CRYPTOGRAPHY AND ANONYMITY: TWO REASONS WHY THE FIRST AMENDMENT FAVORS PEER-TO-PEER TECHNOLOGY

ROBYN WAGNER

FIRST AMENDMENT

SPRING, 2002

I. INTRODUCTION

> "The core problem with copyright is that enforcement of it requires monitoring of communications, and you cannot be guaranteed free speech if someone is monitoring everything you say. This is important, most people fail to see or address this point when debating the issue of copyright, so let me make it clear: You cannot guarantee freedom of speech and enforce copyright law. It is for this reason that Freenet, a system designed to protect Freedom of Speech, must prevent enforcement of copyright."[1]

On Monday morning, October 1, 2000, some 150 members of national and international media organizations crowded at the main entrance to the Federal Court of Appeals building in

[1] Ian Clarke, *The Philosophy Behind Freenet*, THE FREE NETWORK PROJECT, *at* http://freenetproject.org/cgi-bin/twiki/view/Main/Philosophy.

San Francisco.[2] Several of these delegates had arrived as early as 4:15 am, awaiting the 11:00 am start of what would prove to be one of the most notorious trials in the realm of Copyright law: *A&M Records, Inc. v. Napster, Inc.*[3] The case generated the most publicity out of any hearing in Ninth Circuit history.[4] The proceedings were shown live on television, and streamed on the Internet.[5]

According to a Napster Press Release in July of 2000, some 20 million individuals had downloaded its music sharing software.[6] At that time, the Napster service was accessed by over four million individual users per day, with 500,000 concurrent users at any given time.[7] For comparison, AOL claims 1.5 million simultaneous users at any given time.[8] By the time legal proceedings were commenced against the company, an estimated 75 million people worldwide were using Napster on a regular basis.[9]

Clearly, the fate of Napster would be of keen interest to millions of people. And, on February 12, 2001, the electronic world watched as the Ninth Circuit returned its unanimous decision against the service.[10] Though the service continues to exist with a radically altered business model,[11] many of Napster's users referred to the decision as one that "killed Napster."[12] What the decision did not do, however, was to kill the public's desire to trade files freely, especially music files. Indeed, ever more sophisticated and powerful alternatives to Napster continue to sprout, attracting former Napster users in droves.[13] In a real sense, Napster's demise served as a catalyst, driving software designers to create file sharing systems more robust against legal attack, and spurring users to adopt these increasingly sophisticated systems. Napster was a revolutionary program for one primary reason: it brought file sharing to the mainstream public. When Napster was no longer provided a viable means for file sharing was not reduced, it shifted to whatever service could continue to provide access to content.

New technologies periodically threaten to eliminate content owners' abilities to enforce their copyrights, and American copyright law has been at odds with such technologies since its

---

[2] *See* David Kravets, *Napster Hearing: Media Circus*, AP NEWSWIRES, October 1, 2000.

[3] 239 F.3d 1004 (9th Cir. 2001) [hereinafter Napster III].

[4] *See* Kravets, *supra* note 2 (According to court administrator, Terry Nafsi, "Without a doubt, this is the most in terms of the number of media we had in the building.")

[5] *Id.*

[6] Press Release, Napster, Inc., Community of Napster Users Now Exceeds 20 Million; Music Lovers of All Ages and Diverse Interests Drive Record Adoption Rate (July 19, 2000) (available *at* http://www.napster.com/pressroom/pr/20Million.html).

[7] *Id.*

[8] *Id.*

[9] *See* A&M Records, Inc. v. Napster, Inc., 114 F.2d 896, 902 (N.D. Cal. 2000) [hereinafter Napster I].

[10] Napster III, 239 F.3d 1004 (9th Cir. 2001). The court denied Napster's request for a rehearing before the full court. *See* A&M Records, Inc. v. Napster, Inc., No. 00-16401 (N.D. Cal. June 22, 2001) (panel reh'g & reh'g en banc denied).

[11] *See Napster Copyright Policy*, NAPSTER, INC., *at* http://www.napster.com/terms/.

[12] *See, e.g.*, James Campion, *Who Killed Napster?*, *at* http://www.jamescampion.com/cheknapster.html.

[13] *See* Charles Herold, *There's Life After Napster – Lots of It*, ON Magazine (July 10, 2001), *at* http://www.onmagazine.com/on-mag/head_to_head/article/0,9985,166981,00.html. Indeed, there are so many alternatives that websites such as http://www.zeropaid.com exist to rate file sharing applications and help consumers stay apprised of new features and developments in file sharing technologies.

inception.[14] In nearly every case, however, copyright has adjusted to the new technology, frequently finding an unexpected trove of revenue for the copyright holders who had so decried the new technology.[15] Examples of such technologies include piano rolls,[16] phonorecords,[17] motion pictures,[18] cable television,[19] photocopiers,[20] video cassette recorders ("VCRs"),[21] and digital audio tapes ("DATs").[22]

Modern file sharing technologies, such as Napster, present yet another such new technology which threatens the rights of copyright holders. The "descendants" of Napster, however, offer something more. By incorporating strong cryptography and anonymity into modern file-sharing systems, they potentially offer unparalleled avenues of speech. The result pits the First Amendment squarely against the Copyright Act in an unprecedented manner.

II. FILE SHARING

An estimated forty million people worldwide used the Internet in 1996.[23] By 2000, the Internet had more than 200 million users.[24] This exponential growth of Internet use has brought users an unprecedented ability to view, share, and store copyrighted works.[25] The ability of individuals to share computer files is not a new phenomenon, however.

---

[14] Trotter Hardy, *Copyright and "New Use" Technologies*, 23 NOVA L. REV. 659, 672-86 (1999); Mary L. Mills, *New Technology and the Limitations of Copyright Law: An Argument for Finding Alternatives to Copyright Legislation in an Era of Rapid Technological Change*, 65 CHI.-KENT L. REV. 307, 308 (1989).

[15] Arthur R. Miller, *Copyright Protection for Computer Programs, Databases, and Computer-Generated Works: Is Anything New Since CONTU?*, 106 HARV. L. REV. 977, 982 (Mar. 1993) (footnotes omitted); *See generally* Sony Corp. of Am. v. Universal City Studios, Inc., 464 U.S. 417 (1984) (ruling on the legality of Videocassette Recorders ("VCRs")). Today the entertainment industry has transformed videocassette sales and rentals into a $ 10 billion a year market with a total of $ 250 billion invested in VCRs and VHS programming. Joe Ryan, *Blank Video Tape Market Trends*, PRC NEWS, Jan. 11, 1999, at 5.

[16] *See, e.g.*, White-Smith Music Publ'g Co. v. Apollo Co., 209 U.S. 1 (1908) (holding that creating rolls containing copyrighted music for player pianos was not an infringing act).

[17] *See, e.g.*, Stern v. Rosey, 17 App. D.C. 562 (1901) (holding that creating a phonorecord of copyrighted material did not violate the Copyright Act, because it was neither "publishing" nor "copying" within the meaning of the Act).

[18] *See, e.g.*, Kalem Co. v. Harper Bros., 222 U.S. 55, 63 (1911) (holding that since the motion picture Ben Hur was a photographic interpretation of a copyrighted story, a public exhibition of the film constituted infringement); Edison v. Lubin, 122 F. 240, 242 (3d Cir. 1903) (stating motion pictures are similar to photographs and are copyrightable).

[19] *See, e.g.*, Fortnightly Corp. v. United Artists Television, Inc., 392 U.S. 390, 399 (1968) (holding that a cable company relaying copyrighted content did not "perform" the content, and thus did not infringe upon the Copyright Act).

[20] *See, e.g.*, Williams & Wilkins Co. v. United States, 487 F.2d 1345, 1359 (Ct. Cl. 1973), *aff'd* 420 U.S. 376 (1975) (holding that because it was a nonprofit institution devoted to the advancement of medical knowledge, a medial journal publisher's photocopying constituted "fair use").

[21] *See, e.g.*, Sony Corp. of Am. v. Universal City Studios, Inc., 464 U.S. 417 (1984).

[22] Congress addressed concerns about DAT recorders and DATs in the Audio Home Recording Act of 1992 ("AHRA"), Pub. L. No. 102-563, 106 Stat. 4237 (1992) (codified at 17 U.S.C. 1001-10).

[23] *See* Brandon K. Murai, *Online Service Providers and the Digital Millennium Copyright Act: Are Copyright Owners Adequately Protected?*, 40 SANTA CLARA L. REV. 285 (1999).

[24] *See id.*

[25] *See* M. ETHAN KATSH, LAW IN A DIGITAL WORLD 216 (1995).

File sharing[26] was first developed at Sun Microsystems for their UNIX operating system[27] and allowed for the public and private sharing of computer data within a computer network.[28] To protect data from unauthorized access on a network, various levels of access privileges can be employed, allowing specific individuals access to specific files, while preventing others from accessing the same data.[29] The primary benefit of file sharing is that information may be accessed and distributed substantially more quickly, easily, and cheaply than physical transfers.[30] As stated above, the UNIX operating system and other mainframe systems have employed file sharing for many years.[31] These mainframes were generally used in the earlier days of the Internet, which began as a network designed by the military to withstand disasters, including nuclear war.[32] To further this end, the system was designed to maintain its integrity, even if portions failed,[33] and a decentralized structure was employed so that a user could send and receive information with another user, without having to go through a centralized point.[34]

As the Internet matured and became more commercial, it was adopted by the general public. Individuals have gained the ability to share information at great distances,[35] and to use protocols such as the file transfer protocol ("FTP") to download and copy files onto their hard drives.[36]

A. An Overview of Peer-To-Peer Networking

Generally, when an individual user views a Web page from his home computer, he does not have a direct connection to that particular Web page. Instead, the user's computer sends a request to his provider, which then sends the request to the server containing the Web page. The Web server then transmits the requested data back to the individual's service provider, which sends the page contents to the individual who requested it.[37] As an example, suppose a user with

---

[26] The term, "file sharing," generally refers to sharing files digitally – by transmitting the files electronically, instead of mailing physical copies of electronic media, such as by mailing a floppy disk through the postal service. *See File Sharing*, *at* http://whatis.techtarget.com/definition/0,,sid9_gci212119,00.html [hereinafter File Sharing].

[27] *See Company Information: Sun History*, SUN MICROSYSTEMS *at* http://www.sun.com/aboutsun/coinfo/history.html.

[28] *See* File Sharing, *supra* note 26.

[29] *See id.*

[30] *See id.*

[31] *See id.*

[32] One of the original systems, called ARPANET, was developed in 1969 through the efforts of the military and universities engaged in military defense projects. *See, e.g.*, Reno v. ACLU, 521 U.S. 844, 849-50 (1997).

[33] *Id.*

[34] "The ARPAnet became the first computer network in the nation, and in it, each computer was an equal partner. That 'peer-to-peer' concept remains the fundamental idea in networking." John Markoff, *Creating a Giant Computer Highway*, N.Y. TIMES, Sept. 2, 1990, at 1.

[35] *See* Murai, *supra* note 23, at 286 (stating the last five to ten years of advancement in computer technology have allowed individuals to interact through a digital medium, where they formerly had been unable to communicate due to geographic considerations).

[36] *See* File Sharing, *supra* note 26.

[37] Jesse Berst, *How Napster and Friends Will Turn the Web Inside Out*, ZDNET ANCHORDESK (Apr. 24, 2000), *at* http://music.zdnet.com/misc/opinion/2000_ 04 _24_nap.html.

a Comcast cable modem wishes to view a web page at Hotmail.[38] The user's web browser sends a request for the web page to a Comcast server, which then forwards the request to a Hotmail server. Hotmail then sends the requested content back to the Comcast server, which delivers the content to the requesting user.

A peer-to-peer ("P2P") network, in contrast, operates more like the original Internet transmissions than typical web connections. In a P2P network, all computers have equal status, both sending out requests for information, and responding to requests for information.[39] In effect, the user's computer becomes a server, obviating the need for a large, central server to distribute content to other users.[40] Moreover, while a user's computer uploads information to other computers, it may also simultaneously download information.[41] Napster's premiere in November 1999 created a sort of P2P renaissance, reminding Internet developers of the power of P2P technology.[42] One substantial result of the recent re-adoption of P2P technology is the manner in which users search for content on the Internet. The traditional method of Internet searching is for a person to visit a search engine, such as Google,[43] type in a query, and wait for a response. Google and other similar engines periodically index the text found on all of the web pages contained in its catalogue. When a user queries Google, the search engine examines its catalogue, and returns the results to the inquiring user.[44] The results may be outdated, since the search engines update their information only periodically. In contrast, P2P networks offer the ability to provide for "real-time" searches.[45] Thus, it is possible that with the wide adoption of P2P technology, every site on the Internet could be interconnected and indexed with up-to-the-minute results.[46]

Before delving into the greater implications of P2P technology, a working knowledge of the evolution of P2P networks themselves becomes necessary, including an exploration of the copyright problems necessitating the evolution of these networks.

---

[38] http://www.hotmail.com.

[39] *See* David Streitfeld, *The Web's Next Step: Unraveling Itself; Software Threatens Search Engines*, WASH. POST, July 18, 2000, at A01.

[40] *Id.*

[41] *Id.*

[42] *See* Ariana Eunjung Cha, *E-Power to the People; New Software Bypasses Internet Service Providers*, WASH. POST, May 18, 2000, at A01.

[43] http://www.google.com.

[44] According to a report by BrightPlanet (http://www.brightplanet.com), the largest, most comprehensive search engines, including Google, analyze approximately one billion of the reported 550 billion web sites in existence. *See The Deep Web: Surfacing Hidden Value*, BrightPlanet, *at* http://128.121.227.57/download/deep_web_whitepaper.pdf.

[45] Gene Kan, developer of Gnutella, a Napster alternative, has founded a company called Gonesilent.com, which is building InfraSearch, a search engine based on P2P technology. *See* John Healey, *Search Engines Go Further and Wider as Technologies Tap More Resources: Getting a Better View*, HOUS. CHRON., June 23, 2000, at 1.

[46] *Id.*

B. Copyright Infringement

1. Copyright Protections

Intellectual property protection, in the form of Copyright, is rooted in the United States Constitution.[47] Under the Copyright Act, the following broad category of original works of authorship[48] may be protected: (1) literary works,[49] (2) musical works, (3) dramatic works, (4) choreographic works, (5) pictorial, graphic, and sculptural works,[50] (6) motion pictures,[51] and (7) sound recordings.[52]

Three basic requirements must be met for a work of authorship to qualify for copyright protection. First, the work must be original[53] meaning that it may not be copied from another source.[54] Next, the work must not consist entirely of "ideas," but must also contain some amount of "expression."[55] Finally, the work must be fixed in a "tangible medium of expression...from which it can be perceived, reproduced, or otherwise communicated, either directly or with the aid of a machine or device."[56] Thus, U.S. copyright protection begins as soon as an original work of authorship is fixed, for example, as soon as a pen touches paper and original sentences are recorded.[57]

Copyright can constitute potentially valuable protection for intellectual property because, subject to a few limitations, it gives a copyright owner[58] certain exclusive rights, including the right to control the distribution of the work, the right to copy the work, and the right to make

---

[47] U.S. CONST. art. II, § 8, cl. 8.

[48] 17 U.S.C. § 102 (1988 & Supp. IV 1992).

[49] *Id.* § 101. "'Literary works' are works, other than audiovisual works, expressed in words, numbers, or other verbal or numerical symbols or indicia, regardless of the nature of the material objects, such as books, periodicals, manuscripts, phonorecords, film, tapes, disks, or cards, in which they are embodied." *Id.* Computer software programs are protected as literary works accordingly.

[50] "'Pictorial, graphic, and sculptural works' include two-dimensional and three-dimensional works of fine, graphic, and applied art, photographs, prints and art reproductions, maps, globes, charts, diagrams, models, and technical drawings, including architectural plans. Such works shall include works of artistic craftsmanship insofar as their form but not their mechanical or utilitarian aspects are concerned." *Id.*

[51] "'Motion pictures' are audiovisual works consisting of a series of related images which, when shown in succession, impart an impression of motion, together with accompanying sounds, if any." *Id.*

[52] "'Sound recordings' are works that result from the fixation of a series of musical, spoken, or other sounds, but not including the sounds accompanying a motion picture or other audiovisual work, regardless of the nature of the material objects, such as disks, tapes, or other phonorecords, in which they are embodied." *Id.* Sound recordings were added to the Copyright Act under the Sound Recording Act of 1971, Pub. L. No. 92-140, 85 Stat. 391.

[53] *See, e.g.*, Baker v. Selden, 101 U.S. 99, 102 (1879).

[54] *Id.*

[55] 17 U.S.C. § 102(b) (1978).

[56] *See id.* § 102(a); *see also id.* § 101 ("A work is 'fixed' in a tangible medium of expression when its embodiment in a copy or phonorecord, by or under the authority of the author, is sufficiently permanent or stable to permit it to be perceived, reproduced, or otherwise communicated for a period of more than transitory duration.").

[57] 17 U.S.C. § 302(a) (1988 & Supp. IV 1992).

[58] Section 202 of the Copyright Act distinguishes between ownership of a copyright itself, and ownership of "any material object in which the work is embodied." 17 U.S.C. § 202 (1988 & Supp. IV 1992). Ownership of a particular object, for example, a paperback copy of a Stephen King novel, does not of itself convey any rights in the copyrighted work embodied in the object, such as a right to make a motion picture based on the novel.

derivative works.[59] Any person or entity which violates any of the exclusive rights of a copyright owner is an infringer of the copyright.[60] Both civil and criminal remedies are available under the Copyright Act. In a civil action, an infringer can be held liable for actual damages and any profits which the infringer may have made from the infringement,[61] or for statutory damages, at the copyright owner's choice. Statutory damages can range from $500 to $20,000 per non-willful infringement, and up to $100,000 per willful infringement.[62] A prevailing copyright owner in a civil infringement action may also be awarded attorneys' fees and court costs.[63] The court may also order the destruction or forfeiture of all infringing copies, plates, molds, tapes, negatives, or other articles used for reproduction.[64]

2. Copyright Infringement on the Internet

The Internet provides a means of inexpensive, accurate, and prompt distribution of digital information such that effectively anyone with access to an ordinary personal computer and a connection to the Internet can send or receive that information with minimal effort.[65] This information can include text, sound, images, software, and other data. Access to the Internet can thus present an impressive challenge to laws that govern the dissemination and duplication of information.[66]

The threat and harm of digital piracy and other copyright infringement is significant, in part, because it is easier to accomplish, and significantly harder to defend against than its analog counterparts.[67] For example, in 1991, it took twelve counterfeiting organizations and hundreds of employees to manufacture approximately twenty-eight million counterfeit audio cassette tapes.[68] In comparison, a handful of web pages could accomplish the same feat electronically within a short period of time, as long as they have a sufficiently fast and solid Internet connection.[69] Moreover, unlike an analog master cassette which will eventually wear out with time, or analog copies of copies which grow progressively worse in quality the further removed

---

[59] *See* 17 U.S.C. § 106 (1988 & Supp. IV 1992). Section 106 of the Copyright Act provides the owner with exclusive rights, as well as the ability to authorize others to execute those rights. The exclusive rights to perform and display the copyrighted work publicly are also provided under this section.

[60] 17 U.S.C. § 501(a)(1998) amended by 17 U.S.C. § 501(a)(Supp. III 1991).

[61] "In establishing the infringer's profits, the copyright owner is required to present proof only of the infringer's gross revenue." The burden then shifts to the infringer "to prove his or her deductible expenses and the elements of profit attributable to factors other than the copyrighted work." 17 U.S.C. § 504(b) (1988 & Supp. IV 1992).

[62] *Id.* § 504(c)(1) & (2).

[63] *Id.* § 505.

[64] *Id.* § 503(b).

[65] Lee Gomes, *Web Piracy is Hitting Hollywood Sooner than the Studios Thought*, WALL STREET J., July 17, 2000, at B1.

[66] *See* 17 U.S.C. § 106 (Supp. IV 1998).

[67] *See Anti-Piracy*, MOTION PICTURE ASSOCIATION OF AMERICA (MPAA), *at* http://www.mpaa.org/anti-piracy.

[68] *See* Stephanie Brown, *The No Electronic Theft Act: Stop Internet Piracy!*, 9 DEPAUL-LCA J. ART & ENT. L. & POL'Y 147, 154 (1998).

[69] *Id.*

they are from the master, a digital copy can be copied perpetually, and perfectly.[70] Digital copies are also significantly less expensive to produce than their analog equivalents.[71] For most film and music studios, the most expensive parts of manufacturing a DVD or CD relate to the promotional costs and packaging, including the plastic case and color inserts.[72] The media itself costs mere pennies per unit to produce.[73]

"It has been estimated that tens of billions of dollars of revenue are lost each year to copyright infringements on the Internet."[74] This sort of statistic is based on the following assumption: If a person makes a digital copy of a book available online, for example, by posting a copy to Usenet, anyone who downloads a copy of that book with not purchase a legitimate copy of the book, thus depriving book publishers of revenue.[75] Using this method of estimation, the software industry has stated that it loses billions of dollars every year to online piracy and digital copyright infringement.[76] The Recording Industry Association of America has similarly projected that its annual losses to digital piracy will reach $3.1 billion by 2005.[77] Widespread Internet piracy of feature-length movies has not yet come into existence, in large part due to the bandwidth and storage requirements which are required.[78] Nonetheless, "the implications of [motion picture] piracy on the Internet are gloomy...."[79] Clearly, the future of copyright enforcement on the Internet appears gloomy as well.

C. Specific P2P Networks

Three primary systems, Napster,[80] Gnutella,[81] and Freenet,[82] each possess unique and distinct characteristics which result in increasing difficulties in enforcing copyright law.

---

[70] *See* Benton J. Gaffney, *Copyright Statutes that Regulate Technology: A Comparative Analysis of the Audio Home Recording Act and the Digital Millennium Copyright Act*, 75 WASH L. REV. 611, 616 (2000).

[71] *Id.*

[72] *Id.*

[73] *Id.*

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

[75] The author strongly disagrees with this method of calculating loss to digital piracy, especially in the book context. A paper copy of a book may be dog-eared, highlighted, and read in the bathtub with ease. An electronic copy, while offering an ability to search for specific passages, is otherwise substantially less convenient, possessing, at least at present, none of the aforementioned benefits. As discussed in the text, the software industry also estimates losses based on a theory that anyone who downloads a pirate copy of a product would otherwise have purchased a legitimate copy if the pirate copy was not available. There are surely many people who would forego the software altogether, if faced with paying full retail price, or not having the software at all.

[76] *See* Business Software Alliance, *Sixth Annual BSA Global Software Piracy Study* (May 2001), *at* http://www.bsa.org/usa/globallib/piracy/statepiracy_study.pdf at 1.

[77] *See Report Says Music Piracy on the Rise: RIAA Cracks Down*, CBC RADIO *at* http://www.infoculture.cbc.ca/archives/musop/musop_09202000_riaa.phtml.

[78] *See generally* Christian John Pantages, *Avast Ye, Hollywood! Digital Motion Picture Piracy Comes of Age*, 15 TRANSNAT'L LAW. 155 (Winter 2002).

[79] Melissa Perenson, *Insecure Seas*, HOLLYWOOD REPORTER, Sept. 25, 2000 (quoting Jack Valenti).

[80] http://www.napster.com.

[81] http://www.gnutellanews.com.

[82] http://www.freenet.org.

