Fordham Law Review

Volume 72 | Issue 3 Article 5

2003

The Spector of Crypto-anarchy: Regulating Anonymity-Protecting Peer-To-Peer Networks

John Alan Farmer

NOTE

THE SPECTER OF CRYPTO-ANARCHY: REGULATING ANONYMITY-PROTECTING PEER-TO-PEER NETWORKS

*John Alan Farmer**

Freenet is a near-perfect anarchy.

—Ian Clarke[1]

PROLOGUE

In 2000, China's Ministry of Public Security announced the inauguration of a project entitled Golden Shield.[2] This massive electronic monitoring network incorporating voice and face recognition, closed-circuit television, transactional records, and Internet surveillance, among other technologies, is designed to improve the efficiency of law enforcement.[3] One author reported that the government envisioned the Golden Shield as a "database-driven remote surveillance system" that would enable it to gain immediate access to records on all Chinese citizens and to monitor their activities through networks of cameras.[4]

Two years later, the peer-to-peer network Freenet China launched.[5] Users who install the Freenet software on their computers may author, publish, store, and read files anonymously.[6] Because the network is decentralized—not controlled by a central authority—it

*J.D. Candidate, 2004, Fordham University School of Law. I am deeply grateful to Sonia K. Katyal for her encouragement, generosity, and many insights.

1. John Markoff, *Cyberspace Programmers Confront Copyright Laws*, N.Y. Times, May 10, 2000, at A1.

2. Warren Allmand, International Centre for Human Rights and Democratic Development, Executive Summary to Greg Walton, China's Golden Shield: Corporations and the Development of Surveillance Technology in the People's Republic of China (2001), *at* http://www.ichrdd.ca/frame2.iphtml?langue=0.

3. *See id.*

4. *Id.*

5. Jennifer 8. Lee, *Guerrilla Warfare, Waged With Code*, N.Y. Times, Oct. 10, 2002, at G1 (discussing computer programmers who use technology to promote activist causes).

6. *See infra* Part I.C.2.iii.

can be shut down only by disabling each individual user's computer.[7] And because there are thousands of users, each of whom is anonymous and untraceable, this outcome is unlikely.[8] The Falun Gong, a spiritual group banned by the Chinese government, began to use the network to publish, store, and read prohibited texts anonymously and thus without fear of persecution.[9]

If one views the Falun Gong as a subversive organization, Freenet's ability to protect anonymous communication is a harm. By contrast, if one views it as a minority sect persecuted by a government intent on silencing nonsanctioned voices, this ability is a benefit. Yet, the network itself cannot distinguish "harmful" from "beneficial" expression, thus posing this central question: How does one find a way to mitigate the harms while simultaneously protecting the benefits that may result from providing anonymity on anonymity-protecting peer-to-peer networks? The answer to this question is not just of concern to persons living in totalitarian nations such as China. In 2002, the U.S. Department of Defense disclosed that it was developing Total Information Awareness, since renamed Terrorism Information Awareness, a new weapon in its arsenal against terrorism with striking similarities to the Golden Shield.[10]

INTRODUCTION

"A specter is haunting the modern world, the specter of crypto anarchy," warned Tim May, one of the first cypherpunks, in his "Crypto Anarchist Manifesto" of 1988.[11] His language wryly echoes

---

7. *See infra* Part I.C.2.iii.

8. *See infra* Part I.C.2.iii.

9. *See* Michael S. Chase & James C. Mulvenon, *You've Got Dissent! Chinese Dissident Use of the Internet and Beijing's Counter-Strategies* 41–42 (2002), *available at* http://www.rand.org/publications/MR/MR1543/MR1543.ch1.pdf. The authors note that pro-democracy activists, Falun Gong practitioners, and other dissidents in China may increasingly turn to anonymity-protecting peer-to-peer networks to exchange information. *Id.* Although discussions with dissidents suggest that to date they have used such networks to download documents such as the *Tiananmen Papers*, there is less evidence to support the contention that the use of this technology to exchange politically sensitive materials is widespread. *Id.* Indeed, as in the United States, most users in China are probably more interested in using p2p networks to share music files. *Id.*

10. *See infra* Part I.B.2.ii.

11. Tim May, *The Crypto Anarchist Manifesto* (1988), *at* http://www.tamerlane.ca/library/cp/tcm/cam.htm. A collection of May's writings is available at http://www.tamerlane.ca/library/cp/tcm/. The cypherpunks are a loosely organized group of techno-activists. The term "cypherpunk" probably first appeared in Eric Hughes's "A Cypherpunk's Manifesto" (1993). *See* http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci769961,00.html (last visited Oct. 14, 2003) (search for term "cypherpunk" on searchWebServices.com). It combines two concepts: (1) "cyberpunk": the belief that individuals who possess the requisite motivation and technological expertise (sometimes known as "hackers") can resist the efforts of powerful governments and businesses to use technology to control society; and (2) the use of strong encryption to preserve privacy ("ciphertext" is

the opening of the Communist Manifesto.[12] But the specter of which he spoke is computer technology with the capacity to enable totally anonymous communication—technology that prevents users from ever knowing the legal identity of the other users with whom they communicate. May predicted this development will "alter completely the nature of government regulation, the ability to tax and control economic interactions, the ability to keep information secret, and will even alter the nature of trust and reputation."[13] His prediction has proved to be prescient in many respects.

Encryption technologies, anonymous remailers, and most recently what this Note calls "anonymity-protecting peer-to-peer" ("p2p") networks like Free Haven, Publius, and Freenet have made more routine the anonymous communication about which May cautioned.[14] In recent years, a convergence of factors has made such networks the locus of growing moral and legal attention. These factors include: increased concern about national security in the wake of the September 11, 2001 terrorist attacks, the consequent threat to civil liberties posed by the government's attempts to extend its online surveillance powers,[15] the migration of online music and video piracy to non–anonymity-protecting p2p networks like Kazaa and Gnutella in the wake of the *Napster* decision,[16] and the consequent threat to individual privacy as the copyright enforcement strategies of organizations such as the Recording Industry Association of America

---

encrypted text). *Id.* Cypherpunks believe strong encryption is a tool that may be used to protect individual privacy. They argue that the benefits of using strong encryption—the protection of privacy in a world in which surveillance is becoming more pervasive—outweigh its costs—its potential use by criminals and terrorists. *Id.*

12. The Communist Manifesto (1848) begins: "A spectre is haunting Europe—the spectre of communism. All the powers of old Europe have entered into a holy alliance to exorcise this spectre: Pope and Tsar, Metternich and Guizot, French Radicals and German police-spies." Karl Marx, *Manifesto of the Communist Party*, *in* The Portable Karl Marx 203 (Eugene Kamenka ed., 1983). In addition to the parallels May draws between the "specters" of communism and crypto-anarchy, note also the opposition both authors draw between the old order and the new—a tendency that pervades the rhetoric of techno-activists. *See, e.g.*, John Perry Barlow, *A Declaration of the Independence of Cyberspace*, Electronic Frontier Foundation (1996), *at* http://www.eff.org/Publications/John_Perry_Barlow/barlow_0296.declaration.

13. May, *supra* note 11.

14. *See infra* Part I.C.2.

15. *See infra* Part I.B.2

16. *See* A & M Records, Inc. v. Napster Inc., 114 F. Supp. 2d 896 (N.D. Ca. 2000), *aff'd*, 239 F.3d 1004 (9th Cir. 2001) (holding that plaintiff record companies and music publishers that brought a copyright infringement action against a filesharing service established a prima facie case of direct copyright infringement; the users' activities did not amount to fair use of the copyrighted works; and plaintiffs demonstrated a likelihood of success on the merits of their contributory infringement and vicarious infringement claims). The literature on *Napster* is voluminous. For a concise overview of the issues, see Grace J. Bergen, *The* Napster *Case: The Whole World Is Listening*, 15 Transnat'l Law. 259 (2002) (discussing *Napster* and its impact on the music industry).

("RIAA") and the Motion Picture Association of America ("MPAA") become more aggressive.[17]

This Note argues that the provision of anonymous communication on anonymity-protecting p2p networks is entitled to the protection of the First Amendment and, moreover, that the benefits of providing anonymous communication via this technology outweigh the costs. Part I explores the potential of these networks to play an increasingly important role in the preservation of freedom of expression on the Internet as online surveillance by both businesses and government expands. Part II examines the difficulty of developing a regime for regulating expression on these networks that protects the benefits of providing anonymous communication via this technology while simultaneously mitigating the harms. Finally, Part III concludes that regulation of these networks by code—the implementation and enforcement of rules of behavior through the instructions embedded in the software and hardware that define a network's architecture—may be more desirable and effective than regulation by law, even though it is not without cost.

I. THE SOCIETY OF SURVEILLANCE

This part discusses the threat to freedom of expression posed by the expansion of the "society of surveillance."[18] It examines this development through the lens of Oscar H. Gandy, Jr.'s analytic framework of the "panoptic sort," which describes the systematic implementation of surveillance technology by businesses and government to monitor ordinary persons and to use the information gathered to sort these subjects according to their presumed economic or political benefit or cost.[19] It focuses specifically on recent surveillance measures and initiatives that extend or would extend the Internet as a crucial technology of surveillance.[20] These initiatives and measures may restrict online freedom of expression, insofar as the knowledge that one may be watched may lead to increased self-censorship as users refrain from modes of expression that are not illegal, but merely questionable, controversial, or unpopular. This part concludes by examining how anonymity-protecting p2p networks such as Free Haven, Publius, and Freenet have attempted to resist this type of self-censorship, as well as traditional censorship, by operating

17. *See* Sonia K. Katyal, *Privacy v. Piracy: The New Surveillance*, 54 Case W. Res. L. Rev. (forthcoming 2004).

18. For a discussion on the "society of surveillance," see, e.g., David Lyon, The Electronic Eye: The Rise of Surveillance Society (1994).

19. *See* Oscar H. Gandy, Jr., The Panoptic Sort: A Political Economy of Personal Information 1–2 (1993); *see also infra* Part I.A.

