed the anonymity that is a hallmark of online communications."[61] In its first opinion involving cyberspace,[62] the Supreme Court ruled that the online censorship provisions of the Communications Decency Act were unconstitutional.

---

53. *See* Donald J. Karl, Note, Comments & Legislative Reviews, *State Regulation of Anonymous Internet Use After* ACLU of Georgia v. Miller, 30 ARIZ. ST. L.J. 513, 530 n.179 (1998) (referring to GA. CODE ANN. § 16-9-93.1(a) (Harrison 1997)).

54. *See* GA. CODE ANN. § 16-9-93.1(a) (Harrison 1997).

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

56. Karl, *supra* note 53, at 527 (citing *ACLU*, 977 F. Supp. at 1235 (enjoining Ga. from enforcing the anti-anonymity act)).

57. Reno v. ACLU, 521 U.S. 844, 858 (1997).

58. ACLU v. Reno, 31 F. Supp. 2d 473, 476 (E.D. Pa. 1999).

59. *Id.*

60. *See generally Reno*, 521 U.S. 844; *see also* Electronic Privacy Information Center, *EPIC Hails Supreme Court Internet "Indecency" Decision: Opinion "Preserves Both Free Speech and Personal Privacy," available at* http://www2.epic.org/cda/epic_sup_ct_statement.html (June 26, 1997).

61. Electronic Privacy Information Center, *supra* note 60.

62. *See id.*

4. Supreme Court Stance on Cyberspace Anonymity

Although the U.S. Supreme Court has never had the opportunity to consider a narrowly tailored statute restricting cyberspace anonymity,[63] the expanding nature of cyberspace may present the Court with an anonymity-rights question in the near future. However, the Court has commented on the nature of communication in cyberspace. In its opinion striking down the Communications Decency Act, the Supreme Court noted that cyberspace 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."[64] It also noted that cyberspace "can hardly be considered a 'scarce' expressive commodity" because "[i]t provides relatively unlimited, low-cost capacity for communication of all kinds."[65] "Scarce" expressive commodities, such as radio and television frequencies, have limited bandwidth[66] and are therefore subject to stricter government regulation. This suggests that while not supporting the notion of true anonymity at all costs, the Supreme Court believes that cyberspace should, more so than other mediums of speech grant a wide latitude in the realm of First Amendment rights.

D. *Scholarly Opinions*

Scholars have weighed in on both sides of the issue. Many noted scholars in the field of anonymity are strongly opposed to truly anonymous communication in cyberspace.

Professor Trotter Hardy poses perhaps the most significant argument in the legal literature for a total statutory ban on anonymous remailers in cyberspace.[67] Hardy recognizes that the vast majority of truly anonymous communication in cyberspace arrives from anonymous remailers, and he concludes that "the only effective deterrent to the problems of anonymous remailers will be to *prohibit them altogether*."[68] He even concedes that he prefers the admittedly "rather drastic solution" of complete prohibition of anonymous remailers to the lesser evil of imposing strict liability on the remailer operator.[69]

Other critics of true anonymity take Hardy's less drastic approach, and believe that there is not enough liability for operators of true anonymity

---

63. *See* Karl, *supra* note 53, at 533.

64. Reno v. ACLU, 521 U.S. at 850-51.

65. Id. at 870.

66. *See* NICHOLAS NEGROPONTE, BEING DIGITAL 23-24 (Alfred A. Knopf 1995).

67. *See* Trotter Hardy, The Proper Legal Regime for "Cyberspace," 55 U. PITT. L. REV. 993, 1050 (1994); *see also* du Pont, *supra* note 43.

68. *See* Hardy, *supra* note 67, at 1051 (emphasis added).

69. *Id.*

systems. Marie Stockton advances the argument that anonymous remailer operators "should be held contributorily liable for [copyright] infringement."[70] The unacceptable alternative, she argues, is to "pursue no legal redress at all."[71] To gain a full understanding of Stockton's argument, it is important to note that it is based upon the incorrect assumption that *criminals* are the only people who use truly anonymous communication:

> It is this author's contention that the only people who really need to obtain untraceable electronic anonymity are individuals who have illegal motivations.[72]
>
> . . . .
>
> . . . [U]sers who have legitimate reasons for wanting to send anonymous messages are free to seek out a remailer service that provides both traceable anonymity and has a reputation for not disclosing the identities of its users unless compelled to do so by law.[73]

Similarly, George P. Long sees only the criminal uses of anonymous communication. He believes that providing easy access to anonymity in Cyberspace is the same as "[a]ccording an anonymous user complete immunity from prosecution."[74] Long argues that such immunity would eventually lead to the creation of "havens for criminal activity . . . [that would] not only subvert any positive, humanitarian purpose that might come from such a [system], but it would also run counter to the law's views regarding anonymity."[75]

On the other hand, scholars such as Jonathan I. Edelstein support anonymity systems for the masses. Edelstein contends that "[a] complete ban on anonymous remailers, as some authorities have advocated . . . would have a drastic chilling effect on legitimate political, therapeutic, and recreational uses of the Internet."[76] Edelstein states that there should be "absolute protection of anonymity in messages which express political or religious opinions," and that "the confidentiality of persons participating in on-line self-help or therapy groups should also be preserved."[77] The

---

70. Stockton, *supra* note 9, at 321.

71. *Id.*

72. *Id.* at 321.

73. *Id.* at 328.

74. George P. Long, *Who Are You?: Identity and Anonymity in Cyberspace*, 55 U. PITT. L. REV. 1177, 1205 (1994).

75. *Id.*

76. Edelstein, *supra* note 29, at 275-76.

77. *See id.* at 277.

Supreme Court reflected Edelstein's position in its 1995 decision in *McIntyre* holding an Ohio statute prohibiting the distribution of anonymous campaign literature unconstitutional.[78]

Despite abuses of anonymous communication by people who break laws and harm others, and despite governmental and scholarly concern over these abuses, individuals cannot be legally or technologically barred from sending anonymous messages. Moreover, many governments and scholars recognize the importance of assuring the general public easy access to anonymity systems. Of course, by the term "general public," I mean the non-hacker community. Computer hackers have historically been able to cloak themselves in true anonymity in cyberspace, and will continue to do so in the future regardless of government regulation or any noisy academic opinion. Hacker activities do not affect my proposal because "what hackers do doesn't define what the effect of law as code is on the balance of the non-hacker public."[79] Therefore, this Article is directed towards anonymous messages sent by the non-hacker, civilian people who rely on more conventional and less technical methods of interaction. Because of anonymity abuses (hacker and non-hacker alike), and despite the benefits and legal protections for anonymity, the major obstacle of remailer operator liability still threatens to seriously hinder the continuation of effective public anonymity systems in cyberspace.

III. ANONYMITY REMAILERS

The most common device through which anonymous messages are sent is called a "remailer." Remailers are computers located throughout the world that strip messages of the sender's name and address, and forward, or "re-mail" them to the recipient. Anyone can send a message plus a forwarding address to a remailer, and the remailer will deliver the stripped down message to the address. Furthermore, anonymous remailers are exceptionally easy to set up: one of the "original universal remailers matured from concept to completion in a single afternoon. The operation of an anonymous remailer has been described as 'trivia[ly] easy'"[80] by John Helsingius, an early remailer pioneer.[81] It is also inexpensive by organized crime's standards: in his operational heyday, Helsingius spent approximately five to seven hundred dollars monthly to maintain and operate his service.[82] When a message is sent through several remailers in

78. *See supra* note 24 and accompanying text.

79. *See* Lawrence Lessig, *The Zones of Cyberspace*, 48 STAN. L. REV. 1403, 1408 n.17 (1996); *see also* du Pont, *supra* note 43, at n.139.

80. Edelstein, *supra* note 29, at 266.

81. *See infra*, § III.A.

82. *See* Edelstein, *supra* note 29, at 266.

a row before it arrives at its destination, it can become truly anonymous.[83] Only access to each one of the remailer's files can betray the original sender's true identity, and the majority of respectable remailer operators do not keep records, or if they do, they do not release them.