1. Napster

a) Introduction

College student Shawn Fanning created file-sharing application Napster after being frustrated by his difficulty in finding MP3 music files on traditional Internet servers.[83] At the time, he was a student at Boston's Northeastern University, and had never written a software application before.[84] Napster was introduced to the public in November 1999 and rapidly grew into an Internet goliath, backed by millions of venture capital dollars and over 40 million users worldwide.[85] By September 2000, Napster users had shared some 1.39 billion songs,[86] and approximately one million users were logged into the system at any given time.[87] Napster, Inc., projected that by the end of the year 2000, it would have over 75 million users[88] and its software would be installed, or have been installed, on approximately thirty percent of all personal computers.[89]

A large percentage of the attention surrounding Napster is the result of high-profile lawsuits[90] brought by the Recording Industry Association of America ("RIAA")[91] and well-known artists.[92] In effect, Napster has been placed in the national spotlight for the notoriety of these cases, and as a shining example of how copyright law is complicated by the Internet and its continuing evolution.[93]

---

[83] *See generally* Testimony of Shawn Fanning, founder of Napster, Inc., before the Senate Committee on the Judiciary ¶¶ 6-12 (Oct 9, 2000), *at* http:// judiciary.senate.gov/1092000_sf.htm. Prior to Napster, music and other content were generally only available if someone posted that content to a web page or newsgroup, or sent it via email. *See A&M Records, Inc. v. Napster, Inc.*, 114 F. Supp. 2d 896, 905-06 (N.D. Cal. 2000).

[84] *See Napster Has Struck a Major Chord,* MILWAUKEE J. & SENTINEL, July 30, 2000, at 25D.

[85] *See id.*; Napster, *Napster News*, (Dec. 22, 2000), *at* http:// newsletter.napster.com/ archive/dec2000.php.

[86] *See* Steven Bonisteel, *Napster By Subscription? Not Anytime Soon, Experts Say,* NEWSBYTES (Oct. 3, 2000), *at* http://www.newsbytes.com/pubNews/00/156115.html.

[87] *See* Charles C. Mann, *As Judgment Day Looms, Napster Offers Users an Even More Diabolically Satisfying Experience*, INSIDE.COM (Oct. 30, 2000) *at* http://www.inside.com/story/Story_Cached/0,2770,13276_9_12&uscore;1,00.html.

[88] Benny Evangelista, *Napster Must Halt Music Swapping*, SAN FRANCISCO CHRONICLE, July 27, 2000, at A1.

[89] Dick Kelsey, *Napster Present on 30 Percent of PCs-Report*, NEWSBYTES (Oct. 24, 2000) *at* http://www.newsbytes.com/pubNews/00/157141.html.

[90] *See, e.g.*, Napster I, 114 F. Supp. 2d 896 (N.D. Cal. 2000).

[91] The RIAA is a trade association representing the majority of large record labels in the United States audio recording industry. State v. Awawdeh, 864 P.2d 965, 966 (Wash. Ct. App. 1994). RIAA members produce and distribute approximately ninety percent of all the audio recordings sold in the United States. *RIAA: About Us,* RIAA, *at* http://www.riaa.com.

[92] *See, e.g.*, Metallica et al. v. Napster Inc. et al., No. 00-0391, complaint filed (C.D. Cal., Apr. 13, 2000), and (Dr. Dre) Young et al. v. Napster Inc. et al., No. 00-04366, complaint filed (C.D. Cal., Apr. 25, 2000).

[93] *See, e.g.*, John Gibeaut, *Facing The Music: You Say You Want A Revolution? Well, The Napster Case and Others Herald the Beginning of a Technological Rebellion That May Alter Traditional Concepts of Copyright Law*, A.B.A. J., Oct. 2000, at 36.

b) How Napster Worked

To use Napster for the first time, a user had first to download a free copy of proprietary Napster software, called MusicShare.[94] The user could then use MusicShare to connect to one of Napster's central servers. At this point, the Napster server would catalogue any music files stored on the user's computer and generate a list of those filenames, making it available to other Napster users.[95] Napster users could then use the MusicShare software to search other users' computers for specific song titles or musicians, receiving a list of files available for download.[96] Files were only available for download if the host computer was online at the time.[97] Users downloaded songs by selecting a song from the list and clicking a "Get Selected Song(s)" button, which would initiate the song's transfer from the host computer to the user's computer.[98]

Users contributed to the Napster community by ripping songs from compact discs and storing them on their hard drives, compressed in the MP3 format.[99] With the increasing availability of high-speed Internet connections, including Digital Subscriber Lines ("DSLs"), cable modems, and dorm room connections, a high-quality, ten megabyte song could take anywhere from a few minutes, to as little as a few seconds to download.[100] The speed with which songs could be downloaded was of great concern to the recording industry, since the majority of the songs made available through Napster software were copyrighted.

c) A&M Records, Inc. v. Napster, Inc.[101]

The RIAA filed suit against Napster in December 1999,[102] alleging both vicarious[103] and contributory[104] copyright infringement. Specifically, the RIAA alleged that were it not for the Napster service, illegal copies of the songs would not have been as widely available.[105] The

---

[94] Napster I, 114 F. Supp. 2d at 905. Appendix Diagram A gives the following demonstration of Napster's operation: (1) The Napster server collects a listing of the host computer's MP3s; (2) The requesting user queries the Napster catalog to determine if the MP3 is available on another user's computer; (3) If the host computer has the MP3, the Napster server will notify the requesting user which host computer has the file; (4) The requesting user contacts the host computer directly, and (5) downloads the file from the host computer.

[95] *Id.*

[96] *Id.* at 905-06.

[97] *Id.* at 904-05.

[98] *Id.* at 906.

[99] MP3 technology was developed by Fraunhofer, a German engineering firm, in 1987, as a means of compressing digital audio files while preserving a high degree of fidelity. The resulting file is several times smaller than an uncompressed audio track. *See MP3 and Beyond, A Brief History of MP3*, ZDNET DEVELOPER, *at* www.zdnet.com/devhead/stories/articles/0,4413,2633688,00.html.

[100] *See* Sharon Watson, *Bandwidth Booster*, INTERNET TELEPHONY, (Oct. 6, 1997) *at* http://www.internettelephony.com/archive/10.06.97/cover.html.

[101] A & M Records, Inc. v. Napster, Inc., 114 F. Supp. 2d 896 (N.D. Cal. 2000).

[102] Complaint at 2, Napster I [hereinafter "Napster Complaint"].

[103] Vicarious infringement of copyright occurs when one "has the right and ability to supervise the infringing activity and also has a direct financial interest in such activities." Fonovisa, Inc. v. Cherry Auction, Inc., 76 F.3d 259, 262 (9th Cir. 1996).

[104] Contributory copyright infringement occurs when "one who, with knowledge of the infringing activity, induces, causes or materially contributes to the infringing conduct of another...." Sony Corp. Am. v. Universal City Studios, Inc. 464 U.S. 417, 487 (1984).

[105] Napster Complaint at ¶57.

Complaint further alleged that Napster refused to maintain a database of infringing files and users, despite an obligation to do so,[106] and that because of this intentional ignorance, Napster could be held vicariously liable for any infringements taking place via its servers.[107]

(1) Digital Millennium Copyright Act[108]

Napster argued that its service qualified for the "safe harbor" provision protections of the Digital Millennium Copyright Act ("DMCA"), and filed a motion for summary judgment.[109] The DMCA insulates Internet Service Providers ("ISPs") from copyright liability so long as they comply with certain statutory requirements designed to facilitate content providers' efforts to protect their copyrighted material.[110] The DMCA defines a "service provider" as "an entity offering the transmission, routing, or providing of connections for digital online communications, between or among points specified by a user, of material of the user's choosing, without modification to the content of the material as sent or received."[111] Napster argued that it was an ISP under 17 U.S.C. § 512 (k)(1)(A), and that because it was merely a "passive conduit" for any information transferred, it was entitled DMCA protections.[112]

The RIAA responded that 512(a) did not apply because the allegedly infringing material was transmitted directly between users' machines[113] and did not go "through" the Napster servers.[114] The plaintiffs further argued that each DMCA section must be analyzed independently[115] and that the narrower subsection 516(d), referring to information location tools such as search engines, was more applicable to the Napster model.[116] The court rejected Napster's 512(a) "safe harbor" argument, and agreed with the RIAA, ruling that Napster neglected to take active steps to curtail copyright infringement as dictated by 512(i).[117]

---

[106] *Id.* at ¶67.

[107] *Id.* at ¶70.

[108] 17 U.S.C. §§ 1201-1332 (Supp. IV 1998).

[109] Napster's Motion for Summary Judgment, A & M Records, Inc. v. Napster, Inc., 114 F. Supp. 2d 896 (N.D. Cal. 2000).

[110] *See id.* §§ 512(a)-(d), (f), (g), (i).

[111] *Id.* § 512(k)(1)(A).

[112] A&M Records, Inc. v. Napster, Inc., No. C 99-05183, 2000 WL 573136, at *5 (N.D. Cal. 2000). Section 512(a) of the DMCA states in relevant part that "[a] service provider shall not be liable for monetary relief...or other equitable relief, for infringement of copyright by reason of the provider's transmitting, routing, or providing connections for, material...or by reason of the intermediate and transient storage of that material...." The ISP is insulated if (1)the initiation of the transmission was not directed by someone other than the ISP, (2)the transmission is automatic, (3)the ISP does not select the recipient, (4)no copies are maintained on the ISP server, and (5)material is transmitted through the server without modification. 17 U.S.C. § 512(a)(1-5)(1998).

[113] Napster, 2000 WL 573136, at *6-7.

[114] Napster I, 114 F. Supp. 2d at 905.

[115] Plaintiffs' Memorandum in Opposition to Defendant's Motion for Summary Adjudication on the Applicability of the 17 U.S.C. § 512(a) Safe Harbor Affirmative Defense, at 1, Napster, 114 F. Supp. 2d at 896.

[116] *Id.* DMCA § 512(d) states that an ISP that links to infringing material is protected if, *inter alia*, it does not know that the material is infringing, it should not know that the material is infringing, it quickly removes or disables access to the material, and it does not financially benefit from the activity. 17 U.S.C. § 512 (d) (1) (A)-(C), (2)(1998).

[117] Napster, 2000 WL 573136, at *10. Section 512(i) limits copyright liability only if the service provider "has adopted and reasonably implemented, and informs subscribers and account holders of the service provider's system or network of, a policy that provides for the termination in appropriate circumstances of subscribers and

(2) Sony Corp. of America v. Universal Studios[118]

Next, the RIAA filed a Motion for Preliminary Injunction to force Napster to halt its services pending the outcome of the case at trial.[119] The RIAA argued that the "tens of millions of copies of copyrighted music" which had been transferred by Napster inflicted irreparable harm upon the RIAA.[120] It was during this phase of litigation that Napster first attempted to invoke the United States Supreme Court decision of *Sony Corp. of America v. Universal Studios*, which held "the sale of copying equipment ... does not constitute contributory infringement if the product is widely used for legitimate, unobjectionable purposes. Indeed, it need merely be capable of substantial noninfringing uses."[121] Napster argued that its service had "numerous and substantial non-infringing uses" and thus should be free of liability.[122]

(3) Preliminary Injunction and Stay Pending Appeal

At the end of the Preliminary Injunction hearing, the trial court granted the RIAA's motion, finding that the RIAA had a "strong likelihood of success on the merits" concerning the vicarious and contributory liability claims.[123] The court rejected Napster's fair use affirmative defense and its interpretation of the applicability of *Sony*.[124]

Trial court Judge Patel provided an unanticipated bench decision, ruling that beginning at midnight on Friday, July 28,[125] Napster was prohibited from "causing or assisting or enabling or facilitating or contributing to the copying, duplicating or ... other infringement upon all copyrighted songs, musical compositions or material in which plaintiffs hold a copyright or with respect to plaintiffs' pre-1972 recordings in which they hold the rights."[126] According to Judge Patel's ruling, then, Napster was not required to shut down, but instead had to devise and implement a way to prevent users from trading infringing files.[127] Judge Patel's ruling appealed to a where there's a will, there's a way mentality, suggesting that the clever Napster creators should be able to find a way to implement her ruling.[128]

---

account holders of the service provider's system or network who are repeat infringers...." 17 U.S.C. § 512(i)(A) (1998).

[118] 464 U.S. 417 (1984).

[119] RIAA Notice of Joint Motion and Joint Motion of Plaintiffs for Preliminary Injunction; Memorandum of Points and Authorities, A & M Records, Inc. v. Napster, Inc., Nos. C 99-5183 MHP, C 00-0074 MHP., 2000 WL 1182467, at *1 (N.D. Cal. Aug. 10, 2000).

[120] Napster I, 114 F. Supp. 2d at 925.

[121] 464 U.S. 417, 442 (1984).

[122] Napster's Opposition to Plaintiff's Motion for Preliminary Injunction, at 2, Napster I, 114 F. Supp. 2d at 896.

[123] Transcript of Proceedings at *1, Napster I, 114 F. Supp. 2d 896 (N.D. Cal. 2000).

[124] *Id.* at *5.

[125] Lee Gomes, *Federal Judge Brings Halt To Download Service As of Midnight Friday*, WALL ST. J., July 27, 2000, at A3.

[126] Transcript of Proceedings at *8, Napster I, 114 F. Supp. 2d 896 (N.D. Cal. 2000).

[127] *Id.*

[128] *Id.* at *6. Judge Patel stated from the bench that she was "sure that anyone as clever as the people are who wrote the software in this case are clever enough, as there are plenty of those minds in silicon valley to do it, can come up with a program that will help to identify infringing items as well."

Napster filed a Motion for Stay Pending Appeal with the Ninth Circuit Court of Appeals.[129] The Ninth Circuit granted the motion mere hours before the injunction was to be enforced,[130] and heard oral arguments on the injunction on October 2, 2000.[131] At oral argument, the panel focused primarily on Napster's ability to identify copyrighted files traded through its system, as well as its duty to block those files from its service.[132] Judge Beezer found it particularly troublesome that the RIAA expected the court to hold Napster liable for the actions of its users, questioning "[h]ow are they expected to have knowledge of what comes out of some kid's computer in Hackensack, N.J., and is transmitted to Guam?"[133]

2. Gnutella

a) Introduction

Gnutella[134] was one of the first pure P2P predecessors of Napster.[135] Gnutella is different from Napster for two reasons. First, it is not backed by any corporate entity, and second, Gnutella does not operate with the assistance of any centralized servers.

Gnutella was created by Justin Frankel, while he was employed by Nullsoft, a subsidiary of America Online ("AOL").[136] Frankel wrote the program in his personal time and posted an executable version of the program on an AOL site without AOL's permission.[137] AOL promptly disavowed Gnutella as an "unauthorized freelance project," and removed the code within a few hours.[138] Nonetheless, thousands of people had already downloaded the software by that point, and the proverbial cat was out of the bag.[139] Shortly after Gnutella's release, other programmers examined and reverse-engineered[140] the program, creating an open-source[141] version of it.[142]

---

[129] Napster Motion for Stay Pending Appeal, Napster I, 114 F. Supp. 2d 896.

[130] A&M Records, Inc. v. Napster, Inc., 2000 WL 1055915, at *1 (9th Cir. 2000).

[131] Matt Richtel, *Napster Case: Hard Queries On Copyrights*, N.Y. TIMES, Oct. 3, 2000, at C01. The oral arguments are available in MP3 format. *The Napster Case: Oral Arguments Before the U.S. Court of Appeals for the Ninth Circuit*, Findlaw.com, (Oct. 2, 2000), *at* http://legalnews.findlaw.com/legalnews/lit/napster /index5.html.

[132] Lee Gomes, *Napster Case Judges Grill Industry Side*, WALL ST. J., Oct. 3, 2000, at A3.

[133] P.J. Huffstutter, *Napster Buys Some Time as Judges Consider Appeal Copyright*, L.A. TIMES, Oct. 3, 2000, at C1.

[134] Pronounced "NEW-tella," the name is a combination of "GNU," the open-source method under which the program was written, and "Nutella," a hazelnut and chocolate spread. Lianne George, *Gnutella: The Future of Online Music?*, TORONTO STAR, July 27, 2000 at FF05.

[135] Scott Rosengerg, *Revenge of the File Sharing Masses!*, *at* http://www.salon.com (July 20, 2001).

[136] Ariana Eunjung Cha, *E-Power to the People: New Software Bypasses Internet Service Providers*, WASH. POST, May 18, 2000, at A01.

[137] Fred Vogelstein, *Is It Sharing or Stealing? Entertainment Moguls May Not Be Able to Stop Napster and Gnutella*, U.S. NEWS & WORLD REP., June 12, 2000, *at* http://www.usnews.com/usnews/issue/000612/share.htm.

[138] Amy Harmon, *Free Music Software May Have Rattled AOL*, N.Y. TIMES, Mar. 20, 2000, at C4.

[139] *See* Giancarlo Varanini, *Shawn Fanning on Napster*, ZDNET MUSIC (Mar. 1, 2000) *at* http://music.zdnet.com/download/features/napster/index.html.

[140] "Reverse engineering is the task of examining a piece of equipment to some level and...using that information to engineer the piece of equipment to do the same job and substantially in the same configuration." SI Handling Sys., Inc. v. Heisley, 581 F. Supp. 1553, 1567, (E.D.Pa. 1984).

[141] "An open standard describes a programming standard in which everyone that participates agrees to discuss and make any changes publicly. In other words, it is a programming standard over which no one company has proprietary control...." Bristol Tech., Inc. v. Microsoft Corp, 114 F. Supp. 2d 59 (D. Conn. 2000). The public is

Through the work of groups of largely unassociated volunteers, the Gnutella project continues to evolve.[143]

Instead of employing an intermediary, Gnutella technology allows users to connect directly to one another. The result is a potentially vast web of users[144] strung throughout the Internet.[145]

b) How Gnutella Works

The Gnutella network functions in a manner substantially different from that of Napster. As discussed in Section II.C.1.B, Napster relied on a central server design, in which users connected to Napster servers which in turn connected them to other Napster users. The Gnutella system is decentralized, however, meaning that users connect directly to one another without the assistance of a large intermediate server. Indeed, users may act as intermediaries for one another, allowing a single user to connect to thousands of other users in a unique web structure.[146] This can be analogized to a situation in which by one user shaking another user's hand, both users are simultaneously introduced to every person either user has ever met.[147]

As with Napster, the content made available within the Gnutella network is limited to whatever information Gnutella users provide access to on their computers while they are online.[148] However, unlike Napster, which is limited to the trading of MP3 or other music files, Gnutella enables users to search for files of any type, including movies, software, and text

---

often encouraged by open source software creators to modify and improve upon computer programs, in contrast to most commercial software where the owner does not permit users to view or to modify the software code. *See* Janelle Brown, *The Gnutella Paradox*, SALON.COM (Sept 29, 2000) *at* http://www.salon.com/tech/feature/2000/09/29/gnutella_paradox/.

[142] *See* Amy Harmon, *For Many Online Music Fans, Court Ruling is Call to Arms*, N.Y. TIMES, July 28, 2000, at 1A.

[143] These volunteers present a vastly different legal target from Napster, Inc., if they present any target at all. "Nerd Herd," a group of three programmers headed by Gene Kan, are contributors to the Gnutella project. When asked what would happen if the Recording Industry Association of America would pursue legal action against Nerd Herd, Kan replied, "I'd be curious to see them try...I mean, you can't get blood from a turnip. They wouldn't stand a lot to gain except maybe a few beat-up cars." *See* Varanini, *supra* note 139.

[144] It is estimated that approximately 40,000 computers are connected through Gnutella at any one time, and that on any given day, users offer approximately two million files of music, movies and other material. *See* Lee Gomes, *Gnutella Keeps Growing – And Growing*, ZDNET (May 28, 2001) *at* http://zdnet.com.com/2102-11-529887.html.

[145] *See* Akansha Atroley, Napster: Music to Most Ears, COMPUTERS TODAY (Aug. 15, 2000) *at* http://www.india-today.com/ctoday/20000801/trends.html.

[146] Gnutella users begin by connecting with a server which is already connected into the Gnutella network. That server then relays some of the addresses of servers with which is has recently connected, and the user's computer may connect to some of them as well. *See* Akansha Atroley, *Napster: Music to Most Ears*, COMPUTERS TODAY, Aug. 15, 2000, at 80, *at* http://www.india-today.com/ctoday/20000801/trends.html. Once the user's computer has connected to a handful of other servers, the user may then run searches on any of those servers, which will in turn be passed on to other servers, allowing ultimately for the search of several thousand servers at once. *See* Chris Sherman, *Napster: Copyright Killer or Distribution Hero?*, ONLINE, Nov. 1, 2000.

[147] A diagram of this facet of Gnutella is available at http://gnutella.wego.com.

[148] This is in contrast to Freenet, discussed *infra* Section II.C.3, where files are distributed among users throughout the system, allowing other users to access the files even after the originating user has disconnected from the system.

documents.[149] As a result, and due to the increasing availability of high-speed Internet connections, the movie industry is increasingly voicing the same sky-is-falling complaints against file sharing technology as was voiced previously by the music industry.[150]

c) Legal Implications

Gnutella's network architecture creates jurisdictional and other complications to the legal enforcement of copyright. This is so for several reasons, though primarily due to its lack of centralized servers and the nature of open-source software.

Suggestions have been made that America Online could potentially be held liable for copyright violations committed by Gnutella users, because of the "role" which America Online played in its creation.[151] However, as stated above, America Online did not sanction the project, promptly removed it from its servers upon discovery, and disavowed knowledge of Gnutella's creation. It thus appears highly unlikely that the company could be sanctioned for its "role" in the creation of the program. More importantly, substantial transformations have been made to the program since Justin Frankel first released Gnutella,[152] and it likewise appears highly difficult to hold America Online liable for a product today which looks vastly different from the one initially created by one of its employees and posted to its servers.

Copyright holders have traditionally sued centralized targets because such companies are readily identifiable, and have a specific physical presence in a known jurisdiction.[153] They are, after all, typically corporate entities, who have offices, letterhead, and employees, no different from any other company.[154]

In high contrast to Napster, Gnutella is open-source software, not officially owned by a single entity.[155] Because the application is freely distributed and may be modified by anyone who so desires,[156] several different versions of the software have been created since the original version was released, and hundreds of people have contributed to the project.[157] The result is that copyright holders are left in a much more difficult practical position. Without a central, corporate entity to sue, copyright holders would be forced to sue individual programmers or

---

[149] Amy Kover, *Napster: The Hot Idea of the Year: Lawsuits May Kill Napster, But The Concept Behind The Company Could Revolutionize Infotech and Reinvigorate The PC Industry*, FORTUNE, June 26, 2000, at 128.

[150] *See* Gary Gentile, *Movie Industry Battling Internet Pirates Hollywood Facing Napster-Like Issues with DVD Films*, CHI. TRIB., Aug. 13, 2000, at 7.

[151] America Online was named as a third-party defendant in Arista Records, Inc. v. MP3Board, Inc., No. 00 Civ. 4660 (S.D.N.Y. filed June 23, 2000). *See* Brad King, *MP3Board Targets AOL*, WIRED NEWS (Aug. 22, 2000) *at* http://www.wired.com/news/business/0,1367,38369,00.html.

[152] Brown, *supra* note 141.

[153] *See generally*, Wendy M. Pollack, *Tuning In: The Future of Copyright Protection for Online Music in the Digital Millennium*, 68 FORDHAM L. REV. 2445, 2468 (2000).

