Michigan Telecommunications and Technology Law Review

Volume 7 | Issue 1

2001

Criminalization of True Anonymity in Cyberspace, The

George F. du Pont
Northwestern University School of Law

COMMENT

THE CRIMINALIZATION OF TRUE ANONYMITY IN CYBERSPACE

*George F. du Pont**

Cite as: George du Pont, *The Criminalization of True Anonymity in Cyberspace*, 7 MICH. TELECOMM. TECH. L. REV. 191 (2001), *available at* http://www.mttlr.org/volseven/du pont.html.

* J.D. candidate, Northwestern University School of Law, May 2001; B.A., Brown Universiy, 1997; Email: email@georgedupont.com. This article is dedicated to Beatrice Borden, whose strength and courage continues to inspire me.

INTRODUCTION

Anonymity, often considered a cornerstone of democracy and a First Amendment guarantee, is easier to attain than ever before due to the recent emergence of cyberspace. Cyberspace[1] enables anyone to communicate, via text, sound, or video, to hundreds or thousands of other people, nearly instantaneously and at little or no cost. As of July 2000, more than 143 million adults had access to cyberspace in the United States,[2] and over 359 million had access worldwide.[3] Those numbers are growing rapidly. Due to the nature of the technology, identities in cyberspace are easily cloaked in anonymity. Once a message sender's identity is anonymous, cyberspace provides to the masses the means to perpetrate widespread criminal activity[4] with little chance of apprehension.

Debate rages about how, and by whom, cyberspace and cyber-anonymity should be governed.[5] In a report to former Vice President Al Gore, Attorney General Janet Reno found a need for greater control of anonymous communication in cyberspace.[6] Reacting to several high-profile attacks on major e-commerce web sites,[7] former

---

1. "Cyberspace" is generally considered to be a combination of the Internet, e-mail, Bulletin Board systems, Internet Service Provider domains, etc. *See* Reno v. American Civil Liberties Union, 521 U.S. 844, 849–54 (1997).

2. The Nielsen//NetRatings Universe is defined as all members (2 years of age or older) of U.S. which currently have access to the Internet. *See* Nielsen//NetRatings statistics at the NUA Ltd. Homepage, *available at* http://www.nua.ie/surveys/how_many_online/n_america.html (last visited Sept. 1, 2000)(on file with Michigan Telecommunications and Technology Law Review (MTTLR)).

3. *See* NUA Ltd. Homepage, *available at* http://www.nua.ie/surveys/how_many_online/world.html (last visited Sept. 1, 2000)(on file with MTTLR).

4. The low cost, ease of use, and potentially anonymous nature of cyberspace makes it an attractive medium for fraudulent scams, child sexual exploitation, and "cyberstalking." *See* OFFICE OF THE ATTORNEY GENERAL, CYBERSTALKING: A NEW CHALLENGE FOR LAW ENFORCEMENT AND INDUSTRY: A REPORT TO THE VICE PRESIDENT (August 1999), *available at* http://www.usdoj.gov/criminal/cybercrime/cyberstalking.htm (last modified Oct. 18, 1999) [hereinafter Attorney General] (on file with MTTLR).

5. "The FBI is constantly lobbying for so-called key-recovery features that could give them access to a person's private key to unlock their encrypted data. Law enforcement and powerful intellectual property owners—such as the record and music industries—don't want Net users to be completely anonymous because obviously, that makes them harder to bust if they are suspected of trafficking pirated material or committing other Net-based crimes." Courtney Macavinta, *New Product Guarantees Online Anonymity*, CNET News.com (December 13, 1999), *available at* http://www.cnet.com (last visited Sept. 1, 2000)(on file with MTTLR).

6. *See* Attorney General *supra* note 4.

7. During the week of February 7, several major e-commerce web sites were the target of "denial of service attacks" by hackers. These sites included, Yahoo, eBay, Amazon.com, Buy.com, E*Trade, and CNN.com. They were temporarily crippled by the attacks, leaving customers unable to access them. Evan Hansen & John Borland, *New Assault Weapons Pose*

President Clinton underscored the opinion that the government needs to maintain a watchful eye on cyberspace.[8] On the other side of the debate, some scholars see cyberspace as something that requires, and is capable of creating, its own law and legal institutions.[9] Many in cyberspace, with the help of some purists,[10] have declared independence from all governmental control, and urge a regime of guidelines and self-governance.[11] Some factions promote anarchy, and applaud when their anonymous Zorro figures commit acts considered criminal by mainstream society,[12] while others

---

Threat to Web, CNET News.com (Feb. 8, 2000), *available at* http://www.cnet.com (last visited Sept. 1, 2000)(on file with MTTLR).

8. President Clinton told CNN.com that the recent cyber-attacks on e-commerce "underscore a need for the government to focus on protecting the Internet itself." *Clinton Taking Up Web Security with Experts, a Leading Hacker*, A. P. INDEX (Feb. 15, 2000), at 1, *available at* http://www.siliconvalley.com (last visited Sept. 1, 2000)(on file with MTTLR).

9. *See* David R. Johnson & David Post, *Law and Borders—The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367, 1367 (1996); *see also The Domain Name System: A Case Study of the Significance of Norms to Internet Governance*, 112 HARV. L. REV. 1657, 1657 n.2. (1999).

10.

> Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather.
>
> We have no elected government, nor are we likely to have one, so I address you with no greater authority than that which liberty itself always speaks. I declare the global social space we are building to be naturally independent of the tyrannies you seek to impose on us. You have no moral right to rule us nor do you possess any methods of enforcement we have true reason to fear.
>
> . . .
>
> We will spread ourselves across the Planet so that no one can arrest our thoughts.

John Perry Barlow, *A Declaration of the Independence of Cyberspace*, *at* http://www.eft.org/~barlow/Declaration-Final.html (Feb. 8, 1996)(on file with MTTLR).

11. *See id.*

12. Some web sites advocate cyber-anarchy, cyber-terrorism and e-commerce disruption. The Anarchist Action Network states three goals: 1) to counter defamation of anarchy and anarchists in the media, 2) to foster cooperation, mutual aid, public space, compassion, understanding, sharing, community—especially among young people who may not realize alternatives to authoritarian control structures of the society into which they were born, and 3) to challenge the authority of all institutions and sources of coercion. Anarchist Action Network, *available at* http://www.zpub.com/notes/aadl.html (last visited Mar. 23, 2001).

The Hackers Homepage disclaimer states "We WILL NOT answer emails from anyone asking about illegal activities, or how to use our products for illegal activities . . . they will automatically be deleted. All products [sold by the web site] are designed for testing and exploring the vulnerabilities of CUSTOMER-OWNED equipment, and no illegal use is encouraged or implied. We WILL NOT knowingly sell to anyone with the intent of using our products for illegal activities or uses. It is your responsibility to check with the applicable laws of your city, state, or country." The Hackers Homepage, *available at*

attempt to provide controversial new services to the mainstream public.[13]

Despite the fact that no one sovereign controls cyberspace, it is not an ungoverned and lawless frontier; many actions in cyberspace have

---

http://www.hackershomepage.com (last visited Mar. 23, 2001). However, some of the Internet products available for sale at The Hackers Homepage site include:

Membership Sites Password Hacker: "Use this software to hack into most Internet sites that use membership sign-on screens." The Hackers Homepage, *available at* http://www.hackershomepage.com/section7.html (last visited Mar. 23, 2001).