All of this anonymous communication has created a major obstacle for remailer operators: more and more irate recipients of offensive or illegal anonymous communications are attacking the remailer operators that pass on the messages. Some scholars even question whether a firm that has been anonymously attacked must "file a lawsuit and subpoena [the remailer's] records in order to determine the true identity of the harasser."[84] The answer is no. Subpoenas are neither the sole nor the most effective manner to obtain information from a remailer and bring it to its knees. The dilemma increases when the communication is so anonymous that even the remailer operator does not know the identity. An injured party's only recourse in such a situation is directly against the remailer itself.

Therefore, despite the fact that remailers are very easy to set up and operate,[85] lawsuits from injured parties or strong-arm tactics from government agencies such as the FBI have created an exceptionally negative atmosphere for remailer operators. Whenever a remailer is forced to divulge the identity of an anonymous message sender, that remailer's reputation as a reliable system for anonymity is immediately tarnished. However, remailers that do not keep transmission records are often forced to close under the threat of operator liability if they continue operating. As one scholar points out, "a legal regime which places vicarious criminal liability on operators whose services are abused by criminals would make operation of anonymous remailers impractical, if not impossible" and "would have the same practical effect as an outright ban on anonymous remailers."[86]

The result is that remailers, which can serve a valuable and constitutional purpose to the entire population, often fold under the pressure applied by governments or a few disgruntled recipients.[87] As a result, most remailers are created and operated by hackers and technology enthusiasts who are willing to risk lawsuits and strong-arm tactics from government agencies for the public good or for more personal reasons. While these services are valuable, they are often unreliable and technically confusing for those who need them most because at any given moment it is unclear which remailers are operating, or where they can be found. Even

---

83. *See* Froomkin, *supra* note 3, at 418.

84. *See* Mike Tonsing, *The 'Network of Networks' Begets Opportunities and Challenges Or, Roadkill Prevention in the Information Age*, 47 FED. LAW. 18, 19 (2000).

85. *See* Edelstein, *supra* note 29, at 265-66.

86. *Id.* at 277.

87. *See id.* at 275-79.

web sites dedicated to providing the general public with directories of available remailers are consistently outdated on a daily basis. One famous remailer directory located at www.publius.net, referenced in countless law review articles about remailers, has not been updated since August 6, 1998.[88] Furthermore, once a member of the general public does locate a remailer, it may remain unclear how to operate them easily and effectively, or to determine exactly the degree of anonymity they will ultimately provide.

It is true that "very effective Internet anonymity requires only two things: cryptographic tools, and willing remailer operators."[89] Early on, remailer operators were more than willing; they were dedicated to their service because they believed in access to true anonymity for all. Although cryptography became and remains an integral component of remailer operation, the continued success of remailers hinges upon the willingness of the operators. As one scholar put it, "[t]he key here is to have implicit faith and trust in the people operating the service."[90] In a disclaimer entitled "Trust No One," Zero-Knowledge Systems,[91] a peer-based anonymity system in cyberspace acknowledges that one of its "system deficiencies" is that "users must trust Zero-Knowledge to not record any association" between them and a user.[92]

Recently, that vital public trust has been widely eroded as remailer operators become less than willing to protect their users in the face of liability. While most remailer operators consider hacker attacks and other cyber-troublemakers to pose an exciting challenge to their technical skills,[93] few are willing to assume liability for the contents of the messages that cross their systems. This burden of liability is presently so strong that true anonymity remailers cannot operate for an extended period of time; most shut down shortly after they are created. As a result, most current remailers are either not true anonymity remailers, or are so technically complicated that the average citizen in need of true anonymity is effectively unable to use them. Below is a brief outline of remailer evolution.

---

88. *See* http://www.publius.net/rlist.html (last visited Sept. 25, 2001).

89. *See* Froomkin, *supra* note 3, at 424.

90. SCHWARTAU, *supra* note 35, at 156.

91. *See supra* note 132 and accompanying text.

92. Russell Samuels & Ed Hawco, *White Paper; Untraceable Nym Creation on the Freedom 2.0 Network*, at 8, *available at* http://www.zeroknowledge.com/alternate/policy.asp (last modified Apr. 1, 2001).

93. *See* David Mazieres & M. Frans Kaashoek, *The Design, Implementation and Operation of an Email Pseudonym Server*, Proceedings of the 5th ACM Conference on Computer and Communications Security, ¶ 1 (1998), *available at* http://www.lcs.mit.edu/impact/perspective ?name=9901 (last visited Sept. 25, 2001).

A. *Early Remailers*

The first "anonymous" remailers, created in 1988,[94] were actually traceable pseudo-anonymous remailers because they kept some record of the sender's identity. Most of the early users wanted to post anonymous messages to electronic bulletin boards, such as Usenet's "alt.sexual.abuse.recovery," and did not mind that they were technically not acting anonymously. However, this world of pseudo-anonymous bliss came crashing down in February 1995, when the Finnish police obtained a warrant to search the user logs of the most famous first-generation remailer pioneer, "anon.pennet.fi."

As it turned out, someone had posted anonymous messages to the bulletin board "alt.religion.scientology" that contained copyrighted and trade-secret information from the Church of Scientology. These documents contained the secret core beliefs of the Church of Scientology; only the deeply committed, true believing members of the church who paid their way to the top were permitted access to the documents. High-level Scientologists were worried that non-true-believers would misinterpret the documents and misjudge the Church of Scientology.[95] Scientology officials contacted Interpol, which in turn enlisted the aid of the Finnish police. John Helsingius, the computer scientist who operated anon.pennet.fi, surrendered the identity of the anonymous poster, believing that the only alternative would have been to watch the police seize the entire database.[96]

While it operated, anon.pennet.fi offered accessible, pseudo-anonymity to the masses for free. However, when confronted by the Church of

---

94. *See* Edelstein, *supra* note 29, at 245.

95. The documents explained that,

> [t]he final (secret) stage of [Scientology] asserts that in fact people are composed of clusters of "thetans" that are the spirits of dead space aliens, who were brought to earth 75 million years ago by an evil intergalactic tyrant named Xenu, and who were killed [by him] with hydrogen bombs in volcanoes. These spirits were captured afterwards by Xenu on electronic ribbons, and were given implants that kept them from remembering any of this. Since each of these thetans has a reactive mind, "auditing" must be performed on all of the millions or billions of these to get them to "blow" (be exorcised), at which point the primary (or operating) thetan controlling the body will realize his godhead, with power over matter, energy, space, and time (MEST), including the power to create galaxies and life." According to the documents, the easiest way to blow the alien spirits from your body is to join the Church of Scientology.

See Scientology FAQs and General Information, *available at* http: //www.factnet.org/Scientology/scifaq.htm; *see also* http://pw2.netcom.com/~seekon/summaryframe. html.

96. *See* Froomkin, *supra* note 3, at 422.

Scientology, it cracked under pressure. A few months later, public distrust forced the shut down of the remailer. Currently, the anon.penet.fi web site contains the following statement, posted in 1996:

> Anon.penet.fi is closed! News: Service now totally closed! Despite the service being almost closed, and only providing a very minimal service to support some especial (sic) groups and enabling people to re-establish other communication channels, it was still continuously attacked by spammers sending hundreds of thousands of junk mail messages — causing a lot of costs! Because the totally clueless abuse by the scum junk mailers, I now have to close down even the restricted form of the service :-(. . . Due to both the ever-increasing workload and the current uncertain legal status of the privacy of e-mail in Finland, I have closed down the anon.penet.fi anonymous forwarding service. . . . Thank you for a very interesting time on the net![97]

B. *Remailers Evolve*

After witnessing the hard lessons learned by the first generation of remailers operators, remailers began to evolve into a second, wiser, and tougher generation. A recent second-generation[98] remailer experiment, "nym.alias.net," purposely picked up where the first generation of remailers left off. Dubbed an "untraceable" remailer and created by MIT graduate student David Mazieres and his advisor Professor M. Frans Kaashoek, nym.alias.net operated for two years and attempted to overcome what its creators identified as the two main types of attacks on remailers: attempts to expose anonymous users, and attempts to silence them.[99] Mazieres and Kaashoek recognized that certain types of remailer use, such as electronic eavesdropping, cripplingly heavy traffic, and offensive hacker attacks could "either force an anonymous server to shut down or else destroy its utility to other people."[100]

Although nym.alias.net operated as a standard remailer in that it stripped all messages of their identifying addresses and forwarded them towards their assigned destinations through a chain of other remailers, it also incorporated "several technical innovations" that made it less vulnerable to

---

97. *See* http://www.pennet.fi (last visited Sept. 25, 2001).