[154] Cases of this fashion include Napster I, 114 F. Supp. 2d 896 (N.D. Cal. 2000), UMG Recordings, Inc. v. MP3.Com, Inc., 92 F. Supp. 2d 349, (S.D.N.Y. 2000), and UMG Recordings, Inc. v. MP3.Com, Inc., 92 F. Supp. 2d 349, (S.D.N.Y. 2000).

[155] *See* Varanini, *supra* note 139.

[156] *See* Tom Kirchofer, *Ruling Unlikely to Stop Free Music Downloads*, BOSTON HERALD, July 28, 2000, at 28.

[157] Varanini, *supra* note 139.

users of Gnutella. This could easily result in a public relations nightmare if the 40 million Napster users are any indication of public sentiment toward file sharing. Moreover, any such litigation would pose a jurisdictional nightmare, given the geographical diversity of Gnutella users.[158] Indeed, it appears highly unlikely that the minimal damages which could be recovered from infringing Gnutella users could justify the cost and time required to assert jurisdiction and litigate actions against potentially millions of individuals in a plethora of jurisdictions.

3. Freenet

a) Introduction

United Kingdom programmer Ian Clarke has developed a P2P file sharing system, Freenet, which offers copyright enforcers a potentially insurmountable hurdle.[159] Like Gnutella, Freenet is a decentralized network, lacking any central servers which store content.[160] However, unlike the Gnutella network, where users directly query each other for files, allowing them to be identified, Freenet "requests pass though a number of computers that never know where the request originated from."[161] As a result, Freenet offers its users absolute anonymity.[162]

Ian Clarke developed the system in large part to help defeat Internet censorship:[163]

> Philosophically I was very interested in the whole idea of freedom of information, and I was somewhat concerned by what I saw as increasing moves to impose censorship on the Internet. While in 1998, when I first started to think about this, this hadn't really begun in earnest, my fears have really been justified in the past two or three years in terms of a number of Western governments making increased efforts to both monitor and censor the Internet in ways that simply wouldn't be tolerated if applied to more conventional means of communication, such as the postal service or the telephone networks.[164]

---

[158] Some of the jurisdictional issues presented by the Internet have been analyzed by the American Bar Association. American Bar Association, *Achieving Legal and Business Order in Cyberspace: A Report on Global Jurisdiction Issues Created by the Internet, at* http://www.kentlaw.edu/cyberlaw/docs/drafts/draft.rtf.

[159] Clarke developed while he was a student at Edinburgh University, Scotland. *See* Jennifer L. Schenker, *The Infoanarchist: Could This 23-Year-Old Irish Programmer Begin to Unravel the Web?*, TIME MAG., July 17, 2000, at 42.

[160] It is generally stated that the technical similarities between Gnutella and Freenet end here. *See* Damien Cave, *Information Just Wants to be Freenet,* SALON.COM (Aug. 28, 2000) *at* http://www.salon.com/tech/view/2000/08/28/uprizer/index.html.

[161] Joseph Gallivan, *Freenet On The Move-Creator's New Firm Will Sell Music Online*, N.Y. POST, July 31, 2000 (quoting Ian Clarke).

[162] *See* John Markoff, *The Concept of Copyright Fights for Internet Survival*, N.Y. TIMES ON THE WEB (May 10, 2000) (Including Ian Clarke's statement that "Freenet is a near-perfect anarchy.").

[163] Clarke also proselytizes about the impending demise of intellectual property, and recognizes Freenet's hand in contributing to that demise. *See* Jan Hopkins, *Freenet Founder*, CNNFN: STREET SWEEP, May 10, 2000 ("The idea that you can treat information like you might treat real estate or gold is something that may have been possible to enforce in the past, but now with modern communication technology and particularly with systems like Freenet, that's just not a reality anymore.") (quoting Ian Clarke).

[164] Richard Koman, *Free Radical: Ian Clarke has Big Plans for the Internet*, O'REILLY NETWORK (Nov. 11, 2000) *at* http://www.openp2p.com/lpt/a/p2p/2000/11/14/ian.html

Clarke was concerned about censorship both in Western countries,[165] and in countries more traditionally associated with draconian censorship laws.[166]

b) How Freenet Works[167]

Ian Clarke has described how Freenet works by way of a non-technical analogy:

> "You could look at it like an ant colony where instead of food you have pieces of information, and instead of ants you have requests, which travel around this network. Freenet, when you request a piece of information on Freenet, you ask your local Freenet node for that information. If it has the information itself, it will obviously return it to you. If not, it will forward that request on to another node that is more likely to have that information - and nodes in the network actually learn with time how to better route information through the network - so they additionally move information closer to where the demand for that information is, so that when you request a piece of information, immediately after you requested it a copy of that information will reside on your computer and the computers close to you for a short amount of time. If you or other people close to you then request that information, they will receive that information immediately. So this is really the way that it dynamically moves information closer to demand."[168]

The Freenet network is thus comprised of nodes and keys. Each user's computer (a "node") stores and retrieves encrypted files which can be unlocked by text string "keys."[169] Nodes shuffle keys back and forth upon request, attempting to find encrypted files on their drives which the keys will unlock.[170] Because each node may request information on its own behalf, or may instead be inquiring on behalf of another node, it is extremely different to determine who originated the search.[171] If a file is unlocked, it is stored for a finite period of time on both the

---

[165] *Id.* ("The first Western country to really impose what I viewed as somewhat Draconian censorship on the Internet was Australia, which came up with these laws whereby it had a list of Web sites that were censored and any Internet service provider in Australia that did not restrict access to that list of Web sites could be subjected to huge fines. The way that that list was generated was - in terms of the accountability of the people who were coming up with this list of what should and shouldn't be censored on the Internet - extremely dubious. Subsequently, the United Kingdom had a Regulation of Internet Powers bill, which has now become law, that allows the security services to monitor all Internet traffic, and that was extremely worrying.")

[166] *Id.* ("In countries like China and Saudi Arabia, the Internet is very, very heavily censored. Certainly Freenet could still be used there to communicate securely and to share information securely. But whereas in Western countries it's very unlikely that encryption, for example, would be banned, that is possible in countries like China. Now in terms of their ability to enforce that ban - it will be extremely costly to do that, they could just ban Freenet full stop.")

[167] Freenet relies heavily on principles of strong cryptography, mathematics, and network and system architecture of a highly technical nature. As a result, this section is somewhat over-simplified and condensed. For a more thorough treatment of Freenet's Architecture, see *Freenet Paper, infra* note 169.

[168] Richard Koman, *Free Radical: Ian Clarke has Big Plans for the Internet*, O'REILLY NETWORK (Nov. 11, 2000) *at* http://www.openp2p.com/lpt/a/p2p/2000/11/14/ian.html [hereinafter "Free Radical"].

[169] Ian Clarke et al., *Freenet: A Distributed Anonymous Information Storage and Retrieval System*, Anonymous Information Storage and Retrieval System in Designing Privacy Enhancing Technologies: International Workshop on Design Issues in Anonymity and Unobservability, LNCS 2009, ed. by H. Federrath. Springer: New York (2001) [hereinafter "Freenet Paper"].

[170] *Id.*

[171] *Id.*

requesting party's node, as well as some other node along the path which the request took.[172] One of the purposes of having these temporary copies is that more popular content is made available to more users simultaneously, helping the system maintain efficiency.[173]

c) Legal Implications

Freenet presents significant challenges both to enforcement and to prosecution of copyright violation, in large part due to Ian Clarke's five design goals in creating Freenet.[174] These goals include: (1) anonymity for both providers and consumers of content; (2) deniability of knowledge of specific content for content providers; (3) resistance to third-party attempts to limit or prevent access to information; (4) efficient routing and dynamic storage of information; and (5) fully decentralized network operations.[175] Any one of these features would present a distinct challenge to copyright enforcement online. As discussed below, a combination of these features presents a likely insurmountable bar to copyright enforcement.

(1) Anonymity for Content Providers and Consumers

Perhaps the most fundamental improvement Freenet makes over the Napster and Gnutella systems is its ability to effectively conceal the source of any content residing within the system.[176] Napster users were fairly easy to identify, as were the nature and content of whatever files they may have shared.[177] Determining the identities of Gnutella users and the content which they trade is more difficult than with Napster, but it is not impossible.[178] Freenet's architecture, however, makes it virtually impossible to track the source of information available on the network.[179] It is similarly impossible for a copyright holder to prosecute an infringer without the ability to determine either the identity or the physical location of that infringer.

(2) Content Deniability Through the Use of Strong Cryptography

---

[172] *Id.* A side effect of this design is that a copyright holder attempting to enforce copyright by searching for files on nodes will actually cause the file to propagate, a highly counter-productive result. *Id.*

[173] *See Free Radical*, *supra* note 168 ("If you look at the Web, if 1,000 people in the U.K. request the same document from the United States, the same information travels across the Atlantic 1,000 times. That...struck me as being highly inefficient in terms of network-bandwidth usage, which was, and still is, a somewhat valuable commodity. So one of the things that Freenet does is it actually moves information around and dynamically replicates information to reduce the load on the network bandwidth. So in that specific example, if 1,000 people in the U.K. request the same document from the U.S. and they were using Freenet, it would only need to travel over the Atlantic once, and thereafter it would be stored locally and distributed within the U.K. - or within Europe, depending on where the demand was.") (quoting Ian Clarke).

[174] *Id.*

[175] *Id.*

[176] *Id.*

[177] In preparation of its suit against Napster, the group, Metallica, hired a firm to determine which Napster users were trading Metallica files. Napster was presented with a list of over 300,000 Napster usernames who had traded Metallica songs. *See Napster Users Offering Pirated Metallica Songs Identified by Lawyers*, WALL ST. J., May 3, 2000.

[178] This would have to be accomplished by tracing the Internet Protocol (IP) addresses offering files back to the owners of a computer. *See Child Pornography Exchange Through Napster and Gnutella*, INTERNETNEWS.COM (Jan. 10, 2001) *at* http://www.internetnews.com/bus-news/article/0,,6_556161.00.html.

[179] *See Freenet Paper*, *supra* note 169.

One of Ian Clarke's goals in developing Freenet was to remove any culpability of node owners for the content stored on their computers.[180] He effectuated this by ensuring that Freenet users could not determine the content of any files which they stored.[181] Freenet was designed so that a node which passes information on to a requesting node also keeps a copy of that information in case of future requests.[182] These files are encrypted, however, and a key is not retained by the storing node.[183] The result is that while it is theoretically possible for a person to determine the contents of their Freenet node, it is extremely difficult mathematically to do so.[184]

The result is that is extremely difficult to impossible for law enforcement or others to determine whether a particular Freenet user has unlawful content on his computer. Similarly, even if a user wished to know the contents of his Freenet node, perhaps to remove any unlawful or other specific content, it would be equally difficult to impossible for him to do so.[185]

This deniability of knowledge of the content of one's Freenet node potentially provides Freenet users with two defenses under the Digital Millennium Copyright Act ("DMCA").[186] The DMCA provides a "safe harbor" to ISPs under which they cannot be held liable for transitory "digital network communications"[187] and system caching.[188]

The "transitory digital network communications" category appears most applicable to Freenet users because the transmission is initiated by someone other than the user, the transmission was automated, the user does not select the recipients, and the material is not modified by transmission.[189]

An equally convincing argument lies in the fact that mirroring information on a user's machine might well constitute "system caching" under § 512(b). This is so because Freenet users do not directly access the information contained within their node, but the node instead serves to cache information for others.[190]

If users are unable to determine the nature or content of information stored on their computers, it appears extremely unlikely that they could be held liable for that content.

(3) Resistance to Third-Party Interference

---

[180] *Id.*
[181] *Id.*
[182] *Id.*
[183] *Id.*
[184] *Id.*
[185] *Id.*
[186] 17 U.S.C. § 512 (1998). *See supra* text accompanying notes 110-112.
[187] *Id.* § 512(a).
[188] *Id.* § 512(b).
[189] *Id.* § 512(a)(1)-(5).
[190] *See* Netword, LLC v. Centraal Corp., No. 98-1023-A, 1999 U.S. Dist. LEXIS 1957, at *7 n.5 (E.D. Va. Jan. 12, 1999) (defining system caching as "when a computer stores information in its memory, and at the direction of a software command, searches or polls that information to find the desired result").

Freenet propagates files each time they are requested, making a copy of the file on both the requester's node, and on another, unknown user's node.[191] So, for example, if Alice requests file.txt from Bob, a copy of file.txt will also be copied, untraceably, onto Charlie's node. This functions as a sort of immune system, and as one commentator has described it, "turns the enforcement of copyright into a game of whack the mole."[192] After all, if an adversary somehow disables nodes containing a particular file, each time the file was requested from that node, it was also copied to some other, unknown node, which likely remains a viable download source.[193] This portion of the Freenet design substantially frustrates a copyright holder's ability to search the system for potentially infringing content. If for example, Metallica attempted to search for its content on Freenet as it did on Napster,[194] instead of being provided with a convenient list of infringing users, the searches themselves would serve to propagate any infringing files throughout the system.[195]

(4) Efficient Routing and Dynamic Storage

In addition to Freenet's barriers to legal and technological attack, the efficiency of the system is protected by substantial technological measures. Each time a Freenet node passes files to another node, it retains information about the transfer and the other node's configuration, allowing future transfers to that node to be more efficient.[196]

Napster's method of distribution actually slowed down requests, because they were routed through a central Napster server before continuing on to a source computer.[197] Gnutella was decentralized, but similarly inefficient, at least for large-scale implementation.[198] Indeed, some have suggested that Gnutella has an inherent design flaw which prevents it from working once the base of users grows too large.[199] In contrast, Freenet lacks this design flaw, and its design is reported to be the most scalable and efficient of all the P2P systems.[200]

(5) Fully Decentralized Network Operations

As with users of the Gnutella network, Freenet nodes connect with each other directly, using other nodes as intermediaries as necessary. Also as with Gnutella, Freenet's decentralized

---

[191] *See Freenet Paper*, *supra* note 169.

[192] Damien A. Riehl, *Peer-to-Peer Distribution Systems: Will Napster, Gnutella, and Freenet Create a Copyright Nirvana or Gehenna?*, WM. MITCHELL L. REV. 1761, 1785 (2001).

[193] *See Freenet Paper*, *supra* note 169. Another benefit of this system is that it helps prevent a form of network congestion, sometimes referred to as the "Slashdot effect," in which the demand for popular content outstrips the supply of bandwidth, resulting in a server crash. *See Free Radical*, *supra* note 169.

[194] *See* Charles C. Mann & Roger Parloff, *Napster Playing Dumb, Experts Say: Programmers Say the Company Could Easily Block Most of the Infringing Files From Its Directory*, THESTANDARD.COM (Oct. 18, 2000) *at* http://www.thestandard.com/article/display/0,1151,19487-0,00.html.

[195] *See* Rich Miller, *Freenet's 'Free Flow' May Cause Problems*, MINNEAPOLIS/ST. PAUL TRIB., July 4, 2000, at 9E.

[196] *See Freenet paper*, *supra* note 169.

[197] *Id.*

[198] *Id.*

[199] *See* Brown, *supra* note 141.

[200] *See* Anna Dorfman & Mark Rinzel, *Recording Industry Wins Injunction to Shut Down Napster*, SILICON ALLEY DAILY (July 27, 2000) *at* http://www.siliconalleydaily.com/issues/sar07272000.html.

nature makes it practically impossible to shut down the entire system, because the only way to bring about the demise of the system is for some authority to shut down every node.[201] The difficulty of accomplishing such a feat is readily apparent, especially when one considers the global nature of the Internet. Indeed, Ian Clarke has repeatedly emphasized the resistance of the network against attempts to shut it down, stating in an almost Dr. Frankenstein way, that even if he wanted to, he could not destroy his creation.[202]

III. REMOVING THE P2P MENACE

As Declan McCullagh has stated, "technology has begun to supplant law, and at an accelerated pace."[203] This may be both a welcome and inevitable development, especially when technology is used to protects rights such as privacy and free speech, which can be especially vulnerable to technological advances.[204] Some suggest that copyright, too, should be protected technologically, as well as legally.[205] As discussed below, however, applying both technological, and legal measures against Freenet, will have little, if any success.

A. Technological Measures: The Failings of Digital Rights Management

Commentators frequently assert that technological safeguards present the best option to combat copyright infringement.[206] These technological safeguards come in many forms and "protect" a wide variety of content.[207] Commonly referred to as "digital rights management" ("DRM"), the protections afforded by these technological safeguards are largely chimerical.[208] More importantly, in order for such measures to be truly effective, they would have to deny all unauthorized access to a work, including lawful and often highly desirable access, such as fair use.[209] The predominant forms of DRM rely on the technologies of encryption and watermarking.[210]

---

[201] *See* Amy Harmon, *For Many Online Music Fans, Court Ruling is Call to Arms*, N.Y. TIMES, July 28, 2000, at 1A.

[202] *Id.* Clarke has said, "If someone put a gun to my head and said, 'Shut this down,' I would be unable to do so." *Id.*

[203] Declan McCullagh, *Technology As Security*, 25 HARV. J.L. & PUB. POL'Y 129 (2002).

[204] *Id.*

[205] *Id.*

[206] *See, e.g.*, Riehl, *supra* note 192, at 1789.

[207] *Id.*

[208] *See* Mark S. Manasse, *Why Rights Management is Wrong*, WORKSHOP ON DIGITAL RIGHTS MANAGEMENT FOR THE WEB, Jan. 23, 2001, *at* http://www.w3.org/2000/12/drm-ws/pp/compaq.html.

[209] A through treatment of this particular topic would require many pages and so lies outside the scope of this paper. Indeed, at a recent conference on Computers, Freedom, and Privacy, "five hours of presentations and debate over the issues of fair use and DRM...produced a wealth of questions and one clear answer: that it is too early in this era of technological innovation to start locking down digital content." Scarlet Pruitt, *Law Experts Leery of DRM Solution*, INFOWORLD.COM (Apr. 17, 2002) *at* http://www.infoworld.com/articles/hn/xml/02/04/17/020417hndrm.xml.

[210] *See* Brad King, *Fight Rages Over Digital Rights*, WIREDNEWS (Jan. 16, 2001) *at* http://www.wired.com/news/politics/0,1283,41183,00.html.

1. Encryption[211]

One method of protecting digital content is to encrypt the content, requiring a key to gain access to the information.[212] The goal of using encryption for DRM is to prevent unauthorized parties from using the file, so that even if such a file were traded on Napster, Gnutella, or Freenet, its content would be inaccessible to anyone not holding the proper key.[213]

The primary problem with relying on encryption technology for DRM is that the encryption algorithms employed are often extremely easy to break. These weak algorithms are fundamentally different from the strong cryptography discussed in Section IV, and are often broken shortly after they are released.[214] One of the more notorious recent examples is found in the facts surrounding Universal City Studios, Inc., v. Reimerdes,[215] and the hacking of the encryption found on Digital Versatile Discs ("DVDs").[216] The motion picture industry caused "CSS technology"[217] to be developed, and touted CSS as a virtually unbreakable way of protecting the thousands of movies released on DVD.[218] This protection scheme was broken by a 15-year-old Norwegian boy, Jon Johansen, and two other unknown persons, because Johansen wished to view lawfully purchased DVDs on his Linux computer.[219] Johansen developed a computer program, DeCSS, which allowed users to decrypt their DVDs, allowing them full access to copy and modify the movies.[220] The suit arose when 2600 Magazine posted the source code to DeCSS on its web site.[221]

Indeed, in the 1980s, encryption was found to be an unacceptable method of deterring software piracy.[222] At the time, software developers used such techniques in an attempt to prevent users from creating multiple copies of software.[223] The practice was generally discontinued, however, because it did little to prevent piracy, and actually interfered with legitimate users' lawful use of the software.[224]

Encryption's general unsuitability for DRM, at least so far, was well summed by Judge Ferguson: "As sure as you or I are sitting in this courtroom today, some bright young

---

[211] *See* Section IV, *infra*, for general information on cryptography.
[212] *See* Universal City Studios v. Reimerdes, 111 F. Supp. 2d 294, 308 (2000).
[213] Riehl, *supra* note 192, at 1790.
[214] *See, e.g.*, Reimerdes, 111 F. Supp. 2d at 311.
[215] 111 F. Supp. 2d 294 (2000).
[216] *Id.*
[217] CSS is an abbreviation of "Content Scramble System." *Id.* at 308.
[218] *Id.* at 309-10.
[219] *Id.* at 311.
[220] *Id.*
[221] *Id.* at 303.
[222] *See* Brown, *supra* note 141.
[223] Barak D. Jolish, *Scuttling the Music Pirate: Protecting Recordings in the Age of the Internet*, 17 SPG ENT. & SPORTS L. 9, 11 (1999).
[224] The software caused problems, for example, whenever users upgraded their operating systems or installed new hardware. *Id.*

entrepreneur...is going to come up with a device to unjam the jam. And then we have a device to jam the unjamming of the jam and we all end up like jelly."[225]

2. Watermarking

The other frequently touted technology for deterring digital piracy is "watermarking."[226] Watermarking has gained a lot of public attention recently due to the Secure Digital Music Initiative ("SDMI"), a consortium organized in December of 1998.[227] Approximately 180 companies comprise the initiative, including music hardware manufacturers and members of the recording industry.[228] The SDMI has been working since 1998 on a music standard which it plans to implement in two phases.[229] The first phase was completed June 28, 1999, and allows portable music devices to play both "secure" files such as Windows Media files, as well as "nonsecure" files such as those in MP3 format.[230] The second phase would require that only SDMI-watermarked files be allowed to play on SDMI-compliant players.[231] Thus, the SDMI-compliant players of the future would not play MP3 music files,[232] something likely to enrage the millions of consumers who have become quite attached to the MP3 format over the last six years.[233]

One of the main reasons that the SDMI has been unable to move forward to phase two of its scheme is that at least two of the five protection technologies proposed for the final standard can be compromised.[234] In September 2000, the SDMI sponsored a contest, offering $10,000 to anyone who could remove one of their watermarks from a file.[235] SDMI received 447 submissions, and awarded $5,000 to each of two teams who succeeded in breaking a watermark.[236]

---

[225] *See* Rebecca J. Hill, *Pirates of the 21st Century: The Threat and Promise of Digital Audio Technology on the Internet*, 16 SANTA CLARA COMPUTER & HIGH TECH. L.J. 311, 311 (2000) (citing Paul Goldstein, *Copyright's Highway: The Law and Lore of Copyright from Gutenberg to the Celestial Jukebox*, 159 (1994), citing JAMES LARDNER, FAST FORWARD, 119-20 (1987)).

[226] *See* King, *supra* note 210.

[227] Sam Costello, *Digital Music Security Initiative Nearly Ready*, CNN.COM (Sept. 22, 2000) *at* http://www.cnn.com/2000/TECH/computing/09/22/SDMI.pre pidg/index.html.

[228] *Id.*

[229] Janelle Brown, *Is the SDMI Boycott Backfiring?*, SALON.COM (Oct. 3, 2000) *at* http://www.salon.com/tech/feature/2000/10/03/hacksdmi_fallout/index.html.

[230] The first phase was designed so that manufacturers could begin to comply with the standard before the standard was finalized. Stephen M. Kamarsky, *Managing Copyright in Digital Marketplace System May Be Redefined by Music Distribution War*, N.Y.L.J., Oct. 18, 1999, at S4.

[231] Costello, *supra* note 227.

[232] *Id.*

[233] *Id.*

[234] John Leyden, *Digital Music Security Systems Cracked*, VNUNET.COM (Nov. 9, 2000) *at* http://www.vnunet.com/News/1113843.