H@tmail/Eud@ra Email Hacking: "Easy methods to hack into someone's H@tmail/Eud@ra account and view their email." (Note that "Hotmail" and "Eudora" are purposely misspelled). *Id.*

Computer Pranks Collection: "This CD contains dozens of pranks that can be used to annoy your victim. Pranks include: CD drive opening and closing, printer randomly printing, windows moving about the screen, buttons moving before you can click on them with your mouse, fake start menu, fake deletion of files and many more. Easy to install and will drive your victim nuts. They'll be calling tech support thinking something is wrong with their computer." *Id.*

Internet Site Ripper: "Have you ever found an Internet site that was too good to be true, and you wanted to save everything on it to your hard disk? Well, this software does jut that. It is a ripper and site scanner. It can also download, in many instances, areas of membership protected sites that are usually impossible to view without paying a fee." *Id.*

Answering Machine Scanner/Hacker: "Use this device to access someone else's answering machine. This device will scan all possible codes. Change someone else's messages, change their access code, listen to their message, possibly gain access to free long distance calling, etc. Works with most machines ... $100." The Hackers Homepage, *available at* http://www.hackershomepage.com/section1.html (last visited Mar. 23, 2001).

Pager Hacking & Bomber Software: "This CD is filled with texts and software pertaining to hacking pagers. Learn to encode and decode Pagers. It contains several programs for reprogramming most pagers. Several hardware interfaces are included. Also includes frequencies, capcodes, passwords, universal programming adapter and discriminator pinpoints. This complete collection contains everything you wanted to know on how to hack these units. PAGER BOMBER: Use this software and your computer to activate all pagers within a certain area code. All pagers will beep and display whatever number you entered. Imagine the expression on the person's face when they receive thousands of calls asking the reason for being paged. CD-ROM $125." *Id.*

GSM Cell Phone Hacking: "This CD contains everything currently available that can be used to hack GSM digital and analog phones. Includes hard-to-find, experimental software and texts for most phones. Nothing beats being able to call anyone you want for free." *Id.*

Of course, no self-respecting hacker would be caught without a *File Shredder:* "Includes a 'panic button' that will delete all your sensitive files with the click of a button faster than you can say 'search warrant.' Invaluable to businesses, hackers, and anyone with secrets, skeletons, stored on their computer." The Hackers Homepage, *available at* http://www.hackershomepage.com/section7.html (last visited Mar. 23, 2001).

13. For a more mainstream-oriented approach to anonymous mischief, PoisonPen.com offers its customers "anonymous email services for ex-girlfriends, ex-boyfriends, disgruntled employees, targets of unwanted sexual advances and ticked-off people everywhere." While the company "strictly prohibits" profanity and vulgarity, it charges $8 to email anonymous, "private, explicit words to the enemy." Evan Hansen, *Start-up Sells Email Services to Revenge Seekers*, CNET News.com, Nov. 16, 1999, at 1, *available at* http://www.cnet.com (last visited Sept. 1, 2000)(on file with MTTLR).

consequences in the real world.[14] Some states have recently entered the fray and taken matters into their own hands, legislating against anonymity both in and out of cyberspace.[15] Even though cyberspace does not fit neatly into existing constitutional categories,[16] courts have found that these recent anti-anonymity statutes, regardless of whether they are aimed at cyberspace, are too broad and violate the First Amendment.[17]

The question of whether a state or the federal government can create a narrowly tailored restriction on cyberspace anonymity without violating the First Amendment remains unresolved, however.[18] The Supreme Court has not directly addressed the issue, but it may soon consider the constitutionality of criminalizing certain kinds of cyber-anonymity in light of the unique nature of cyberspace. This comment explores the various forms of anonymity, examines the First Amendment status of anonymity in and outside of cyberspace, analyzes relevant scholarly commentary, and concludes that a narrowly tailored legislative restriction on "true" anonymity in cyberspace would not violate the First Amendment.

I. BACKGROUND

There are two different kinds of anonymity: true anonymity and pseudo-anonymity.[19] Too often, scholars and court opinions fail to sufficiently address this distinction. Dialogue on the issues of anonymity legislation and First Amendment protection suffers on account of this lack of distinction between true and pseudo-anonymity. This comment will distinguish true and pseudo-anonymity, two completely different forms of expression, with differing degrees of political and social value and constitutional protection.

---

14. Companies often take action against anonymous abuses in cyberspace by trying to unveil the identity of the abuser. "Online services in the United States have been flooded with subpoenas demanding to unmask the identities of anonymous posters—a request that companies sometimes honor." *See* Hansen, *supra* note 13.

15. *See* discussion *infra* Part II.A.

16. *See* Donald J. Karl, *State Regulation of Anonymous Internet Use After* ACLU of Georgia v. Miller, 30 ARIZ. ST. L.J. 513, 530 n.179 (1998); *see generally* Reno v. ACLU, 521 U.S. 844 (distinguishing the Internet from zoning precedents for adult movies and bookstores, as well as precedents regarding broadcast media).

17. *See* discussion *infra* Part II.A.

18. "[W]hether a narrowly tailored Internet anonymity restriction might pass constitutional muster under the First Amendment remains an open question." *See* Karl, *supra* note 16, at 533.

19. Noah Levine, *Establishing Legal Accountability for Anonymous Communication in Cyberspace*, 96 COLUM. L. REV. 1526, 1528 n.9 (1996)(citing Mike Goodwin, *Who Was That Masked Man?*, Internet World, Jan. 1995, at 22).

A. *True Anonymity*

Truly anonymous communication is untraceable. Indeed, only coincidence or purposeful self-exposure will bring the identity of the mystery message sender to light; the identity of a person acting in a truly anonymous manner can not be definitively discovered through any amount of diligence. Attempts can be made to discover the identity of the sender through inference, but any concrete trail of clues betraying the message sender has been erased by circumstance, the passage of time, or by the sender herself. Although some forms of truly anonymous communication, such as political speech, are considered valuable, this form of anonymity has exceptional potential for abuse because the message senders cannot be held accountable for their actions.

B. *Pseudo-Anonymity*

Pseudo-anonymous communication, on the other hand, is inherently traceable. Though the identity of the message sender may seem truly anonymous because it is not easily uncovered or made readily available, by definition it is possible to somehow discover the identity of a pseudo-anonymous message sender. Pseudo-anonymity has significant social benefits;[20] it enables citizens of a democracy to voice their opinions without fear of retaliation against their personal reputations, but it forces them to take ultimate responsibility for their actions should the need somehow arise. Although governments could abuse their ability to uncover the identity of people acting pseudo-anonymously, it is not in the government's interest to break that trust; by respecting pseudo-anonymous identities, governments can often avoid the far more dangerous abuses stemming from true anonymity.

C. *Anonymity Applied*

Before cyberspace existed, anonymous communication was much more expensive and time consuming.[21] Nevertheless, concealed identities in communications are historically common.[22] Pseudo-anonymous communication was especially prevalent before and during the American Revolution, when it was common to use nicknames and codes when sending letters.[23] Truly anonymous communication in conventional media, however, was difficult to achieve, and only became more difficult as technology progressed over the decades. Today, for a letter to be

20. *See* DAVID H. FLAHERTY, PRIVACY IN COLONIAL NEW ENGLAND 118 (1972).
21. *See id.*
22. *See id.*
23. *See id.*

truly anonymous, the sender would have to keep the letter sterile and devoid of fingerprints or other traceable materials such as regional dirt, glue, paper, and ink.[24] Additionally, individual typewriter keys leave a unique, traceable signature, and postmarks force senders to travel great, random distances to hide their origins. Untraceable phone calls have to be brief and routed through numerous satellites (or made from an obscure pay phone), and voices must be electronically cloaked.[25] True anonymity before cyberspace, while attainable, required people to go to great lengths and expense.