98. Second generation remailers are often called "type-2" remailers.

99. David Mazieres & M. Frans Kaashoek, *The Design, Implementation and Operation of an Email Pseudonym Server*, Proceedings of the 5th ACM Conference on Computer and Communications Security 1, *available at* http://www.lcs.mit.edu/impact/perspective?name=9901 (last visited Sept. 25, 2001).

100. *Id.* at 2.

attack than earlier remailers.[101] Mazieres and Kaashoek attempted to accomplish three goals with nym.alias.net: first, to build a remailer that could be used and abused by "people outside of computer science research" (otherwise known as civilian, often quasi-technophobic individuals); second, to protect the secrecy of the identities of the users even if the remailer computers are compromised by outside parties; and third, to provide a robust anonymous email service that "people can rely on."[102]

The nym.alias.net project accomplished most of its goals. Examples of the types of attacks nym.alias.net encountered and overcame include:

"Exponential mail loops" and *"bulk mailing pyramid schemes,"* or piles of email specifically intended to flood the server. Their solution: limit the amount of mail any given account can send or receive each day;

"Mail-bombs," or batches of mail arriving at a faster rate than the server can manage, intended to overload the server. Their solution: limit the rate at which any person can send mail to the server;

"Reverse Mail-bombs," or email sent to nym.alias.net's own "Help Desk" requesting a response in the name of an innocent third party. When the third party received the mail from nym.alias.net, many became annoyed because they believed that nym.alias.net was sending them junk mail. Their solution: the next time a reverse mail bomb is sent, blindly expose the requesting party's true email address to the injured third party, and let the two parties resolve it;

"Encrypted mail-bombs," or encrypted batches of mail arriving at a faster rate than the server can manage, intended to overload the server. Their solution (despite the fact that they do not know whether this ever occurred): requires users to confirm reply blocks,[103] forcing the sending computer to confirm every message it sends, thereby complicating the attack "enough that other misuses of the system become easier," thereby luring troublemakers away from sending encrypted mail-bombs;

"Creation of many accounts," which result in slowing down the server. Their solution: require reply block confirmation. (Creation of many accounts did not become a major problem due to the time-consuming nature of physically creating new accounts.);

---

101. *Id.* at 1.

102. *Id.* at 3.

103. A "reply block" is a simple concept executed in an exceedingly complicated manner. Essentially, it is a partially encrypted piece of information that, in the right context, points towards the identity of a message sender. A somewhat simplified analogy is that examining a reply block is like examining a small portion of a mysterious person's fingerprint. Depending on the path the message traveled, it may be impossible to discover the identity contained in the reply block, just as it may be impossible to discover who left a fraction of a fingerprint. A reply block is only one piece of the puzzle of a sender's identity, and is of little use without other data located outside of the remailer.

"Spam," or junk email that annoys recipients. Despite knowledge that loads of spam were flowing through the server, Mazieres and Kaashoek refused to filter mail based on content, because this would amount to censorship. The result was angry recipients of spam could not contact the anonymous sender, so they took out their anger on the remailer. Several remailers in the nym.alias.net chain were forced to shut down due to too many complaints. Their solution: block all "blind carbon copies" so addressees could see who else was receiving the spam, and create "spam traps" that entice mail to be delivered to them, then temporarily cut off the account of anyone sending mail to those traps;

"INN Exploit," or password stealing. Essentially, hackers could take advantage of a bug in a popular computer program called INN by tricking the program into sending a computer owner's secret passwords to the hacker through nym.alias.net. Their solution: install an outgoing exponential mail loop from computers using INN. Although as many as 512 passwords may have been stolen before the exponential mail loop kicked in, once in place it stopped passwords from reaching the requesting hackers, and instead bounced the passwords to the surprised computer owners.[104]

While nym.alias.net's mission did not focus on the actual liability of remailer operators, the data it collected on how to ward off various attacks directed towards remailer functionality and how to maintain a user-friendly service continues to be of vital importance to development of the remailer community. For example, nym.alias.net developed useful ways to avoid keeping user logs. It was the existence of user logs that destroyed anon.pennet.fi; governments and angry recipients of anonymous messages often demand that remailers keep logs of the true identities of their users, but logs are inherently dangerous to the anonymity of the users and the longevity of the remailer service. Instead of keeping logs, nym.alias.net simply exposed repeat abusers upon request, or terminated offending accounts. Once nym.alias.net was made aware of an abuse, it began automatically attaching the offender's true email address to the messages before they were delivered to the victim.[105] During this process, nym.alias.net never kept a record of an abusive sender's identity. Although this identity exposure betrays the user's assumption of anonymity and goes against the spirit of anonymous remailers, it is considered an appropriate way to combat without storing every single identity in a user log.

However, the nature of nym.alias.net's successes highlight one of the project's biggest failures in its two years of operation: it was not strongly challenged by the government, and operator liability never became an issue. The closest Mazieres and Kaashoek came to a government shut-down was

104. *See* Mazieres & Kaashoek, *supra* note 99, at 10-15.

105. *See id.* at 17.

when "one of their worst nightmares" came true: a user posted child pornography with a nym.alias.net alias. As Mazieres and Kaashoek tell it,

> The FBI contacted us. They sent a subpoena. We complied, and disclosed the reply block for the nym. Of course, a reply block doesn't necessarily give one the identity of a user. What we turned over to the FBI can only have helped if they used it to issue more subpoenas.[106]

Because nym.alias.net did not keep user logs, Mazieres and Kaashoek could not identify the child pornographer. Had the pornographer acted again using the same alias, his true email address could have been recorded onto his message and sent along with it. However, this did not happen because the pornographer did not strike again via nym.alias.net. In a comment that reflects the dangerous reality of operating a remailer, Mazieres and Kaashoek expressed relief that they escaped liability relatively easy, compared to the histories of past remailer operators:

> The experience was not as bad as we had feared. The FBI did not seize our equipment. They did not threaten us or try to intimidate us. They did not ask us to start keeping logs, or try to convince us to shut down. We feared child pornography more than anything, but this happened and nym.alias.net survived.[107]

Despite the fact that nym.alias.net did not face major liability challenges, it collected very useful operating data that must be incorporated into any future generation remailer.

C. *Advanced Remailers Today*

Remailers operating today take full advantage of the lessons learned during the last decade and a half of evolution. Currently, truly anonymous remailers are classified as "Mixmaster" remailers, which rely on high levels of encryption, and require users to install anonymizing programs on their computers. It is interesting to note that the system employed by Mixmaster-type remailers is so securely anonymous that it is actually impossible for a message recipient to reply to a message sender. The unfortunate result is that anonymous two-way transactions over the Internet generally require the use of a public forum meeting place, or use of a pseudo-anonymous remailer, such as a remailer that keeps some form of identity logs.[108]

---

106. *See id.* at 16.
107. *See id.*
108. *See* Edelstein, *supra* note 29, at 243 n.69.