20. *See infra* Part I.B.

beyond the gaze of unauthorized surveillance in an effort to restore a vision of the Internet as a technology of individual autonomy.[21]

A. *The Panoptic Sort*

In the late eighteenth century, Jeremy Bentham invented the term "panopticon" to describe his model prison.[22] This prison consisted of a ring of transparently fronted cells radiating around a central observation tower.[23] From this tower, guards could perfectly observe the activities of each prisoner.[24] Yet, because the tower's windows were shielded by blinds and because certain architectural features prevented light from radiating from the tower's observation rooms, the prisoners could never see the guards who were watching them.[25] According to Michel Foucault, in the panopticon, power is exercised by means of two properties.[26] First, it is visible: the inmate constantly has before his eyes the sight of the central observation tower from which he is watched.[27] Second, it is unverifiable: the inmate knows he is always subject to surveillance, but he never knows whether he is being watched at any particular moment.[28] Because the inmate knows he is always subject to surveillance, he must submit to the authority of the guards at all times to avoid being punished for what may be perceived as misconduct; yet, because the guards are invisible to the inmate, continuous surveillance is unnecessary.[29] In this respect, the panopticon induces in the subject "a state of conscious and permanent visibility" that ensures that the system of power it embodies functions automatically and that its effects are permanent, even if its operation is discontinuous.[30]

Building on the link Foucault made between visibility and power, Oscar H. Gandy, Jr., who has written extensively on the political economy of communication and information, has developed the concept of the "panoptic sort" to describe a fundamental feature of contemporary U.S. society.[31] The panoptic sort refers to the use of

---

21. *See infra* Part I.C.

22. *See* Jeremy Bentham, The Panopticon Writings 29 (Miran Bozovic ed., 1995). Bentham's panopticon writings consist of a series of letters he wrote in 1787 and two postscripts he wrote in 1790 and 1791. These documents were published as *Panopticon, or, The Inspection-House, &C* (1791). *Id.* at 1, 29. The Bozovic edition includes the complete text of *Panopticon*. *Id.* at 29.

23. *Id.* at 35–36.

24. *See id.* at 43–44.

25. *Id.* at 35–36.

26. Michel Foucault, Discipline and Punish: The Birth of the Prison 201 (Alan Sheridan trans., 1979).

27. *Id.*

28. *Id.*

29. *Id.*

30. *Id.*

31. *See* Gandy, *supra* note 19. Gandy is the Herbert Schiller Professor of Communication at the Annenberg School for Communication, University of

technology by businesses and government to subject ordinary people to invisible surveillance; to collect, process, and share data generated through their daily activities as consumers and citizens; and then to sort them according to their presumed social, political, or economic value or threat.[32] While businesses use the technology of the panoptic sort to generate consumer profiles that enable them to market their products more efficiently, law enforcement officials use it to identify potential security threats.[33]

But in spite of the panoptic sort's potential social benefits, its use incurs a cost: restricting individual autonomy by unnecessarily constraining individual decision-making.[34] The panoptic sort greatly expands the range of communications that businesses and government can subject to surveillance and to the generation of the records used to identify, classify, assess, and make decisions about a person's options.[35] As a result, the knowledge that one is being watched can produce changes in individual behavior with both positive and negative social and psychological effects.[36] On the positive side, surveillance may deter people from illegal acts they might otherwise be tempted to commit if they know that they are not being watched.[37] In this respect, it helps ensure that people are held accountable for their actions and communications. On the negative side, surveillance may constrain people from engaging in expressive conduct that is not illegal, but merely controversial, unpopular, or questionable.[38] Like the inmate in Foucault's account of Bentham's panopticon, a person who knows she is subject to continuous surveillance by unseen actors might internalize these constraints by censoring her expressive conduct to avoid the mere possibility of discipline and punishment.[39]

Pennsylvania. His many other publications include *Exploring Identity and Identification in Cyberspace*, 14 Notre Dame J.L. Ethics & Pub. Pol'y 1085 (2000) (examining the relationship between identity and identification in cyberspace transactions); *Legitimate Business Interest: No End in Sight? An Inquiry Into the Status of Privacy in Cyberspace*, 1996 U. Chi. Legal F. 77 (arguing that businesses have an interest in being informed about individuals because of the information's strategic importance; that they have the resources to collect, process, and share this information with increasing efficiency; that there is a growing disparity between what individuals know about these businesses and what businesses know about them; and that this disparity has consequences for the political economy).

32. Gandy, *supra* note 19, at 1, 2, 15. Several recent articles have documented the acceleration of this trend. *See, e.g.*, Noah Shachtman, *Bush's Year of U.S. Surveillance*, wired.com (Jan. 2, 2003) (summarizing surveillance initiatives implemented in 2002), *at* http://www.wired.com/news/privacy/0,1848,57005,00.html; Lauren Weinstein, *Year in Privacy: Citizens Lose*, wired.com (Dec. 30, 2002) (discussing threats to privacy emerging in 2002), *at* http://www.wired.com/news/privacy/0,1848,56954,00.html.

33. *See* Gandy, *supra* note 19, at 55–70.

34. *Id.* at 180.

35. *Id.*

36. *Id.*

37. *Id.*

38. *Id.*

39. *Id.*

In addition to restricting individual autonomy by encouraging self-censorship, the panoptic sort risks reducing personhood to a mere "profile" in a manner that undermines the integrity of the public sphere.[40] Businesses and government use the information collected through surveillance to develop profiles of their subjects and sort them into categories.[41] For example, an airline may monitor the flight records of a passenger to determine whether he is likely to be a terrorist.[42] Or an online bookstore may monitor the purchases of a customer to determine whether she is likely to purchase certain products it sells.[43] In this respect, the process of sorting is a technology by which the monitoring entity may exercise control over the autonomy of the subjects of its surveillance.[44] But, as Gandy notes, "[t]o the extent that the panoptic sort, as an extension of technical rationalization into the social realm of consumer and political behavior, depends on a reduction of the skills of individuals . . . , the market and the political or public sphere . . . are transformed and are placed at risk."[45] The panoptic sort is the antithesis of a model of communication that aims to maximize the individual's freedom to negotiate her options through the exercise of her autonomy in complex social interactions. It limits individual autonomy by increasing the range of communications subject to a classificatory system that determines a person's social, political, and economic options based on a profile generated from records of actions that themselves reflect the constraints imposed by surveillance.[46]

B. *The Panoptic Sort in the Internet Context*

Foucault describes the panopticon as "a machine for dissociating the see/being seen dyad: in the peripheric ring, one is totally seen, without ever seeing; in the central tower, one sees everything without

---

40. *Id.*

41. *Id.*

42. Recently, without passengers' consent or knowledge, the airline JetBlue gave about five million passenger records to a Defense Department contractor conducting a government terrorist-screening study whose methods closely resembled those of the controversial Terrorism Information Awareness project. A group of passengers subsequently filed a class action lawsuit against the carrier. *See Fliers File Suit Against JetBlue*, wired.com (Sept. 23, 2003), *at* http://www.wired.com/news/privacy/0,1848,60551,00.html; Noah Shachtman, *JetBlue Customers Feel the Pain*, wired.com (Sept. 27, 2003), *at* http://www.wired.com/news/privacy/0,1848,60599,00.html; Ryan Singel & Noah Shachtman, *Army Admits Using JetBlue Data*, wired.com (Sept. 23, 2003), *at* http://www.wired.com/news/privacy/0,1848,60540,00.html.

43. Amazon's personalized recommendations system recommends books to consumers based on their previous purchases on the site. *See* Amazon.com, *at* http://www.amazon.com (last visited Oct. 15, 2003).

44. Gandy, *supra* note 19, at 179–81.

45. *Id.* at 3.

46. *Id.* at 180.

ever being seen."[47] This definition might describe the Internet as well: end users on the peripheries of the networks that the Internet comprises are totally seen, without ever seeing the entities monitoring their communications; and monitoring entities have the potential to see everything without ever being seen.[48] Although many Internet users have grown so accustomed to browsing the Internet "anonymously" that they assume such activity is an inherent right,[49] anonymity is no longer the Internet's default condition. Indeed, both businesses and government have invisibly subjected Internet users to increasing surveillance in recent years.[50] Since 1999, businesses have increased their surveillance of Internet users through the use of "spyware," and government has increased its surveillance through measures such as the USA PATRIOT Act ("USAPA"), proposed measures such as the Domestic Security Enhancement Act ("DSEA"), initiatives such as Carnivore, and proposed initiatives such as Terrorism Information Awareness ("TIA").[51] Anonymity-protecting p2p networks such as Free Haven, Publius, and Freenet are like "safe houses" on the Internet.[52] Users of these networks may protect their anonymity as long as they remain within the networks' confines. But as soon as they walk out of the door to browse the World Wide Web, send or receive emails, share files, or engage in other activities in which they cannot engage within the networks themselves, they expose their legal identities. Thus, although these networks attempt to resist the society of surveillance, they must do so by withdrawing from it. In this respect, the resistance they offer is powerful, but limited.

1. Businesses

In the manner Gandy describes, businesses have attempted to perfect their marketing strategies by dramatically increasing surveillance of Internet users' activities and developing user profiles from the information they collect.[53] For several years they have used "cookies"; when a user visits a website that incorporates this

47. Foucault, *supra* note 26, at 201–02.

48. For an analysis of the Internet as a panoptic technology, see Shawn C. Helms, *Translating Privacy Values With Technology*, 7 B.U. J. Sci. & Tech. L. 288, 291–93 (2001) (exploring anonymity, its social value, and how best to protect this value on the Internet).

49. Jessica Litman, Digital Copyright 11 (2001).

50. Ian Clarke et al., *Protecting Free Expression Online With Freenet*, IEEE Internet Computing 40 (Jan.–Feb. 2002), *available at* http://freenet.sourceforge.net/papers/freenet-ieee.pdf; *see also* Elbert Lin, *Prioritizing Privacy: A Constitutional Response to the Internet*, 17 Berkeley Tech. L.J. 1085, 1099–1107 (2002) (describing threats to informational privacy posed by computer databases).