But all of that has changed.[26] The advent of cyberspace has vastly increased communication on a global scale.[27] Higher speed communication at minimal cost, combined with ever-improving technology, has ushered in an era of easily accessible, truly anonymous communication. Unique new forms of pseudo-anonymous communication have also developed. Citizens and legislatures alike have responded to these changes with both well-founded and ill-founded beliefs and confusion.[28] These beliefs have recently begun to clash, leading to showdowns in the real world, in cyberspace, and in courtrooms. These conflicts are discussed below.

There are many different ways to communicate in cyberspace,[29] and hence many ways to communicate anonymously. On one level of interaction, individuals can assume pseudonyms, enter virtual "chat rooms," and converse with others on nearly any subject. On another level of interaction, individuals can create and view web pages. The identities of the people engaged in these forms of communication are not always

---

24. Levine, *supra* note 19, at 1528.

25. *Id.*

26. *Cf.* NICHOLAS NEGROPONTE, BEING DIGITAL 4–5 (1995)(discussing the move away from communications employing physical objects towards completely digital communications media).

27. "As Moore's Law (the assertion that every eighteen months, processing power doubles while cost holds constant) continues its relentless journey into the realm of smaller, cheaper, and faster, the acceleration of new technology introductions will increase. As it does, Metcalf's Law (the assertion that the more people who use your software, your network, your standard, your game, or your book, the more valuable it becomes, and the more new users it will attract, increasing both its utility and the speed of its adoption by still more users) is there to spread them around." LARRY DOWNES, UNLEASHING THE KILLER APP 21–28 (1998).

28. "The anonymity question is further muddied by a great deal of confusion about what constitutes privacy in electronic communication. The agitation regarding the use of high levels of cryptography to protect the 'privacy' of electronic messages should not be confused with the question of true anonymity of message sources." Anne Wells Branscomb, *Anonymity, Autonomy, and Accountability: Challenges to the First Amendment in Cyberspaces*, 104 YALE L.J. 1639, 1675 (1995).

29. *See* Reno v. ACLU, 521 U.S. 855, 851 (1997).

easy to discover.[30] However, changes in the technology that control cyberspace can effectively eradicate some forms of truly anonymous communication.[31] For example, the implementation of Internet Protocol version 6 ("IPv6") would improve the ability of law enforcement to track cyberspace communication through unique identifiers attached to every computer's IP number.[32]

Anonymous communication can be conducted through "anonymous remailers."[33] An anonymous remailer is a service that receives an email, strips it completely of the true sender's identifying information, and forwards the message to the email address specified by the sender. With some experience, a person can use anonymous remailers to send untraceable, truly anonymous messages.[34]

Most remailers do not keep records of the identities of the people using their service. Ones that do are not used by people intending to send truly anonymous messages, because any record of their identity would leave a traceable path, thereby rendering their message only pseudo-anonymous. As this comment will discuss below, there is a disincentive for anonymous remailers to keep records of the identities of their users.[35] This disincentive only perpetuates the problems stemming from truly anonymous email. Governments, on the other hand, have an incentive to make all anonymous remailers keep records, thereby transforming them into merely pseudo-anonymous communication devices.

Although anonymous remailers constitute the bulk of truly anonymous communication in cyberspace, there are other ways to achieve true anonymity. Accounts on Internet email services, such as Hotmail.com or USA.net are available to anyone for free upon request. Although these services ask for the user's name and address, this infor-

30. People take nicknames in Internet chat rooms to protect their identity from others in the room. Although the host of a chat room usually has access to their real identities, this information can be falsified. Likewise, although all WWW page domains must be registered to a paying individual or company, several services (such as Tripod.com) exist that provide free WWW pages in exchange for (easily falsified) personal information.

31. Not only is it socially undesirable, but it is technologically impossible to eradicate all truly anonymous communication. Recent anonymous attacks on e-commerce sites are considered to be "part of the price of the success of the Internet." *Web Security*, *supra* note 8. Additionally, "most analysts predict that such attacks will become a fixture of the digital landscape." Hansen & Borland, *supra* note 7.

32. *See* Courtney Macavinta, *Internet Protocol Proposal Raises Privacy Concerns,* Cnet News.com, (Oct. 14, 1999), *available at* http://news.cnet.com/news/0-1005-200-852235.html (last visited January 15, 2001)(on file with MTTLR); *see also Domain Name System, supra* note 9.

33. As of November 4, 1999, there were 20 remailers up and running. *See* Ralph Levien, *Remailer List, available at* http://www.cs.berkeley.edu/~raph/remailer-list.html (last visited November 4, 1999)(on file with MTTLR).

34. *See* Attorney General, *supra* note 4.

35. Levine, *supra* note 19, at 1557.

mation is rarely verified.[36] Therefore, any message sent is only traceable to the computer that sent it. Anyone accessing the Internet from a public terminal (assuming they are not recognized or later identified visually), can keep his or her true identity a secret. Public Internet connections are easy to find: many libraries and sidewalk cyberspace cafes offer Internet access.

Despite the fact that truly anonymous messages can be sent without the use of an anonymous remailer, anonymous remailers pose the greatest problem for legal control. Although anti-remailer legislation might shut down some poorly funded basement hackers, the world-wide nature of cyberspace allows dedicated truly anonymous remailers to function as advertised, because the remailer operators can avoid legislation by moving outside the jurisdiction.[37]

D. *First Amendment*

1. Historically

The First Amendment to the United States Constitution reads in part that "Congress shall make no law . . . abridging the freedom of speech, or of the press . . . ."[38] The Amendment "was designed to prevent the majority, through acts of Congress, from silencing those who would express unpopular or unconventional views."[39] The Amendment's purpose is to encourage formation of public forums into which messages may be inserted without censorship.[40] Although most courts and commentators agree that protecting freedom of speech is important to fostering the marketplace of ideas,[41] practitioners also recognize that the First Amendment does allow some regulation that may limit free

36. *See* Attorney General, *supra* note 4.

37. This has already happened. On December 13, 1999, Zero-Knowledge Systems introduced a Montreal, Canada-based anonymous remailer called "Freedom," "for those who want to troll the Net incognito." "With Freedom, users' online activities are encrypted and routed through a globally distributed network of servers that make it impossible to know where users are physically located or who they really are. To ensure that people's actual identities are not linked to their Freedom pseudonyms, they will buy $10 tokens and cash them in for nyms. So all Zero-Knowledge ever knows about a person is that he or she purchased a token, according to the company. 'Zero-Knowledge has no data that can be used to compromise a user's privacy,' said Austin Hill, the company's president." *Macavinta, supra* note 5. Hill is "not worried" about possible legal problems: "We're not exporting or building encryption [from within] the United States . . . We took an active stance to educate law enforcement [such as] the Department of Justice. Generally the conversation is 'can you build a backdoor?' and we say 'No.'" *See id.*

38. U.S. CONST. amend. I.

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

40. Branscomb, *supra* note 28, at 1676.

41. ACLU v. Reno, 31 F. Supp. 2d at 476.

speech.[42] In other words, the Amendment does not guarantee individuals the right to say whatever they want without accountability in all cases.

2. Relationship with Anonymity

Anonymity has historically been recognized as valuable for free speech.[43] Indeed, Justice Black noted that "[p]ersecuted groups and sects from time to time throughout history have been able to criticize oppressive practices and laws either anonymously or not at all."[44] Black went on to remind us that "even the arguments favoring the ratification of the Constitution advanced in the Federalist Papers were published under fictitious names."[45]

Most historical political examples, however, relate to communication of a merely pseudo-anonymous nature. The identity of an author employing a pseudonym is usually known to at least a select few, such as an editor or publisher, and can be traced to the author if abused or if otherwise absolutely necessary. For this reason, pseudo-anonymous communication is relatively safe for society, and exceptionally valuable to the perpetuation of the ideals of free speech. Truly anonymous communication, on the other hand, is far more prone to abuse, and therefore, is ultimately more dangerous.