[235] John Borland, *SDMI Offers $10,000 Challenge to Hackers*, CNET NEWS.COM (Sept. 8, 2000) *at* http://news.cnet.com/news/0-1005-200-2730039.html.

[236] *See* Leyden, *supra* note 234.

B. Legal Measures

Congress routinely responds to the legal dilemmas created by technological innovations.[237] Legislative remedies can frequently resolve problems present at the time that bills are argued, however, laws broad enough to cover future innovations, yet narrow enough to remain effective are difficult to create.[238] For example, the Audio Hone Recording Act of 1992 ("AHRA")[239] was passed by Congress in response to growing concerns about the use of digital audio tapes ("DATs") for audio piracy.[240] DATs did not see much popularity within the consumer arena, however the AHRA has been stretched in an attempt to fit it to new technologies, including the Diamond Rio MP3 player.[241]

Congress has conducted a number of legislative hearings related to the use of Napster and other P2P technology,[242] but as of this writing, legislators have chosen not to take specific action against P2P technology.[243] In May 2000, the Progressive Policy Institute authored a paper recommending that Congress amend the DMCA to require that Napster users and users of similar organizations be held more accountable for their actions.[244] The paper's recommendations are highly dated, several times referencing "service providers" like Napster, and failing to address the fact that technologies such as the Gnutella and Freenet networks do not likely constitute service providers under the DMCA.[245] As described throughout Section II of this paper, any law aimed specifically at combating the technology of Napster would likely fail to simultaneously combat the technology of later technologies, especially Freenet. And, any legislation drafted broadly at controlling P2P technology in general faces at least two formidable hurdles. First, such a law would likely restrict or constrain technological advances to a level unacceptable to society,[246] especially consumers who appear to favor music sharing, regardless of whether such

---

[237] *See generally* Jessica Litman, *Copyright Legislation and Technological Change*, 68 OR. L. REV. 275 (1989).

[238] *See* Sheldon W. Halpern, *Copyright Law in the Digital Age: Malum In Se and Malum Prohibitum*, 4 MARQ. INTELL. PROP. L. REV. 1, 12-13 (2000) (addressing the difficulties inherent in enacting legislative remedies).

[239] Pub. L. No. 102-563, 106 Stat. 4242, codified at 17 U.S.C. §§ 1001-1010 (1992).

[240] *See generally* Gary S. Lutzker, *DAT's All Folks: Cahn v. Sony and the Audio Home Recording Act of 1991– Merrie Melodies or Looney Tunes?*, 11 CARDOZO ARTS & ENT. L.J. 145, 174-75 (1992).

[241] *See generally* Recording Industry Ass'n Am. v. Diamond Multimedia Systems, Inc., 180 F.3d 1072 (9th Cir. 1999). *See also* Lisa M. Needham, *A Day in the Life of the Digital Music Wars: The RIAA v. Diamond Multimedia*, 26 WM. MITCHELL L. REV. 1135 (2000).

[242] *See* Sean Silverthorne, *Mr. Napster Goes to Washington*, ZDNET NEWS, July 11, 2000, *at* http://www.zdnet.com/zdnn/stories/news/0,4586,2601519,00.html.

[243] The public's seeming adoration of MP3 technology may serve some basis for this hesitation on Congress' part. At one of the hearings, Sen. Patrick Leahy, D-VT stated that "[i]f you write a song...you ought to be rewarded for that. At the same time let's not strangle the baby in the crib. Let's make it work." Reuters, *Napster Users Mount E-Mail Campaign*, ZDNET.COM (July 18, 2000) *at* http://www.zdnet.com/zdnn/stories/news/0,4586,2604615,00.html.

[244] Shane Ham & Robert D. Atkinson, *Napster and Online Piracy: The Need to Revisit the Digital Millennium Copyright Act*, PROGRESSIVE POLICY INSTITUTE (May 1, 2001) *at* http://www.ppionline.org/ndol/print.cfm?contentid=646.

[245] *Id.*

[246] There are several arguments for opposing copyright legislation in light of rapid technological advances. *See* Trotter Hardy, *Copyright and "New Use" Technologies*, 23 NOVA L. REV. 659, 672-86 (1999); Mary L. Mills, *New Technology and the Limitations of Copyright Law: An Argument for Finding Alternatives to Copyright Legislation in an Era of Rapid Technological Change*, 65 CHI.-KENT L. REV. 307, 308 (1989); Jessica D. Litman,

music is copyrighted.[247] More importantly, to be truly effective at combating a technology such as Freenet, Congress would need to regulate its two strongest improvements over Napster, cryptography and anonymity. The remainder of this paper argues that both of these improvements have a long history of protection under the First Amendment, and play such an overwhelmingly important role in guaranteeing Free Speech in an electronic age, that attempts at regulating them are constitutionally repugnant.

IV. CRYPTOGRAPHY

> "It must be that as soon as culture has reached a certain level, probably measured largely by its literacy, cryptography appears spontaneously – as its parents, language and writing probably also did. The multiple human needs and desires that demand privacy among two or more people in the midst of social life must inevitably lead to cryptology wherever men thrive and wherever they write."[248]

This Section posits that creation of programs which permit strong cryptography, as well as use of such programs, are both constitutionally protected under the First Amendment. To appreciate why this is so, a basic understanding of what cryptography is and how it works is necessary.

A. Definitions

Cryptologists, or those who study cryptography and cryptanalysis, use a variety of terms for their science which are generally not familiar to lawyers.[249] Cryptography is the art of devising and using methods of concealing the contents of messages, using techniques including codes and ciphers.[250] Cryptanalysis is the reverse art of breaking cryptographic methods.[251]

A code is a means of communication which relies on a map of one set of terms to another set of terms, for example, sometimes referred to as a code book.[252] A cipher allows a person to encrypt a message regardless of its content.[253] A good example of the distinction between codes and ciphers is given by Professor Froomkin: "Paul Revere's 'one, if by land, and two, if by sea' was a code. If the British had landed by parachute, no quantity of lanterns would have sufficed

---

Copyright Legislation and Technological Change, 68 OR. L. REV. 275 (1989); Sheldon W. Halpern, *Copyright Law in the Digital Age: Malum In Se and Malum Prohibitum*, 4 MARQ. INTELL. PROP. L. REV. 1, 12-13 (2000).

[247] DecisionQuest conducted a study for the National Law Journal and found that 41.5 percent of 1,000 potential jurors believe that trading copyrighted music for personal use should be lawful. Dick Kelsey, *Jury Pool Survey—Napster's Chances Good*, NEWSBYTES, Oct. 10, 2000, *at* http://www.newsbytes.com/pubNews/00/156450.html.

[248] *See* DAVID KAHN, THE CODEBREAKERS 84 (1967).

[249] *Id.* at xvi.

[250] *See* A. Michael Froomkin, *The Metaphor is the Key: Cryptography, The Clipper Chip, and the Constitution*, 143 U. PA. L. REV. 709, 713 (1995) [hereinafter "Metaphor"].

[251] *Id.*

[252] *Id.*

[253] *See* KAHN, *supra* note 248, at xiii-xvi.

to communicate the message."[254] The modern cryptographic systems discussed at more length in Section IV.C are all ciphers.

One of the goals of cryptography is the ability to create messages which only certain, intended people can read.[255] Such people are referred to as recipients.[256] An adversary is a person who wishes or attempts to access the contents of communication without permission from the communicants, for whatever reason, benign or malicious. "The original message is called a plaintext. The disguised message is called a ciphertext. Encryption means any procedure to convert plaintext into ciphertext. Decryption means any procedure to convert ciphertext into plaintext."[257] An algorithm is the formal name for a cipher, and is a mathematical function used to encrypt or decrypt a message.[258] A single-key, or symmetric key system is one in which both the sender and receiver share a single key which they use to encrypt and decrypt a message.[259] Historically, all ciphers were single-key ciphers.[260] Within the last twenty or thirty years, however, public-key systems have been developed, allowing for one key to encrypt a message, and a different key to decrypt the message.[261]

B. Historical Cryptography

As far back as 1900 B.C., humans engaged in the practice of altering their communications in an attempt to preserve privacy. The tomb walls of Khnumhotep II are carved with cryptic messages considered to constitute the earliest use of cryptography.[262] The earliest known pottery glaze formula was written in code on a Mesopotamian cuneiform tablet in about 1500 B.C.[263] Around 500-600 B.C., Hebrew scribes writing the Book of Jeremiah invented a substitution cipher that was stronger than one Julius Caesar would use much later for military secrecy.[264]

The Greeks were the first people known to use cryptography for militaristic purposes.[265] It is from "kruptós," the ancient Greek word for "hidden," that cryptography is derived.[266] The Spartans used cryptography as early as 500 B.C.[267] In their method, the sender and the receiver each possessed a wooden rod of the same dimensions.[268] The sender would wind a "tape" of papyrus around his rod and mark down a message on the tape.[269] Once removed from the rod, the

---

[254] *See Metaphor*, *supra* note 250, at 713.
[255] *Id.*
[256] *Id.*
[257] Eric Bach et al., *Cryptography FAQ* § 3, Oct. 31, 1994, *at* http://rtfm.mit.edu/pub/usenet/news.answers/cryptography-faq/part03.
[258] *See Metaphor*, *supra* note 250, at 714.
[259] *Id.*
[260] *Id.*
[261] *Id.*
[262] Kahn, *supra* note 248, at 75.
[263] *Id.* at 75.
[264] *Id.* at 77.
[265] *Id.* at 82.
[266] Melis Jackob, *History of Encryption*, SANS.ORG, Aug. 8, 2001, http://rr.sans.org/encryption/history.php.
[267] KAHN, *supra* note 248, at 82.
[268] *Id.*
[269] *Id.*

message would appear unintelligible to anyone not possessing a matching rod of the same dimensions.[270] To read the message, the recipient wound the tape around his own rod, easily discerning the intended message.[271] Julius Caesar used a shift cipher for military secrecy around 50 B.C.[272] The so-called Caesar cipher disguised the plaintext of the message by shifting every letter in the message by three characters to the right.[273] So, for example, "A" became "D," "B" became "E," and "X" wrapped around to "A." Thus a message "RETURN HOME" becomes "UXWXUQ KRPH." The Kama Sutra of Vatsayana enumerates secret writing as the 44th and 45th of the 64 arts (yogas) in which men and women should be well-versed.[274]

Cryptography began its steady development in western civilization around the 13th century, primarily in Italy.[275] Around 1250, Roger Bacon not only described several ciphers, but wrote: "A man is crazy who writes a secret in any other way than one which will conceal it from the vulgar."[276] In the mid 1400s, an amateur cryptographer named Leon Battista Alberti developed the first polyalphabetic cipher.[277] The techniques required to beak the cipher were not published until some 400 years later.[278] His cipher offered more security than the *nomenclator*, the popular cipher of his lifetime, but was not widely used until the invention of the telegraph.[279] The first printed book on cryptography appeared in 1518 and was written by Johannes Trithemius.[280]

Contributions by amateurs such as Alberti are not atypical. Indeed, "[i]t was the amateurs of cryptology who created the species. The professionals, who almost certainly surpassed them in cryptanalytic expertise, concentrated on down-to-earth problems of the systems that were then in use but are now outdated. The amateurs, unfettered to those realities, soared into the empyrean of theory."[281] From 1500 to 1900, amateur cryptosystems far outstripped government cryptosystems in use and security. Indeed, the private sector has a long history of leading the government in producing secure cryptosystems. "Cryptanalysis may traditionally be found in government agencies but cryptography is a normal civilian pursuit. In particular, history shows that even during the life of the NSA, private citizens have had access to cryptography as strong as anything the Agency has produced."[282] In 1795, Thomas Jefferson designed a cipher system that was later used by the U.S. Army from 1923 until 1942.

---

[270] *Id.*
[271] *Id.*
[272] *Id.* at 83.
[273] *See Cryptography, at* http://www.trincoll.edu/depts/cpsc/cryptography/caesar.html.
[274] *Gallery*, ODYSSEY TECHNOLOGIES, *at* http://www.odysseytec.com/Gallery/intro.htm. The date of the Kama Sutra is unknown, but it is believed to be between the first and fourth centuries, A.D. *See* Carl Ellison, *Cryptography Timeline*, Oct. 19, 2001, *at* http://world.std.com/~cme/html/timeline.html.
[275] KAHN, *supra* note 248, at 106.
[276] *Id.* at 90.
[277] *Id.* at 127.
[278] *Id.*
[279] KAHN, *supra* note 248, at 192.
[280] *Id.* at 130-36.
[281] *Id.* at 125-26.
[282] KAHN, *supra* note 248, at 268.

C. *Modern Cryptography*

> "There are two kinds of cryptography in this world: cryptography that will stop your kid sister from reading your files, and cryptography that will stop major governments from reading your files..."[283]

Substitution and shift ciphers are laughably insecure by today's standards. However, they were secure enough to protect military information when they were first conceived. The rise of the personal computer has greatly contributed to the widespread availability and use of cryptography seen today.[284] Cryptosystems of the past relied on humans to carry out often complex and tedious tasks, creating a sort of upper limit on both the prevalence of their use in ordinary society, and in the sophistication of the ciphers themselves.[285] Modern computers, however, are very suitable for performing such tasks – allowing for the implementation of vastly more complex and secure cryptosystems.[286]

1. Strong Cryptography

The strength of a cryptosystem can be calculated and proved, and often relies on an underlying assumption, such as the difficulty of a mathematical problem. A cryptosystem is called "strong" if large amounts of resources[287] are required in order to break it. The ciphers mentioned in Section IV.B are *not* strong.[288]

2. Symmetric Cryptosystems

In a symmetric cryptosystem (also known as a "secret key" cryptosystem), both the sender and the receiver share the same key, which is used both for encryption and decryption.[289] Symmetric cryptosystems are very fast, and their strength depends largely upon the length of the key.[290] Symmetric cryptosystems work very well for communications between two parties.[291] When multiple parties are included in the communication, however, symmetric cryptosystems become decreasingly appropriate.[292]

3. Asymmetric Cryptosystems

In an asymmetric cryptosystem (also known as a "public key" cryptosystem), the sender and receiver each possess two unique keys: a public (or "encrypting") key and a private (or

---

[283] BRUCE SCHNEIER, APPLIED CRYPTOGRAPHY, Preface (2d ed. 1995).
[284] *See* KAHN, *supra* note 248, at 271.
[285] *Id.*
[286] *Id.*
[287] Such as time, computing power, or specialized hardware.
[288] They are referred to as "weak" cryptosystems.
[289] *See* Bert-Jaap Koops, *The Crypto Controversy: A Key Conflict in the Information Society*, 38 KLUWER L. INT'L 35-36 (1999).
[290] *Id.* at 42.
[291] *Id.* at 35-36.
[292] Because there is only one key involved, a large number of recipients will compromise the security with which Alice can send out messages. *Id.* at 36.

"decrypting") key.[293] The public key is distributed as widely as possible.[294] The private key is very closely guarded.[295] The encryption/decryption process works as follows.

Suppose Alice wishes to send a message to Bob. Alice obtains a copy of Bob's unique public key, uses it to encrypt the plaintext, and sends it to Bob. Bob then uses his private key to decrypt the message. Should Bob wish to reply to Alice, he encrypts a message under Alice's public key, and Alice may then decrypt the message with her private key. A major advantage of this scenario is that Alice may use this method to communicate with Bob and Charlie at the same time, without compromising the security of any one's keys.

D. Modern Uses of Cryptography[296]

Recent innovations in computer and communications technologies have substantially altered the ways in which parties can communicate and exchange information. The improvements in speed and efficiency provided by digital technologies also present new challenges to the privacy and security of any transmissions made in a global communications infrastructure.[297] As a result, the methods for protecting the security of paper-based communications, such as envelopes and locking file cabinets, are being replaced electronically by modern encryption methods.[298]

As discussed in Section II, millions of people use the Internet every day. A substantial portion of these people also use cryptography every day, often without knowing it.[299] Secure Socket Layer ("SSL") encryption allows for secure access to particular web sites.[300] Such sites are accessed through the prefix "https://" instead of the more common "http://" prefix.[301] The encryption technology is integrated almost seamlessly into most modern web browsers, and often the only indication that a user has that encryption is being employed, is a small image of closed lock when a page is employing encryption, and an image of an open lock when it is not.[302] SSL is regularly used by commercial web sites, such as Amazon.com, whenever a customer is providing sensitive financial or delivery information.[303]. Indeed, the widespread availability of encryption to protect customer information is a major reason for the success of electronic

---

[293] *See id.* at 36.

[294] *Id.*

[295] *Id.*

[296] For a particularly enjoyable explanation by one attorney of his own uses for modern cryptography, including both personal and professional uses, see Lee Bruner, *Secure E-mail: A Service You Owe to your Clients*, 26-JUL MONT. LAW. 32 (2001).

[297] *See* Global Internet Liberty Campaign, *The Importance of Cryptography*, CRYPTOGRAPHY AND LIBERTY 1998, Feb. 1998, *at* http://www.gilc.org/crypto/crypto-survey.html.

[298] *Id.*

[299] Business-to-business web sites allow businesses direct and immediate access to their suppliers. *Id.* The Internet economy is projected to reach $2.8 trillion by 2003 in large part due to the popularity of business-to-business sites. *Id.*

[300] *See SSL Encryption*, SECURITY.TAO.CA, *at* http://security.tao.ca/ssl.shtml.

[301] *Id.*

[302] *Id.*

[303] Such information may include, for example, a credit card number, bank account number, telephone information, shipping address.

commerce.[304] Without SSL encryption, the names and credit card numbers of hundreds of thousands of online customers would be sent, in the clear, over networks, readily exposing them to fraudulent use.[305]

Another way people commonly use cryptography online is to protect the security of their e-mail messages.[306] Regardless of whether messages contains birthday greetings, jokes, customer information, legal documents, or trade secrets, users generally expect that their electronic mail is offered at least the same security provided by depositing an envelope with the U.S. Postal Service.[307] Just as with connections made to web pages, however, e-mail messages are not secure unless they are protected by strong cryptography. A number of methods of securing email are presently available, each offering varying degrees of security, user-ease, and compatibility with other programs.[308]

One of the most compelling uses strong cryptography receives is the protection of human rights-related information. Secrets must be kept safe to break the stories which crack oppressive regimes. Human rights workers realize this, and have been quick to adopt the tools which give them the unprecedented ability to securely transmit sensitive information.[309] In general, human rights scandals frequently implicate hostile regimes, whether they are governmental or private entities, who possess state-of-the-art technology, and lots of it.[310] Such technology can analyze and store digital communications effortlessly, and will only improve with time.[311] The ability to eavesdrop on an oppressed citizen, attempting to communicate with a party outside such a regime, could well spell death both for that citizen, as well as for the information he may be trying to convey.[312] Phil Zimmerman, the author of "PGP," an extremely popular e-mail encryption tool, regularly receives heartfelt thanks from human rights field workers who rely on his program to protect themselves against such sophisticated regimes.[313]

---

[304] *See generally* Andres Rueda, *The Implications of Strong Encryption Technology on Money Laundering*, 12 ALB. L.J. SCI. & TECH. 1, 28-28 (2001) (describing the rise of the market for airline tickets, as well as consumers' ability to "readily purchase through the Internet everything from stocks to books, groceries, pet food, and movie tickets.").

[305] For example, more than 100,000 credit card numbers issued by over 1,000 different banks, were stolen by a single online individual who employed a packet sniffer to examine unencrypted network traffic. *See* Coates & Bonorris, *Digital Money: Electronic Cash May Make Sense*, THE FUTURIST, Aug.-Sept., 1998, at 22. Packet sniffing is rendered ineffective by the deployment of strong cryptography. *See* Lorah McArdle, *Beyond Encryption*, SDMAGAZINE.COM, Jan. 2001, *at* http://www.sdmagazine.com/documents/s=735/sdm0101i/0101i.htm.

[306] SCHNEIER, *supra* note 283, at 577-84.

[307] *See* Sean Stark, *Secure Messaging*, SANS INSTITUTE, Dec. 21, 2000, *at* http://rr.sans.org/email/messaging2.php.

[308] *Id.*

[309] *See* Geoffrey Gordon, *Breaking the Code: What Encryption Means for the First Amendment and Human Rights*, 32 COLUM. HUM. RTS. L. REV. 477, 479 (Spring 2001).

[310] *Id.* at 480.

[311] *Id.*

[312] *Id.*

[313] *See* Phil Zimmerman, *PGP and Human Rights*, *at* http://bau2.uibk.ac.at/sg/pgp-necessity.html. Portions of one such letter follow. "Dear Phil, This is a short note to say a very big thank you for all your work with PGP. We are part of a network of not-for-profit agencies, working among other things for human rights in the Balkans. Our various offices have been raided by various police forces looking for evidence of spying or subversive activities. Our mail has been regularly tampered with and our office in Romania has a constant wiretap. Last year in

E. Regulation of Cryptography

> "Judges understand books. They understand that when the government denies people the ability to write, distribute, or sell books, there is something very fishy going on. The government might be able to pull the wool over a few judges' eyes about jazzy modern technologies like the Internet, floppy disks, fax machines, telephones, and such. But they are unlikely to fool the judges about whether it's constitutional to jail or punish someone for putting ink onto paper in this free country."[314]

The export of strong cryptography from the United States was historically regulated by stringent munitions export controls, alongside tanks, missiles, and other weapons of war.[315] The specific provisions were found under the Department of State's International Trafficking in Arms Regulations ("ITAR"),[316] promulgated under the Arms Export Control Act of 1968 ("AECA"),[317] and allowed the President to control the import and export of any defense articles or services at his discretion.[318]

As discussed in Section IV.B, throughout much of civilization, cryptography has benefited from a wealth of research and development in the public sector, especially by amateurs. After the First World War, however, this situation began to change.[319] During the 1930s and 1940s, a few treatises on the subject were published, and a handful of papers were published openly, however their contents grew increasingly further behind the state of the art.[320] Between 1949 and 1967, cryptographic literature in the public domain was virtually non-existent.[321] However, in 1967, David Kahn published an extensive history of cryptography, *The Codebreakers*.[322] The book was significant not because it contained any novel ideas, but because the remarkably complete treatment of the history of cryptography enjoyed good sales,

---

Zagreb, the security police raided our office and confiscated our computers in the hope of retrieving information about the identity of people who had complained about their activites. [sic] In every instance PGP has allowed us to communicate and protect our files from any attempt to gain access to our material as we PKZIP all our files and then use PGP's conventional encryption facility to protect all sensitive files. Without PGP we would not be able to function and protect our client group. Thanks to PGP I can sleep at night knowing that no amount of prying will compromise our clients. I have even had 13 days in prison for not revealing our PGP pass phrases, but it was a very small price to pay for protecting our clients. I have always meant to write and thank you, and now I am finally doing it. PGP has a value beyond all words and my personal gratitude to you is immense. Your work protects the innocent and the weak, and as such promotes peace and justice, quite frankly you deserve the biggest medal that can be found. Please be encouraged that PGP is a considerable benefit people in need, and your work is appreciated." *Id.*

[314] ELECTRONIC FRONTIER FOUNDATION, CRACKING DES, 4-2 (1998).

[315] *See generally*, Christopher D. Hoffman, *Encrypted Digital Cash Transfers: Why Traditional Money Laundering Controls May Fail Without Uniform Cryptography Regulations*, 21 FORDHAM INT'L L.J. 799, 844-4

[316] *See* 22 U.S.C. § 2778(a),(b)(2) (1994).