51. *See infra* Part I.B.2.

52. *See infra* Part I.C.2.

53. Gandy, *supra* note 19, at 95–122.

technology, the site automatically places a small text file, known as a cookie, on the user's computer hard drive that collects personal information about the user.[54] More recently, some businesses have begun to use spyware, also known as "adware."[55] Whenever users view certain unsolicited emails or visit certain websites, these programs automatically install themselves on the users' computers, often without the users' knowledge.[56] Some spyware programs simply transmit carefully targeted advertisements to users, others collect information about the users' online activities and report it to marketing companies, and still others may even change users' browser settings.[57]

With one exception, discussed below, in practical terms anonymity-protecting p2p networks cannot adequately protect Internet users from spyware. To engage in certain types of online commercial activities, users must leave the networks' confines, visit the sites from which they desire to obtain products or services, and possibly expose their computers to spyware programs. Among the businesses that use spyware are certain non–anonymity-protecting filesharing services; Kazaa, for example, bundles spyware with its own free software as a

54. *See, e.g.*, Luke J. Albrecht, Note, *Online Marketing: The Use of Cookies and Remedies for Internet Users*, 36 Suffolk U. L. Rev. 421 (2003) (examining the legality of online marketers' use of cookies by surveying court decisions focusing on the application of federal statutes consumers have used to assert claims against such marketers). The only information available in a cookie is that which the user herself gives to the website and that which the site in turn saves on the cookie. *Id.* at 422. Businesses justify the use of cookies on the ground that they permit users to complete online transactions more efficiently. *Id.*

55. *See* John Borland, *Spike in "Spyware" Accelerates Arms Race*, CNET news.com (Feb. 24, 2003) (describing the expansion of spyware and efforts to combat it), *at* http://news.com.com/2102-1023-985524.html; *see also* James R. Hagerty & Dennis K. Berman, *Caught in the Net: New Battleground Over Web Privacy: Ads That Snoop*, Wall St. J., Aug. 27, 2003, at A1. In 2001, Senator John Edwards introduced the Spyware Control and Privacy Protection Act of 2001, S. 197, 107th Cong. (2001) (requiring that software made available to the public include clear notice if it incorporates spyware). There has been no legislative action on this bill since it was introduced. For analysis of the legal implications of spyware, see Paige Norian, Comment, *The Struggle to Keep Personal Data Personal: Attempts to Reform Online Privacy and How Congress Should Respond*, 52 Cath. U. L. Rev. 803, 805 n.14 (2003) (concluding that Congress should pass two current proposals for a comprehensive online privacy law because they provide consumers with stronger privacy protections of personal information); Erich D. Schiefelbine, Comment, *Stopping a Trojan Horse: Challenging Pop-up Advertisements and Embedded Software Schemes on the Internet Through Unfair Competition Laws*, 19 Santa Clara Computer & High Tech. L.J. 499 (2003) (describing adware technology and examining whether underlying justifications of unfair competition laws support or condemn the use of pop-up advertisements).

56. Borland, *supra* note 55. Drive-by downloads, Borland notes, operate by initiating a download process when a user visits a Web site. Even though a prompt typically requests the user's permission before initiating the download, inexperienced users may mistakenly believe the prompt is a normal function and click "yes." *Id.*

57. *Id.*

source of revenue.[58] Thus, whenever a new user downloads Kazaa Media Desktop, she, often unknowingly, is downloading spyware as well. By sharing files only on anonymity-protecting p2p networks, such users may avoid this exposure.[59]

2. Government

As Gandy describes, government, in addition to businesses, subjects an increasingly wide range of communications to surveillance and uses the information it collects to develop Internet user profiles—but for interests such as tax collection, law enforcement, and the protection of national security.[60] Legislation such as the USAPA has expanded the government's surveillance powers.[61] Proposed legislation such as the DSEA, nicknamed "PATRIOT II" by its critics, is intended to extend these powers even further.[62] In addition, the government has developed initiatives such as Carnivore and TIA to implement these powers.[63]

i. *The USA PATRIOT Act and the Domestic Security Enhancement Act*

On October 26, 2001, President George W. Bush signed into law the USAPA, perhaps the most far-reaching of recent government surveillance measures.[64] In February 2003, the Center for Public Integrity, a nonprofit organization that investigates and analyzes public service, government accountability, and ethics-related issues, revealed that the Department of Justice was preparing legislation entitled the DSEA.[65] Amending over fifteen different statutes, the

58. *Id.* Kazaa quietly bundles spyware produced by Brilliant Digital Entertainment. *Id.* The most common spyware source is Gator. *Id.* Some companies have developed software to block spyware programs. *See* John Borland, *In the Trenches of Techno-Rebellion*, CNET news.com (June 25, 2002) (discussing efforts to develop anti-spyware programs), *at* http://news.com.com/2009-1023-937861.html.

59. In August 2003, Kazaa announced the release of an ad-free version of its software entitled "Kazaa Plus." In contrast to Kazaa Media Desktop, which is supported by advertising, Kazaa Plus is available only for a fee. *See 'Kazaa Plus' Launched*, Kazaa (Aug. 28, 2003), *at* http://www.kazaa.com/us/news/kazaa_plus.htm.

60. Gandy, *supra* note 19, at 55–60.

61. *See infra* Part I.B.2.i.

62. *See infra* Part I.B.2.i.

63. *See infra* Part I.B.2.ii.

64. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001) (codified as amended at 18 U.S.C. § 3127 (2001)). *See* Michael T. McCarthy, *USA Patriot Act*, 39 Harv. J. on Legis. 435 (2002) (examining the USAPA from the perspective of how it balances the need for more powerful executive authority to fight terrorism with congressional and judicial oversight to protect individual rights).

65. The Center for Public Integrity obtained a draft of the Act, dated January 9, 2003, and published it on its website. *See* Domestic Security Enhancement Act of

USAPA grants domestic law enforcement and foreign intelligence agencies new surveillance powers. The DSEA would expand these powers further. Although a comprehensive discussion of the expanded powers that involve Internet use is beyond the scope of this Note, some of the more important ones are analyzed below.[66]

First, the USAPA expands law enforcement's authority under the Foreign Intelligence Surveillance Act by providing that "pen register" and "trap and trace" surveillance authority—the authority to monitor the origins and destinations, but not the contents, of communications over electronic communications devices—applies to the Internet and is permissible when a judge certifies that the information collected is relevant to an ongoing criminal investigation.[67] Showing probable cause or reasonable suspicion of criminal activity is unnecessary. The USAPA restricts such surveillance to a communication's addressing information; a communication's contents may not be collected. The USAPA does not define "contents," however.[68] Thus, it is unclear whether law enforcement authorities may monitor certain types of Internet usage, such as visiting URLs while browsing and entering

---

2003, *at* http://www.publicintegrity.org/dtaweb/downloads/Story_01_020703_Doc_1.pdf; *see also* Charles Lewis & Adam Mayle, Center for Public Integrity, Special Report: Justice Dept. Drafts Sweeping Expansion of Anti-Terrorism Act: Center Publishes Secret Draft of 'Patriot II' Legislation (Feb. 7, 2003), *at* http://www.publicintegrity.org/dtaweb/report.asp?ReportID=502&L1=10&L2=10&L3=0&L4=0&L5=0; Declan McCullagh, *Perspective: Ashcroft's Worrisome Spy Plans*, CNET news.com (Feb. 10, 2003) (discussing threats to individual rights posed by major provisions of DSEA), *at* http://news.com.com/2010-1071-983921.html?tag=fd_nc_1. This legislation has not yet been introduced, but in September 2003, President Bush gave a speech at the FBI Academy in Quantico, Virginia, in which he urged the expansion of federal law enforcement powers. *See* Charles Lewis, Center for Public Integrity, The Bush Administration Pushes to Expand the Patriot Act (Sept. 17, 2003), *at* http://www.publicintegrity.org/dtaweb/report.asp?ReportID=535&L1=10&L2=10&L3=0&L4=0&L5=0; *see also* Press Release, The White House, President Bush Discusses Homeland Security at FBI Academy (Sept. 10, 2003), *at* http://www.whitehouse.gov/news/ releases/2003/09/20030910-6.html.

66. *See* Ronald L. Plesser et al., *USA PATRIOT Act for Internet and Communications Companies*, Computer & Internet Law., Mar. 2002, at 2–9 (providing a section-by-section analysis of USAPA as it relates to the Internet).

67. Section 215 redefines a pen register device as "a device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted, provided, however, that such information shall not include the contents of any communication." USA PATRIOT Act of 2001, § 215; *see also* Plesser et al., *supra* note 66, at 4–5. Similarly, it redefines a trap and trace device as "a device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication, provided . . . such information shall not include the contents of any communication." *Id.* § 215; *see also* Plesser et al., *supra* note 66, at 4–5.

68. Orin S. Kerr, *Internet Surveillance Law After the USA Patriot Act: The Big Brother That Isn't*, 97 Nw. U. L. Rev. 607, 644–45 (2003) (defending Internet surveillance measures enacted by the USAPA).

terms into search engines like Google, without collecting the "contents" of those communications. Civil liberties organizations argue that they may not because URLs often have embedded content.[69]

Second, the USAPA expands the circumstances under which Internet Service Providers ("ISPs") must or may disclose user information to law enforcement authorities. Section 210 expands the types of subscriber records law enforcement authorities may obtain from ISPs by subpoena, which does not require court review, to include records documenting the periods that users spend online, the temporarily assigned addresses that uniquely identify their computers from all other computers during these periods, and means and sources of payment.[70] Section 211 permits cable operators that provide Internet service to respond to law enforcement authorities' requests for subscriber information without notifying the subscribers.[71] Section 212 permits ISPs voluntarily to disclose subscriber information, excluding the contents of subscriber communications, if they reasonably believe an emergency involving immediate danger of death or serious physical injury to any person requires disclosure.[72]

Third, section 802 expands the scope of surveillance by expanding the crime of domestic terrorism.[73] Domestic terrorism now encompasses activities "dangerous to human life" that violate criminal laws; that seem to be intended "to intimidate or coerce" civilians or to influence government policy through intimidation or coercion; and that take place primarily within the United States.[74] Civil liberties organizations argue that this definition may result in the classification of legitimate protest activity as domestic terrorism, especially if violence is involved.[75] Under this view, controversial "hacktivist" organizations conceivably could be targeted.[76]

Fourth, the DSEA includes numerous provisions involving Internet

69. American Civil Liberties Union, Surveillance Under the USA PATRIOT Act, *at* http://www.aclu.org/news/NewsPrint.cfm?ID=12263&c=206 (last visited Oct. 15, 2003); *see also* Electronic Frontier Foundation, EFF Analysis of the Provisions of the USA PATRIOT Act That Relate to Online Activities (Oct. 31, 2001), *at* http://www.eff.org/Privacy/Surveillance/Terrorism_militias/20011031_eff_usa_patriot_analysis.html [hereinafter EFF, *Analysis*].