Hyper-cautious users can go even further into the world of absolute anonymity if they create their own "Nymserver" or "Newnym." They must simply establish a false email address that forwards messages to a real address via a chain of "cypherpunk" remailers that reencrypt the message between each remailer.[109] Advocates of this method of anonymity note that, "*if done properly*, it is nearly impossible to trace." However, the problem is that laypeople cannot even begin to "do it properly," much less comprehend what the instructions mean, and therefore risk exposing themselves. In a document entitled "Nym Creation For Mere Mortals," a remailer-information site attempts to "explain in great detail how to set up an account . . ., complete with examples and sample syntax." Despite helpful walk-throughs such as this, it remains a challenging task for a minimally computer literate individual to secure an anonymous "nym."[110]

Ironically, even *The Complete Idiot's Guide to Protecting Yourself Online* warns users of the complicated nature of remailers. "The more complicated the remailer, the more secure it is and the harder it is for anyone to trace your address. If you're super-paranoid, you have to do a bit more work because you'll want to use super-secret remailers."[111] This in turn begs the question, exactly how well will a "super-paranoid complete idiot" be able to send an anonymous message?[112]

The bottom line is that truly anonymous remailers, as they exist today, are elements of highly complex systems that are constantly in danger of being shut down. Current systems may work for individuals well versed in remailer and Internet technology, but these systems do not provide the general population with reliable, easy to attain, true anonymity.

IV. REMAILERS EVOLUTION HITS A WALL

Up until now, and despite their liability problems, remailers have continued to evolve and adapt in a series of generations based upon technological breakthroughs.[113] While technological advances will certainly continue,[114] the present major technological remailer evolution has reached

---

109. *See* SCHWARTAU, *supra* note 35, at 158.

110. *See* Anonymity: Index, *available at* http://www.stack.nl/galactus/remailers.index-anon.html (last visited Sept. 25, 2001).

111. *See* Preston Gralla, *The Complete Idiot's Guide to Protecting Yourself Online*, MacMillian Computer Publ'g, Ind., 1999, at 128.

112. My proposal, *infra* § V, takes even these poor souls into account.

113. *See supra* § III.B (referring to the nym.alias.net experiments and solutions, which are excellent examples of these technological breakthroughs).

114. "As Moore's Law continues its relentless journey into the realm of the smaller, cheaper, and faster, the acceleration of new technology introductions will increase." *See* Larry Downes & Chunka Mui, *Unleashing the Killer App; Digital Strategies for Market Dominance*, 1998 HARV. BUS. SCH. PRESS 28-29.

a plateau. Today, minor technical advances are only appreciated or comprehended by extreme enthusiasts. Meanwhile, the new liability pressures faced by remailers are far harder to overcome than the past barrage of hacker attacks. True anonymity remailers are useful while they exist, but most crack under the pressure of operator liability. As a result, the standard remailer model as a reliable true anonymity tool for the masses has failed.

The new weak link in the remailer chain is the actual person who operates the remailer, and no technological innovation can change their fear of liability and repercussions. Michael Froomkin commented that in the face of strict liability for remailer operators, "most reasonable people" would likely decide that continued operation of their remailer would be "an unacceptable risk."[115] Froomkin imagined several related "creative lawsuits" that remailer operators might reasonably have to face, including a common law tort of concealment of the sender's identity,[116] a claim of conspiracy with the sender,[117] and a RICO claim.[118] Of course, these creative lawsuits may never succeed, but they raise valid issues and could cost remailer

---

115. *See* Froomkin, *supra* note 3, at 425.

116. *See id.* at 426.

117. Froomkin notes that,

> [a] conspiracy charge would be difficult since it would [be] difficult to prove the element of agreement [between the message sender and the remailer operator] that is a necessary part of a conspiracy. It is difficult to say that Bob conspires with a stranger, even if he leaves a tool lying in plain sight, knowing that criminals are likely but not certain to come by and use it. If Bob is really ignorant of the identity, content, and purposes of the messages he retransmits, he can plausibly say that there is no agreement between him and the conspirator, and that he should be no more liable for the misuse of his remailer than the rental car company that leases a car to a terrorist.

Id.

118. "A RICO claim against a remailer could also founder on the lack of agreement." *Id.* at 426.

> The circuits conflict as to whether a defendant must agree to 'personally commit' the predicate acts in a RICO conspiracy but none of the circuits have done away with the need for some sort of agreement between the parties to the conspiracy. The Third, Fourth, Fifth, Sixth, Ninth, and Eleventh Circuits hold that the defendant's agreement to personally commit RICO predicate acts is not required.... According to these circuits, the government need only prove that the defendants directly or indirectly conspired to conduct RICO activity. The First, Second, and Tenth Circuits require the government to prove that the defendant agreed to 'personally commit' two or more predicate acts in a RICO conspiracy.

Id. at 426, n.93.

operators money to defend, and therefore act as a deterrent.[119] Creative lawsuits aside, actual lawsuits are booming; one scholar writing for the American Bar Association exclaimed that "[w]e are seeing an explosion around the country of libel-lawsuits that would never have been brought before, that get down to what I would call the trivial and the mundane because now many trivial and mundane comments are being broadcast."[120]

Unfortunately, hypothetical lawsuits, neither trivial nor real, can be prevented based solely upon advances in technology. As Froomkin stated, "in the absence of . . . a jurisdiction capable of offering a safe haven for remailers, the cornerstone of Internet anonymity currently relies entirely on the kindness of strangers."[121] It is now time for the strangers to assume identities, and for the remailer industry to undergo a further evolution. The evolution of remailers will remain stagnate, regardless of further breakthroughs in technology, until the new weak links gets the attention that they desperately need: operator liability protection.

V. THE EVOLUTION MUST CONTINUE: MY PROPOSAL FOR OFFERING

Based upon the above analysis, there are several economic disincentives to maintaining remailers: they do not make money, and they expose their operators to legal liability. If individual remailers could operate free of liability, they would be able to exist beyond their first subpoena or angry FBI visit, become easy to locate for the users who need them most, and even have the potential to make money by displaying advertisements to their users.

Many commentators have already proclaimed that the recent business revolution on the Internet has ushered in a need for a "corresponding development of revolutionary new legal theories to govern its use."[122] Although creating a liability-free remailer may seem impossible to many, it may just be as improbable as creating a new form of corporation, as David G. Post proposed in 1996:[123]

> Corporation law has a long history of attempting to strike [a balance between costs and benefits], and I propose that we begin developing a form of corporate law for cyberspace, rules regarding the

119. *See id.* at 426.

120. Jeffrey Ghannam, *Libel Online: Suit Raised Issue of Protection for Anonymous Web Comments*, 87 ABA J. 28 (Mar. 2001).

121. *See* Froomkin, *supra* note 3, at 427.

122. Jay Eisenhofer & Sidney S. Liebsman, *Caught by the Net*, BUS. L. TODAY, Sept.-Oct. 2000, at 40, 46.

123. *See* Post, *supra* note 41.

> formation of these entities and the protections that they will be afforded, in order to completely address the (seemingly unrelated) question of the regulation of anonymous speech.[124]

Although Post did not spell out the details of his proposed cyberspace corporate form, his idea to develop concepts of corporate limited liability for cyberspace-oriented businesses is an excellent one. Post noted the "'democratizing' impulse" that is an integral byproduct of the Internet, and stated that his proposal was only strengthened by the "relatively sudden increase in each individual cyberspace citizen's ability to participate in public collective action without formalities or legal barriers of any kind."[125] With a nod to the evolutionary history of the corporate form,[126] Post commented on the future of anonymity regulation and proclaimed that, "[j]ust as the doctrine of corporate limited liability itself developed as a means of encouraging individual entrepreneurial participation in the economic life of the nation, so too should the benefits of these new forms of public participation be weighed carefully before adopting any regulation [hindering or eliminating the use] of anonymity."[127]

The next question therefore becomes: how elaborate does this hypothetical new corporate structure have to be to achieve its goals? Even the most basic corporate structure has historically afforded its managers and directors limited liability for their actions on behalf of the corporation. For this reason, I believe that a limited liability remailer could be created from several corporations working in conjunction with each other, each one "owning" and operating a single hard drive over which anonymous messages could be sent. The end-users of the system would not care which hard drive remailed their message; they would simply select one from the pool. Any subpoena for a sender's identity would involve only the hard drive that sent the message, enabling the other hard drives to continue with the remailer's business. I believe that this system would leave remailer operators free of liability because it would be absorbed by the individual corporation that owned the hard drive. Furthermore, the system would have a greater chance of weathering legal attacks, because even if the subpoenaed hard drive was physically removed and placed in a police

---

124. *Id.* at 161.