[317] *See* 22 U.S.C. § 2778 (1994) (originally named "The Foreign Military Sales Act" at PUB. L. NO. 90-629, 82 Stat. 1326").

[318] 22 U.S.C. § 2778 (a)(b)(2).

[319] *See* Costas Christoyannis, *What is Cryptography*, *at* http://www.hack.gr/users/dij/crypto/overview/whatis.html.

[320] *Id.*

[321] *Id.*

[322] Kahn, *supra* note 248.

introducing thousands of previously unaware people to the topic of cryptography.[323] Perhaps as a direct result, a handful of cryptography papers appeared in the public sector soon after.[324]

Public interest in cryptography greatly escalated in the late 1970s and early 1980s as people growingly realized the importance of protecting the enormous amount of information that was increasingly being made available electronically. Accordingly, the specialty of computer security was added to academic colleges and universities around the U.S.[325] It was at this time that the National Security Agency, traditionally the cryptographic heart of the U.S. government, began its attempts to quash it.[326] The NSA cited policies of denying knowledge for the public's own good, economic efficiencies, and the need for uniformity in computer information security, as the reasons for its campaign to restrict access to strong cryptography in the public sector.[327]

The first tactic the NSA tried was to limit the funding of academic cryptographic research. In particular, in 1977, the NSA informed the director of the Division of Computer Research at the National Science Foundation (NSF) that federal law granted the NSA sole control over all cryptography.[328] The director consulted with NSF lawyers and challenged the NSA's claim, at which point the NSA backed off and offered to review proposals sent to the NSF.[329] The NSF agreed on the condition that the NSA review proposals only on the basis of their technical merits.[330] The NSA continued to adopt a very liberal interpretation of the export controls and attempted to prevent scientists from presenting papers on cryptography at technical conferences.[331] For example, in 1977, NSA employee Joseph Meyer sent a letter on personal stationary to the Institute of Electrical and Electronics Engineers (IEEE) informing them that their upcoming conference would violate export controls.[332] He argued that presenting "technical data" in a public forum would constitute an illegal export.[333] When confronted with the letter, the NSA claimed that Meyer was speaking on his own behalf and did not express the views of the NSA.[334] Many people dismiss this claim, however, arguing that it was simply another way in which the NSA attempted to scare academic researchers.[335] Eventually, the State Department revised the export regulations to specifically exempt "scientific communications" from the controlled "technical data" list.[336]

The 1951 Invention Secrecy Act allows the U.S. Patent Office "to forward applications to government agencies which have an interest in the area. The agencies can then classify the

---

[323] *See Christoyannis, supra* note 319.

[324] *Id.*

[325] *See* BRUCE SCHNEIER & DAVID BANISAR, THE ELECTRONIC PRIVACY PAPERS, 294-95 (1997) [hereinafter "Electronic Privacy Papers"].

[326] *Id.* at 295.

[327] *See* Renae Angeroth Franks, *The National Security Agency and its Interference with Private Sector Computer Security*, 72 IOWA L. REV. 1015, 1024(1987).

[328] *Id.*

[329] *Id.*

[330] *Id.*

[331] *Id.*

[332] *Id.*

[333] *Id.*

[334] *Id.*

[335] *Id.*

[336] *Id.*

proposal if they feel it threatens national security."[337] Under the Act, inventors receiving notice that their inventions have been classified are ordered not to discuss the patent under penalty of a $10,000 fine and two year jail sentence. Traditionally, the Act applied only to government scientists and others who signed secrecy statements before commencing research.[338] In 1978, however, the NSA attempted to use the act to classify products invented by civilians.[339]

Professor George Davida of the University of Wisconsin, and research Carl Nicolai were the first civilians targeted by the NSA under the Invention Secrecy Act.[340] Davida devised a way to perform high-speed encryption on networks, and Nicolai invented an analog voice encryption device that he intended to sell for $100.[341] They each filed for a patent, and were informed by mail that their devices had been classified. Professor Davida ignored the mail and "went public."[342] As a result, the NSA claimed that the classification of both devices had been accidental, and rescinded the orders.[343]

Suffering from the negative public perception gained as a result of the Davida/Nicolai fiasco, the NSA moved on to another tactic. At a conference in 1979, Director Inman stated, "there is a very real and critical danger that unrestrained public discussion of cryptographic matters will seriously damage the ability of the government to conduct signals intelligence."[344] Director Inman insisted that it was crucial to the well-being of the nation that the NSA and private industry reach an agreement on the development of cryptography, and that restrictions on the kinds of research performed were of utmost importance.[345]

The American Association for the Advancement of Science (AAAS) disagreed:

> "Whereas freedom and national security are best preserved by adherence to the principles of openness that are a fundamental tenet of both American society and the scientific process, be it resolved that the AAAS opposes governmental restrictions on the dissemination, exchange, or availability of unclassified knowledge."[346]

In 1996, the U.S. export controls were further revised to explicitly permit the export of any material printed in books or on *paper* in any format.[347] Emphasis is placed on paper because the 1996 revision did not include electronic works among the material exempted from export controls. Accordingly, while a wide variety scientific research was increasingly being discussed and published in online forums, cryptographic research continued to be published exclusively on

---

[337] *Id.*
[338] *Id.*
[339] *Id.*
[340] *Id.* at 296.
[341] *Id.*
[342] *Id.*
[343] *Id.*
[344] NSA Director Inman, *The NSA Perspective on Telecommunications Protection in the Nongovernmental Sector*, Presentation before the Armed Forces Communications Electronics Ass'n, 1979.
[345] *Id.*
[346] *Id.* at 297.
[347] *See* CRACKING DES, *supra* note 314, at 4-3.

paper.[348] It was also in 1996 that President Clinton removed strong encryption technologies from the Munitions List, governed by ITAR,[349] and transferred the technology to the Commerce Control List, issued by the Department of Commerce Bureau of Export Controls ("BXA").[350]

Encryption regulations were a vestige from the Cold War. As the fear that encryption exports would fall into Soviet hands died away, the government increasingly listed possession and use of cryptography by terrorists and other criminals as its chief motivation for maintaining export controls.[351] This position was regularly espoused by FBI Director Louis Freeh.[352] In the private sector, however, encryption export regulations were increasingly scrutinized by the computer industry, academicians, and members of the civil liberties communities with skepticism, and more frequently, with outright scorn.[353] The frustration of software developers and other opponents of encryption regulation ultimately led to a series of legal challenges.

F. Source Code Is Speech

As discussed in greater detail below, the final outcome of the export regulation challenges proves critical to analysis of Freenet. Both the Ninth Circuit Court of Appeals, and the Sixth Circuit Court of Appeals have ruled that computer source code is expressive speech, protected by the First Amendment.[354]

---

[348] *Id.*

[349] Exec. Order No. 13026, 61 Fed. Reg. 58,767, (Nov. 19, 1996).

[350] *Id.* (stating that while similar products are available internationally, these technologies nonetheless continue to pose a substantial threat to national security and United States foreign relations).

[351] *See* Karim K. Shehadeh, *The Wassenaar Arrangement and Encryption Exports: An Ineffective Export Control Regime that Compromises United States' Economic Interests*, 15 AMERICAN UNIV. L. REV. 271, 283-84 (1999).

[352] "Widespread use of robust non-recoverable encryption is beginning to devastate our ability to fight crime and terrorism. Uncrackable encryption allows drug lords, terrorists, and even violent gangs to communicate about their criminal intentions without fear of outside intrusion. This type of encryption also allows these same people to maintain electronically stored evidence to their crimes beyond the reach of law enforcement. For example, convicted spy Aldrich Ames was instructed by his Soviet handlers to encrypt computer file information that was passed to them. Ramzi Yousef, convicted with others for plotting to blow up between five and twelve United States owned commercial airliners in the Far East, used encryption to protect criminal information on his laptop computer. Major international drug traffickers are increasingly using telephone encryption devices to frustrate court-authorized electronic surveillance. Unfortunately, these types of situations will occur with more frequency as inexpensive encryption becomes more readily available to the public." Prepared Statement of Louis J. Freeh, Director of Federal Bureau of Investigation Before the Senate Appropriations Committee Foreign Operations Subcommittee, FED. NEWS. SERV., Apr. 21, 1998 at 2.

[353] Robert Kuttner, *How 'National Security' Hurts National Competitiveness*, HARV. BUS. REV. 140, 143 (Jan -Feb. 1991). The required licensing requirements

[354] The ITAR regulations were challenged in 1996 in Karn v. United States Dep't of State, 925 F. Supp. 1 (D.D.C. 1996), resulting in a ruling that "source codes are merely a means of commanding a computer to perform a function," and not protected by the First Amendment. *Id.* at 9. As explained in detail in Section IV.F, however, other Circuits have adopted the opposite position, perhaps due to society's increasing comfort, familiarity, and dependence upon computers.

1. Bernstein v. U.S. Dep't of State[355]

Daniel Bernstein created a cryptosystem which he dubbed "Snuffle," while working as a graduate student at the University of California Berkeley.[356] Snuffle encrypts and decrypts messages on a per character basis, while the transmission is in progress, instead of once the transmission is complete.[357] With Snuffle, Bernstein was able to prove that a one-way hash function[358] could serve as the basis of a per character zero-delay encryption method, an idea which advanced the field of cryptography.[359]

Bernstein wanted to share his findings with the scientific community for peer review, specifically by posting his research results and the Snuffle source code on the Usenet group sci.crypt.[360] Under the encryption regulations in effect at the time, however, Bernstein was prohibited from "disclosing...or transferring technical data to a foreign person, whether in the United States or abroad."[361] Bernstein's desire for peer review, coupled with his fear that discussing his software at academic conferences, publishing it in an academic journal, or posting Snuffle online, led him to seek the State Department's guidance on the best way to share his discovery without incurring legal trouble.[362] Bernstein conceived of three separate presentations of his idea: (1) a paper titled "The Snuffle Encryption System," containing mathematical equations and an analysis of Snuffle; (2) the source code to two Snuffle programs, snuffle.c (the encrypting software) and unsnuffle.c (the decrypting software); and pseudo-code, or prose explaining how to write the source code for snuffle.c and unsnuffle.c.[363]

Several months elapsed, and the State Department advised Bernstein that Snuffle constituted a munition under the ITAR, and would require a license to export, in any format.[364] A voluminous exchange of contentious correspondence with the State Department, the Department of Defense, and the Department of Commerce followed, and Bernstein was ultimately informed that the academic paper was not a munition and could be exported, but that the source code programs and the pseudo-code would require an export license.[365]

In 1995, Bernstein challenged the constitutionality of the State Department's decision (and thus the ITAR) in a suit filed against the NSA and the State Department in the Northern District of California. Bernstein alleged that export controls on cryptography constitute an

---

[355] 945 F. Supp. 1279 (N.D. Cal. 1996) [hereinafter "Bernstein I"].

[356] Bernstein I, 922 F.Supp. at 1428-29.

[357] *See* Bernstein v. U.S. Dept. of Justice, 176 F.2d 1132, 1136 (9th Cir. 1999) [hereinafter "Bernstein IV"] (explaining that Snuffle's zero-delay capability allows for quicker and easier communication between users).

[358] A one-way hash function is a procedure that is easy to compute in one direction, but difficult to compute in the reverse. An example offered by Bruce Schneier is that of writing a message on a plate, smashing the plate, and asking a friend to reconstruct the message.

[359] Bernstein IV, 176 F.3d at 1135-36 n. 1.

[360] Bernstein I, 945 F. Supp. at 1430.

[361] 22 C.F.R. § 120.17(4) (1994) (defining an "export" subject to the Department of State's jurisdiction).

[362] Bernstein IV, 176 F.3d at 1136.

[363] An electronic copy of this letter can be found at http://www.eff.org/pub/Privacy/ITAR_export/Bernstein_case/Letters/920630_cj.letter.

[364] Bernstein IV, 176 F.3d at 1136.

[365] *Id.* at 1136 n. 2

"impermissible prior restraint on speech, in violation of the First Amendment."[366] The State Department responded that it was regulating conduct and not free speech, and filed a motion to dismiss the case on the grounds that the First Amendment was not implicated.[367]

Judge Marilyn Patel[368] ruled that source code was protected by the First Amendment and that the ITAR regulations acted as an impermissible prior restraint,[369] stating "this court can find no meaningful difference between computer language, particularly high-level languages...and German and French...like music and mathematical equations, computer language is just that, language, and it communicates information either to a computer or to those who can read it."[370]

On appeal, the Ninth Circuit focused on the narrow question of whether restrictions on the export of encryption source code constituted an impermissible prior restraint.[371] The Ninth Circuit agreed that encryption software was expressive language under the First Amendment, and that prior restraint protections applied.[372] The court went on to hold that a prepublication licensing regime such as that implemented in the ITAR, had a chilling effect on encryption speech,[373] and that Supreme Court precedent demands a "heavy presumption" against the validity of such prior restraints.[374] The Ninth Circuit noted that the export regulations gave its administrators "boundless discretion" to deny licenses whenever they deemed that the export would be inconsistent with "U.S. national security and foreign policy interests."[375] Because the regulations effectively discouraged scientific discussion by permitting the government to capriciously withhold export licenses, the Court found the regulations were a constitutionally impermissible restraint on speech.[376]

Bernstein was heard by a three-judge panel,[377] and the government requested an *en banc* review, complaining that a failure to reverse would "gravely compromise the ability of the United States to control the export of encryption products to potentially hostile foreign parties."[378] The Ninth Circuit withdrew the panel's decision in response,[379] but before the case could be heard *en banc*, President Clinton issued a new set of export regulations and rendered the

---

[366] D.J. Bernstein, Bernstein v. U.S. Dep't of State et al., Civil Action No. C95-0582-MHP, United States District Court for the Northern District of California, 21 Feb. 1995.

[367] *See* ELECTRONIC PRIVACY PAPERS, *supra* note 325, at 329.

[368] Perhaps ironically, Judge Patel also heard Napster I, as Chief Judge Patel.

[369] Bernstein I, 922 F. Supp. at 1439 (holding that source code is constitutionally protected speech); *see also* Bernstein v. U.S. Dept. of State, 974 F.Supp. 1288, 1290 (N.D. Cal. 1997) [hereinafter "Bernstein II"] (holding the ITAR an unconstitutional prior restraint).

[370] Bernstein I, 922 F. Supp. at 1435-36.

[371] Bernstein IV, 176 F.3d at 1138.

[372] *Id.* at 1141.

[373] *Id.* at 1143 n. 17.

[374] *Id.*

[375] *Id.* at 1139; 15 C.F.R. § 742.15(b) (1998).

[376] *Id.* at 1145.

[377] *Id.* at 1135 (the presiding Justices were Bright, Fletcher, and Nelson).

[378] Appellants' Petition for Panel Hearing and Rehearing En Banc at 1, 192 F.3d 1308 (9th Cir. 1999) (No. 97-16686).

[379] *Bernstein v. United States Dep't of Justice*, 192 F.3d 1308, 1309 (9th Cir, 1999).

case moot.[380] Commentators have suggested that without this change in regulations, it is likely that the issue would have likely reached the Supreme Court.[381] Given the Supreme Court's reverence for the Internet's First Amendment capacity two years prior, it appears possible that the Court would have upheld the Ninth Circuit's ruling.[382]

2. Junger v. Daley[383]

When faced with its own challenge to encryption export regulations, the Sixth Circuit effectively adopted the decision in *Bernstein*.[384] The plaintiff in *Junger v. Daley* was a professor of law at Case Western Reserve University who taught a course on computers and the law.[385] Professor Junger maintained a class-related web page, and as encryption was one of the topics discussed in the course, he wished to place encryption source code and lecture notes on that page for his students.[386] Knowing that his desires might run afoul of the export regulations, Junger submitted three applications to the Commerce Department on June 12, 1997, "requesting determinations of commodity classifications for encryption software programs and other items."[387] The Commerce Department informed Junger that he may hand out paper copies of the first chapter of his textbook, *Computers and the Law*, including the source code contained within, but that he was prohibited from posting the identical material on the class website format without an export license.[388]

Junger filed suit against the NSA and Commerce Department in August of 1996, challenging the export controls on First Amendment grounds.[389] District Court Judge James Gwin granted summary judgment in favor of the Commerce Department, maintaining that programming languages were not entitled to First Amendment protection because they were merely functional, and not expressive.[390] Junger appealed the decision, and the Sixth Circuit reversed,[391] explaining that "all ideas having even the slightest redeeming social importance"

---

[380] *See* Plaintiff's Brief Requesting Remand to District Court, *Bernstein v. United States Dep't of Justice*, 192 F.3d 1308 (9th Cir. 1999) (No. 97-16686) (arguing that changes in export regulations "appear to impact the legal and factual context of the case.")

[381] *See, e.g.*, John Scheinman, *Government Trying to Maneuver in Bernstein Encryption Fight*, ELECTRONIC COMMERCE NEWS, Oct. 18, 1999; Lee Bruno, *Strong Crypto Unleashed?*, DATA COMMUNICATIONS, June 7, 1999.

[382] ACLU v. Reno, 521 U.S. 844, 870 (1997) ("This dynamic, multifaceted category of communication includes no only traditional print and news services, but also audio, video, and still images, as well as interactive, real-time dialogue. Through the use of chat rooms, any person with a phone line can become a town crier with a voice that resonates farther than it could from any soapbox. Through the use of Web pages, mail exploders, and newsgroups, that same individual can become a pamphleteer. As the District Court found, 'the content on the Internet is as diverse as human thought.'").

[383] 209 F.3d 481 (6th Cir. 2000).

[384] Bernstein IV, 176 F.3d at 1145; *Junger*, 209 F.3d at 485.

[385] *Junger*, 209 F.3d at 483.

[386] *Id.*

[387] *Id.*

[388] *Id.* at 484.

[389] *Id.* Junger filed his action to make a facial challenge to the regulations. *Id.*

[390] Press Release, *Ohio ACLU Files Brief in Internet Appeal: Cleveland Law Professor Seeks Right to Publish Encryption Information Online*, Mar. 2, 1999, *at* http://jya.com/pdj-aclu.htm.

[391] *Junger*, 8 F. Supp. 2d at 712, 723-24, *rev'd*, 209 F.3d at 485 (reversing and remanding so that an inquiry could be conducted into whether Junger could bring a "facial challenge" under the recently revised Export Administration Regulations).

have the full protection of the First Amendment, including those concerning "the advancement of truth, science, morality, and arts."[392] The Circuit also enumerated the times which the Supreme Court has expressly extended constitutional protections to nontraditional forms of communication including modern music, artwork, and nonsensical poetry.[393] It explained that though source code, like a musical score, is unintelligible to those not trained in how to read its content, both types of communication are equally expressive in character, and constitutional protections apply equally.[394]

3. Conclusion: Freenet's Source Code is Constitutionally Protected

It is extremely difficult and inefficient for even experienced programmers to write computer instructions in the binary terms which computers understand. As a result, programmers generally write source code for computer programs in so-called "high level" languages.[395] They then employ compiler programs which transform human-readable source code into binary, or object code, which can be read by computers.[396] Both the Ninth and Sixth Circuits appropriately found that source code was meant to be understood by humans, and was a scientific language, similar to mathematics, by which cryptographers could communicate technical ideas.[397] Indeed, any doubt that programming languages are not expressive can be immediately dispelled by examining any of the hundreds of poems written in the Perl programming language.[398] Based on the precedent established in both *Bernstein* and *Junger*, it appears highly likely that the source code of Freenet is fully protected by the First Amendment. Moreover, in January 2000, encryption export regulations were revised "to allow the export...of any encryption commodity or software to individuals, commercial firms, and other non-governmental end-users in all destinations."[399] Though substantial concerns and criticism of U.S. export policy remain,[400] such revisions represent a substantial step forward in bringing U.S. encryption policy in line with procedural requirements of set forth by the Supreme Court in *Freedman v. Maryland*.[401] The new regulations substantially liberalize export controls on source code, in line with the spirit of *Bernstein* and *Junger*.[402] Within the context of Freenet, perhaps

---

[392] *Junger*, 209 F.3d at 484, quoting *Roth v. United States*, 354 U.S. 476, 484 (1957) quoting 1 JOURNALS OF THE CONSTITUTIONAL CONGRESS 108 (1774).

[393] *Junger*, 209 F.3d at 484. These cases will be discussed in greater detail in Section IV.G.

[394] *Id.* at 484.

[395] *See Source Code*, WHATIS?COM, *at* http://whatis.techtarget.com/definition/0,289893,sid9_gci213030,00.html.

[396] Robert P. Bigelow, *1981: Year of Developments for Software Protection*, LEGAL TIMES, Feb. 15, 1982, at 19.

[397] Bernstein IV, 176 F.3d at 1141; *Junger*, 209 F.3d at 484.

[398] For a sample of such poems, visit *Perl Poetry*, PERL MONKS, *at* http://www.perlmonks.com/index.pl?node=Perl%20Poetry&lastmode_id=131. Perhaps the most succinct example is "die if !($ToBe);" a joke summarizing Hamlet's famous "To be or not to be" colloquy. *Id.*

[399] Revisions to Encryption Items, 65 Fed. Reg. 2492, (Jan. 14, 2000).

[400] *See* Rueda, *supra* note 304, at 80.

[401] 380 U.S. 51, 58-60 (1965) (setting forth three procedural safeguards applicable when a licensing imposes a prior restraint on free speech: (1) that the censor seeking to suppress the speech must bear the burden of proof; (2) that any restraint issued must be for a specified brief period of time; (3) that expeditious judicial review be made).

[402] *See* 15 C.F.R. § 740.13(e)(2001).

the most salient revision is an exemption for open source encryption software.[403] Under the current regime, the Internet posting of "publicly available" source code is permissible unless specifically intended to reach the countries of Cuba, Iran, Iraq, Libya, North Korea, Sudan, or Syria.[404] Thus, any attempts at regulating or prohibiting Freenet must first confront the potentially formidable right of its creators to "speak" its source code.[405] The inquiry does not end there however.

G. Encrypted Speech is Protected Speech

> "Prohibiting the use of a particular form of cryptography for the purposes of making communication intelligible to law enforcement is akin to prohibiting someone from speaking a language not understood by law enforcement."[406]

Neither the *Bernstein* nor the *Junger* courts reached the question of whether there is a First Amendment right to encrypted speech. Indeed, the question has not been squarely addressed in any reported United States case. Nonetheless, as discussed below, First Amendment principles clearly establish such a right.[407]

Judge Learned Hand delivered an interesting commentary on encrypted speech in *Reiss v. National Quotation Bureau*,[408] a copyright case in which Judge Hand ruled that a book full of coined words was a "writing" protected by the Copyright Act.[409] He wondered:

> "Suppose some one devised a set of words or symbols to form a new abstract speech,...a kind of blank Esperanto....Mathematics has its symbols, indeed a language of its own, Peanese, understood by only a few people in the world. Suppose a mathematician were to devise a new set of compressed and more abstract symbols, and left them for some conventional meaning to be filled in."[410]

Judge Hand believed that employing such a language would constitute "writing."[411]

---

[403] License Exception TSU-740.13. *See* 15 C.F.R. § 740.13 (2001).

[404] *Id.*

[405] The efficacy of such regulation, even if Constitutionally permissible is highly suspect. *See* Rueda, *supra* note 304, at 81 (thoroughly describing the impossibility of keeping encryption technology out of the hands of undesirables).

[406] Daniel J. Weitzner, *The Clipper Chip, Key Escrow and the Constitution*, NETWORKS & POLICY, 1, 4 (Summer 1993).