70. USA PATRIOT Act of 2001, § 210; *See also* Plesser et al., *supra* note 66, at 3.

71. § 211; *see also* Plesser et al., *supra* note 66, at 3.

72. § 212; *see also* Plesser et al., *supra* note 66, at 3.

73. § 802; *see also* Plesser et al., *supra* note 66, at 3.

74. § 802; *see also* Plesser et al., *supra* note 66, at 3.

75. ACLU, *supra* note 69; *see also* EFF, *Analysis*, *supra* note 69.

76. Hacktivism is the act of hacking into a computer system to disrupt it and call attention to a political or social cause. A person who performs such an act is termed a "hacktivist." A hacktivist might, for example, place a critical text on the home page of a popular website that embodies a viewpoint she opposes or launch a denial-of-service-attack to shut down the site. *See* http://searchsecurity.techtarget.com/gDefinition/0,294236,sid14_gci552919,00.html (last visited Oct. 14, 2003) (search for term "hacktivism" on SearchSecurity.com).

surveillance that would expand the powers enumerated in the USAPA. For example, if a person is suspected of activities threatening national security, for up to forty-eight hours the FBI and state police, without a court order, may monitor the websites she visits, the search terms she enters in search engines, and the persons with whom she communicates through email and instant messaging.[77] The normal duration of electronic surveillance orders would be extended from thirty to ninety days.[78] Penalties for persons convicted of federal felonies who have knowingly or willfully used encryption would be enhanced—effectively boosting maximum prison terms for every crime covered, given the integration of encryption into so many technologies.[79] And authorized electronic surveillance of a multifunction electronic device, such as a Blackberry, would be permitted to include interception of communications through any of the device's functions.[80] The Center for Public Integrity has been particularly critical of this expansion of domestic intelligence surveillance.[81]

Neither the USAPA, nor the DSEA address anonymity-protecting p2p networks directly. Nevertheless, the expansion of law enforcement officials' surveillance powers over Internet communications may gradually encourage Internet users to begin using these networks for both legitimate and illegitimate purposes.[82] On the one hand, these networks may appeal to users concerned about increased government surveillance and censorship in the wake of the USAPA. For example, a controversial hacktivist organization classified as a terrorist group under the USAPA's new definition of domestic terrorism may publish information about its program on an anonymity-protecting p2p network so that law enforcement officials cannot trace and arrest the publisher or delete the file. Ian Clarke, the developer of Freenet, has stated that the terrorist attacks of September 11, 2001 and the subsequent enactment of the USAPA have shown that the need for anonymity-enabling p2p networks is more urgent than many had thought and that he has received numerous emails attesting to this conclusion.[83]

---

77. Domestic Security Enhancement Act of 2003, *at* http://www.publicintegrity.org/dtaweb/downloads/Story_01_020703_Doc_1.pdf.

78. *Id.* at 7.

79. *Id.* at 22.

80. *Id.* at 8.

81. Lewis & Mayle, *supra* note 65.

82. Indeed, since the enactment of the USAPA, the business of companies such as Anonymizer, a service that enables anonymous Internet browsing, and other such firms has increased. In July 2003, the service had 90,000 paying subscribers—quadruple the number it had at the same time in 2002. *See* Sean Marciniak, *Web Privacy Services Complicate Feds' Job*, Wall St. J., July 3, 2003, at B4 (discussing the proliferation of identity-shielding products like Anonymizer that protect users from government surveillance).

83. *See* John Borland, *Ian Clarke's Peer-to-Peer Debate*, CNET news.com (May 6,

Nevertheless, the growing popularity of anonymity-protecting p2p networks raises the possibility that some users will be tempted to use them for illegitimate purposes.[84] In this regard, Clarke dismisses increased concern that networks like Freenet could become, for example, refuges for terrorists seeking to avoid government surveillance.[85] He argues that such networks enable the widespread dissemination of information, not secret communication, and thus are unsuited for the plotting of terrorist acts.[86] This argument, however, seems to minimize the fact that the lack of effective search engines on these networks has the potential to render certain communications virtually, if not actually, secret.[87] Thus, the role of anonymity-protecting p2p networks in the wake of the USAPA raises the central difficulty with which we began: the necessity of finding a way to mitigate the harms that may result from online anonymity while simultaneously protecting its benefits.

ii. *Carnivore and Terrorism Information Awareness*

In addition to legislative measures such as the USAPA and the DSEA, initiatives such as Carnivore and TIA reflect the extension of the panoptic sort to an increasingly wide range of Internet communications.[88] In July 2000, the *Wall Street Journal* reported that the FBI was developing a diagnostic tool entitled Carnivore to implement court-ordered surveillance of electronic communications.[89] Concerned about the growing number of criminal suspects, including terrorists, hackers, and spies, who use the Internet to communicate with one another or their victims, the FBI developed Carnivore to intercept and collect electronic communications that are the subject of a court order while ignoring those that are not.[90] An agent positions Carnivore in an ISP's network so that Carnivore can intercept the suspect's communications exclusively.[91] If Carnivore detects the

---

2002) (focusing on Freenet's role in the post–September 11 era), *at* http://news.com.com/2102-1082-899662.html.

84. One author has described networks such as Freenet as "law-defying P2P architectures." *See* Mathias Strasser, *Beyond* Napster*: How the Law Might Respond to a Changing Internet Architecture*, 28 N. Ky. L. Rev. 660, 707–10 (2001) (defining "law-defying P2P architectures" as networks that cannot be regulated within the current legal framework).

85. Borland, *supra* note 83.

86. *Id.*

87. *See, e.g.*, *infra* Part I.C.2.ii.

88. *See* Gandy, *supra* note 19, at 55–60.

89. Neil King, Jr. & Ted Bridis, *FBI's Wiretaps to Scan E-Mail Spark Concern*, Wall St. J., July 11, 2000, at A3 (discussing the Internet industry's criticism of Carnivore).

90. Federal Bureau of Investigation, Carnivore: Diagnostic Tool, *at* http://www.fbi.gov/hq/lab/carnivore/carnivore2.htm (last visited Oct. 14, 2003).

91. *Hearing on Carnivore Diagnostic Tool Before the Senate Comm. on the Judiciary*, 106th Cong. (2000) (statement of Donald M. Kerr, Assistant Director,

suspect's identifying information in a communication, the communication is segregated from the network's data flow for additional filtering or storage.[92] The FBI emphasizes that during this process, "no FBI personnel are seeing any information—all of the information filtering/processing . . . is occurring exclusively 'within the box.'"[93] At the conclusion of the automated process, only communications authorized by court order are made available for human review.[94] Civil liberties organizations and ISPs, however, have expressed concern that the FBI can use Carnivore to collect information it lacks the legal authority to collect, including unauthorized email addressing information, instant messaging content, and records of URLs the suspect has visited.[95] They also argue that Carnivore lacks adequate oversight controls, and several commentators have questioned its constitutionality.[96]

Even more controversial than Carnivore is TIA. In 2002, the Defense Department's Defense Advanced Research Projects Agency ("DARPA"), which helped develop the Internet, disclosed it was developing "Total Information Awareness," a new weapon in its arsenal against terrorism.[97] In a gesture that could not have been more Foucauldian, TIA's website initially featured an image of an all-seeing eye above a pyramid and the slogan "scientia est potentia" (knowledge is power).[98] Incorporating data search, pattern

---

Laboratory Division, Federal Bureau of Investigation), *available at* http://www.fbi.gov/congress/congress00/kerr090600.htm.

92. *Id.*

93. *Id.*

94. *Id.*

95. Trenton C. Haas, Note, *Carnivore and the Fourth Amendment*, 34 Conn. L. Rev. 261 (2001) (arguing that Carnivore constitutes unwarranted intrusion on the privacy rights of nontargeted Internet users in violation of their Fourth Amendment rights).

96. *See* Frank J. Eichenlaub, *Carnivore: Taking a Bite Out of the Fourth Amendment?*, 80 N.C. L. Rev. 315 (2001) (concluding that Carnivore is a useful law enforcement tool but requires minor adjustments to satisfy the legitimate privacy concerns it raises); Haas, *supra* note 95; Gina Tufaro, Note, *Will Carnivore Devour the Fourth? An Exploration of the Constitutionality of the FBI Created Software*, 18 N.Y.L. Sch. J. Hum. Rts. 305 (2002) (concluding that Carnivore is unconstitutional because it invades Internet users' reasonable expectation of privacy and suggesting legal remedies).

97. *See* Robert O'Harrow, Jr., *Air Security Focusing on Flier Screening*, Wash. Post, Sept. 4, 2002, at A1 (first major newspaper article announcing DARPA's initiative to create a "total information awareness" system using the Internet, databases, and other technology to expose terrorists and their activities).