125. *Id.* at 164.

126. *See id.* at 164 n.55 (citing Stephen B. Presser, *Thwarting the Killing of the Corporation: Limited Liability, Democracy, and Economics*, 87 NW. U.L. REV 148, 155-56 (1996)) (discussing the historical background of adoption of limited liability statutes); Stephen B. Presser, *Piercing the Corporate Veil* S 1.03, at 1-14 (Clark Boardman Callaghan, 1993); Paul Halpern et al., *An Economic Analysis of Limited Liability in Corporation Law*, 30 U. TORONTO L.J. 117, 118-19 (1980) (discussing the arguments in support of limited liability in England regarding its expected effects on the "investments of savings by the middle and working classes").

127. *See* Post, *supra* note 41.

evidence room, the rest of the hard drive pool would continue operating and the remailer would not shut down. This corporate structure, if feasible, would be a breakthrough in the field of cyber-anonymity, and could provide the first *reliable* limited liability remailer system to the masses.

This proposed corporate structure may be overly complex, have too many variables, and if used by itself might not serve its intended goal of providing guaranteed liability protection to remailer operators. Therefore, I believe that the best approach to the question of limited liability for remailer operators is to consider this new corporate structure, and at the same time directly address the issue of liability head-on, however unpopular or unorthodox a concept.

Curtis Karnow did just that when he proposed legal recognition of the "e-person" as a way to assure legal rights for individuals who act in cyberspace. The concept behind an "e-person," which currently exists only in theory, is essentially an anonymous or pseudo-anonymous identity used in cyberspace with the legally recognized right to establish credit and conduct business much like any other naturalized individual.[128] Although the concept of the e-person is admittedly far-fetched, Karnow's proposal indicates a movement towards recognition of the unique nature of cyberspace. Taking all of these considerations into account, I believe that the most effective way for remailer operators to attain limited liability is for the United States government to *grant them limited liability in a safe haven, in exchange for co-operation.*

This brings us to the next controversial issue: co-operation with remailers. True anonymity remailers exist because the public trusts them. The day the public loses trust, the remailer ceases in utility as a system for anonymity. As a result, there are two cardinal rules that are simply *not broken* by remailer operators, because it would destroy their credibility and user base. First, remailer operators never control or monitor the content of the message sent across their services.[129] Second, operators of true anonymity remailers never keep user logs. Any proposed limited liability system must respect and preserve these two cardinal rules. I believe that the creation of a new corporate form specifically tailored to limit remailer operator liability, combined with a guaranteed safe haven for remailers in exchange for co-operation, may be the winning combination for the next successful generation of remailers because it provides safety valves for the government without breaking the cardinal rules.

My proposal would conflict with few current laws. Perhaps most importantly, few statutes, if any, stand in the way of limited liability for

---

128. *See id.* at 168 n.63 (citing Curtis E. A. Karnow, *The Encrypted Self: Fleshing Out the Rights of Electronic Personalities*, 13 J.MARSHALL J. COMPUTER & INFO. L. 1, 4 (1994)).

129. *See* Froomkin, *supra* note 3, at 425; *see also infra* text accompanying note 151.

remailer operators who abide by the two cardinal rules.[130] Nevertheless, critics often argue that, no matter what the system, *someone* has to be liable for anonymous offenses. In the absence of the offending party's identity, the remailer operator is often called upon to take the fall.[131]

Critics ask me: Why does it have to be all about remailers? Perhaps another remailer revolution is a misdirected approach to the problem of continued access to true anonymity in cyberspace. Certainly, there are other ways to forward the cyberspace anonymity causes, without going through the trouble of creating new corporate structures and an entire new area of limited liability. Remailers are not the only way to send anonymous messages in cyberspace; as long as Alice is not recognized by her neighbors or her stalkers, she can go to a public library or local cyber-cafe and create a free Hotmail.com email account under a false name, and send anonymous emails that can only be traced back to that computer! But Alice must once again be careful not to leave any fingerprints, and she should wear a fake mustache or make sure there are no hidden security cameras that could betray her identity if traced.

Obviously, technology can replace a fake mustache. There are remailer-free ways to use cyberspace to send anonymous, untraceable messages. For example, people can use "peer based" networks such as *Gnutella, Crowds,* and *Aimster* to send anonymous messages. However, it still remains to be seen whether these peer-based systems provide liability-free, true anonymity.

Peer-based networks are essentially huge groups of computer enthusiasts all over the world who leave their computers running a special cyberspace network program day and night. Anyone with the right technology may join a peer-based network; a peer may even live next door to you. These systems operate much like the now-infamous Napster software networks, except without the central directory hub. In the Napster network, a user contacts Napster.com and asks the central computer if it knows about anyone who has a specific song on their hard drive.[132] If the central Napster computer knows where the song can be found, it connects the person requesting to the person who listed the song. One person then downloads, via the Internet, the song directly off the other person's hard drive (i.e., the song is not stored on Napster's computer).

---

130. "It does not appear that third party system operators or administrators have a statutory duty to disclose, or to refrain from disclosing," an anonymous message sender's identity. *See* Post, *supra* note 41, at 139 n.30.

131. For an in-depth analysis of all of the arguments brought up in this section, *see infra*, § *VI, Examining My Proposal.*

132. This is what got Napster in trouble; it was accused of aiding and abetting intellectual property thieves.

Peer-based systems are almost identical to the Napster system, with one major exception: peer-based systems have no central computer. The result is that the legal risk of operating a peer-based system is minimized "because their operators will have no practical means of knowing what type of information is exchanged" across the system.[133] People using Gnutella or Aimster who want to download a song just send an email out into the void of cyberspace to about seven other random people running Gnutella or Aimster networking programs, and each recipient either replies in the affirmative or forwards the message to the same amount of *different* people on the network, minus one. Any number between two and seven will work, but anything higher can potentially create exponentially large requests, flooding the Internet with trillions of requests and slowing down the network. In the end, the message bounces around to thousands of "peers" in the system, but because of the network design, no peer knows for sure where the original message originated. All they know is that the request came from another member of the network, but they do not know which one, since any given message is equally likely to have originated from any given member of the network. Of course, the message had to originate from someone in the peer group, and that cuts down the possible message senders to the finite number of peers in the system. As one expert on peer-based systems pointed out, a peer list must include everyone in the world for any given message receiver to have *zero information* on the message sender.[134] Fortunately for members of peer-based systems, there are already enough other peers in the system for a message originator to be nearly untraceable.

A few corporations have already embraced the concept of commercial peer-based anonymity systems: a Canadian company called Zero-Knowledge Systems unveiled a peer-based network called "Freedom,"[135] a few British programmers have unveiled the peer-based "Freenet" network, and even AT&T is experimenting with a peer-based anonymity service called "Publius" operating over the Crowds network.[136] All of these services enable people to send truly anonymous, untraceable messages to anyone in the world. This has sparked strong reactions from other companies and the government. Edgar Bronfman, the president of Seagram,

---

133. Robert Batchelder, *Commentary: Record Labels in Denial About Peer-to-Peer*, Special to CNET New.com, *available at* http://www.news.cnet.com/news/0-1005-201-4824189-0.html (Feb. 14, 2001).

134. *See* Michael Stutz, *Anonymity by Degrees*, WIRED NEWS.COM, ¶ 3 (1997), *available at* http://www.wired.com/news/technology/1,1282,7331,00.html (last visited Sept. 25, 2001).

135. See Courtney Macavinta, *New Product Guarantees Online Anonymity*, CNET NEWS.COM, at 5, ¶ 2 (1999), *available at* http://news.cnet.com/news/0-1006-200-1491501.html (last visited Sept. 25, 2001).