[407] The right to keep one's thoughts private is generally found in the Fourth, and sometimes Fifth Amendments. A substantial body of academic work exists examining the right to use encryption products based on these Amendments. *See, e.g.*, Henry R. King, *Big Brother, the Holding Company: A Review of Key-Escrow Encryption Technology*, 21 RUTGERS COMPUTER & TECH. L.J. 224 (1995).

[408] 276 F. 717 (S.D.N.Y. 1921).

[409] *Id.* at 718.

[410] *Id.*

[411] *Id.* at 719.

1. Preliminary Arguments in Favor of Protections for Encrypted Speech

A number of arguments can and have been made that encrypted speech is "pure speech," and deserving of the highest of Constitutional protections.[412] The first such argument is that encrypted speech is itself a language of its own. Encrypted speech can easily be analogized to a language which only two people speak–the sender, and the recipient. As the Ninth Circuit expressed in *Bernstein*, the decision to "speak in a language other than English [implicates] pure speech concerns....Speech in any language is still speech, and the decision to speak in another language is a decision involving speech alone."[413] This argument is somewhat imprecise, however, because when two people communicate via encrypted speech, two messages are being transmitted. The first, appears as gibberish to everyone who does not possess a key. For example, an eavesdropper might be presented with the following text: "L WKLQN WKH SUHVLGHQW VWLQNV." The second, is the underlying message, in this case, "I THINK THE PRESIDENT STINKS." In *Hurley v. Irish-American Gay, Lesbian & Bisexual Group of Boston*,[414] the Court stated that "a narrow, succinctly articulable message is not a condition of constitutional protection, which if confined to conveying a 'particularized message,' would never reach the unquestionably shielded painting of Jackson Pollock, music of Arnold Schonberg, or Jabberwocky verse of Lewis Carroll."[415] Thus, the Supreme Court has held that gibberish is entitled to Constitutional protection. Were "L WKLQN WKH SUHVLGHQW VWLQNV" the extent of the message being transmitted, an argument may be made under *Hurley* that it is entitled to First Amendment protection. Because the message contains two meanings, however, one could argue that the communication is *more* deserving of Constitutional protection. A political statement such as "I THINK THE PRESIDENT STINKS," lies at the core of what the Founding Fathers sought to protect in the First Amendment.

The aforementioned arguments in favor full First Amendment protection for encrypted speech are somewhat novel. The strongest, and most illustrative argument in favor of finding encrypted speech is protected under the First Amendment, is the argument that speaking in code is an ancient liberty.

2. Encrypted Speech is an Ancient Liberty[416]

The Supreme Court has repeatedly examined the history of a number of social practices and customs as part of the Twentieth Century process of incorporating portions of the Bill of Rights in the Fourteenth Amendment of the United States Constitution.[417] The Court has specifically characterized particularly deserving customs and practices as "essential" to "ordered liberty," or "fundamental."[418] Indeed, the Court has reviewed a series of cases recognizing and defining so-called ancient liberties in expression, relying on the historical norms and intentions

---

[412] *See* John P. Collins, *Speaking in Code*, 106 YALE L.J. 2691, 2694 (1997).

[413] *See Bernstein*, 922 F. Supp. at 1435 (quoting , 922 F. Supp. at 1435 (quoting *Yniguez v. Arizonans for Official English*, 69 F.3d 920, 935 (9th Cir. 1995) (*en banc*), vacated as moot, 117 S. Ct. 1055 (1997)).

[414] 515 U.S. 557 (1995).

[415] *Id.* at 569 (citation omitted).

[416] The term comes from *Hague v. Comm. for Indus. Org.*, 307 U.S. 496 (1939).

[417] *See* John A. Fraser, III, *The Use of Encrypted, Coded and Secret Communications is an "Ancient Liberty" Protected by the United States Constitution*, VA. J.L. & TECH. 2, 3 (1997).

[418] *Id.*

of the Founding Fathers and other early Americans, as well as British legal traditions. Such cases include door-to-door canvassing for political or religious purposes,[419] leafleting,[420] use of sidewalks and streets for political and other discourse,[421] posting signs on private property,[422] picketing,[423] printing and distribution of political cartoons,[424] and public demonstrations and parades.[425] The Court has also recognized as "fundamental" the right to teach foreign languages to children, even in times of war.[426]

The aforementioned ancient liberty cases contribute two useful rules to the application of the Constitution to ancient forms of expression or communication. First Amendment jurisprudence recognizes a distinction between expressive conduct and speech.[427] The former may generally be regulated based on a "rational basis" standard, while regulation of the latter is reviewed under either "strict scrutiny" or "intermediate" review standards.[428] The first contribution made by the ancient liberty cases is that the Supreme Court regularly relies on the "ancient" nature of certain kinds of expression to avoid making a speech/conduct distinction.[429] Thus, when an ancient liberty is involved, what may otherwise constitute conduct may nonetheless receive full First Amendment protection.

The second contribution which can be gleaned from the line of ancient liberty cases has been described by commentators as a rule of law for determining whether or not a form of communication is protected.[430] The proffered rule suggests that a form of expression or communication is protected if it meets the following three-part test: (1) it is historically demonstrated to have been widely used at the time of the adoption of the Bill of Rights; (2) it was sanctioned in use by the Founding Fathers; and (3) it has continued in use.[431] If an expression or mode of communication satisfies the test, it may not be prohibited, and may only be regulated if abused to accomplish some illegal purpose.[432]

Applying the aforementioned test to encrypted speech, it appears highly likely that it is protected as an ancient liberty.

---

[419] *Martin v. Struthers*, 319 U.S. 141 (1943).
[420] *United States v. Grace*, 461 U.S. 171 (1983).
[421] *Hague v. Comm. for Indus. Org.*, 307 U.S. 496 (1939).
[422] *City of Ladue v. Gilleo*, 512 U.S. 43 (1994).
[423] *Carey v. Brown*, 447 U.S. 445 (1980).
[424] *Hustler Magazine v. Falwell*, 485 U.S. 46 (1988).
[425] *Hurley v. Irish-American Gay, Lesbian and Bisexual Group of Boston*, 515 U.S. 557 (1995).
[426] *Meyer v. Nebraska*, 262 U.S. 390 (1923).
[427] *Clark v. Community for Creative Non-Violence*, 468 U.S. 288 (1984).
[428] *Turner Broadcasting Sys. v. FCC*, 512 U.S. 622 (1994).
[429] For example, the Court held that consumer boycotts were an ancient practice protected by the Constitution, and thereby avoided having to explain how refusing to transact with Claiborne Hardware was not "conduct." *NAACP v. Claiborne Hardware*, 458 U.S. 886 (1982). In a subsequent boycott case, the Court also held that secondary boycotts were impermissible conduct, not protected by the Constitution. *Int'l Longshoreman's Ass'n v. Allied Int'l*, 456 U.S. 212 (1982). It appears that the distinction lay with organized labor's lack of historic roots.
[430] *See* Fraser, *supra* note 417, at 17.
[431] *Id.*
[432] *Id.*

a) Encrypted Speech Was In Common Use at the Time the Bill of Rights was Adopted

Methods of secret communication were well known and widely used in England during the Eighteenth Century.[433] A number of cryptography treatises were published in England between 1593 and 1776, as were books on the use of codes, ciphers, and other techniques of concealing the content of a message.[434] Such known techniques included the use of parables in scripture, secret inks and papers, hieroglyphics and other secret uses of symbols, modified alphabets, and fire and smoke signals.[435] Indeed, a number of notable members of British history have used ciphers, including Geoffrey Chaucer, Roger Bacon, and Mary Queen of Scots.[436] Similarly, the House of Lords allowed the introduction of deciphered writings in the 1723 trial of Bishop Francis Atterbury,[437] and by 1720, the Royal Mail in London opened and deciphered diplomatic messages on a nightly basis.[438]

Secret communications were regularly made in Colonial America as well, often in attempts to defeat British agents and censors.[439] Indeed, two luminaries of American history, Benjamin Franklin, and Thomas Jefferson, extensively used and extolled the virtues of cryptography in the days preceding the American Revolution. In 1748, Benjamin Franklin printed an early American text on the use of codes and ciphers authored by George Fisher.[440] Such a text was of critical importance in colonial America due to the British practice of opening and reading private mail, as well as risks that mail might be stolen from postal carriers.[441] A young Thomas Jefferson employed ciphers long before the war, in correspondence concerning his unsuccessful attempts to court a young lady.[442] As the political climate in colonial America heated, the need for cryptography to protect the communications of those fighting for a new nation increased dramatically.[443]

b) The Use of Encrypted Speech was Sanctioned by the Founding Fathers

One of the earliest acts of the Continental Congress was to pass an order that its Committee in charge of foreign correspondence use "cyphers."[444] Americans used codes and ciphers from the beginnings of the Revolution in 1775, to foment, support, and execute a successful rebellion against the British. Early Americans also used cryptography for private correspondence, as well.[445] As one author has stated, "As rebels and conspirators, the young

---

[433] *Id.* at 18.
[434] *Id.*
[435] *Id.*
[436] *See* KAHN, *supra* note 248, at 90-91, 121-24.
[437] *Id.* at 170-71
[438] *Id.* at 171-74.
[439] *See* Fraser, *supra* note 417, at 20.
[440] *Id.*
[441] *Id.*
[442] *Id.*
[443] When the Committees of Secret Correspondence was formed to oppose the Stamp Act of 1765, a great wealth of knowledge in the ways to maintain communications secrecy was available. *Id.*
[444] *Id.* at note 62.
[445] Fraser, *supra* note 417, at 21.

nation's leaders...turned to codes and ciphers in an effort to preserve the confidentiality of their communications."[446] Indeed, the Early American landscape is full of cryptographic communications authored, received, and intercepted by such luminaries as George Washington,[447] John and Abigail Adams,[448] Thomas Jefferson,[449] James Monroe,[450] James Madison,[451] John Jay,[452] and Benjamin Franklin.[453] This list is far from exhaustive, and amply demonstrates that the Revolutionary era was a time ripe with the regular use of cryptography by the Founding Fathers and other notable early Americans.[454] Perhaps the most telling example of the use of cryptography in early America is found in a letter sent by Thomas Jefferson on August 28, 1789, to James Madison, in which he commented on the proposed First Amendment in partially encrypted prose.[455]

c) The Use of Encrypted Speech Continues to Flourish Today

The widespread use of cryptography has continued since the adoption of the Constitution, to the patenting of Samuel Morse's telegraph, through the modern day. Jefferson and Madison regularly relied on ciphers to discuss "the increasing hostility to the excesses of the French Revolution and the stresses and strains of organizing an opposition party...."[456] There is likewise evidence that Alexander Hamilton used ciphers to communicate with relatives and

---

[446] David W. Gaddy, *Introduction* to RALPH E. WEBER, MASKED DISPATCHES: CRYPTOGRAMS AND CRYPTOLOGY IN AMERICAN HISTORY (1993).

[447] As commander of the Continental Army, General Washington regularly came into contact with secret British messages, as well as messages sent by Benedict Arnold. *See* KAHN, *supra* note 248, at 176-80. After the adoption of the Constitution, cryptography continued to play an important role for Washington, in the form of encrypted presidential correspondence. *See* Fraser, *supra* note 417, at 41. In 1786, Reverend William Gordon made a gift of a cipher for correspondence to George Washington, a gift for which Washington offered heartfelt thanks. *Id.* at

[448] The Adams' regularly used ciphers to correspond while John Adams was away from home. *See* Fraser, *supra* note 417, at 23.

[449] The father of the Declaration of Independence has also been referred to as "the father of American cryptography," by noted cryptography historian David Kahn. KAHN, *supra* note 248, at 195. During the Revolution, Jefferson frequently encrypted communications to guard his private thoughts as well as protect confidential information and political insights. *Id.* He was not only an extensive user of cryptography, but also developed cryptographic systems, including a "cipher cylinder," which was unsurpassed for military communication purposes until the 1920s, and remained in use by the United States Navy until 1967. *Id.* at 192-95.

[450] James Monroe took a cipher with him to Paris in 1803 so that he could communicate with Thomas Jefferson regarding the Louisiana Purchase. Fraser, *supra* note 417, at 25.

[451] As a close confidant of Thomas Jefferson, it was inevitable that Madison, too, would regularly use cryptography for private correspondence, correspondence with Virginia officials, and fellow Revolutionaries. *Id.*at 26.

[452] The first Chief Justice of the United States Supreme Court used cryptography as early as October 1779, to correspond on personal matters while in Europe. He was also required to encipher all significant diplomatic correspondence. *Id.* at 27.

[453] In addition to printing a 1748 book on ciphers, Franklin also invented a "homophonic substitution cypher" in 1781 while living in Paris. *Id.* at 33. Franklin also employed cryptography in his international correspondence on behalf of the Continental Congress. *Id.*

[454] Edmund Burnett carefully recorded the use of cryptography by other early Americans not listed above. *See* Edmund Cody Burnett, *Ciphers of the Revolutionary Period*, 22 AMERICAN HISTORICAL REVIEW 329 (1917).

[455] *See* Fraser, *supra* note 417 at 43.

[456] *Id.* at 45.

political associates while in office.[457] Indeed, "[i]n the years after 1780, Jefferson, James Madison, James Monroe, and a covey of other political leaders in the United States often wrote in code in order to protect their personal views on tense domestic issues confronting the American nation. Employing many codes and a few ciphers, they sought safety for their dispatches: they built security fences to protect their correspondence from political rivals and American postal officials."[458] Aaron Burr and his associates relied on cryptography in their efforts to establish a new government in a territory under Spanish control,[459] and Chief Justice Marshall, familiar with cryptography as part of his diplomatic duties,[460] allowed the decrypted transcripts into evidence.[461]

It is beyond the scope of this paper to provide a full review of post-1800 cryptographic developments. It is nonetheless important to note that the need for secrecy and confidential communications has continued throughout the development of America. Indeed, history is clear on two points: (1) the public sector has maintained a high demand for cryptographic products;[462] and (2) the federal government's expression of a desire to restrict the use of cryptography by private citizens did not occur until after 1960.[463]

In 1805, an unknown author published a book in Hartford Connecticut with the impressive title, *A Dictionary to Enable Any Two Persons to Maintain A Correspondence with a Secrecy Which is Impossible for Any Other Person to Discover.*[464] A number of other cryptographic books were also published in America during this time, and for decades to come.[465] But, it was the rise of the railroad industry,[466] followed by the invention of the telegraph in 1844,[467] which spurred on the next truly impressive wave of demand for codes and ciphers among the general public.[468]

---

[457] *Id.* at 46.

[458] *See* WEBER, *supra* note 446, at 6.

[459] *See United States v. Burr*, 4 Cranch 455, 8 U.S. 455, 5 F.Cas. 2 (1807).

[460] *See* WEBER, *supra* note 446, at 84.

[461] *Id.* at 12. This is an extraordinary treason case, in part because of the weakness of the cryptographic evidence, as discussed in KAHN, *supra* note 248, at 186-87.

[462] KAHN, *supra* note 248, at 825-26, 836-53.

[463] During the first two World Wars, Presidents Wilson and Roosevelt issued Executive Orders or other proclamations severely restricting the ability of aliens to communicate in foreign languages by telephone or wire, as well as their ability to possess or use ciphers. *See* J. Gregory Sidak, *War Liberty, and Enemy Aliens*, 67 N.Y. U. L. REV. 1402, 1413 n. 57 (1992); *Metaphor, supra* note 250, at 851 & n. 612. The ability of citizens to do similar things was unregulated.

[464] KAHN, *supra* note 248, at 192. The text listed words and syllables in alphabetical order, suggesting means for concealing the meaning of correspondence using the dictionary. *Id.*

[465] In 1829, James Swaim published a book intended for prisoners, in which he advised the use of coded speech to communicate through cell walls. David Shulman, An Annotated Bibliography of Cryptography (1976), at 1-33. William Thompson published a textbook for the instruction of the blind in 1832, and included in it a chapter on cryptography. *Id.* at 1-34.

[466] Anonymous, *Cryptography, or Methods of Secret Writing Described,* AMERICAN RAIL ROAD JOURNAL (1833).

[467] ITHIEL DE SOLA POOL, TECHNOLOGIES OF FREEDOM, 25-26 (1983).

[468] KAHN, *supra* note 248, at 189.

Described as making "cryptography what it is today,"[469] in addition to the secrecy offered by use of cryptography, Morse's telegraph created a demand among the public for codes and ciphers because the sender and recipient could save money by shortening their message lengths.[470] For businesses, the use of pre-arranged telegraphic codes could potentially amount to a significant amount of savings. As a result, hundreds of codes and ciphers were published, along with instructions on how to employ them to conceal a telegram's content.[471]

It is difficult to gauge to what extent the national economy is dependent on encryption, but as stated in Section IV.B, a staggering amount of electronic commerce is dependent on information security, and thus cryptography.[472] Other examples include the heavy use of cryptography in the industries of finance, oil and mining, broadcasting, banking, telephony, fiber optics, signature authentication, digital television, and countless others.[473] In particular, potentially every business imaginable could use cryptography to prevent business espionage and protect trade secrets and other corporate assets.[474] Moreover, the sheer volume of cryptographic publications available today presents a strong indication of the continuing pervasiveness with which cryptography affects modern American society. In 1945, Joseph Galland published a comprehensive bibliography of printed materials concerning cryptography.[475] Galland notes ten American treatises on cryptography between 1872 and 1943,[476] and forty-four commercial ciphers or codes published in the United States between 1832 and 1942.[477] Galland cites forty-seven articles published in American periodicals after 1840, written by authors including Edgar Allan Poe and Herbert Yardley.[478] More recently, Bruce Schneier lists some 1653 unique publications and articles as reference in his book, *Applied Cryptography*, the vast majority of which were written after 1950.[479]

d) Additional Arguments Against Cryptography Bans and Other Regulations

As an ancient mode of expression, any attempt at regulating or banning encryption technology could run afoul of a number of Constitutional provisions, including the Fourth Amendment,[480] Fifth Amendment,[481] and the general Right to Privacy found in a combination of the First, Third, Fourth, Fifth, Ninth, and Fourteenth Amendments.[482] Such arguments lie

---

[469] *Id.*
[470] *Id.*
[471] *See,* Shulman, *supra* note 465, at 2-14.
[472] A report published by the National Research Council describes the United States encryption market in terms of strong demand met by multiple domestic and international vendors. National Research Council, *Cryptography's Role in Securing the Information Society*, ch. 2 (May 30, 1996) [hereinafter "NRC Report"].
[473] KAHN, *supra* note 248, at 824-44.
[474] *Id.* at 824-25.
[475] JOSEPH GALLAND, AN HISTORICAL AND ANALYTICAL BIBLIOGRAPHY OF THE LITERATURE OF CRYPTOGRAPHY, (1945).
[476] *Id.*
[477] *Id.*
[478] *Id.*
[479] SCHNEIER, *supra* note 283, at 675-741.
[480] *See Metaphor, supra* note 250, at 823-33.
[481] *Id.* at 833-38.
[482] *Id.* at 838-43.

outside the scope of this paper, yet the vital interests of the Founding Fathers are implicated by the types of interests they protected by the use of strong cryptography. After all, "in the early Republic, a well-constructed code could make private letters secure from political enemies, foreign foes, and highway robbers in America."[483]

(1) Cryptography Offers Protection of Dissidents

Viewing such historical luminaries as George Washington, Thomas Jefferson, and John Adams, as dissidents with communications in need of protection is a concept which is potentially difficult to comprehend.[484] Nonetheless, history shows that they and their compatriots relied on the secrecy of communications to rebel against the British government, gaining protection for their thoughts of social and political dissent. The ability of a speaker to communicate in confidence to a selected audience remains of critical importance to the continuing survival of privacy and free speech in a modern electronic age.[485]

(2) Cryptography Offers Protection for Developing Ideas

A compelling demonstration of the protection which encryption afforded developing ideas during the era of the Founding Fathers is evidenced in the use which George Washington and Innes made of cryptography while opposing the Kentucky Resolves.[486] The soon-to-be first President felt, as a private citizen, that he should act privately and confidentially to assist and instruct Innes in undermining the majority of the Kentucky legislature, shunning the glare of publicity, and employing a cipher to do so.[487]

(3) Cryptography Offers Protection of Political Expression

The protections offered by cryptography to political expression are easily evidenced by the enciphered correspondence which Jefferson and Madison exchanged during the Adams administration, as they sought to create an opposition party.[488] They relied on the governmental mail service to exchange their letters, and relied on encryption to protect their plans and intentions contained within those letters.[489] This occurred in an era when federal judges regularly instructed juries that criticism of the federal government constituted sedition.[490] That the Republican party emerged in the 1800 federal elections with Jefferson as its Presidential candidate, is due in large part to the planning executed through the use of secret correspondence

---

[483] *Weber*, *supra* note 446, at 98.

[484] *See* Fraser, *supra* note 417, at 76.

[485] *See* Lawrence Lessig, *The Path of Cyberlaw*, 104 YALE L.J. 1743, 1749-50 (1995).

[486] In March 1789, George Washington corresponded with Henry Innes concerning Kentucky's threatened secession from the newly-formed Union. THE WRITINGS OF GEORGE WASHINGTON (John C. Fitzpatrick ed., 1944). Washington enjoined Innes to use a "cypher" in the correspondence regarding their efforts to defeat the secessionists. It was in this same correspondence which Washington looked upon his taking of the Presidential office with some trepidation, but regarded it his duty. *Id.*

[487] *Id.*

[488] *See* Fraser, *supra* note 417, at 78.

[489] *Id.*

[490] *See* Weber, *supra* note 417, at 352-56.

made possible by ciphers which at the time were extremely difficult, if not impossible, for the government to break.

(4) Cryptography Offers Protection of Privacy

Abigail Adams summed up the Founders' use of cryptography to protect personal privacy when she stated that there were certain personal topics which she could not address in correspondence with her husband due to the lack of having ciphers while he was in Paris.[491] After being acquitted of treason charges, Aaron Burr employed a cipher to correspond with his daughter, hoping to protect himself and his daughter from further governmental attention.[492] Jefferson and Madison spoke of their romantic intentions through the use of ciphers.[493] Randolph similarly corresponded with Madison about his wife's cancer through the use of encryption.[494]

Today, encryption is widely used to secure information on networked computer systems, to protect privacy, to discourage and prevent industrial espionage, and to protect the confidentiality and integrity of a wide array of files, records, and electronic mail.[495]

3. Attempts at Forbidding or Regulating Encrypted Speech Should Face a Strong Presumption of Unconstitutionality.

Based on the above analysis, it appears highly likely that use of encryption is an ancient liberty, and that the Supreme Court would hold it protected by the First Amendment accordingly. Encryption was widely used at the founding of the United States, was sanctioned by the Founding Fathers, and continues in use today. Indeed, throughout every era in American history, citizens have relied on and exercised their ability to speak freely and confidentially on topics, to audiences of their choosing.