3. In Cyberspace

The low cost of operating in cyberspace enables people sending truly anonymous messages to operate on a scale never before possible.[46] The adage that freedom of the press is limited to those who owned one,[47] or those who are willing to stand on a soapbox and yell, no longer applies. Now, "in the medium of cyberspace anyone can build a soap box out of web pages and speak her mind in the virtual village green to an audience larger and more diverse than any the Framers could have imagined."[48]

---

42. *See* Attorney General, *supra* note 4.

43. Mark Twain (Samuel Langhorne Clemens), O. Henry (William Sydney Porter), Voltaire (Francois Marie Arouet), George Sand (Amandine Aurore Lucie Dupin), George Eliot (Mary Ann Evans), Charles Lamb (sometimes wrote as "Elia"), Charles Dickens (sometimes wrote as "Boz"), and Benjamin Franklin (employed numerous different pseudonyms) all cloaked their identities with various levels of anonymity. McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 342 n.4 (1995).

44. Talley v. California, 362 U.S. 60, 64 (1960), *quoted in McIntyre*, 514 U.S. at 342.

45. *See Talley*, 362 U.S. at 64–65, *quoted in McIntyre*, 514 U.S. at 342.

46. DOWNES, *supra* note 27, at 5.

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

48. *Id.*

Additionally, there will always be a way to send anonymous communication in cyberspace. No legislature is capable of physically preventing a dedicated individual from communicating in a truly anonymous form. This fact, however, has hardly prevented governments from trying to criminalize true anonymity in cyberspace.

II. CURRENT STATUS OF ANONYMITY REGULATION

Freedom has its consequences. Because attaining true anonymity in cyberspace is relatively easy, the medium is prone to abuse. Abuses of anonymity lead to increased costs for individuals, businesses, courts, and society, and unsurprisingly, legislatures have begun to respond.[49]

A. *Statutes Criminalizing Cyberspace Anonymity*

Historically, legislative attempts to criminalize anonymity have 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.[50] As a result of this overbroad criminalization of protected forms of speech, recent anti-anonymity statutes have failed.[51]

1. Attorney General Report

The Attorney General's August 1999 report on cyberstalking recognized the possible dangers stemming from true anonymity.[52] Although the report recommended that legislatures create statutes addressing the problems of true anonymity, it failed to offer specifics regarding exactly

49. See Press Release, American Civil Liberties Union, *Supreme Court Rules: Cyberspace Will be Free! ACLU Hails Victory in Internet Censorship Challenge, available at* http://www.aclu.org/news/n062697a.html (June 26, 1997). Although *ACLU v. Miller* and *American Liberty Association v. Pataki* were the first challenges to state attempts to regulate cyberspace, currently more than 20 states have passed or are considering passing laws that regulate cyberspace. *See id.*

50. "The threat of an 'electronic Pearl Harbor' was raised in March 1999 by then-Deputy Defense Secretary John Hamre, who predicted in congressional testimony that cyberterrorists would target America's commercial interests." *Web Security, supra* note 8. In response, President Clinton stated on February 15, 2000 that the major e-commerce attacks of the week before "were a source of concern," but were not "an electronic Pearl Harbor." *Id.*

51. *See* discussion *infra* Parts II.A.ii, II.A.iii.

52. *See* Attorney General, *supra* note 4.

how to word such a statute.[53] 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.[54]

2. American Civil Liberties Union v. Miller

In 1996, the legislature of the state of Georgia passed a statute specifically aimed at combating anonymity in cyberspace by an overwhelming margin.[55] Georgia insisted, when pressed, that the legislation did not impose unconstitutional content-based restrictions on the right to communicate anonymously.[56] Instead, Georgia claimed that the legislation only forbade "fraudulent transmissions or the appropriation of the identity of another person or entity for some improper purpose."[57] The bill's sponsor claimed that the legislation did not apply to "fictitious or pen names or anonymous communications on the Internet . . ."[58] The District Court of Georgia found that this was "over-broad and threatened irreparable harm to the plaintiffs from continued self-censorship."[59] The Court found that the law criminalized both truly anonymous and pseudo-anonymous communication in cyberspace.[60]

---

53. *See id.* ("Care 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.").

54. As more and more people begin using their cable connections to gain access to cyberspace, the Cable Communications Policy Act (CCPA) may limit the ability of law enforcement agencies to track down stalkers and other criminals acting anonymously in cyberspace because the CCPA prohibits the disclosure of cable subscriber records to law enforcement agencies without a court order and advance notice to the subscriber. *See id.*; *see also* 47 U.S.C. §§ 551(c), (h) (2000).

On the other hand, Lawrence Lessig noted that some cable television companies offering high speed Internet access have attempted to deny competing Internet Service Providers access to their cable networks. Steve Lohr, *Policing the Internet: Anyone But Government*, N.Y. TIMES, Feb. 20, 2000, § 4 (Week in Review) at 3. This could theoretically force the Internet users on that network to give up all forms of true anonymity.

55. *See* Karl, *supra* note 16, at 517 (referring to Act No. 1029, 1996 Ga. Laws 1505–06, codified at GA. CODE ANN. § 16-9-93.1 (1996)).

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

57. *Id.*

58. Karl, *supra* note 16, at 522 (quoting Brief in Opposition to Plaintiffs' Motion For Preliminary Injunction, ACLU of Ga. v. Miller, 977 F. Supp 1228 (N.D. Ga. 1997)(No. Civ.A.1: 96(V2475MHS), *available at* http://www.inteliview.com/aclupbi.txt)).

59. Karl, *supra* note 16, at 527; *see also* ACLU v. Miller, 977 F. Supp at 1235 (enjoining Georgia from enforcing the anti-anonymity act).

60. The Georgia law provides that it is illegal for any person to knowingly transmit data through a computer network if that data uses individual names, trade names, registered trademarks, logos, official seals, or copyrighted symbols to falsely identify the person or entity sending the data. See GA. CODE ANN. § 16-9-93.1(a) (Harrison Supp. 1997).

3. Decency Regulation

Title V of the Telecommunications Act of 1996 is known as the "Communications Decency Act of 1996."[61] The purported goal of the law was to regulate the access of minors to "indecent" and "patently offensive" speech in cyberspace.[62] The law was very hard to implement without infringing on constitutionally protected speech, due to the nature of the technology controlling cyberspace. 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,"[63] the Communications Decency Act required people transmitting any content in cyberspace to verify the age and identity of all potential recipients of "indecent" material.[64] 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."[65] In its first opinion involving cyberspace,[66] the Supreme Court ruled that the online censorship provisions of the Communications Decency Act were unconstitutional.

A New York case, *American Library Ass'n v. Pataki*,[67] addressed a state law similar to the federal Communications Decency Act of 1996.[68] However, the issues raised in that case very closely parallel those raised in *ACLU v. Miller*.[69] The New York legislature attempted to criminalize all cyberspace communication deemed "harmful" to minors.[70] The plaintiffs in the case complained that the New York law unconstitutionally infringed their First Amendment rights.[71] The Southern District of New York struck down the law and ruled that it violated the Commerce Clause, without reaching the First Amendment issues.[72] Nevertheless,

---

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

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

63. *Id.*

64. Reno v. ACLU, 521 U.S. at 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) (on file with MTTLR)

65. *See* EPIC, *supra* note 64.

66. *See id.*

67. 969 F. Supp. 160 (S.D.N.Y. 1997).

68. *See* Reno v. ACLU, 521 U.S. 844 (1997).

69. *See* Karl, *supra* note 16, at 534.