98. Jeffrey Rosen, *The Year in Ideas: Total Information Awareness*, N.Y. Times, Dec. 15, 2002, § 6 (Magazine), at 128. DARPA withdrew the logo after it became a "lightning rod" for public criticism of TIA. *See* DARPA's Information Awareness Office (IAO) and Terrorism Information Awareness (TIA) Program, Frequently Asked Questions 6 (Feb. 2003), *at* http://www.darpa.mil/iao/TIA_FAQs.pdf [hereinafter DARPA]. DARPA explained that it had selected the slogan "scienta est potentia" because this phrase "means 'Knowledge is power.' With the enabling technologies being developed by the office, the United States will be empowered to

recognition, and privacy protection policies, TIA is designed to discover, extract, and link data from independent electronic databases to identify individuals as potential terrorists and detect terrorist threats before they occur.[99] This technology grows out of that used to develop the World Wide Web, which has made possible the integration of thousands of databases without centralizing the information.[100] Although civil liberties groups and members of Congress widely criticized the project, it was revealed in December 2002 that a prototype was already in place and being tested by military intelligence organizations.[101]

In February 2003, Congressional negotiators resolved that TIA could not be used against Americans and also agreed to restrict further research on the project without congressional consultation.[102] In May, DARPA submitted a report to Congress in which it stressed that "[s]afeguarding the privacy and civil liberties of Americans is a bedrock principle."[103] It also announced that TIA's new name was "Terrorism Information Awareness"—a change motivated by its desire to make "absolutely clear" that its objective in "pursuing these efforts is to protect U.S. citizens by detecting and defeating foreign terrorist threats before an attack."[104] In July, however, the Senate passed the 2004 defense appropriations bill with a provision that effectively removes all funding from TIA.[105]

Gandy has observed that as awareness of the surveillance represented by the panoptic sort increases—exemplified by measures such as the USAPA and the proposed DSEA and initiatives such as Carnivore and TIA—attempts to resist and attempts to withdraw will emerge.[106] Anonymity-protecting p2p networks constitute both types of attempts. They are attempts to resist the panoptic sort in that their purpose and effect is to disrupt surveillance.[107] In this regard, they may even be used to host "mirrors"—websites that have been copied from one computer server to another so that the site is available from

implement operational systems to thwart terrorist attacks like those of September 11, 2001." *Id.*

99. *See* DARPA, *supra* note 98, at 1–2.

100. *See* John Markoff & John Schwartz, *Many Tools of Big Brother Are Now Up and Running*, N.Y. Times, Dec. 23, 2002, at C1.

101. *Id.*

102. Adam Clymer, *Congress Agrees to Bar Pentagon From Terror Watch of Americans*, N.Y. Times, Feb. 12, 2003, at A1.

103. Defense Advanced Research Projects Agency, Report to Congress Regarding the Terrorism Information Awareness Program 27 (May 20, 2003), *at* http://www.darpa.mil/body/tia/tia_report_page.htm.

104. *Id.*

105. *See* Department of Defense Appropriations Act of 2004, H.R. 2658, 108th Cong. § 8124 (2003).

106. Gandy, *supra* note 19, at 3.

107. *See infra* Part I.C.2.

more than one location—of sites at risk of being hacked or banned.[108] But they are also attempts to withdraw in that they are self-contained entities that have barricaded themselves from the rest of the Internet like fortresses in the wilderness.[109] To understand their dual status within the society of surveillance, it is useful to describe in detail the ideologies that have motivated the developers of these networks and the technologies that embody these ideologies.

C. *Resisting the Panoptic Sort*

Free Haven, Publius, and Freenet are the three most important anonymity-protecting p2p networks that have emerged since 1999. These networks offer the possibility of virtually absolute freedom of expression by incorporating technologies that enable users to author, publish, store, and read files on the network with virtually complete anonymity.[110] They resist censorship because these functions are not subjected to control and because the networks themselves cannot easily be shut down by traditional legal means.[111] Even if a court were to issue an injunction against Freenet, for example, as the Ninth Circuit issued an injunction against Napster,[112] the developers would be compelled to cease operations, but the network itself would persist because control is dispersed among the individual computers that comprise it, rather than located in a central server.[113] Although the three networks share a common technological foundation and a commitment to the premise that technology has the potential to protect freedom of expression through the provision of anonymous communication resistant to surveillance and censorship, subtle technological and ideological differences distinguish them.[114] Freenet, the most well-known of the three networks, offers the most radical interpretation of freedom of expression—one that contests traditional First Amendment jurisprudence in its absolutism.[115]

1. p2p Networks

A p2p network is a type of network architecture in which two or more computers are directly connected over the Internet without the use of a central server to mediate their connection.[116] In a p2p

108. *See* http://searchstorage.techtarget.com/sDefinition/0,,sid5_gci212579,00.html (last visited Oct. 15, 2003) (search for term "mirror" on searchStorage.com).
109. *See infra* Part I.C.2.
110. *See infra* Part I.C.2.
111. *See infra* Part I.C.2.
112. A & M Records, Inc. v. Napster Inc., 239 F.3d 1004, 1011 (9th Cir. 2001).
113. *See infra* Part I.C.2.
114. *See infra* Part I.C.2.
115. *See infra* Part I.C.2.
116. Michael Miller, Discovering P2P 4 (2001); Clay Shirkey, *Listening to Napster*, *in* Peer-to-Peer: Harnessing the Benefits of a Disruptive Technology 21 (Andy Oram

network, each computer on the network has the ability both to receive and to distribute data; accordingly, each is known as a "peer" (or "node").[117] Because there is no central server, all the peers function as equals, and control over the network is consequently dispersed among them.[118] Michael Miller, author of several primers on Internet technologies, has defined five key properties of a typical p2p network: (1) the network enables real-time data transmission between the peers; (2) each peer can function as both a client and a server; (3) the peers provide the network's primary content; (4) the network places control over the system in the peers themselves, not in a central server; and (5) the network accommodates peers that are not always connected to the network (that is, it tolerates variable connectivity).[119] These properties enable peers to distribute content to other peers without censorship because intrapeer communication is potentially anonymous and not controlled by any intermediary.

At the Internet's inception, the p2p model was predominant, but it was not the model that was to prevail.[120] By the mid-1990s, the invention of the World Wide Web in 1991 and the subsequent transformation of the Internet into a mass medium had facilitated the rise of "client-server" networks.[121] In a typical client-server network, all communications are routed through the server.[122] Thus, the server has the capacity both to monitor communications (for example, by producing logs of the user's browsing activities) and to control them (for example, by filtering access to certain URLs or chat rooms, deleting objectionable files on the system, terminating the user's service, or revealing the user's identity to law enforcement authorities). This capability serves the interests of businesses, which had begun to recognize the Internet's commercial potential,[123] and government, which had begun to become concerned about the unrestricted circulation of content perceived to be harmful to the public. Thus, although client-server networks may have socially beneficial uses, they also have the potential to limit freedom of expression on the Internet by rendering communication vulnerable to

---

ed., 2001).

117. Miller, *supra* note 116, at 18.

118. *Id.*; *see also* Nelson Minar & Marc Hedlund, *A Network of Peers: Peer-to-Peer Models Through the History of the Internet*, *in* Peer-to-Peer: Harnessing the Benefits of a Disruptive Technology 16 (Andy Oram ed., 2001).

119. Miller, *supra* note 116, at 19. Shirkey describes the key characteristics of a p2p network as the ability to permit "variable connectivity and temporary network addresses" and to "give the nodes at the edges of the network significant autonomy." Shirkey, *supra* note 116, at 22.

120. *See* Minar & Hedlund, *supra* note 118, at 4.

121. *Id.* at 9.

122. *See* http://searchnetworking.techtarget.com/sDefinition/0,,sid7_gci211796,00.html (last visited Oct. 14, 2003) (search for term "client/server" on searchNetworking.com).

123. Lawrence Lessig, Code and Other Laws of Cyberspace 205 (1999).

monitoring and censorship.[124] In this respect, they are symptomatic of the expansion of the panoptic sort that Gandy describes.[125]

A convergence of technological, social, political, and legal developments contributed to the resurgence of p2p networks in the late 1990s. Personal computers became more powerful; connections to the Internet more reliable, more permanent, and faster;[126] and the ability of networks to harness the dormant resources of computers not connected to the network at all times increased.[127] With more sophisticated technological infrastructures, ordinary users were no longer limited to using the Internet to send and receive email or browse the Web. They began to use their computers to connect to one another directly to form "user-created search engines, virtual supercomputers, and filesystems."[128] The most common types of p2p networks that emerged include instant messaging systems such as ICQ Instant Messenger (launched 1996); distributed computing projects such as SETI@home (launched 1999); filesharing systems such as Napster (launched 1999), Gnutella (launched 1999), and Kazaa (launched 2000); and anonymity-protecting p2p networks such as Free Haven (launched 1999), Freenet (launched 1999), and Publius (launched 2000).[129]

The developers of anonymity-protecting p2p networks have stressed p2p's capability to resist and withdraw from the order of the panoptic sort.[130] For these developers, the primary virtue of p2p technology is the ability to protect freedom of expression by offering anonymous, censorship-resistant communication during an era in which online surveillance is increasing.[131] Like mainstream filesharing services such as Napster, Gnutella, and Kazaa, anonymity-protecting p2p networks like Free Haven, Publius, and Freenet enable users to

---

124. Adam Langley, *Freenet*, *in* Peer-to-Peer: Harnessing the Benefits of a Disruptive Technology 123 (Andy Oram ed., 2001).

125. *See supra* Part I.A.

126. Lawrence Lessig, The Future of Ideas: The Fate of the Common in a Connected World 135 (2001).

127. Shirkey, *supra* note 116, at 22.

128. Minar & Hedlund, *supra* note 118, at 3.

129. *See* ICQ Instant Messenger, *at* http://web.icq.com (last visited Oct. 14, 2003); SETI@home, *at* http://setiathome.ssl.berkeley.edu (last visited Oct. 14, 2003); Gnutella, *at* http://www.gnutella.com (last visited Oct. 14, 2003); Kazaa, *at* http://www.kazaa.com/us/index.htm (last visited Oct. 14, 2003); Free Haven Project, *at* http://www.freehaven.net (last visited Oct. 14, 2003); Publius, *at* http://cs1.cs.nyu.edu/waldman/publius (last visited Oct. 14, 2003); Free Network Project, *at* http://freenet.sourceforge.net (last visited Oct. 14, 2003).