Modern cryptography has provided virtually impenetrable protection to these communications, including protection against legitimate law enforcement investigations.[496] As such, federal law enforcement officials regularly make damning arguments that unfettered access to cryptography allows terrorists, child pornographers, kidnappers, and drug dealers to execute their crimes outside the watchful eye of law enforcement.[497] Such arguments are often

---

[491] *Id.* at 101.
[492] *Id.* at 95.
[493] *Id.* at 86.
[494] *See* Fraser, *supra* note 417, at 23.
[495] *See Metaphor*, *supra* note 250, at 718-26, 728-30.
[496] "[T]he development and widespread deployment of cryptography that can be used to deny government access to information represents a challenge to the balance of power between the government and the individual. Historically, all governments under circumstances that further the common good, have asserted the right to compromise the privacy of individuals[;] ... unbreakable cryptography for confidentiality provides the individual with the ability to frustrate assertions of that right." NRC Report, *supra* note 472, at § 8.1.3.
[497] *Id.* at § 3.2-3.3; *see, e.g.*, Committee Hearings of the U.S. House of Representatives, Committee on International Relations, Pages 55-56 (statement of FBI Director Louis Freeh) ("With unbreakable non-key recovery encryption proliferated, we will be out of the public safety business in terms of any real-time understanding or response capability, not just in the big cases, but kidnapping cases also, the things that we need to be in front of.")

persuasive, especially in the wake of major criminal investigations.[498] Moreover, a strong argument can be made that the existence of Freenet, potentially sounding the death-knell of copyright enforcement online, presents a strong government interest in regulating or prohibiting encryption.[499] Nonetheless, after applying a combination of logic and Constitutional law, however, it appears that regulations capable of creating truly effective controls on encryption's misuses are precluded.[500]

a) The Invention of the Computer is Irrelevant to the Analysis

While widespread access to computers was obviously not present in the late Eighteenth century, inventions such as Jefferson's "cipher wheel" offered the practical equivalent of modern cryptography.[501] Jefferson protected himself against private interlopers and the government alike by raising a shield of privacy around his statements and intentions through the use of cryptography. It would thus be seemingly absurd to suggest that the likes of Jefferson, Washington, Adams, and the other Founding Fathers, would have willingly surrendered the protections offered by cryptography in exchange for greater ease on the part of the government to crack the messages.[502] One of the major purposes for which the Founders *employed* encryption was government frustration. It would thus appear absurd to suggest that the Founders would have condoned a government ban on the use of ciphers and codes which were too strong for the government's convenience.

Nonetheless, one could argue that the speed and ease with which the average American could potentially encrypt his communications renders the modern practice of communications secrecy fundamentally different from the sort of protections in which the average early American indulged. This argument, too, is specious. It is difficult to see how widespread availability of strong cryptography could make American citizens less trustworthy than they were at the time of this nation's founding, nor does it make sense that the government is any more responsible or honest today. Moreover, child pornographers, terrorists, kidnappers, and copyright pirates will undoubtedly continue to use cryptography regardless of whether or not it is legal. As a rule,

---

[498] *See, e.g.*, Steven Levy, *Did Encryption Empower These Terrorists?*, MSNBC.COM *at* http://www.msnbc.com/news/627390.asp.

[499] It is possible that Congress might attempt to pass a specific ban on Freenet, on the assumption that such a ban would be content neutral. Unfortunately, this paper is sufficiently long to preclude an analysis of whether such legislation would survive a court challenge.

[500] Given the widespread availability of encryption products, both domestically and internationally, as well as the efficacy of those products, it appears that nothing short of a virtual ban on encryption could restore the government's ability to eavesdrop effectively. So-called key-escrow schemes are often presented as a "solution" to this problem, however this author strongly disagrees. Unfortunately, the details of key-escrow lie outside the scope of this paper.

[501] That the U.S. government used Jefferson's invention, or modified versions of it, into the 1900s, is a testament to the governmental perception of the cipher wheel's strength as a militaristic device. *See* KAHN, *supra* note 248, at 192-95.

[502] A quote by Benjamin Franklin seems apropos: "They that can give up essential liberty to obtain a little temporary safety deserve neither liberty nor safety." Benjamin Franklin, Historical Review of Pennsylvania, in Bartlett's Familiar Quotations 348 (Emily Morison Beck ed., 1980).

international criminal enterprises regularly pay premium prices for communications secrecy, and a complete ban on encryption within the United States would have little effect on this practice.[503]

b) Logical Analysis

The anti-terrorist rhetoric put forth against encryption by law enforcement officials and others fundamentally compromises human rights interests in the modern digital age. Considering the number of people subjected to harsh societal considerations, and the resulting financial and other anguish which oppression causes, one of the strongest counter-arguments is that the number of persons aided by strong cryptography substantially outweighs those who could be harmed by the same technology.[504]

"Because of foreign and domestic threats to liberty and freedom, codes and ciphers became integral elements in American public and private communication."[505] This summation of early America is no less true today. Should the courts have a chance to visit the right of Americans to use cryptography today, perhaps through litigation of Freenet, they will be forced to decide whether the government's interest in protecting copyright outweighs the ancient liberty of secret communication. It is hoped and believed by this author that judges will do so with complete knowledge of the history of encrypted communications and will uphold this ancient liberty.

V. ANONYMITY

The second technical innovation on which Freenet depends is untraceability, or anonymity. The analysis of whether a law prohibiting or regulating electronic anonymity is similar to that of one touching upon encryption, with one difference. The Supreme Court has had multiple occasions to rule on the protections afforded anonymity under the First Amendment.

A. Traditional Anonymous Speech

Anonymity can be a tool for both benevolent and malevolent uses.[506] This was true long before the advent of modern computing, and the framework for the anonymity debate appears easily demarked. Some suggest that anonymity's contributions to free discourse outweigh any harm that it may cause, or, that the alternatives—a ban on or censorship of anonymous speech—are more destructive of a free society than any such harms.[507] As the Supreme Court has noted,

---

[503] *See* NRC Report, *supra* note 472, § 3.2.4.

[504] *See* Geoffrey Gordon, *supra* note 309, at 489.

[505] *See* WEBER, *supra* note 446, at 107-108.

[506] This is true of a wide variety of technologies. As Scott Charney and Ken Alexander note, "history teaches that criminals will frequently abuse new technologies to benefit themselves or injure others. Automobiles are an apt example. Designed to provide transportation for law-abiding individuals, the automobile soon became a target (*e.g.*, car theft, car-jacking), a tool (*e.g.*, the getaway car in a bank robbery), and a weapon (*e.g.*, hit-and-run). Clearly, computers are following the same route." *Computer Crime*, 45 EMORY L.J. 931, 934 (1996).

[507] One author suggests that "[t]here are numerous situations in which anonymity seems entirely appropriate and even desirable. Psychologists and sociologists point out that people benefit from being able to

"It is plain that anonymity has sometimes been assumed for the most constructive purposes."[508] Others suggest that truly anonymous communications' inherent lack of accountability presents a way for criminals to remain safely above and outside the law's reach—and suggest at least some forms of anonymity should be regulated or subjected to an outright ban.[509] Certainly, Freenet's potential for eradicating effective copyright enforcement presents a serious governmental concern.

1. Anonymity Cast in a Positive Light

As with encryption, American anonymous rhetoric boasts and benefits from a rich history of use dating to the founding days of the United States.[510] The Federalist Papers[511] are perhaps the finest example of how anonymous rhetoric has benefited American social development. Authored by "Publius,"[512] the work may never have been published or distributed had the authors been forced to reveal their true identities. Similarly, the pre-Revolutionary War "Letters of Junius" pseudononymously espoused a wealth of constitutional rhetoric during the years 1767–1772, including sentiment that ultimately influenced the content of the Bill of Rights.[513] Junius's true identity remains unknown today.[514]

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

---

assume different personae. It is therefore natural that individuals use electronic communication to disguise themselves,....The media often cite 'a prominent source' who does not wish to be identified, and pseudonymous authors have long been with us, sometimes in the past to prevent disclosure that the writer was female for fear her work would not be published were her gender known....Anonymity has also been protected in cases in which actual retaliation or harm may ensue if the source of the writing is known, as in the case of whistle-blowers or political dissidents under authoritarian regimes." Ann Wells Branscomb, *Anonymity, Autonomy, and Accountability: Challenges to the First Amendment in Cyberspace*, 104 YALE L.J. 1639, 1642 (1995).

[508] Talley v. California, 362 U.S. 60, 65 (1960).

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

[510] A strong argument can be made that anonymous discourse is protected as an ancient liberty in the manner of encrypted speech. Because such an argument closely parallels that already discussed in Section IV, it is not addressed here.

[511] THE FEDERALIST PAPERS (Clinton Rossiter ed., 1961).

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

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

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

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

Id. (citations omitted).

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

A form of anonymity—substituting a number for a name—is employed by the New Mexico Law Review when assessing the writing skills of prospective journal members. Indeed, this technique of "blinding" academic submissions is similarly employed by law schools around the country during examinations. Moreover, authors in general have a history of adopting pseudonyms,[515] for varying reasons.

American jurisprudence also supports the use of anonymity. Throughout the course of this country's history, the Supreme Court has affirmed the benefits inherent in anonymity—particularly among dissidents.[516] In *NAACP v. Alabama ex. rel. Patterson*,[517] for example, the Supreme Court held that the right of anonymous association is protected by the guarantee of free speech in the Constitution, and that a state had no power to compel a local chapter of the NAACP to disclose a list of the names of its members. Of great concern, had the state prevailed, was that bigots might use the disclosed identities to target and harm NAACP members. As explained by the Court, "It is hardly a novel perception that compelled disclosure of affiliation with groups engaged in advocacy may constitute...restraint on freedom of association...."[518]

A more recent case, *McIntyre v. Ohio Elections Commission*,[519] illustrates both the importance of anonymity and the unique legal problems it presents. *McIntyre* was centered on the actions of Mrs. Margaret McIntyre, who distributed leaflets at a public meeting at the

---

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

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

[517] 357 U.S. 449 (1958).

[518] *Id.* at 462.

[519] 514 U.S. 334 (1995).

Blendon Middle School in Westerville, Ohio, expressing opposition to a proposed school tax levy. Some of the leaflets identified her as the author; others merely indicated that the leaflets expressed the views of "Concerned Parents and Taxpayers."[520] Mrs. McIntyre subsequently was fined for her actions by the Ohio Elections Committee for violating a statute that provided:

> [n]o person shall write, print, post, or distribute, or cause to be written, printed, posted, or distributed, a notice, placard, dodger, advertisement, sample ballot, or any other form of general publication which is designed to...promote the adoption or defeat of any issue...through flyers, handbills, or other nonperiodical printed matter, unless there appears on such form of publication in a conspicuous place or is contained within said statement the name and residence or business address of the chairman, treasurer, or secretary of the organization issuing the same, or the person who issues, makes, or is responsible therefore.[521]

The Court stated the issue in the case as "whether an Ohio statute that prohibits the distribution of anonymous campaign literature is a 'law...abridging the freedom of speech' within the meaning of the First Amendment."[522] Throughout its opinion, the Court eloquently referenced the "important role in the progress of mankind" that anonymous literature in all forms has played:[523]

> Anonymity...provides a way for a writer who may be personally unpopular to ensure that readers will not prejudice her message simply because they do not like its proponent. Thus, even in the field of political rhetoric, where the identity of the speaker is an important component of many attempts to persuade, the most effective advocates have sometimes opted for anonymity. [There is] a respected tradition of anonymity in the advocacy of political causes. This tradition is perhaps best exemplified by the secret ballot, the hard-won right to vote one's conscience without fear of retaliation.[524]

The Court concluded,

> Under our Constitution, anonymous pamphleteering is not a pernicious, fraudulent practice, but an honorable tradition of advocacy and of dissent. Anonymity is a shield from the tyranny of the majority. It thus exemplifies the purpose behind the Bill of Rights, and of the First Amendment in particular: to protect unpopular individuals from retaliation—and their ideas from suppression—at the hand of an intolerant society. The right to remain anonymous may be abused when it shields fraudulent conduct. But political speech by its nature will sometimes have unpalatable consequences, and, in general, our society accords greater weight to the value of free speech than to the dangers of its misuse. Ohio has not shown that its interest in preventing the misuse of anonymous election-related speech justifies a prohibition on all uses of that speech.[525]

---

[520] *Id.* at 337.
[521] *Id.* at 338 n.3 (citing OHIO REV. CODE ANN. § 53599.09(A)).
[522] *McIntyre*, 514 U.S. at 336.
[523] *Id.* at 341 (quoting Talley v. California, 362 U.S. 60, 64 (1960)).
[524] *Id.* at 342-43 (internal quotations and footnotes omitted).
[525] *Id.* at 357 (citations omitted).

"Anonymity" appears at issue in a strange sense in *McIntyre*. The Ohio Statute did indeed "prohibit the distribution of anonymous campaign literature."[526] Mrs. McIntyre's actions, however, were not anonymous at all. She attended a meeting and, acting in a fashion that ensured that her identity was evident to all, distributed campaign literature without her identification on the literature itself. Upon reflection, there appear to be two elements to the offense with which Mrs. McIntyre was charged: (1) anonymous communication via "a notice, placard, dodger, advertisement, sample ballot, or any other form of general publication which is designed to...promote the adoption or defeat of any issue";[527] and (2) a non-anonymous action sufficient to allow her to be identified and charged. Both elements were required, but only the first was prohibited by the Ohio legislature. The second element was more a consequence of a general truth that rules can only be enforced by identifying a party against whom to proceed.

2. Anonymity's Darker Side

Justice Scalia summed up the case against anonymity in his dissent in *McIntyre*[528] when he stated, "It facilitates wrong by eliminating accountability, which is ordinarily the very purpose of the anonymity."[529]

Conspiracy, hate speech, libel, disclosure of trade secrets, and other forms of illegal and immoral activity can be furthered easily by anonymous communication. Some of these communications may possess clues to identify their author.[530] Many communications, however, present stark law enforcement problems, particularly in the realms of defamation and intellectual property law.[531]

Signed defamatory messages may carry more credibility than unsigned (anonymous) ones, and may thus be more damaging. Nevertheless, anonymous defamatory messages are not necessarily harmless. As Michael Froomkin has suggested, "Most people would probably be upset to discover a series of unsigned posters accusing them of pedophilia tacked to trees or lampposts in their neighborhood."[532] Similarly, a victim of anonymous accusation is unlikely to be appeased by assertions that the anonymous attacker lacks credibility.[533] As Sissela Bok has argued, a society in which "everyone can keep secrets impenetrable at will," whether they be "innocuous...[or] lethal plans,...would force us to disregard the legitimate claims of those persons who might be injured, betrayed, or ignored as the result of secrets inappropriately kept."[534]

---

[526] *Id.* at 338 n.3 (citing OHIO REV. CODE ANN. § 53599.09(A)).

[527] *Id.*

[528] 514 U.S. 334 (1995).

[529] *Id.* at 385 (Scalia, J. dissenting).

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

[531] *See* A. Michael Froomkin, *Flood Control on the Information Ocean: Living with Anonymity, Digital Cash, and Distributed Databases*, 15 J. L. & COM. 395, 402 (1996).

[532] *Id.* at 404.

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

[534] SISSELA BOK, SECRETS: ON THE ETHICS OF CONCEALMENT AND REVELATION 16, 28 (McGraw-Hill 1984).

Aside from providing a tool for criminals, anonymity also is denounced frequently for limiting access to truth. Ironically put forth in an anonymously authored article,[535] the argument is that "disclosure advances the search for truth,"[536] because anonymous propaganda "makes it more difficult to identify the self interest or bias underlying the argument."[537] Justice Black, a noted First Amendment absolutist, shared this viewpoint. He believed mandatory identity disclosure would enhance the freedom of speech, and that Congress should require the disclosure of foreign agents "so that hearers and readers may not be deceived by the belief that the information comes from a disinterested source. Such legislation implements rather than detracts from the prized freedoms guaranteed by the First Amendment."[538] Anonymity has been referred to as "a dangerous weapon" in recent months.[539]

The potential damage to society's ability to confront and remedy legitimate claims is, perhaps, anonymity's most compelling detractor. In addition to the above-noted commentators, the argument has popular resonance, as illustrated in a *Wall Street Journal* column critiquing the growth of anonymous communication on the Internet.[540] Such sentiment was expressed similarly by a more moderate writer, acknowledging that while anonymity has its merits, "[p]ermitting anonymity for the purpose of removing any vestige of accountability for abusive behavior...is not likely to be tolerated in the Networld."[541]

B. Digital Anonymous Speech

Any digital communication can theoretically be made anonymous. "Anonymizing" web proxies,[542] for example, permit users to browse the World Wide Web without revealing to observers the pages they have visited.[543] The most commonly-employed tools of digital anonymity at the present time, however, are anonymous remailers.[544] Because use of Freenet is

---

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

[536] *Id.* at 1109.

[537] *Id.* at 1111.

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

[539] *See* William Jackson, *More Personal Info Would Mean More Air Safety*, WASHINGTONPOST.COM, May 3, 2002, *at* http://www.newsbytes.com/news/02/176351.html, quoting Sun CEO, Scott McNealy.

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

[541] Branscomb, *supra* note 507, at 1675; *cf.* George P. Long, III, Comment, *Who Are You?: Identity and Anonymity in Cyberspace*, 55 U. PITT. L. REV. 1177, 1205 (1994) ("[I]f law enforcement authorities are precluded from obtaining the identities of anonymous users, illegal activities will proliferate.").

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

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

[544] A thorough analysis of the legality of running an anonymous remailer, as well as an extensive review of the technology and history involved, is presented by this author in *Don't Shoot the Messenger: Limiting the Liability*

still largely limited to developers and others with a high degree of technical sophistication, it is difficult to gauge to what uses the system would be put by the average citizen. As such, the following section relies predominantly on anonymous remailers as an example of the kinds of speech which digital anonymity allows.

1. Anonymous Remailer Technology

Anonymous remailers exclusively handle electronic mail, and with it, posts to mailing lists, bulletin boards, and Usenet groups.[545] And, though the workings of remailer technology are somewhat opaque, use of one of several user-friendly software programs[546] or a simple web page[547] permits anyone with access to the Internet, and the requisite inclination, to send secure, anonymous email.

Tangible anonymous messages require that an author go to great pains to avoid connecting himself with his publication. This is especially so in an era where modern forensic techniques can easily lift fingerprints off a document and DNA from the saliva on an envelope. Digital messages, in contrast, bear only the identifying marks added by the sender or by intermediate relay systems used in the course of that message's delivery.[548] Thus, without those marks, and absent internal clues in the message itself,[549] there is nothing inherent in the message that can reveal the sender's identity.

While the operation and security of anonymous remailers vary, they share one feature in common: they strip away the identifying information at the top of the message and forward it on with a new header attached.[550] Were this all that remailers did, however, little security would be gained, particularly against a powerful adversary. Just as a facially anonymous letter mailed at the post office may be laden with clues for a forensic detective, so too may the author of an insecurely "anonymized" digital message be subject to discovery.[551]

---

of Anonymous Remailer Operators, which is scheduled for publication in the Winter 2001 edition of the New Mexico Law Review (expected in print in late May, 2002).

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

[546] *See* http://www.skuz.net/potatoware.html.

[547] *See* http://www.gilc.org/speech/anonymous/remailer.html.

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

[549] *E.g.*, "Hi Jim, this is Fred."

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

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

By implementing cryptographic tools widely available on the Internet,[552] and by routing, or "chaining" messages through a series of remailers, users can ensure three things vital to preserving the true anonymity of their messages.[553] First, none of the remailer operators will be able to read the text of the message, because it has been encrypted in a fashion that requires the cooperation of each operator in turn before the message can be read.[554] Second, neither the intended recipient, nor any of the remailer operators in the chain (other than the first remailer operator to receive the message) can identify the sender of the message without the cooperation of every prior operator. Finally, as a result of the first two assurances, it is impossible for the recipient of the message to connect the message to its sender without the cooperation of every single anonymous remailer operator in the chain. As referenced above, "cooperation" would most likely involve each remailer keeping a log of all data that flowed through it, as well as the willingness of each operator to share this information with the recipient. Many remailer operators refuse to keep logs as a matter of principle and practice, indicating that there is a strong likelihood that the necessary information does not exist. Moreover, even if logs were maintained by each remailer operator, if remailers are located in assorted countries, compelling all of the operators to disclose such logs could present a potentially insurmountable barrier.[555]

As described in Section II.C.3.b, the anonymity offered by Freenet in many ways parallels that of the anonymous remailer. Most importantly, for the sake of analysis, however, is that both offer virtually impenetrable protections against discovery of the underlying author or transmission. The next section explains why modern citizens use anonymous remailers, and to what uses Freenet might be put.

---

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

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

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

Flood Control, *supra* note 531, at 423.

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

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

2. Why People Use Remailers[556]

Few people wish to be remembered for every word they utter. Nevertheless, some reluctant speakers are deserving of encouragement. Corporate whistle-blowers and associates at law firms may well fear losing their jobs; victims of all manners of abuse may suffer harm if their identities are discovered; and those criticizing political movements, religions, or cults may likewise fear retaliation.[557] Human rights workers and others speaking out against repressive governments or advocating revolution may have the most to fear, however, given the budgets and force available to those governments they oppose.[558] Even in seemingly free countries such as this one, it can be unsafe to criticize the government at certain times and places.[559] Perhaps ironically, remailers can also be used in the place of telephone "crime stopping hotlines."[560] As discussed below, people in each of these situations have successfully used anonymous remailers to conceal their identities while expressing themselves.[561] Indeed, anonymous remailers were initially created to encourage and allow individuals to communicate who, without the guarantee of privacy, would not otherwise participate in certain beneficial discussions.[562]

The traditional notion of a right to free speech may work well in the case of verbal expression, but it may cease to have its intended purpose in the face of retaliation that may occur

---

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

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

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

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

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

[561]

> Abused as a child, an adult decides to share his story with a support group. A young woman who has tested positive for HIV discusses her feelings with others affected by the AIDS virus. After observing illegal activities at his company, a man debates the implications of "blowing the whistle" on his employer. A dissident in China publishes some of his banned writings. For privacy reasons, all four individuals wish to remain anonymous. These scenarios would not be unique in today's society, except that they are occurring daily over an extensive computer network known as the Internet.
>
> George P. Long, III, *supra* note 541, at 1178.

[562] "The capability was designed to encourage open discussions among victims of child abuse or AIDS and originally was used only in such groups." William Bulkeley, *Censorship Fights Heat Up on Academic Networks*, WALL ST. J., May 24, 1993, at B1.

decades later.[563] As a method of communication, sending electronic mail can be as casual and timely as a telephone call; however, it can also be stored and accessed with exponentially greater ease than traditional letters or audio recordings of conversations. If the storage of that email is not protected, the message can be accessed by anyone with the time and ability to sift through the records of any of the systems that may have intercepted that message.[564] Posts made to mailing lists, message boards, or Usenet are particularly susceptible to this, and as data collection technology improves, it becomes increasingly likely that archives will be maintained and made searchable indefinitely.[565]

Many people live in communities that are violently intolerant of their social, political, or religious views. They may use remailers to network with those more understanding of their situation. As one poster to alt.privacy.anon-server wrote,

> I consider myself to be a fairly good example of why anonymous remailers are needed on the Net. To be blunt, I am bisexual, a pervert and a witch. I also live in Alabama, where at least two of the three are illegal. In a worst-case scenario, I could lose my job, have my career ruined, face prosecution and possibly even have to deal with violence.[566]

Anonymous communication can also allow for the creation of digital personae, which may be liberating to some.[567] This ability to create such personae may enhance the quality of speech and debate available on the Internet. A communication that discloses no information on the author's identity—including age, race, sex, and national origin—means that the author must be judged solely on the content of his message. This makes stereotyping and bigotry extremely difficult, potentially encouraging parties to discuss the merits of ideas, rather than the prejudiced views of the speaker.[568]

---

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

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

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

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

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

[568] For a glimpse at the potential ramifications of "blinded" speech in an "identity-conscious society and legal world," see Clark Freshman, *Were Patricia Williams and Ronald Dworkin Separated at Birth?*, 95 COLUM. L. REV. 1568, 1576-1577 (1995) (book review); Christopher A. Ford, *Administering Identity: The Determination of "Race" in Race-Conscious Law*, 82 CAL. L. REV. 1231 (1994).