70. The legislature criminalized any cyberspace communication that "in whole or in part, depicts actual or simulated nudity, sexual conduct or sado-masochistic abuse, and which is harmful to minors." *Id.* (quoting American Libraries Ass'n v. Pataki, 969 F. Supp. at 163 (quoting N.Y. Penal Law § 235.21(3)(1996)).

71. *See* Karl, *supra* note 16, at 534.

72. *Id.*

free-speech advocates hailed the outcome of the case as a victory. Ann Beeson, an ACLU national staff attorney who argued the case before Judge Preska, declared that the *Pataki* and *Miller* decisions meant that "whatever limits the Supreme Court sets on Congress's power to regulate the Internet, states are prohibited from acting to censor online expression."[73] While it is true that state legislators have had no further success in regulating cyberspace, Ms. Beeson's statement fails to take into account the possibility that a narrowly tailored anonymity restriction might survive First Amendment scrutiny.

B. *Supreme Court Stance on Cyberspace Anonymity*

Although the Supreme Court has never had the opportunity to consider a narrowly tailored statute restricting cyberspace anonymity,[74] the expanding nature of cyberspace may present the Court with an anonymity-rights question in the near future. The Court has, however, 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."[75] Additionally, it noted that cyberspace "can hardly be considered a 'scarce' expressive commodity" because it provides "relatively unlimited, low-cost capacity for communication of all kinds."[76] "Scarce" expressive commodities, such as radio and television frequencies, have limited bandwidth[77] and are therefore subject to stricter government regulation.

Proponents of the Communications Decency Act claimed that it would protect children while promoting cyberspace expansion.[78] The Supreme Court did not agree; it found that the Communications Decency Act "lack[ed] the precision that the First Amendment requires when a statute regulates the content of speech," and therefore acted as a hindrance on the desired expansion of cyberspace communication.[79] The Court declared that as "a matter of constitutional tradition, in the absence of evidence to the contrary, we should presume that governmental

73. Press Release, American Civil Liberties Union, *New York Judge Prohibits State Regulation of Internet, available at* http://www.aclu.org/news/n062097c.html (June 20, 1997) (on file with MTTLR).

74. *See* Karl, *supra* note 16, at 533.

75. Reno v. ACLU, 521 U.S. 844, 850–51 (1997).

76. *Id.* at 870.

77. NEGROPONTE, *supra* note 26, at 23–24.

78. *See* Reno v. ACLU, 521 U.S. at 885.

79. *Id.* at 874.

regulation of the content of speech is more likely to interfere with the free exchange of ideas than to encourage it."[80] Based upon the Supreme Court's current sentiment, for any future legislation restricting cyberspace anonymity to have a chance of passing the Court's First Amendment scrutiny, the legislation must be very narrowly tailored, focused on specific problem areas, and non-detrimental to the expansion of the medium.

C. *Anonymity Outside of Cyberspace*

Courts consider cyberspace unfamiliar territory that does not fit neatly into existing constitutional categories, and when applying anonymity law, the courts will often turn to analogy.[81] If and when a narrowly tailored cyberspace anonymity restriction faces the Supreme Court, the Court will likely examine the protections of anonymity outside of cyberspace, such as political speech.

Historically, it seems that courts regard pseudo-anonymous communication as relatively safe and highly valued, and, therefore, highly protected under the First Amendment.[82] On the other hand, courts have not protected truly anonymous communication from legislative attacks unless there are compelling reasons at stake, such as when the communication constitutes political speech.[83] Court opinions do not always make these distinctions as clear as possible, however. When courts protect anonymous speech under the First Amendment, they often combine the concepts of true anonymity and pseudo-anonymity in their opinions without acknowledging it. A confused, misleading or ambiguous opinion only adds confusion to the discussion of anonymity regulation.

For example, in *McIntyre v. Ohio Elections Commission*, a case that has come to stand as the backbone for modern First Amendment protection of true anonymity, the Supreme Court ruled that Ohio's statutory prohibition against distribution of any anonymous campaign literature violated the First Amendment.[84] The Ohio statute at issue in the case declared that:

> "No person shall write, print, post, or distribute . . . any . . . form of general publication which is designed to . . . promote the adoption or defeat of any issue . . . unless there appears on such form of publication in a conspicuous place or is contained within said statement

80. *Id.* at 885.
81. *See* Karl, *supra* note 16, at 530.
82. *See infra* Part II.
83. *See infra* Part II.
84. *See* McIntyre v. Ohio, 514 U.S. 334, 357 (1995).

> the name and residence . . . [of] the person who issues, makes, or is responsible therefore."[85]

On April 27, 1988, Margaret McIntyre, her son, and a friend distributed leaflets that were made on her home computer.[86] The leaflets discussed a proposed school levy tax, and many were signed "CONCERNED PARENTS AND TAX PAYERS."[87] The Ohio Election Commission found that Mrs. McIntyre's distribution of unsigned leaflets violated § 3599.09(A) of the Ohio Code, and imposed a fine of $100.[88]

The Ohio Supreme Court affirmed McIntyre's fine, but the United States Supreme Court reversed, stating that the Ohio statute violated the First Amendment.[89] The Court expounded on the historical importance of political anonymity: "Anonymous pamphlets, leaflets, brochures and even books have played an important role in the progress of mankind."[90] The Court declared that "the interest in having anonymous works enter the marketplace of ideas unquestionably outweighs any public interest in requiring disclosure [of identity] as a condition of entry."[91]

The Court then drew an inappropriate analogy from a nonpolitical context: the pervasive practice of grading law school examination papers "blindly," "i.e., under a system in which the professor does not know whose paper she is grading."[92] This example is misleading, because the case relates to true anonymity, but the example is one of pseudo-anonymity. Although this example is dicta, it reflects the Court's reasoning patterns and stands as a good indication of how the distinction between true anonymity and pseudo-anonymity is easily overlooked by judges and lawmakers. The Court's law school example is one of pseudo-anonymity, not one of true anonymity, because the identity of the student is discoverable; the law school administration knows which exam belongs to which student. Indeed, after the professor grades the exam, the system matches the grade with the student's identity. In *McIntyre*, the Court recognized via this example that pseudo-anonymity is a very valuable and desirable form of communication protected by the First Amendment, but the Court failed to recognize that

---

85. *Id.* at 338 n.3.
86. *Id.* at 337.
87. *Id.*
88. *Id* at 338.
89. McIntyre v. Ohio, 514 U.S. 334, 339, 357 (1995).
90. *Id.* at 341.
91. The opinion went on to state, "Accordingly, an author's decision to remain anonymous, like other decisions concerning omissions or additions to the content of a publication, is an aspect of the freedom of speech protected by the First Amendment." *Id.* at 342.
92. *Id.* at 342 n.5.

this example is misleading when offered in a case relating to true anonymity. Instead of offering this blind grading example, the Court should have offered an example of true anonymity to bolster its argument that handing out anonymous political leaflets is constitutional.

The Court's holding regarding true anonymity, illustrated in the opinion's somewhat misleading but nevertheless compelling footnote 6,[93] is that political speech is valuable and worth protecting, even if it is truly anonymous.[94] Regardless of the confusing examples contained in the opinion, *McIntyre* stands for Constitutionally protected truly anonymous communication.[95]

1. Limits of True Anonymity Protection

Despite the Supreme Court's holding in *McIntyre v. Ohio*, not all forms of truly anonymous political communication are protected under the First Amendment. A couple of states have successfully outlawed masks and disguises in attempts to legislate against and control the Ku Klux Klan.[96] The legislature in Fredericksburg, Virginia successfully criminalized "wearing any mask, hood or other device . . . so as to conceal the identity of the wearer, to be or appear in any public place."[97] The legislature of Georgia confronted "the dangers to society posed by anonymous vigilante organizations" when it passed a similar statute prohibiting the "wear[ing] a mask, hood, or device . . . to conceal the identity of the wearer" in public.[98] The Georgia Supreme Court drew a

---

93. Footnote 6 of *McIntyre* reads:

"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.'"