130. John Borland, *Networks Promise Unfettered File Swapping*, CNET news.com (June 19, 2001) (discussing Freenet's efforts to develop a wholly anonymous, virtually untraceable mode of communicating and file-sharing via the Internet), *at* http://news.com.com/2100-1023-268604.html. Some commentators have classified such projects within the context of "hacktivist" groups, which use digital technology to promote social and political activism. *See* Lee, *supra* note 5, at G1.

131. *See* Miller, *supra* note 116, at 44.

share files directly with one another.[132] Nevertheless, they differ from such filesharing services in several respects. First, mainstream filesharing services are usually for-profit entities, while, to date, anonymity-protecting p2p networks have usually been nonprofit research projects operated by people who donate their time, labor, and expertise out of their commitment to the principles the projects embody.[133] Second, the former are not motivated by a coherent political philosophy, while the latter are. This philosophy is grounded in part on the premise that the provision of anonymous communication is necessary to protect freedom of expression in an environment in which it is under attack from both businesses and government.[134] It is also grounded in part on the premise that technology, rather than law, provides the most effective means of securing this freedom.[135] Moreover, the developers of anonymity-protecting p2p networks have articulated their philosophical programs in carefully reasoned position papers and, in the case of Freenet, manifesto-like texts.[136] Third, the former do not strive to provide absolute anonymity, while the latter do. Indeed, the latter were specifically motivated by the formers' inability to provide truly anonymous communication.[137] This issue has become especially timely in the wake of the D.C. Circuit's two recent decisions in *In re Verizon Internet Services, Inc.* ordering an ISP to disclose to the plaintiff, the RIAA, the identity of a Kazaa user who had anonymously downloaded over 600 copyrighted songs without authorization—a decision that has unleashed a flood of subpoenas from the RIAA.[138] Finally, the formers' impact has been momentous,

132. *See infra* Part I.C.2.

133. Free Haven, Publius, and Freenet fit this description. *See* Free Haven Project, *at* http://www.freehaven.net (last visited Oct. 15, 2003); Publius, *at* http://cs1.cs.nyu.edu/waldman/publius (last visited Oct. 15, 2003); Free Network Project, *at* http://freenet.sourceforge.net (last visited Oct. 15, 2003).

134. *See infra* Part I.C.2.

135. *See infra* Part I.C.2.

136. Compare the loosely organized group of programmers associated with Hactivismo, who are motivated by similar concerns. For example, one of the clauses of The *Hactivismo* Declaration (2001), a document inspired by the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights, declares "that we will study ways and means of circumventing state sponsored censorship of the Internet and will implement technologies to challenge information rights violations." Hactivismo, The Hactivismo Declaration, *at* http://hacktivismo.com/about/declarations/en.php (last visited Oct. 15, 2003).

137. *See* Roger Dingledine et al., *Free Haven*, *in* Peer-to-Peer: Harnessing the Benefits of a Disruptive Technology 161 (Andy Oram ed., 2001). For example, the authors note, Napster enabled the band Metallica to identify users who were sharing copies of the band's songs without its permission and to force Napster to remove these users from the system. Similarly, Gnutella lured Gnutella users to a website that claimed to offer child pornography and then published their Internet Protocol addresses on a "Wall of Shame." *See id.*

138. *In re* Verizon Internet Servs., Inc., 257 F. Supp. 2d 244 (D.D.C. 2003); *In re* Verizon Internet Servs., Inc., 240 F. Supp. 2d 24 (D.D.C. 2003). For an analysis of this

while the latters' has been more limited. For example, as of May 2003, Kazaa had been downloaded over 230 million times, while Freenet had been downloaded 1.2 million times.[139] Mainstream filesharing services have been more popular than anonymity-protecting p2p networks in part because the latter are much more difficult to use. In particular, the latter typically lack efficient search mechanisms, making the location of desired files more challenging.[140] As these anonymity-protecting p2p networks become more user-friendly, however, their appeal is likely to become more widespread.

2. Anonymity-Protecting p2p Networks

It is necessary to understand the technology of anonymity-protecting p2p networks to grasp the difficulties legislators face in drafting legislation that regulates the technology effectively. This discussion focuses on a central issue of primary legal significance: How each of the most important such networks—Free Haven, Publius, and Freenet—strives to solve the problem of achieving anonymity while maintaining accountability.

There are four types of anonymous communication on the Internet.[141] First, traceable anonymous communication permits users to transmit unencrypted communications through intermediaries without disclosing their personal identities.[142] Only the intermediaries can identify the sender. If a court finds a communication unlawful, it may order the intermediary to disclose the sender's identity. Second, untraceable anonymous communication permits users to transmit encrypted communications through multiple intermediaries that decrypt and then re-encrypt the communications at each link in a

---

case, see Katyal, *supra* note 17. As of late August 2003, the RIAA had issued over 1,300 subpoenas to filesharers. *See RIAA Reveals Method to Madness*, wired.com (Aug. 28, 2003) (describing techniques the RIAA uses to investigate unauthorized filesharing), *at* http://www.wired.com/news/digiwood/0,1412,60222,00.html. It announced it was suing 261 individuals, including a twelve-year-old girl with whom it subsequently settled. *See* Katie Dean, *Schoolgirl Settles With RIAA*, wired.com (Sept. 10, 2003) (discussing the RIAA's lawsuits against individuals accused of unauthorized filesharing), *at* http://www.wired.com/news/digiwood/0,1412,60366,00.html; *see also How to Tell If the RIAA Wants You*, wired.com (July 26, 2003) (discussing the Electronic Frontier Foundation's creation of an online database of subpoenas issued by the RIAA against filesharers), *at* http://www.wired.com/news/digiwood/0,1412,59785,00.html.

139. *See* Kazaa, Kazaa Media Desktop Sets Most Downloaded Software Record (May 26, 2003), *at* http://www.kazaa.com/us/news/most_downloaded.htm; Free Network Project, What Is Freenet?, *at* http://freenet.sourceforge.net (last visited Oct. 15, 2003).

140. *See* Strasser, *supra* note 84, at 708.

141. This model derives from Rob Kling et al., *Assessing Anonymous Communication on the Internet: Policy Deliberations*, 15 Info. Soc'y 79, 81–82 (1999) (examining fundamental aspects of anonymous social behavior to ground policy debates on anonymous communication on the Internet).

142. *Id.* at 81.

chain until the communication reaches its final destination.[143] No single intermediary knows the communication's full path; thus, the sender retains a greater degree of anonymity. Nevertheless, if a court finds the communication unlawful, it could attempt to enforce a disclosure order by retracing the communication's path link by link to the sender—a difficult, if not impossible, task. Third, traceable pseudonymous communication functions like traceable anonymous communication except that users are known by pseudonyms that they select.[144] Because intermediaries usually retain a log with users' identifying information, senders can be traced if necessary. Fourth, untraceable pseudonymous communication functions like untraceable anonymous communication except that, again, users are known by pseudonyms that they select.[145] In contrast to untraceable anonymous communication, however, users may ensure that their personal identities remain undisclosable, but maintain a continuous pseudonymous identity.

Anonymity-protecting p2p networks attempt to provide untraceable anonymous or untraceable pseudonymous communication. Moreover, within either of these models, these networks must assign a level of anonymity to four types of communication functions.[146] A network is author-anonymous when it prevents users from linking a file to its author. It is publisher-anonymous when it prevents users from linking a file to the peers, nodes, or servers that publish, upload, or insert the file into the network. It is server-anonymous when it prevents users from linking the file to the peers, nodes, or servers that store the file. It is reader-anonymous when it prevents users from linking the file to the users who request or download the file. Finally, in spite of the attempts these networks make to protect the anonymity of these communication functions, it is probably impossible to guarantee absolute anonymity for all users at all times. If an adversary has sufficient resources at its disposal, the possibility always exists that it may be able to identify a user.[147]

A central tension in anonymity-protecting p2p networks is the conflict between anonymity and accountability. Sociologists assume that identification typically encourages people to abide by norms because most people desire to gain the positive approval of or to avoid negative sanctions from others; to achieve these results, people must be identifiable.[148] When communication is anonymous, people

143. *Id.* at 81–82.
144. *Id.* at 82.
145. *Id.*
146. This Note's classificatory system is a modified version of the one proposed in Dingledine et al., *supra* note 137, at 163–65.
147. *Id.* at 165.
148. Gary T. Marx, *What's in a Name? Some Reflections on the Sociology of Anonymity*, 15 Info. Soc'y 99, 105 (1999) (suggesting types of identity knowledge,

can avoid sanctions because they cannot as easily be held accountable for the information they transmit. They cannot be identified, and they cannot be indicted and prosecuted for actions that may be unlawful.[149] The participants in a major project on Internet anonymity sponsored by the American Association for the Advancement of Science ("AAAS") concluded that the tension between anonymity and accountability complicates the formulation of legal rules regulating anonymity on the Internet in two ways.[150] First, it is necessary to find a way to mitigate the harms that may result from online anonymity, while simultaneously protecting its benefits.[151] Second, it is necessary to find a way to enforce regulations on anonymous communication effectively, in view of the fact that, by definition, identification, and thus prosecution, of the senders and receivers of unlawful communications are often impossible.[152] The developers of anonymity-protecting p2p networks have approached these problems from technological perspectives. Most have attempted to engineer anonymity-protective accountability mechanisms into their networks or, in the case of Freenet, have declined to emphasize this effort and have chosen instead to protect anonymous communication absolutely.[153]

i. *Free Haven*

Launched in 1999, Free Haven is being developed by computer programmers Roger Dingledine, Michael J. Freedman, and David Molnar.[154] It strives to resist censorship primarily by ensuring the stable, secure, and long-term storage of files.[155] Its goals are anonymity (authors, publishers, and readers of files are anonymous, and the locations of files on the network are unknowable); persistence (the publisher of a file, not the peers that store it, determines the file's life span); flexibility (the network functions smoothly as peers join and

identifying rationales and contexts for anonymity and identifiability, and suggesting a principle of "truth in the nature of naming" that holds that persons who use pseudonyms in personal Internet communications have a duty to indicate that they are doing so).