136. John Borland, *AT&T Developing Web Anonymity, Anti-Censorship Tool*, CNET NEWS.COM, June 30, 2000, at 1.

which owns Universal Studios and the Universal Music Group, reacted by declaring that "We must restrict the anonymity behind which people hide to commit crimes. As citizens, we have a right to privacy. We have no such right to anonymity."[137] The United States Department of Justice contacted Zero-Knowledge and requested that they build in a secret "back door" to their "Freedom" network. Zero-Knowledge declined.[138]

Even the people who created these anonymity systems have reservations about their use. It remains an open question as to what AT&T will do with its Publius network.[139] When America Online discovered that programmers at its Nullsoft online music division had created Gnutella as a development project in early 2000, the company immediately shut the project down.[140] However, before they could contain the software, someone set Gnutella free on the Internet and it quickly spread through the open-source community.[141] Adam Shostack, director of technology for Zero-Knowledge Systems, stated that "We're glad to see people are doing this kind of research, but I would like to see someone come up with a way to enable the good things to happen and put some kind of way in to block the bad things."[142]

The solution to Mr. Shostack's dilemma has already been implemented in the Zero-Knowledge System policies: their peer-based network keeps a form of logs that, with enough manpower, can be pieced together to find the identity of an anonymous offender. In a statement intended to notify users of Zero-Knowledge System's privacy philosophy and policies, the company warned that:

> A concerted court ordered attack on multiple Freedom Server Operators [i.e., peers], could result in a nym's pseudonymity being compromised. If multiple server operators were forced to reveal their encryption keys, it would be possible to determine a particular nym's e-mail address or IP address. In addition, a sufficiently powerful organization could, if so desired, retrieve the informational content of mail sent to regular Internet users by monitoring Internet network access points around the world. Each of these attacks

137. *See id.* at 2.
138. *See* Macavinta, *supra* note 135, at 2.
139. *See* Borland, *supra* note 136, at 2.
140. *See id.*
141. *See id.* ¶ 17.
142. *Id.* ¶ 20.

would require significant resources in order to pursue and force the revelation of keys controlled by third-party Freedom Server Operators.[143]

Although peer-based networks can be used to create a nearly unstoppable, nearly untraceable anonymity system, the peer members of these networks may, in time, face similar liability issues as remailer operators. Despite the fact that there is safety in numbers, there is also the risk of group-wide action; peer-based anonymity networks are essentially complex remailer systems, and if exposed to liability, individual members of peer-based networks may choose not to remail anonymous messages. Eventually, peer-based anonymity systems may fail as members of peer-based networks realize that they need the same operator liability protection this Article proposes for remailers. Furthermore, although companies like Zero-Knowledge can shut off a pseudonym if it is used to commit a crime,[144] the lack of a single operator of a peer-based system makes it very difficult for the government to actually catch second-time anonymous offenders who change their pseudonyms.

VI. EXAMINATION OF MY PROPOSAL

Despite the promises and possibilities of peer-based networks, I believe that remailers provide the simplest, most accessible form of anonymity in cyberspace. Furthermore, remailer technology and its use has developed to a point where the addition of limited operator liability is all that is needed to revolutionize the industry and dramatically effect positive change in how individuals communicate anonymously. Therefore, my proposal focuses on remailers. Because remailers are constantly threatened with closure, and due to the societal value of remailers, I propose that remailer operators be afforded limited liability.

Anonymous remailers are similar to Internet Service Providers (ISPs) such as America OnLine (AOL), because they both act as an intermediary for user communication. ISPs were recently threatened with the same issue of operator liability, and eventually won limited liability. In the early 1990s, two cases came down on either side of the issue of ISP liability: in *Cubby, Inc. v. CompuServe Inc,*[145] the U.S. District Court for the Southern District of New York held that the ISP Compu-Serve was not liable for disparaging statements posted to an online news gossip site because as a "distributor," it had "little or no editorial control" over the contents of the gossip site.

---

143. ZeroKnowledge Freedom Privacy Policy, *available at* http://www.freedom.net/freedomprivacy.html (last visited Sept. 25, 2001).

144. *See* Macavinta, *supra* note 135, ¶ 13.

145. 776 F. Supp. 135, 140-41 (S.D.N.Y. 1991).

However, in *Stratton Oakmont v. Prodigy Servs. Co.*,[146] the Supreme Court of New York held that the ISP Prodigy was liable for disparaging statements posted to an online news site because as a "publisher," it "exercised a degree of editorial control" over the contents of the news site.[147]

In response to ISP uncertainty as to where they stood in terms of distributor or publisher liability, Congress modified Section 230 of the Communications Decency Act to "effectively immunize [ISPs] from liability for information originating with third-party users of the service."[148] Furthermore, recent court decisions use the common law to uphold the thrust of Section 230 retroactively: in *Lunney v. Prodigy Servs. Co.*,[149] the New York State Court of Appeals concluded that under a common law qualified privilege, Prodigy was protected from liability for transmitting email because it "'was not a publisher of the electronic message board messages.'"[150]

As a result of these ISP liability protections, targets of anonymous messages have "tended to view [ISPs] and operators of online message boards as *allies* rather than adversaries."[151] Remailer operators need the same kind of public recognition. Arguably, because remailer operators, as a rule, exercise absolutely no control over the messages sent across their computers, they too should be seen as distributors who "are only liable for defamation if they know or have reason to know of the defamatory article,"[152] and should be given limited liability as well.

However, there is one major difference between ISPs and remailers, and this difference is the lynchpin of critics' arguments: unlike ISPs which ultimately have access to the name, email address, Internet protocol address, and credit card number of their users and can hold them responsible for their illegal actions in the face of a subpoena,[153] remailers cannot hold any anonymous first-time offender accountable. Therefore, the

---

146. 24 Media L. Rep. (BNA) 1794 (N.Y. Sup. Ct. 1995).

147. Smith, *supra* note 1, at 6.

148. *Id.*

149. 723 N.E.2d 539, 542 (N.Y. 1999), *cert. denied*, 120 S. Ct. 1832 (2000).

150. Smith, *supra* note 1, at 6.

151. *Id.* (emphasis added). However, note that because "many cybersmearing cases are dismissed or settled once the company identifies the anonymous speaker, . . . the claims asserted by corporate plaintiffs seldom have been litigated to judgement." *Id.* at 4.

152. *See* Christopher Butler, *Plotting the Return of an Ancient Tort to Cyberspace: Towards a New Federal Standard of Responsibility for Defamation for Internet Services Providers*, 6 MICH. TELECOMM. & TECH. L. REV. 247, 258 n.77 (2000) (citing Restatement (Second) of Torts § 581 cmt. d (1976)).

153. "Although most online providers agree to protect the privacy of their subscribers, the applicable service terms and privacy policies usually permit the provider to disclose subscriber information in response to a subpoena duces tecum." Smith, *supra* note 1, at 6.

argument goes, if remailer operators are not held liable for offending anonymous messages, then no one will.[154]

This argument is flawed, because it is entirely possible to subscribe to an ISP under a false identity, and remain an uncaught first-time offender. Of course, such an undertaking would require planning and strategy, due to an ISP's ability to trace credit card payments, and the occasional ability to trace the sender's Internet protocol address to a physical spot. Nevertheless, ISPs do not always know the identities of their subscribers, and they are not themselves held liable for that mistake. In *Zeran v. America OnLine, Inc.*,[155] the plaintiff injured by anonymous speech from an ISP subscriber "was left without recourse once the court held AOL to be immune from liability as a distributor of third party information content because the messages had been posted by an anonymous person whose identity was never able to be traced."[156]

Although all criminals should be held accountable for their actions, we must not destroy all true anonymity systems in the process. The only way to guarantee true anonymity in *specific* instances is to offer it in *all* instances. To judge whether or not a specific message of a sender's speech will qualify for constitutional protection and true anonymity would require exposure of the content of the speech. This exposure is antithetical to the very essence of true anonymity, and must be avoided in order to preserve anonymity for those who need it. The right to act anonymously "cannot be preserved if it must first be bargained for on a case by case basis."[157] Many forms of anonymity are guaranteed by the First Amendment, and anonymous remailers are so vital to that guarantee that they must be preserved through limited liability to their operators.

Despite the fact that some criminals will abuse the system and get away with it, my proposal will enable socially desirable free speech and anonymity to flourish, and at the same time ensure that repeat anonymous abusers are caught and dealt with at *higher rates than before.*

My proposal of limited liability for remailer operators raises three issues that must be addressed.