Id. at 343 n.6 (citations omitted).

Although this footnote illustrates the value of anonymity, the content of this footnote is misleading because it does not distinguish between the pseudo-anonymous identities of the Federalist Papers authors and the truly anonymous identities of some Anti-Federalists.

94. *Id.* at 341.

95. *See* ACLU of Ga. v. Miller, 977 F. Supp. 1228, 1232 (N.D. Ga. 1997).

96. *See* Karl, *supra* note 16, at 531 n.187.

97. *See id.* at 531–32 (quoting Hernandez v. Superintendent, 800 F. Supp. 1344, 1346 n.1 (E.D. Va. 1992) which held that a mask that is not a necessary part of an identifying costume is not protected symbolic speech).

98. *See id.* at 533–34 (quoting State v. Miller, 398 S.E.2d 547, 549 (Ga. 1990)).

line through anonymity rights, and declared, "when individuals engage in intimidating or threatening mask-wearing behavior, their interest in maintaining their anonymity . . . must give way to the weighty interests of the State."[99] In Georgia, at least, a line exists between forms of valuable true anonymity that courts protect, and true anonymity that can be legislated against.

III. ANALYSIS: THE SUPREME COURT WILL UPHOLD CERTAIN STATUTES THAT CRIMINALIZE ANONYMITY IN CYBERSPACE.

Despite the fact that truly anonymous political communication is generally protected under the First Amendment, it is possible for legislators to create sufficiently narrow statutes targeting anonymity that pass constitutional scrutiny. As discussed above, depending on how compelling the interests at stake are,[100] states can legislate against some forms of true anonymity such as Ku Klux Klan masks, but not other forms, such as unsigned political leaflets. Accordingly, the Supreme Court may allow further restrictions on cyberspace anonymity if the restrictions are limited, target specific evils, and do not burden valuable forms of anonymity, such as truly anonymous political speech and most forms of pseudo-anonymous speech. Commentators are divided, however, on how the restrictions might be crafted.

A. Evaluation of Leading Commentators

Several scholars have addressed forms of anonymity in cyberspace, and each has their own conclusions and recommendations. This comment analyzes the various proposals relevant to the discussion, and then outlines its own proposal.

1. Attorney General's Report

In her report to former Vice President Gore,[101] Attorney General Reno recognized some of the problems that arise from abuses of true anonymity in cyberspace. However, despite its claim to the contrary,[102] the report gave no solid solution or recommendation as to how to crimi-

99. *See id.* at 533 (quoting State v. Miller, 398 S.E.2d at 553).

100. *See id.*

101. *See* Attorney General, *supra* note 4.

102. The "anonymous nature [of cyberspace] make[s] it an attractive medium for fraudulent scams, child sexual exploitation, and increasingly, a new concern known as 'cyberstalking.' [T]his report . . . provides recommendations on how to improve efforts to combat this growing problem." *Id.*

nalize abusive anonymous cyberspace communication.[103] The report simply urged legislators to take "care" when drafting anti-cyberstalking statutes that criminalized forms of anonymous communication, because a "carefully drafted statute can provide broad protections against cyberstalking without running afoul of the First Amendment."[104] This report is useful only insofar as it alerts legislators to the growing problem of anonymous abuses.

2. Trotter Hardy's Proposal

Professor Trotter Hardy poses perhaps the most significant argument[105] in the legal literature for a total statutory ban on anonymous remailers in cyberspace.[106] Professor 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."[107] He concedes that the case for imposing strict liability on the system administrator of the anonymous remailer, instead of shutting it down altogether, is strong.[108] However, he declares that in the end, the "rather drastic solution" of complete prohibition of anonymous remailers is the only solution.[109]

Professor Hardy's solution to fight abuses of anonymous communication in cyberspace by prohibiting anonymous remailers will fail for several reasons. First, although anonymous remailers constitute the bulk of truly anonymous communication in cyberspace, there are other ways to send anonymous messages.[110] Therefore, truly anonymous communication from a different source will undermine any success of his proposal.

Second, his proposal might not pass constitutional scrutiny: some anonymous remailers are really only pseudo-anonymous because they keep a record of the address of each message sender,[111] and therefore enjoy a heightened level of constitutional protection.

Third, while Professor Hardy correctly recognizes that anonymous remailers can operate from anywhere on earth, his solution to the

---

103. *See supra* Part II.A.i.

104. *See* Attorney General, *supra* note 4.

105. Levine, *supra* note 19, at 1540.

106. *See* Trotter Hardy, *The Proper Legal Regime for "Cyberspace,"* 55 U. PITT. L. REV. 993, 1051 (1994).

107. *Id.* at 1051.

108. *Id.*

109. *Id.*

110. *See supra* Part I.C.

111. Levine, *supra* note 19, at 1532.

problem of jurisdictional issues is flawed. He states that because of "the ease with which messages in cyberspace may be routed across national borders, some form of international cooperation, such as a treaty, will be necessary for the prohibition to be effective."[112] He fails to recognize, however, that as long as there exists one spot on earth where there is no international treaty (and perhaps even in places where there is a treaty),[113] anonymous remailers will be able to operate.[114]

3. Noah Levine's Proposal

Like Professor Hardy, Noah Levine recognizes that anonymous remailers are being abused for criminal purposes.[115] Levine agrees that Professor Hardy's proposal is too extreme, and that it raises First Amendment problems.[116] Levine attempts to solve the anonymity abuse problem by "ensuring that there is nearly always a party against which an injured party may seek legal redress."[117] Levine contends that "the best means for achieving such reform is by subjecting remailer administrators to liability for the illegal acts of their users in those circumstances where responsible administration would have prevented the acts in the first place."[118] Levine's proposal urges that a "simple statute" be passed requiring remailers to keep records of sender identities,[119] and providing a safe harbor provision in order to encourage remailer participation.[120] Remailers "would be required to monitor only those us-

112. Hardy, *supra* note 106, at 1051.

113. "No single organization controls any membership in the Web, nor is there any single centralized point from which individual Web sites or services can be blocked from the Web." Reno v. ACLU, 521 U.S. 844, 853 (1997).

114. A case that further undermines Hardy's proposal is GTE Media Services Inc. v. Bellsouth Corp., 199 F.3d 1343 (D.C. Cir. 2000). The Court found that personal jurisdiction could not be based solely on the ability of District residents to access the defendant's web site. Id. at 1345. The defendants must be inhabitants of, transact business in, or be found in the District for the court to have personal jurisdiction. Therefore, a plaintiff in the District of Columbia must supplement its jurisdictional allegations against a remailer in another state through discovery. Discovery against a remailer who does not keep records may prove futile.

115. "[S]uch technology is already creating problems for the legal system by making it impossible to identify a responsible party when assessing civil or criminal liability." Levine, *supra* note 19, at 1527.

116. *Id.* at 1541–42.

117. *Id.* at 1572.

118. Levine notes that "the present law governing the liability of anonymous remailers . . . is confusing and uncertain, . . . [and] to the extent the law is discernable, it creates incentives for administrators to either shut down their remailers or operate them irresponsibly." [i.e., without keeping a list of true identities]. *Id.* at 1557.

119. *Id.* at 1561.