149. *See* Al Teich et al., *Anonymous Communication Policies for the Internet: Results and Recommendations of the AAAS Conference*, 15 Info. Soc'y 71 (1999) (reporting the results of the AAAS Conference: online anonymous communication is morally neutral and should be considered a strong human and constitutional right; online communities should be permitted to set their own policies on use of anonymous communication; users should be informed about the extent to which their identity is disclosed online).

150. *Id.* at 72.

151. *Id.*

152. *Id.*

153. *See infra* Part I.C.2.iii.

154. Free Haven, People, *at* http://www.freehaven.net/people.html (last visited Oct. 14, 2003).

155. Free Haven, *at* http://www.freehaven.net (last visited Oct. 14, 2003).

leave it); and accountability (a "reputation system" helps to limit the harms caused by misbehaving peers).[156] Its developers justify these goals by emphasizing the necessity of protecting anonymous expression.[157] They conclude that the expansion of online surveillance by businesses and government has given rise to new threats against freedom of expression that the law cannot always effectively prevent.[158]

For the developers, Free Haven represents the most recent stage in a tradition advocating the utility of anonymous speech that begins with Thomas Paine's anonymous publication of *Common Sense* (1776) and Alexander Hamilton, John Jay, and James Madison's pseudonymous publication of *The Federalist* papers (1787–88).[159] The tradition encompasses the subsequent use of anonymous publication by persecuted groups to criticize oppressive practices and laws.[160] And it extends to the present. The developers describe Free Haven's potential adversaries as governments, corporations, and individuals.[161] They predict political attacks, in which governments will attempt to discourage use of Free Haven; legal attacks, in which authorities will attempt to shut down or arrest peers; and technical attacks, in which intelligence agencies, businesses, and individuals will attempt to disable the network.[162]

The Free Haven network consists of a "servnet" or community of servers—what other networks term "peers" or "nodes."[163] The

156. Dingledine et al., *supra* note 137, at 159.

157. *See* Roger Dingledine, The Free Haven Project: Design and Development of an Anonymous Secure Data Haven 36–54 (2000) (unpublished masters thesis, Massachusetts Institute of Technology).

158. *Id.*

159. *Id.* at 37.

160. *Id.*

161. Free Haven, Project Description, *at* http://www.freehaven.net/overview.html (last visited Oct. 15, 2003).

162. *Id.*

163. *Id.* Each server on the servnet hosts files from the others in exchange for the opportunity to publish its own files (only servers may publish files). An author wishing to publish a file assigns it an expiration date defining its "life span." Dingledine, *supra* note 157, at 56. She then identifies and secures a publisher—a server willing to store her file. *Id.* at 59. She sends the file to the publisher anonymously, using encryption, an anonymous remailer, or another mechanism of her choice. *Id.* After receiving the file, the publisher divides it into "shares" or fragments (only a subset of shares, not the totality, is necessary to reassemble the file when a reader requests it) and "signs" it with a "lookup key." *Id.* at 56–59. Then, for each share, the publisher locates a server he "trusts," and the two servers trade shares behind the scenes. *Id.* at 59. Servers do not know which shares they store because data constantly migrates from server to server, based partly on chance and partly as a result of trades between servers. *Id.* at 55. To retrieve a file, a reader, who need not be a server, must know the file's lookup key (in some cases, directories may provide her with this information). *Id.* at 59. She then locates a server willing to perform a request for her. *Id.* at 60. This server broadcasts the request to all the servers it knows. *Id.* Servers storing shares of the requested file encrypt and send them to the reader. *Id.* As soon as enough shares arrive, the reader can reassemble and read the

developers have sought to engineer anonymity into the network by attempting to make the distribution of files pseudonymous and untraceable.[164] All of the network's agents—authors, publishers, readers, and servers storing files—use pseudonyms. Moreover, these pseudonymous agents communicate only by secure, encrypted, anonymous communication channels.[165]

Free Haven's developers have also attempted to engineer accountability into the network through what they term "reputation systems."[166] A server creates her reputation by offering to store files for other servers.[167] Once she is integrated into the network, she inserts new files for and trades shares with other servers. By successfully fulfilling these "contracts," she increases her reputation and thus her ability to store her own files on other servers.[168] Servers with good reputations have the most opportunities to store their own files with other servers, and servers with poor reputations the least.[169] In this manner, this system encourages servers to adhere to the network's norms, which include the expectation that servers will not act as freeriders who consume the resources of others, such as disk space and bandwidth, without contributing their own.[170] An automated system tracks the reputations of each server to facilitate compliance.

Crucially, this system is directed primarily toward accountability for resource allocation, not content. It encourages servers to avoid overloading the network with data and monopolizing bandwidth, but not from publishing certain types of files.[171] Toward this end, the network maintains a "content-neutral" policy. Servers agree to store files for other servers without regard to the files' content.[172] Dingledine writes that this "lack of accountability" not only makes Free Haven powerful and useful, but also potentially dangerous because policing content on the network is impossible.[173]

In his master's thesis, Dingledine justifies the impossibility of policing content on Free Haven by arguing that cases such as *ACLU of Georgia v. Miller*, *Lamont v. Postmaster General* and *McIntyre v.*

---

file. *Id.*

164. Dingledine et al., *supra* note 137, at 162.

165. *Id.* at 166. According to its developers, Free Haven provides both "computational" and "perfect-forward" anonymity for authors, publishers, and readers. For a discussion of this topic, see *id.* at 182.

166. *See* Roger Dingledine et al., *Accountability*, *in* Peer-to-Peer: Harnessing the Benefits of a Disruptive Technology 306–28 (Andy Oram ed., 2001).

167. *See* Dingledine et al., *supra* note 137, at 165–66.

168. Roger Dingledine et al., *Reputation in Privacy Enhancing Technologies*, *at* http://freehaven.net/doc/cfp02/cfp02.html (last visited Oct. 15, 2003).

169. *Id.*

170. *Id.*

171. Dingledine et al., *supra* note 166, at 329.

172. Dingledine et al., *supra* note 137, at 168.

173. Dingledine, *supra* note 157, at 36.

Ohio Elections Commission define a constitutionally protected right to speak and to read anonymously.[174] But his analysis fails to recognize adequately that traditional First Amendment jurisprudence does not hold that these rights are absolute. Moreover, he dismisses, perhaps too easily, the potential harms to be expected from anonymous communication on the network. For example, he acknowledges that the unauthorized trading of copyrighted files may result in infringement, but he suggests that new technologies have rendered the traditional copyright regime obsolete and that alternative regimes should be considered.[175] He suggests that the commercial pornography industry will probably ignore Free Haven because the network does not enable businesses to sell their products in a trackable manner.[176] But he simply dismisses the possibility that individual noncommercial users may distribute pornography files, including illegal child pornography, over the network as an "unfortunate consequence" that is a strong argument against developing such a system, without attempting to propose a solution.[177] He also acknowledges that the publication of defamatory statements is a potential problem because files cannot be "unpublished" and because allegedly defamed victims cannot identify defendants to sue.[178] But in response he merely proposes that users should think carefully about the statements they publish because the network cannot be responsible for users who act without thinking first.[179] Finally, he argues for the importance of maintaining content-neutrality: "The Free Haven system is designed to provide privacy for its users; rather than being a persistent publication system, it is designed to be a private low-profile storage system. Requiring

174. *See* McIntyre v. Ohio Elections Comm'n, 514 U.S. 334 (1995) (holding that Ohio's statutory prohibition against the distribution of any anonymous campaign literature violated the First Amendment); Lamont v. Postmaster Gen., 381 U.S. 301 (1965) (holding that a federal statute requiring the Post Office Department to detain and destroy unsealed foreign mail identified as communist political propaganda unless the addressee returns a reply card indicating her desire to receive the mail violated the addressee's First Amendment rights); ACLU v. Miller, 977 F. Supp. 1228 (N.D. Ga. 1997) (holding that Internet users who challenged the constitutionality of a state criminal statute prohibiting Internet transmissions that falsely identify the sender were substantially likely to show that the statute imposed content-based restrictions not narrowly tailored to achieve a compelling state interest); *infra* Part II.B. (discussing these cases); *see also* Dingledine, *supra* note 157, at 37–44. "It is clear both from the United States Constitution, and also from the case law described above and held by the US Supreme Court, that anonymous publication is a legal and protected right for US citizens." *Id.* at 44.

175. Dingledine, *supra* note 157, at 46. He does, however, state: "[W]e consider the fact that Free Haven might be used to further violate copyright and patent[] laws to be an unfortunate consequence of deploying the system. We believe this is a strong argument against developing a system like this." *Id.* at 47.

176. *Id.*

177. *Id.*

178. *Id.* at 48.

179. *Id.* at 49.

operators to read through publication 'submissions' runs counter to this goal."[180] This point of view is certainly valid, but it does not satisfactorily address the legal problems that such a system raises, including the proliferation of child pornography, obscenity, defamation, and other categories of unprotected expression that cannot be linked to an author.

ii. *Publius*

Launched in 2000, Publius was developed by former AT&T researchers Aviel D. Rubin and Lorrie Cranor, and New York University graduate student Marc Waldman, who were motivated by objectives similar to those that motivated Free Haven's developers.[181] Publius's two primary goals are to provide publishers with a high degree of anonymity and to protect from censorship files stored on the network.[182]

Echoing Free Haven's invocation of *The Federalist* papers as a precedent for the network, Publius derived its name from the pen name Hamilton, Jay, and Madison used as *The Federalist* papers' authors (their portraits are even featured prominently at the top of the site's homepage).[183] Publius is rooted squarely in the proposition that publication plays an essential role in struggles for positive social change and that anonymous or pseudonymous publication is particularly important in these struggles.[184] According to its developers, the Internet is a "powerful revolutionary tool[]" that governments may seek to suppress through censorship or physical or economic intimidation of online authors and publishers.[185] Authors may wish to publish files anonymously or pseudonymously to protect themselves from personal harm or out of the belief that readers will accept their work more readily if it is not associated with a person of a particular sex, race, ethnicity, or other identifying characteristic.[186]

---

180. *Id.* at 50.