Aside from psychological benefits that an anonymous poster may gain by finding a community outside his own, there may also be external benefits to a community as a whole. For example, public health is generally improved by wide dissemination of information concerning communicable diseases. Nevertheless, many people would be unwilling to inquire publicly about such information—particularly regarding socially stigmatizing diseases like alcoholism[569] or AIDS for fear of being identified as a potential sufferer.

It is not uncommon for prospective employers to perform searches on job applicants' email addresses to ascertain in which types of online participation they may have engaged.[570] Employers may even perform these sorts of searches on their current employees—to see if they are seeking other employment,[571] to see if they are expressing undesirable opinions about the company or its product, or to see if they are engaging in behavior that may be offensive to the employer.[572] Indeed, the ability to search Internet archives has resulted in a new kind of "absolute accountability"[573] allowing archive searchers to obtain lists of people who have used racist slurs in print, or who have a history of organizing for labor unions.

> Says [Ross] Stapleton, "It's increasingly easy for someone in an HR department to say—'Look, Joe here says that skydiving is cool. Do we want to carry him on the rolls considering that he might die? Jane here is in a lifestyle that the chairman might not find attractive. We might not want to put her forward for the public affairs spot.' I don't have any activities that I don't want to post about. If I did, I would be very cautious."[574]

---

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

[570]

> [P]ostings to the Internet's 33,000 news groups may fall off the edge of Usenet after a week or so, but they live on in databases such as Deja News and the Internet Archive....We can already see the outlines of this new world. When you apply for a job in the high-tech sector, there's a fair chance your prospective employer will use a search engine to scout out your online postings, from late-night musings to intemperate rants fired off to a political news group. Would an employer's decision be colored by information that has nothing to do with a candidate's job qualifications, such as your out-of-the-mainstream religious beliefs, sexual orientation, HIV status or personal habits? Absolutely, and without apology. After all, "character" counts, too.
>
> Joseph D. Lasica, *Your Past Is Your Future, Web-Wise*, THE WASH. POST, Oct. 11, 1998, at C01.

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

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

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

[574] *Id.* (quoting Ross Stapleton).

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

Computer engineers and others employed in research contexts may have more to fear than potential privacy intrusions by their employers. In light of legislation such as the Digital Millennium Copyright Act[575] and the potential for civil litigation under state trade secret laws,[576] many successful reverse engineering[577] attempts are disclosed anonymously via remailers. Thus, in at least some circumstances, remailers protect the legitimate disclosure of information against corporations who have made a habit of challenging all reverse engineering attempts of their products, hoping their competition will fold under the burden of litigation. Computer security information—exploits, bugs, and other similar forms of information—can also be disclosed this way.[578]

People also employ anonymous remailers to prevent "spammers" and other unwanted persons from harvesting their real email addresses.[579] It is important to remember the ramifications of posting one's identity in a public forum, even a seemingly innocuous one.[580] People frequently post very benign messages via remailers for this very reason.[581]

---

[575] Pub. L. No. 105-304 (1998).

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

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

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

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

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

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

[580] For a period of several months, for example, flight attendants posting to the Usenet group rec.travel.air had their personal and work email addresses copied down by an individual who subsequently posted defamatory

Finally, as Patrick Ball, Deputy Director of the American Association for the Advancement of Science's Science and Human Rights program has said, "Encrypted and anonymous communication is very important for human rights activists, and for anyone who needs to denounce violations of human rights committed by repressive regimes."[582] In early 1999, the anonymous remailer network allowed ethnic Albanians to provide first-hand accounts of Serbian atrocities in Kosovo[583] without fear of retribution.[584] Similarly, remailers have often been used by victims of rape, domestic violence, and other sensitive or life-threatening settings to solicit advice.[585]

As Julf Helsingius remarked, "[r]emailers have made it possible for people to discuss very sensitive matters, such as domestic violence, school bullying or human rights issues anonymously and confidentially on the Internet. The closing of [the] anon.penet.fi [remailer] will make it harder to discuss these matters."[586]

For all these lawful uses of remailer technology, there are also many reasons why criminals and perceived criminals may make use of remailers. For example, defamation can

---

remarks about them in other newsgroups. These posts were in the tradition of publishing a person's phone number on a bathroom wall with "For a good time, call" prepended. The lengthy series of posts may be obtained from http://groups.google.com by searching for "remailer" in "rec.travel.air."

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

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

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

[584] On March 26, 1999, Anonymizer.com launched the Kosovo Privacy Project to address the immediate concerns of Kosovars, Serbs, and others reporting on the situation in Kosovo. The project was conceived by Alex Fowler, public affairs director of the Electronic Frontier Foundation, after "seeing messages being posted on Web pages that are just as easy for me to read as they would be for Milosevic and his government agents." Press Release, Anonymizer.com, *supra* note 582.

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

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

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

effectively be made indelible by Internet dissemination. This is so because once it is introduced to the data stream, it may be reproduced and stored in any number of computers.[587]

Trade secrets are also vulnerable in light of anonymous electronic communication. On September 9, 1994, for example, an anonymous person mailed to the Cypherpunks mailing list a message containing what was purported to be the source code for RC4, a proprietary cryptographic algorithm owned by RSA Data Security, Inc.[588] More recently, on October 26, 1999, the source code for CSS authentication was also released via the anonymous remailer network.[589] Public posting, in most cases, tends to reduce the value of a trade secret, thus trade secret disclosure can be particularly damaging to the company that holds it.

Anonymous remailers have a notorious history of being used to disseminate copyrighted works, particularly via Usenet.[590] Many remailers have limits on message sizes that they will accept, thus very little dissemination of pirated music, movies, or software takes place via the remailer network. Nevertheless, textual works, including copies of Frank Herbert's "The Green Brain" and "The Eyes of Heisenberg" have been posted via anonymous remailer to Usenet where others may freely obtain copies of those copyrighted works.[591] Indeed, several of the Church of Scientology's secret doctrinal works are posted with such frequency to Usenet that the documents are effectively always accessible, even without resorting to archives.

Finally, anonymous remailers are frequently accused of being used to distribute criminal content, including child pornography and death threats. And, while the incidence of the former is extremely low, it is possible for criminals to employ remailers to this effect, and death threats are sent through remailers with some frequency. Thus, for all their positive uses, remailers can and will be used for potentially actionable purposes, which raises the question of the legal implications of remailer technology.

3. How Freenet Might Be Employed

Anonymous remailers offer only the ability to transmit limited amounts of text. With Freenet, however, everything from child pornography, to copies of the recent *Harry Potter* movie, to the entire California Bar/Bri review materials, could be traded with impunity and

---

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

[588] *At* http://cypherpunks.venona.com/date/1994/09/msg00304.html.

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

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

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

unaccountability. It is thus fairly easy to envision how Freenet could be used as a favored tool for criminals and copyright violators.

If one envisions "speech" as being mere words, it is difficult to conceive of how Freenet offers an improvement for legitimate anonymous speech over anonymous remailers. There are several reasons, however, why Freenet offers abilities for political and other discourse, previously unseen on the Internet. Two such benefits are listed below.

First, remailer technology generally permits one-to-one communication, by allowing users to send anonymous messages to individual e-mail addresses. It is possible to achieve one-to-many communication by using a remailer to post to a message board; however, such messages are ephemeral and can be removed by message board owners, either intentionally, or as an automatic space-saving function, expiring all messages after they have been made available for some period of time. Freenet allows one-to-one communication, however it also allows for a substantially more convenient and greater way of perpetuating content. History readily demonstrates why perpetuation of controversial media is of interest. One of the primary purposes of the First Amendment is to protect speech which needs protecting.[592] In many cases, ideas which are initially repugnant to the majority of Americans, are eventually tolerated, and in some cases, revered with the passage of time.[593] During the volatile period of incubation before acceptance, however, ideas can be susceptible to eradication. Freenet offers substantial assistance to allowing such ideas to survive their adolescence, however, by offering a technical means for perpetuating ideas.

Second, while remailers offer only text, Freenet offers users the ability to publish audio, video, and data files as well. Thus, where previously anonymous publishers could only distribute short literary works, now, works of visual art, music, audio delivery of speeches, and indeed, video, can potentially be delivered through Freenet. Of particular interest to this author, is the ability of minor party political candidates to publish political advertisements, and debates to the general public – the equivalent of a local public access cable channel, but with a world-wide audience. Similarly, the ability to anonymously disclose whistle-blowing videos to the public-at-large could have a profound effect on the accountability of government officials and others.

---

[592] "[A] function of free speech under our system of government is to invite dispute. It may indeed best serve its high purpose when it induces a condition of unrest, creates dissatisfaction with conditions as they are, or even stirs people to anger. Speech is often provocative and challenging. It may strike at prejudices and preconceptions and have profound unsettling effects as it presses for acceptance of an idea." *Terminiello v. Chicago*, 337 U.S. 1, 4-5 (1949).

[593] Some of the most illustrative examples involve the ever-changing popular consensus on what is obscene, and what is a valuable work of literature. For example, in 1930, Theodore Dreiser's AN AMERICAN TRAGEDY was declared obscene. *Commonwealth v. Friede*, 171 N.E. 472, 473 (Mass. 1930). On the same day, the Supreme Massachusetts Judicial Court held D.H. Lawrence's LADY CHATTERLY'S LOVER obscene. *Commonwealth v. Delacey*, 171 N.E. 455 (Mass. 1930). Such works are now regarded with high Constitutional estimation. *FW/PBS, Inc. v. City of Dallas*, 493 U.S. 215, 251 (1990) (Scalia, J., concurring in part and dissenting in part).

C. Possible Federal "Solutions" to Digital Anonymity

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

> Among those who communicate on the Internet are purveyors of hate and violence. Among the full text offerings on the Internet are detailed instruction books describing how to manufacture a bomb...Anyone with access to the Internet can obtain this recipe for disaster, even a 10-year-old child who can find a glass container and some gasoline...There are also electronic mail discussion groups where information on bomb making can be traded anonymously. One disgusting example is this anonymous message posted on an Internet electronic bulletin board shortly after the Oklahoma City bombing: "Are you interested in receiving information detailing the components and materials needed to construct a bomb identical to the one used in Oklahoma[?]" The information specifically details the construction, deployment, and detonation of high-powered explosives....The individual who posted this message, who cowers in anonymity, deserves condemnation for using the Internet to suggest how the Oklahoma City bombing "could have been better." This is just one of many other examples....Among the issues before us are the extent of such usage of the Internet and whether anything can or should be done to curb it."[594]

The Supreme Court has not yet had the opportunity to consider a narrowly tailored statute restricting Internet anonymity.[595] Nevertheless, as Senator Specter's remarks illustrate, the Court may be presented with an anonymity-based question in the near future.[596] The Court's ruling on such a question may potentially be divined from the Court's opinion in *Reno v. ACLU*,[597] striking down portions of the Communications Decency Act (CDA).

---

[594] *Hearings on "Mayhem Manuals and the Internet" before the Subcommittee on Terrorism, Technology and Government Information of the Senate Judiciary Committee*, 1995 WL 311682 (FDCH) (May 11, 1995) (statement of Senator Arlen Specter).

[595] *See* Donald J. Karl, *State Regulation of Anonymous Internet Use after ACLU of Georgia v. Miller*, 30 ARIZ. ST. L.J. 513, 533 (1998).

[596] A Supreme Court challenge appears especially likely in the wake of the events of September 11, 2001, and Congress's passage of so-called anti-terrorism legislation. *See* Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA PATRIOT Act) of 2001, Pub. L. No. 107-56, 115 Stat. 272. In relevant part, the USA PATRIOT Act gives the Government broader access to information about Internet users. Specifically, subpoenas served on ISPs may now require them to provide, in addition to the basic service information, the means and source of a user's payment for services, including credit card and bank account information. *See* Michael E. Arruda, *Emerging Online Developments,* PRACTICING LAW INSTITUTE PLI Ord. No. G0-00VJ, 11, 16 (2002). Previous law allowed access to basic user information by subpoena, but requires a court order for payment information. *Id.* The change was implemented to limit so-called anonymous Internet registrations. *Id.* The USA PATRIOT Act also gives more leeway to Internet service providers when voluntarily disclosing subscribers' electronic communications to Government entities. *Id.* The USA PATRIOT Act does not directly affect the legality of running or using an anonymous remailer. Moreover, as discussed through out the text of this Comment, any such litigation would be futile at preventing determined terrorists from communicating in perfect secrecy and anonymity. *See, e.g., supra* note 8 and accompanying text. Nonetheless, the USA PATRIOT Act demonstrates an increasing hostility on the part of governments toward anonymous electronic communications. For a brief analysis of e-mail's involvement in the Daniel Pearl situation, see Tom Spring, *Will Anonymous E-Mail Become a Casualty of War?*, PCWORLD.COM, Feb. 11, 2002, at http://www.pcworld.com/news/article/0,aid,83564,tk,dn021102X,00.asp.

[597] 521 U.S. 844 (1997).

In *Reno*, the Court noted that the Internet constitutes "a unique and wholly new medium of worldwide human communication...located in no particular geographical location but available to anyone, anywhere in the world."[598] It further noted that the Internet "can hardly be considered a 'scarce' expressive commodity" because it provides "relatively unlimited, low-cost capacity for communication of all kinds."[599] This was relevant because "scarce" commodities, such as radio and television frequencies, have limited bandwidth[600] and are subject to strict government regulation. The proponents of the CDA claimed that the law would protect children while promoting cyberspace expansion.[601] The Court disagreed. It found that the CDA "lack[ed] the precision that the First Amendment requires when a statute regulates the content of speech," and therefore acted as a hindrance on the desired expansion of Internet communication.[602] The Court noted that "[a]s a matter of constitutional tradition, in the absence of evidence to the contrary, we presume that governmental regulation of the content of speech is more likely to interfere with the free exchange of ideas than to encourage it."[603]

The *Reno* Court's treatment of the Internet was almost reverential in parts, referring to the medium as a "dynamic, multifaceted category of communication includ[ing] not only traditional print and news services, but also audio, video, and still images, as well as interactive, real-time dialogue."[604] The Court emphasized the Internet's unprecedented power at allowing citizens an expressive outlet. "[T]hrough the use of chat rooms, any person with a phone line can become a town crier with a voice that resonates farther than it could from any soapbox. Through the use of Web pages, mail exploders, and newsgroups, the same individual can become a pamphleteer."[605] As noted by the *Reno* District Court, and repeated by the Supreme Court, "the content on the Internet is as diverse as human thought."[606] One could reason that *Reno* stands for the Court's strong affirmation that Free Speech is alive, well, and protected in cyberspace. It is worth nothing that Freenet effectively provides all of the features and virtues of the Internet as stated above, with the added enhancements of two likely ancient liberties: cryptography and anonymity. Based on the Court's past treatment of anonymity, especially its fondness for anonymity in protecting political discourse,[607] it appears likely that a ban on Internet anonymity of the sort required to prohibit use of Freenet, will fail if confronted by the Supreme Court. This is probable because such a law could not be sufficiently narrowly tailored, focused on specific problem areas, or non-detrimental to the expansion of the medium. Short of such a ruling, however, such an assertion remains conjecture and an analysis of regulatory proposals is necessary.

---

[598] *Id.* at 850-51.
[599] *Id.* at 870.
[600] *Cf.* NICHOLAS NEGROPONTE, BEING DIGITAL 4, 23-24 (Knopf 1995).
[601] *Reno*, 521 U.S. at 885.
[602] *Id.* at 874.
[603] *Id.* at 885.
[604] *Id. at 870.*
[605] *Id.*
[606] *Id.*
[607] *See supra* Section II.A.1.

1. Regulatory Control

The harms attendant on anonymous speech are often more easily recognized and more impressive[608] than the often subtle benefits that it may produce. In *McIntyre*, Justice Ginsburg left open the possibility that the Ohio disclosure requirement might be constitutionally permissible in a different context:

> The Court's decision finds unnecessary, overintrusive, and inconsistent with American ideals the State's imposition of a fine on an individual leafleteer who, within her local community, spoke her mind, but sometimes not her name. We do not thereby hold that the State may not in other, larger circumstances require the speaker to disclose its interest by disclosing its identity.[609]

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

As a general matter, information about the identity of the author of an email message does not appear to be protected under U.S. law. While the Electronic Communications Privacy Act[610] prohibits (with certain exceptions) the disclosure of "the contents of any...electronic communication,"[611] the statute does not similarly protect the name of the originator of the message. Accordingly, it does not appear that participants of the Freenet network have a statutory duty to disclose, or to refrain from disclosing, such information.

Some propose that the most effective way of controlling anonymous messaging is to require operators to keep records of sender identities.[612] Such a system might include an "incentive" whereby the operator would be guaranteed "protection from civil and criminal liability when the administrator (1) has acted in good faith, and (2) voluntarily discloses to the authorities the identity of a user engaging in illegal activities."[613] This sort of proposal will not work for a number of reasons.

First, a necessary byproduct of such a proposal is the criminalization of running a Freenet node without maintaining logs. Such proposals neglect to address the strong cryptography underlying the Freenet network. As implemented, law enforcement may be presented copies of

---

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

[609] *McIntyre*, 514 U.S. at 358 (Ginsburg, J., concurring).

[610] 18 U.S.C. §§ 2510-2521(1994).

[611] 18 U.S.C. §§ 2511(c) and 2511(e)(i).

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

[613] *Id.* at 1563.

all data passing through a network and still be unable to recover the identity of users.[614] Short of mandated key escrow, or an outright ban on strong cryptography,[615] any logging system will fail. There are numerous technical implications of requiring a system administrator to maintain logs.[616] Moreover, there is little legal basis for supporting such a log-maintaining requirement.[617]

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

Finally, the classic adage, "when guns are outlawed, only outlaws will have guns," is apropos. The first Cypherpunk remailer was written in a weekend by a single individual.[618] Napster was created by a student with no previous experience writing software applications. Criminals who wish to communicate anonymously will find ways to do so regardless of legislation. Thus, claims that banning public anonymity tools such as Freenet will prevent criminals from cloaking themselves in anonymity are absurd.

---

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

[615] "The FBI is constantly lobbying for so-called key-recovery features that could give them access to a person's private key to unlock their encrypted data. Law enforcement and powerful intellectual property owners—such as the record and music industries—don't want Net users to be completely anonymous because obviously, that makes them harder to bust if they are suspected of trafficking pirated material or committing other Net-based crimes." Courtney Macavinta, *New Product Guarantees Online Anonymity*, CNET News.com (December 13, 2000), http://www.cnet.com. For a thorough treatment of the legal issues of key recovery, see Phillip R. Reitinger, *Compelled Production of Plaintext and Keys*, 1996 U. CHI. LEGAL F. 171 (1996).

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

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

[618] As explained by one of the founders of "Cypherpunks," a collection of cryptography enthusiasts,

> The Cypherpunk—and Julf/Kleinpaste—style remailers were both written very quickly, in just days—Eric Hughes wrote the first Cypherpunks remailer in a weekend, and he spent the first day of that weekend learning enough Perl to do the job. Karl Kleinpaste wrote the code that eventually turned into Julf's remailer (added to since, of course) in a similarly short time:—"My original anon server, for godiva.nectar.cs.cmu.edu 2 years ago, was written in a few hours one bored afternoon. It wasn't as featureful as it ended up being, but it was 'complete' for its initial goals, and bug-free." [Karl_Kleinpaste@cs.cmu.edu, alt.privacy.anon-server, 1994-09-01]. Tim May, *Cyphernomicon 2.4*, *at* http://www2.pro-ns.net/~crypto/cyphernomicon.html.

2. Outright Bans

Some view outright statutory prohibition as the only possible solution.[619] After concluding that a strict liability regulation regime would be inappropriate for a number of reasons, Professor Hardy reluctantly argues that an absolute prohibition is "the only effective deterrent."[620] Given the global diversity of anonymity nodes, Hardy also acknowledges the need for some form of international cooperation to make a prohibition effective.[621]

Such proposals are troublesome for a number of reasons. First, not all Freenet use would be criminal. As discussed above numerous times, anonymity can provide critical social benefits. Second, a prohibition of anonymity drafted so broadly as a complete ban on the use of Freenet would surely be constitutionally defective. The Supreme Court reaffirmed that anonymity is protected under the First Amendment in *McIntyre*.[622] The case only addressed political speech,[623] though, and did not hold that all prohibitions of anonymous political speech would be constitutionally invalid.[624] Therefore, the ruling in *McIntyre* would not necessarily preclude a prohibition of Freenet.[625]

3. Constructive Knowledge Proposals

Noah Levine suggests, in the context of regulating anonymous remailers, that "[a] better approach is to subject the remailer administrator to liability for the illegal acts of...users when the administrator has constructive knowledge of the underlying illegal uses."[626] He defines constructive knowledge in this context as "reason to believe that a specific individual is using the remailer for an illegal purpose."[627] He suggests that in circumstances where operators are "notified by another party (*e.g.*, a victim) of past improper use by one of the remailer's users...[those] remailer administrators should either monitor future messages sent by the same user, or deny that individual the use of the remailer altogether."[628] Applying the sentiment to Freenet, such a suggestion ignores the underlying technological barriers to implementing such a scheme. Freenet makes no distinction between users and operators. They are one in the same, and all are incapable of monitoring messages due to strong cryptography built into the system. A person unable to identify either the source or content of data following through their computer is hardly capable of denying access to specific users or content.

---

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

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

[621] *See id.*

[622] *McIntyre*, 514 U.S. at 357.

[623] *See id.* at 346.

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

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

[626] Levine *supra* note 612, at 1559.

[627] *Id.*

[628] *Id.*

VI. CONCLUSION

Current P2P technology gives millions of users the ability to distribute copies of their favorite books, movies, and songs amongst themselves with impunity. There are two fundamental problems in altering this status quo. First, technological means of copyright enforcement are nearly always circumvented in one way or another, and perhaps more importantly, if such circumventions were not possible, important fair uses of copyrighted material could not take place. Second, the only truly effective legal measures which could be adopted would require a direct upset of fundamental First Amendment rights.

The United States Constitution gives Congress the power "[t]o promote the Progress of Science and useful Arts, by securing for limited Times to Authors and Inventors the exclusive Right to their respective Writings and Discoveries."[629] The Constitution also demands that "Congress shall make no law ... abridging the freedom of speech."[630] A significant problem arises when these two statements are pitted against one another.

Noteworthy legal scholars throughout the history of America have wrestled with this difficult problem.[631] As Melville Nimmer has asked, "Does copyright abridge the First Amendment guarantees of free speech and press?"[632] How can a constitution which protects freedom of speech simultaneously grant Congress the ability to enforce monopolies over speech?[633] As a result of the recent attention to P2P technology, and the general public's increasing ability to infringe digital copyrights, the courts may well be called upon to resolve such questions in the near future. Given the longstanding benefits which encryption and anonymity offer a free society, it is this author's hope that the courts will think very carefully before sacrificing such useful tools of free speech on the alter of copyright enforcement.

---

[629] U.S. CONST. art. I, § 8, cl 8.
[630] U.S. CONST. amend. I.
[631] *See* Lawrence Lessig, *Copyright's First Amendment*, 48 UCLA L. REV. 1057 (2001).
[632] *Id.* at 1058.
[633] *See* Paul Goldstein, *Copyright and the First Amendment*, 70 COLUM. L. REV. 983 (1970).