In the first issue raised by my proposal, critics may attempt to apply to remailer operators the argument that ISPs do not need substantial liability

---

154. *See* Welch & Weinbach, *supra* note 7, at 234. As the court noted in *Religious Tech. Ctr. v. Netcom On-Line Comm. Servs., Inc.*, 923 F. Supp. 1231, 1255-57 (9th Cir. 1995), "[t]he anonymous (or judgment proof) defendant can permanently destroy valuable trade secrets, leaving no one to hold liable for the misappropriation."

155. 129 F.3d 327 (4th Cir. 1997).

156. Butler, *supra* note 152, at 260.

157. Julie E. Cohen, *A Right to Read Anonymously: A Closer Look at "Copyright Management" in Cyberspace*, 28 CONN. L. REV. 981, 1000 (1996).

protection from private individuals harmed by anonymous postings.[158] Some critics of ISP limited liability already commute their analysis to local bookstores and other "distributors of speech," and their next logical step is to oppose limited liability for remailer operators:

> It is hard to justify the current regime [of ISP limited liability] when one considers the fact that a large corporation like AOL is immunized from liability for distributing defamatory materials while the neighborhood bookstore is not. ISPs have become one of our greatest distributors of speech, and it seems both inefficient and unjust to hold them to a lower standard of liability for defamation than all other existing distributors.
>
> . . . .
>
> . . . [A] federal standard imposing some liability [on ISPs] is now necessary because we have a federal, largely court-imposed, standard for ISPs barring virtually all liability.[159]

In response to this first issue, the "non-scarce" nature of cyberspace has irreparably changed the game. ISPs and remailers, truly global in their nature, neither act like, nor are subject to, the same rules as neighborhood bookstores. It is *because* ISPs are "one of our greatest distributors of speech," and therefore it is necessary to hold them to a lower standard of liability. Furthermore, anonymous remailers are arguably our *greatest* distributor of speech, and therefore remailer operators need the highest level of liability protection. While it may be hard for an individual to employ tactics that would shut down AOL, it is altogether too easy for an individual to shut down an anonymous remailer. Therefore, the hard-fought limited liability protection ISPs currently enjoy should extend to remailer operators. In the second issue raised by my proposal, critics could attempt to delay and confound my proposal by bogging it down in the age-old[160] debate of the absence of territorial boundaries and law in cyberspace. To briefly recap highlights from the debate: some scholars believe that cyberspace is truly a lawless new frontier, separate from physical society. In 1996, David Johnson and David Post proclaimed that "efforts to control the flow of electronic information across physical borders — to map local regulation and physical boundaries onto Cyberspace — are likely to prove

158. *See* Butler, *supra* note 152, at 265 (stating "[i]t is far from clear that ISPs need substantial protection against private individuals").

159. *See id.* at 265, 271.

160. In Cyberspace time, "age-old" means the past decade.

futile . . . United States Customs officials have generally given up."[161] In support of this argument, an excellent pseudo-anonymous Harvard Law Review article on the laws of cyberspace reiterates Professor Larry Lessig's belief in "the possibility that legislators will never be able to draft legislation generally applicable to the slippery contours and variegated user-communities of cyberspace without butting up against First Amendment concerns."[162]

However, along a more centrist approach, Lessig does recognize that law can exist in cyberspace, and that during its infancy it should "evolve slowly through a careful application of common law principles, with particular attention paid to the aspects of cyberspace that make Internet transactions unique."[163] In sharp contrast, Judge Frank Easterbrook believes that while cyberspace is indeed unique and novel, the law can take its nature into account. He also states that no unique niche should be carved out of the law for all things cyberspace, any more than a unique niche should be carved out of the law for all things horses.[164]

In response to this second issue, and regardless of the theoretical concepts of law and territorial boundaries in cyberspace, my proposal works in real space, on real soil and in real courts because remailers are physical machines and remailer operators are human. If the United States provided a safe harbor for remailer operators, then all of the world's governments could work with the operators to catch repeat offenders. No rational remailer operator[165] would actively protect an anonymous offender, because they would risk losing their safe harbor and their limited liability. Instead, remailer operators would help the government examine the patterns of first-time offenders, and prove vital to catching second time offenders. In short, granting limited liability to remailer operators, and making them allies instead of adversaries,[166] would create an environment in which productive, socially desirable free speech and anonymity could flourish, while ensuring that more anonymous abusers were caught and dealt with than ever before.

---

161. David Johnson & David Post, *Symposium: Surveying Law and Borders, Law and Borders — The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367, 1372 (1996).

162. Harvard Law Review, *Developments in the Law — The Law of Cyberspace*, 112 HARV. L. REV. 1574, 1582 (1999).

163. *Id.* at 1583 (citing Lawrence Lessig, *Symposium: Emerging Media Technology and the First Amendment: The Path of Cyberlaw*, 104 YALE L.J. 1743, 1745 (1995)).

164. *See* Frank H. Easterbrook, *Cyberspace and the Law of the Horse*, 1996 U. CHI. LEGAL F. 207, 208.

165. "Rational remailer operator" may currently be a contradiction in terms, but with the availability of safe harbors and limited liability, I predict that an entirely new breed of remailer operators will emerge.

166. *See* Smith, *supra* note 1, at 6.

In the third issue raised by my proposal, many critics demand that all anonymous abusers be caught and dealt with after their *first* offense, not if and when they repeat their offense, and that under my proposal most first-time abusers would get off scot-free. There are several different schools of thought to address the difficulty of catching first-time offenders.

A. *Government Chip Proposal*

Some scholars propose that the United States government mandate all new computer devices be outfitted with a chip that attaches the user's identity to every outgoing message. For example, Edelstein proposed that:

> [I]n a manner similar to the "Clipper Chip" or to emerging technologies used to trace financial transactions, the federal government could mandate the inclusion in all new computers of technology which creates a unique and indelible signature on each outgoing message. This would enable the information to be traced to its original source no matter what steps are taken to ensure anonymity en route.[167]

This school of thought will fail miserably in achieving even a small portion of its goals, because any system involving true identities of people passing through anonymous remailers must be a completely voluntary system in order to work. However, this ignores the basic concept of how remailers operate; remailers copy the contents of an incoming text message and paste them into a new outgoing message. All signatures, addresses, and identifying marks are discarded. Nothing in the outgoing message can be "traced to the original source," regardless of the government-mandated chip contained in the original source computer. To his credit, Edelstein did recognize "a number of [additional] drawbacks" to his proposal, including the ever-present danger of the proposed technology being superceded by new technology, and "the possibility that the veil of privacy might be breached by parties other than those authorized to penetrate it."[168]

B. *Forced User-Log Proposal*

Another related school of thought proposes that the government should give limited liability to all remailer operators that keep user logs and "'pierce the pseudonymity veil'"[169] to expose individual offenders to the proper authorities. Noah Levine believes that truly anonymous remailers are

---

167. Edelstein, *supra* note 29, at 282.
168. Edelstein, *supra* note 29, at 283.
169. Post, *supra* note 41, at 160.

operated "irresponsibly" because they do not keep user logs.[170] He proposes that remailer administrators be subjected "to liability for the illegal acts of their users in those circumstances where responsible administration would have prevented the acts in the first place."[171] Although Levine agrees that a safe harbor provision is warranted, he feels that it should only be provided to "those administrators who, acting in good faith, voluntarily choose to reveal the identity of the culpable user."[172]

David Post also believes that remailers should keep user logs:

> Because of the key role that rules regarding intermediary liability play and will play in cyberspace, and the critical importance of traceability in determining whether pseudonymity plays an effective role in limiting liability, it is likely that whatever regulation is imposed in an attempt to control anonymous or pseudonymous communications will be imposed on network intermediaries through, for example, rules regarding their duty (a) to collect verifiable identifying information from subscribers, (b) to turn over that information in specified circumstances, and (c) to refuse to carry communication that come from systems that do not abide by similar traceability rules.[173]

Although Levine's and Post's proposals may work for the very first offense on any given remailer system (before any user discovered that logs were being kept), they would effectively turn a truly anonymous remailer into a pseudo-anonymous remailer. While these policies may be good for people who want to act pseudo-anonymously, seekers of true anonymity will cease to use the remailers. Furthermore, operators are loathe to break one of the cardinal remailer rules against maintaining user logs. Therefore, Levine's and Post's proposals fail to address the problem of liability for truly anonymous remailer operators.