120. *Id.* at 1563. Levine envisions that "an incentive can be provided through a safe harbor provision guaranteeing the remailer administrator protection from civil and criminal liability when the administrator (1) has acted in good faith, and (2) voluntarily discloses to the authorities the identity of a user engaging in illegal activities." *Id.*

ers who are known to present a legal liability because of their past acts."[121]

Although Levine's proposal is theoretically appealing,[122] it will fail in practice for several reasons. First, because a byproduct of Levine's proposal is advocating the criminalization of remailers who do not keep true identity records, the natural result of implementation of his program will be remailer flight from jurisdiction.[123] As discussed above with respect to Professor Hardy's proposal, very little can be done to prevent or address such flight.

Second, like Professor Hardy, Levine fails to recognize that even if all of the anonymous remailers on earth could somehow be controlled, the problem of anonymous cyberspace communication abuse would still not be solved—there are other ways to send an anonymous message. However, as Levine correctly notes, a change in the legal treatment of anonymous remailers in the United States could have an effect on the protocol of accepted cyberspace behavior of foreign remailers.[124]

Levine asserts that his proposal would pass constitutional scrutiny,[125] and it is likely that this is correct, because it promotes pseudo-anonymous remailers and does not bar all truly anonymous communication. Therefore, his proposal might be worth attempting.

What can be done to realistically combat anonymity abuses in cyberspace? Perhaps very little. However, there may be an approach that offers a more realistic solution than Professor Hardy's proposal, promises to be more effective than Levine's proposal, and offers more legislative direction than the Attorney General's report. For crime-fighting purposes, the government can criminalize most true cyberspace anonymity, forcing all non-privileged messages to become pseudo-anonymous, without violating the First Amendment.

---

121. *Id.* at 1560.

122. According to R. H. Coase, "A regulation need not be absolutely effective to be sufficiently effective." *See* Lawrence Lessig, *The Zones of Cyberspace*, 48 STAN. L. REV. 1403, 1405 (1996).

123. Levine incorrectly concludes that "it is highly unlikely that the significant number of domestic remailer administrators would change their country of residence just to be able to continue running their own remailers free from regulation." Levine, supra note 19, at 1564. Levine fails to account for the strong motivations of remailer administrators that he noted earlier in his comment: "[M]ost remailer administrators are . . . motivated by either an interest in having the service available for their personal use or a deep-seated belief in the virtues of anonymity." *Id.* at 1533.

124. *Id.* at 1564.

125. *Id.* at 1542.

B. *Argument*

This comment proposes that, for the express purpose of targeting non-desirable forms of anonymous communication, legislatures can criminalize all non-privileged, truly anonymous communication in cyberspace, and mandate that all anonymous communication in cyberspace be merely pseudo-anonymous.

State and federal governments have attempted to regulate cyberspace anonymity in the past, but their proposals have failed for various reasons, such as the legislation being over-broad and infringing on First Amendment protections of freedom of speech.[126] Legislatures may draft a constitutional regulation of anonymous speech by: (1) narrowly tailoring legislation to target specific crimes; and (2) enabling use of specific technology to ensure that the legislation only affects the targeted crimes.[127]

Given the unique nature of cyberspace, the first requirement is already necessary, and both requirements are possible.[128] Although it will remain forever impossible to eradicate all abusive, truly anonymous communication, both in and out of cyberspace, this proposal is a realistic legislative remedy that will decrease cyberspace anonymity abuses worldwide and pass First Amendment scrutiny.

First, for anti-anonymity legislation to succeed, it must narrowly target specific evils. Governments must recognize that within the distinction between true anonymity and pseudo-anonymity lies the key to legislative restrictions that can pass First Amendment scrutiny. Because some types of true anonymity, such as political speech, are considered valuable and necessary elements of society,[129] the legislation cannot merely target all true anonymity under the assumption that its existence promotes anonymous criminal acts. Legislatures must isolate and target only non-protected truly anonymous speech in cyberspace, such as cy-

---

126. *See supra* Part II.

127. For example, the Supreme Court rejected one legislature's argument that its statute "aimed at providing a way to identify those responsible for fraud, false advertising and libel" because "nothing in the text or legislative history of the ordinance limited its application to those evils." McIntyre v. Ohio Electronics Comm'n, 514 U.S. 334, 343 (1995) (quoting Talley v. California, 362 U.S. 60, 64 (1960)).

128. As stated above, legislatures will never be able to end all truly anonymous communication. Regardless of this fact, statutes criminalizing anonymity must only affect targeted crimes, or they will be struck down by the courts as over-broad. Proper use of technology can insure that narrowly tailored anti-anonymity statutes have only the intended effect.

129. Political speech, crime witnesses, novelists, whistle blowers, and Federalist Paper authors are among the socially valued and protected beneficiaries of truly anonymous communication.

berstalking, child pornography, or libel.[130] The necessary tools to narrowly tailor such legislation for the vast reaches of cyberspace are outlined below.

Second, because technology controls cyberspace, the government must address the technology. While this seems like an obvious point, it is actually quite controversial.[131] The present architecture of cyberspace only fuels the debate.[132] Regardless of the present state of cyberspace, governments can already effect change through technology.

The government must: (A) give away free computer software[133] and take other steps[134] to make pseudo-anonymous communication an attractive, viable alternative to truly anonymous communication; and (B) respect people's cloaked identities.[135] Indeed, the unmasking of an

---

130. *See generally* Walter Pincus, *The Internet Paradox: Libel, Slander & the First Amendment in Cyberspace*, 2 GREEN BAG 2d 279 (1999).

131. David Johnson and David Post assert that "efforts to control the flow of electronic information across physical borders ... are likely to prove futile." Johnson & Post, *supra* note 9, at 1372. On the other hand, Lessig proclaims that "Code (as in software) is an efficient means of regulation." Lessig, *supra* note 122, at 1408.

132. "Just now the architecture of cyberspace is quite imperfect. Indeed, what is central about its present architecture is the anarchy that it preserve.... but this anarchy is just a consequence of the present design. In its present design, cyberspace is open, and uncontrolled; regulation is achieved through social forces much like the social forms that regulate real space ... It could be made different, and my sense is that it is. The present architecture of cyberspace is changing." See Lessig, *supra* note 122, at 1408.

133. The failure of government-created computer programs may raise yet-unanswered problems. *See* Michael Rustad & Lori E. Eisenschmidt, *The Commercial Law of Internet Security*, 10 HIGH TECH. L.J. 213, 245 (1995) ("Many questions arise in trying to apply negligence theory to an Internet security breach caused by a failed security device.").

134. Devices that access cyberspace, including computers, web phones, Web TVs, and Global Positioning System units, are typically assigned an identifier known as an IP address. Since there are a limited number of potential addresses, devices that "dial-up" cyberspace are often assigned "dynamic addresses" that are reassigned to other devices at the end of a call, allowing the address to be used more efficiently. It is difficult to track the users of these devices because their addresses change from call to call or day to day.

A revised addressing scheme vastly increases the number of potential addresses, and the Internet Engineering Task Force (IETF) will soon decide whether dynamic address assignments should persist for much longer periods of time. *See* Macavinta, *supra* note 32. If this occurs, each device will essentially have its own virtual license plate, and all communications stemming from a device will be easily associated with its users. A program that cloaks the sender's IP address via a PGP-like encryption technology would enable truly anonymous communication. However, if a neutral body held the encryption key, the communication would become pseudo-anonymous because the true identity of the user could ultimately be discovered.

135. This second requirement may lead to a new (fairly ironic) problem: the theory that rational governments are likely to increase their eavesdropping activities as technological advances make eavesdropping easier. *See* Karl, *supra* note 16, at 530 n.176; *see also* A. Michael Froomkin, *The Metaphor is the Key; Cryptography, the Clipper Chip, and the Constitution*, 143 U. PA. L. REV. 709, 804–05 (1995) (asserting that rational governments are likely to increase their eavesdropping activities as technological advances make eavesdropping easier).

individual using this technology would be possible only after meeting a very high standard, such as a warrant issued by a judge.[136] While this solution may sound far fetched, it is technologically feasible and within the power of the United States. Additionally, it likely would pass constitutional scrutiny because it provides a level of pseudo-anonymity that approaches true anonymity in its ability to cloak the sender's identity, while eliminating the problems associated with truly anonymous communication.