C. *One-World Government Proposal*

One final school of thought sees a "simpler solution" than the thorny issues of forcing spy chips or keeping user logs: it proposes the creation of an international governing body that would "promulgate rules and regulations governing Internet communication. . . .As such, this body would have the ultimate authority in determining what acts on the Internet are actionable. To deny the need for such an organization would, in effect,

---

170. Levine, *supra* note 39, at 1557.
171. *Id.* at 1558.
172. *Id.*
173. Post, *supra* note 41.

allow the festering of this growing international problem."[174] This proposal is highly flawed for several reasons, including the fact that the world is not yet ready to create an "ultimate Internet authority," and the fact that regardless of any agreement this improbable governing body could eventually reach, it would have absolutely no physical ability to govern global anonymous communication on the Internet or catch first-time offenders.

D. *No Satisfactory Fix-All Response Exists*

The third issue raised by my proposal of limited liability for remailer operators then remains: how do we catch first-time anonymous offenders without forcing operators to break one of the cardinal remailer rules? After examining the issue extensively, I joined the fray and built upon scholarly commentary with my own version of a remailer participation system that both satisfies critics and does not force operators to break one of the cardinal remailer rules.[175] However, based upon the flaws inherent in such a system, I conclude that no satisfactory fix-all response exists. Although I consider my hybrid-system to be more effective than the proposals of leading scholars, it functions only marginally better in reality, which is to say that it misses the mark. For the sake of discussion, I point out the easily identifiable fact that my hybrid-system faces two common yet insurmountable hurdles.

First, despite the fact that no cardinal remailer rules are broken, remailers using this system are *not* true anonymity remailers. Therefore, people looking for true anonymity would be strongly averse to sending messages across these remailers.

Second, can or should people trust the governmental agency in charge of dispensing the decryption key? This goes against conventional wisdom,

---

174. Spencer, *supra* note 40, at 39.

175. Because no true anonymity remailer monitors message content or keeps user logs, I proposed that a message sender's true identity (or at least the originating email address) be encrypted by the first remailer in the chain, and sent along with the message. The only entity that would hold the decryption key would be a government agency; remailers would be utterly unable to comply in any meaningful way with a subpoena seeking the sender's identity. The government agency in charge of holding the decryption key would only relinquish it to the injured party via court order. This proposal satisfies many opponents to limiting remailer liability, because it enables the general public to use remailers and send nearly anonymous messages while maintaining the potential to hold first-time offenders accountable for their actions. However, remailer operators and remailer users would most likely be horrified by this system.

I originally proposed this hybrid system in a different context: as a supplement to a narrowly tailored, constitutionally permissible statutory template aimed at criminalizing specific forms of unconstitutional anonymous speech. For more details regarding the legal ramifications of this hybrid key-encryption system, see du Pont, *supra* note 43.

as authors of messages containing protected political speech could unjustly be in danger of exposure.[176]

For these two reasons alone, I choose not to promote any such system, regardless of whether or not it breaks a cardinal remailer rule, as a means towards catching first-time offenders. My hybrid-system example proves that no such system will consistently work for people wishing to send truly anonymous messages. Therefore, some other way to catch first-time offenders must be implemented; I firmly believe that the need to catch anonymous abusers after their first offense is as high a priority as the need for limited liability for truly anonymous remailer operators.

For example, anonymous abusers such as child pornographers should be caught immediately (and punished harshly) before they can commit repeat offenses. However, a *guarantee* that all first-time abusers be caught bars the possibility of the existence of truly anonymous remailers; the second cannot realistically exist in conjunction with the first.

Therefore, a compromise between the two needs must be reached. This compromise must reflect a realistic attempt to catch first-time abusers, while at the same time enabling truly anonymous, easily-accessible remailers to exist *and* providing their operators with limited liability. Because remailers will be willing to coordinate their efforts, band together with the government and help track down anonymous abusers in exchange for the privilege of limited liability, my corporate structure/ safe-harbor proposal is the best solution to the many problems of anonymity in cyberspace.

VII. CONCLUSION

Anonymity is an absolutely necessary and protected right. Despite advances in peer-based networks, remailers provide the best form of anonymity in cyberspace. However, user-friendly true anonymity remailers are in danger because remailer operators do not have limited liability. Caselaw interpreting the CDA limits ISP liability. This limited liability should be extended to remailers as well.

176. This hurdle is the same one as addressed by Edelstein in his proposal. *See* Edelstein, *supra* note 29, at 283.

No one can prevent[177] the sending of anonymous messages, and no government can regulate the creation of hidden, truly anonymous remailers. If remailers are not permitted in the United States, they can, and surely will, be easily created "offshore," or in countries that do not have extradition treaties with the United States.[178] As Edelstein points out, "it is much easier to establish an anonymous remailer than it is to set up a financial institution, and the 'paper trail' of an anonymous message is much easier to hide."[179] Furthermore, if "an impoverished nation can be persuaded . . . to enact an airtight computer secrecy law, the door will be opened to the creation of 'offshore databases' operated by local contacts for the benefit of organized crime.[180]

It may not even take an "impoverished nation" to create an offshore remailer; on March 6, 2001, a young Canadian entrepreneur named Matt Goyer announced that he intended to build "an offshore Napster that couldn't be touched by the U.S. Government" on the "quasi-independent principality" of Sealand. Located in the North Sea, Sealand is a deserted military base founded by "the self-proclaimed Prince Roy" in 1967. Apparently, Prince Roy won the rights to Sealand after prolonged litigation with Great Britain. Goyer believes that only $15,000 is needed to set up shop and start his Napster clone.[181]

Without limited liability for user-friendly remailers that can be easily utilized by the general public, most truly anonymous messages will either be sent by criminals who understand how to create their own remailers,[182] or through offshore remailers that have no intention of working with

---

177. The concepts of "prevention" and "regulation," are broad and undefined. For example, despite the fact that "Congress has already failed in its efforts to protect minors from the rampant availability of pornography on the Internet," (*See* Harvard Law Review, *supra* note 162, at 1583.), the most effective form of prevention in this case is parental oversight. Compared to parental regulation of pornography entering a house, congressional regulation is nearly useless. This example illustrates how one form of prevention taken by a single individual can be far more effective than other forms taken by large governmental bodies.

178. Spencer notes that "a serious concern arises when [an anonymous remailer] exists outside of United States jurisdiction," because of the decreased possibility that the government could "pursue" the remailer operator in order to force it to disclose the name of the anonymous abuser. *See* Spencer, *supra* note 40, at 25. While I agree that remailer operators need an incentive to remain in the United States, I do not believe that "pursuit" of remailer operators per se is the most effective method of combating anonymous abuses.

179. Edelstein, *supra* note 29, at 280-81 (citations omitted).

180. *Id.* at 266.

181. *See* Richard Stenger, *Entrepreneur Proposes Offshore Napster Clone*, CNN.com, ¶ 9 (2001), *available at* http://www.cnn.com/2001/TECH/internet/03/03/napster.offshore/index.html (last visited Sept. 25, 2001).

182. Edelstein notes that "the next logical step" for criminals who need but cannot access truly anonymous remailers "is to establish their own anonymous remailers for the sole purpose of conducting illegal activities." Edelstein, *supra* note 29, at 265.

foreign governments to trap repeat offenders. However, with limited liability and safe harbors, remailer operators have an exceptionally strong incentive to work together to catch anonymous abusers. While it will remain impossible to catch all first-time offenders who use anonymity systems, my proposal is the best solution because it turns otherwise renegade remailer operators into communitarian allies. Therefore, for the good of society and for the sake of constitutionally protected anonymous speech in cyberspace, the United States must provide a safe harbor for remailer operators by providing them with limited liability.