To increase the effectiveness of this proposal, legislatures would have to take additional steps, but these steps are not crucial to the constitutional viability of this proposal. For example, legislation that forced email service providers to keep logs and verify the identities of their users,[137] combined with legislation that forced local libraries and sidewalk cyberspace cafes to register the identities of people using their computers, would decrease people's ability to send truly anonymous communication.[138] There may even be an attractive alternative to Levine's proposal for anonymous remailers: instead of keeping records of sender names, remailers could simply allow the encrypted IP address of the message sender to pass through unmodified.[139] This would enable message senders to comply with the anti-anonymity legislation while sending messages that are close to truly anonymous.

This proposal is akin to everyone driving with an encrypted license plate, identifiable only with good cause. Opponents complain that the anonymity police would pull people over too often, but access to people's identities would remain in a safe place, accessible only with a proper warrant.[140] These ideas are not new; identity discovery policies are already in effect with other kinds of communication, such as wiretap

---

136. *See* Karl, *supra* note 16 at 530 ("The United States Supreme Court consistently has held that the government may not inquire into a person's private associations.") (Footnote omitted).

137. Internet service providers are asked to keep logs so that if they are attacked, authorities can use the information to help track down the hackers. Joe Wilcox, *Reno Vows Fed Help in Combating Net Vandalism*, CNET News.com (Feb. 9, 2000), *available at* http://news.cnet.com/news/10-1005-200-1546086.html?tag=st.cn.sr.ne.1 (on file with MTTLR).

138. As Ron Dick, chief of the FBI's computer investigation section explained, "Until you get to the keyboard being utilized [by an anonymous message sender], you don't know what you're dealing with." In other words, even if the sender's computer can be identified, the sender herself may remain anonymous. *Biggest Cyberattack Was Simple*, NYTimes.com (Feb. 9, 2000), *available at* http://www.nytimes.com (on file with MTTLR).

139. As always, Hackers will be able to bypass this system and use the remailers to send truly anonymous messages. However, this does not affect my proposal because "what hackers do doesn't define what the effect of law as [a] code is on the balance of the non-hacker public." Lessig, *supra* note 122, at 1408 n.17.

140. Although this statement assumes trust in the United States government, this proposal does not require people to trust the government any more or less than the average citizen does during the course of a day.

and mail read warrants. This policy will not stop all true anonymity,[141] but because it provides for powerful and socially beneficial pseudo-anonymity, it should pass First Amendment muster. And if for political or other socially acceptable reasons, someone needs to send a truly anonymous, constitutionally protected communication through an anonymous remailer that does not keep records, it will remain easy for them to do: just turn off the IP address encryption program and press <SEND>.

CONCLUSION

Despite the impact of high-profile e-commerce attacks, and despite the Justice Department's request for more funds to fight cyber crime,[142] former President Clinton wanted to ensure that the Internet remains "open and free."[143] In July, 1997, Ira Magaziner (then a senior White House policy advisor), declared that because of the "breakneck speed of change in technology, . . . Government attempts to regulate [the Internet] are likely to be outmoded by the time they are finally enacted."[144] This sentiment remains true, but that has not kept legislators from trying to control cyberspace.

Because cyberspace enables truly anonymous communication to flourish on a scale never before experienced, its existence promotes anonymous criminal acts. As the influence of cyberspace increases in society, these acts will only become more prevalent.[145] Although no one

141. Criminals who want to communicate anonymously will find a way to do so, regardless of legislation.

142. "Growing concern over the increased threat of cyber crime has prompted the Justice Department to request another $37 million next year on top of the estimated $100 million already being spent to combat increasingly sophisticated computer criminals." *Justice Department Wants More Funds to Fight Cyber Crime*, CNN.com (Feb. 9, 2000), *available at* http://www.cnn.com/2000/US/02109/cyber.crime.money/index.html (last visited Jan. 15, 2001)(on file with MTTLR).

143. "President Clinton met in the White House Cabinet Room with about 20 industry representatives, national security experts and Attorney General Janet Reno. He said the goal of the meeting was to ensure that the Internet remains 'open and free.'" See *Web Security, supra* note 8.

The President does not, however, want to ensure that the hackers remain free. According to Attorney General Reno, the government is "committed in every way possible to tracking down those who are responsible." Wilcox, *supra* note 137. Reno explained that the F.B.I. will mobilize massive resources to try to hunt down and prosecute the attackers in cooperation with federal, state and local law enforcement, government and private sector computer experts, the intelligence community, and military experts. *Id.*

144. Lohr, *supra* note 54 (alteration in the original).

145. Michael Vatis, director of the National Infrastructure Protection Center, told the Senate Judiciary Committee that the main difficulty in catching cybercriminals is determining where and how the crime was committed. Troy Wolverton & Greg Sandoval, *Net Crime*

can stop a determined person from sending a truly anonymous electronic message, letter, or phone call, authorities can attempt to catch the criminals who do,[146] and legislatures can take preventive action so that it does not happen again. Educated legislators can criminalize most true anonymity in cyberspace and still pass constitutional scrutiny, as long as they provide viable and realistic alternatives for anonymous communication. The pseudo-anonymity requirements proposed by this comment fight crime, and at the same time provide people with enough anonymity for their communications to pass First Amendment scrutiny and promote the ideals of democracy.

Poses Challenge to Authorities, CNET News.com (Oct. 12, 1999), *available at* http://new.cnet.com/news/0-3834-200-850601.html (last visited Jan. 15, 2001)(on file with MTTLR). Vatis says he, "expect[s] to see an increase in hacking by organized crime as the new frontier for large scale theft." David Kennedy, director of research services for Isca.net, a security company that advises Internet companies on how to improve their security, believes that "things will get worse before they get better." *Id.*

146. Steve Lohr, writer for the New York Times, notes that the FBI, Justice Department and FTC are "increasing their computer crime and Internet fraud squads" and that "the issue appears to be mainly one of enforcement, not the need for new laws or policies." Lohr, *supra* note 54.

The FBI recently unveiled a computer system called "Carnivore" that acts as a traditional phone tap for internet communications. Given the identity of an individual and access to that individual's ISP, and given proper legal authorization, the FBI can use Carnivore to examine all of the packets crossing the ISP's network and capture investigated communications. Aside from the problem of actually identifying who to look for and where to look, U.S. Representative Charles Canady, chairman of the House Judiciary Committee's Constitution panel stated that "Carnivore raises the question as to whether existing statutes protecting citizens from 'unreasonable searches and seizures' under the Fourth Amendment appropriately balance the concerns of law enforcement and privacy." *FBI Defends Email Scanner to House Probe*, CNET News.com (July 25, 2000), *available at* http://new.cnet.com/news/0-1005-200-2339615.html (on file with MTTLR).

To top off the issue, Troy Wolverton and Greg Sandoval, staff writers for CNET News.com, say that "although crime might pay, combating it usually doesn't" because "[m]ost online fraud cases involve amounts small enough that authorities often won't investigate." They explain that "[l]aw enforcement officials have been scrambling to catch up with these kinds of criminals—hobbled by insufficient resources and a flurry of trained investigators leaving for the private sector." Wolverton & Sandoval, *supra* note 145. Doug Rehman, president of the Florida Association of Computer Crime Investigators agreed: "Unfortunately I don't think that you're going to see law enforcement catch up with the curve. In many ways, it's easier to commit crimes in cyberspace than in the real world." *Id.*