181. Jenn Shreve, *Avi Rubin: Publius' Public Crusade*, Industry Standard (Sept. 13, 2000) (discussing Rubin's purposes in conceiving Publius), *at* http://www.thestandard.com/article/display/0,1151,18487,00.html.

182. Publius Censorship Resistant Publishing System, Overview, *at* http://cs1.cs.nyu.edu/waldman/publius (last visited Oct. 15, 2003).

183. *Id.* "Anonymous publishing played an important role in the early history of the United States. James Madison, Alexander Hamilton, and John Jay collectively wrote the Federalist Papers under the pen name Publius. This collection of 85 articles, published pseudonymously in New York state newspapers from October 1787 through May 1788, was influential in convincing New York voters to ratify the proposed U.S. Constitution. It is from these distinguished authors that our system gets its name." Marc Waldman et al., *Publius*, *in* Peer-to-Peer: Harnessing the Benefits of a Disruptive Technology 145–46 (Andy Oram ed., 2001).

184. Publius Censorship Resistant Publishing System, *supra* note 182.

185. *Id.*

186. *Id.* As Part II.B. suggests, this reasoning constitutes one of the justifications for anonymous expression the Supreme Court offered in *McIntyre*. Note also that the

Publius is more strongly motivated by the protection of anonymous political expression, as opposed to nonpolitical expression, which might include music and pornography. In fact, Rubin, the grandson of Russian and Polish Jews persecuted for their religious beliefs,[187] notes that he was inspired to develop Publius after learning of a Panamanian radio broadcaster operating during General Manuel Noriega's regime.[188] The broadcaster was repeatedly forced to relocate his transmitter to avoid being shut down and arrested, and he was eventually captured.[189] "If he had access to something like Publius he could have maintained a Web site," Rubin writes. "He could have remained anonymous, and the government couldn't have shut it down."[190] Indeed, he notes Publius is an ideal tool of communication for political dissidents and corporate whistleblowers,[191] as well as critics of powerful organizations such as the Church of Scientology, which, according to Rubin, has used intellectual property law, intimidation, and other means to suppress the dissemination of Church documents.[192]

The Publius network consists of the "Publius Server List," a community of servers running the system software. Like Free Haven's developers, Publius's have attempted to engineer anonymity into the network.[193] Authors remain anonymous because the use of

---

Center for Democracy and Technology, an organization that works to promote democratic values and constitutional liberties in the digital age, hosted a server in Publius's pilot project. *See* Center for Democracy and Technology, CDT Policy Post (Sept. 29, 2000), *at* http://www.cdt.org/publications/pp_6.18.shtml#6.

187. Shreve, *supra* note 181.

188. Elinor Abreu, *Peer-to-Peer—We've Only Just Begun*, Industry Standard (Aug. 28, 2000) (discussing Freenet, Publius, and the emergence of anonymity-protecting p2p networks), *at* http://www.thestandard.com/article/display/0,1151,17757,00.html.

189. *Id.*

190. *Id.*

191. *Id.*

192. Daniel Sorid, *Divided Data Can Elude the Censor*, N.Y. Times, July 27, 2000, at G10 (discussing the development of Publius).

193. When a user wishes to publish a file on the network, the publisher creates a "key" that is used to encrypt the file. Waldman et al., *supra* note 183, at 147. As in Free Haven, the publisher splits the key into shares; only a small number of shares is necessary to re-create the key. *Id.* at 147–48. The system then randomly selects a subset of servers on the network and uploads the file onto each one. *Id.* at 148. More specifically, on each server, the system uploads the entire encrypted file and a single share file, with each server storing a different share. *Id.* Because the file is encrypted, the servers storing the file cannot read it. Moreover, because each file is also given the neutral name "file," the servers cannot even guess its contents—a strategy that enables them plausibly to deny knowledge of its content. *Id.* at 151. After the system has uploaded each file and share on the respective servers, it creates a "Publius URL." *Id.* at 148. The Publius URL, which is displayed in the publisher's browser, is a special code resembling an ordinary, though much more complicated, URL. *Id.* at 151. It contains encrypted information about the servers hosting the shares and the number of shares needed to re-create the key. *Id.* at 148. A reader who wishes to retrieve the file must know its Publius URL. *Id.* The reader enters this URL into a specially configured Web browser that randomly retrieves the encrypted file and

encryption helps to prevent anyone from connecting any file to its author. Encryption also prevents servers from being able to read any file stored on their servers. And publishers, the only agents who know the file's Publius URL, may protect their anonymity by using anonymous remailers whenever they choose to distribute the URL. In addition, the system is censorship-resistant. A file may be deleted only when the publisher chooses to delete it.[194] Furthermore, anticipating the possibility that an adversary may learn a publisher's identity and attempt to force her to delete a file, during the publication process the system offers the publisher a "do not delete" option that, if selected, denies future requests to delete the file.[195] Even if a court ordered the removal of a file from the system, the order would be unenforceable because the file is distributed across multiple servers in many different jurisdictions and may be reassembled from a small number of shares.[196] Rubin maintains that even if seventy percent of the network's servers were shut down, a sufficient number of shares would be available to reconstitute and make accessible most files.[197]

In contrast to Free Haven, Publius has not directly attempted to engineer accountability for either resource allocation or content into the network.[198] Nevertheless, it has done so indirectly by restricting the types of files that may be published on and retrieved from the network. First, Publius limits the size of files that may be published to 100K.[199] This limitation discourages the publication of large files, such as music and video files (including unauthorized copyrighted ones).[200] Second, Publius exploits the network's lack of an efficient search mechanism to make searching for unobjectionable files much easier than searching for potentially objectionable ones.[201] To retrieve a file, a user must know the file's Publius URL. Publius publishes a list of URLs, but it only lists URLs it considers "interesting"—that is,

---

shares from the servers. *Id.* To re-create the key, the system must locate at least three shares. *Id.* These shares are then combined to re-create the key, and the key is used to decrypt the file. *Id.* The system then performs a tamper check, and if the file passes the check, it is displayed in the browser. *Id.*

194. *Id.* at 155.

195. *Id.*

196. Marc Waldman et al., *Trust*, *in* Peer-to-Peer: Harnessing the Benefits of a Disruptive Technology 261 (Andy Oram ed., 2001); Sorid, *supra* note 192.

197. Shreve, *supra* note 181. "The system resists attack because Publius as a whole is robust enough to continue serving files even when many of the hosts go offline." Waldman et al., *supra* note 183, at 146.

198. Dingledine et al., *supra* note 137, at 160.

199. Marc Waldman et al., *Publius: A Robust, Tamper-evident, Censorship-resistant Web Publishing System*, Proceedings of the 9th USENIX Security Symposium (2000), *available at* http://cs1.cs.nyu.edu/~waldman/publius/publius.pdf.

200. John Borland, *AT&T Vows No Censorship on New Network*, CNET news.com (Aug. 7, 2000) (discussing the development of Publius), *at* http://news.com.com/2100-1033-244166.html.

201. *Id.*

primarily files with political content.[202] It does not list files it considers "uninteresting," which would include music and pornography files.[203] This approach offers a partial solution to the difficulty of finding a way to mitigate the harms that may result from online anonymity while simultaneously protecting its benefits: It is relatively easy to read political texts, for example, but relatively difficult—but not impossible—to engage in certain types of unlawful acts, such as copyright infringement and the possession of child pornography.[204] Rubin is at great pains to assert that this strategy is not censorship, but simply a means of providing a "directory for things we think are interesting."[205] Nevertheless, more radical anonymity-protecting p2p networks, such as Freenet, might classify this decision as a type of content restriction that verges on censorship and thus is unacceptable.

iii. *Freenet*

Downloaded over 1.2 million times since its launch in 1999, Freenet is the most widely used anonymity-protecting p2p network.[206] It has five primary objectives: to prevent censorship of files; to provide anonymity for users; to remove any single point of failure or control; to store and distribute files efficiently; and to enable peers, which it terms "nodes," plausibly to deny knowledge of the files stored on their computers.[207] It is based on a system created by the project's primary developer, Ian Clarke, who has been described as the "Che Guevara of the Web" and the "Martin Luther of copyright."[208] Clarke first explained the system in his paper, *A Distributed Decentralised Information and Storage and Retrieval System*, which he wrote as a student at the University of Edinburgh.[209] Although his desire to solve an engineering problem initially motivated his research, he soon began to understand his work's legal, political, and social implications.[210] In contrast to Free Haven and Publius, Freenet

202. *Id.*
203. *Id.*
204. *Id.*
205. *Id.*
206. Free Network Project, *supra* note 139.
207. Langley, *supra* note 124, at 123.
208. Lisa Godson, *Geek or Guru? Ian Clarke, the Irish Inventor of Freenet, Has a Difficult Balancing Act to Perform*, Sunday Times (London), Feb. 3, 2002, LEXIS, News & Bus. (profiling Ian Clarke). To critics, Clarke is a "bogeyman" intent on destroying the traditional intellectual property regime in the name of freedom of expression, while to his advocates, he is a champion of free speech. *Id.*
209. *See* Free Network Project, People, *at* http://freenet.sourceforge.net/index.php?page=people (last visited Oct. 14, 2003).
210. "'I just think to me the technical and political aspects were not separate. They were basically the same thing.'" Godson, *supra* note 208 (quoting Ian Clarke). Clarke has also stated: "[My motivation was] [n]ot to create havoc with copyright or even a way around censorship. . . . I was fascinated by complex systems which consisted of individuals following simple rules, where no one individual was

attempts to protect online freedom of expression in absolute terms through the provision of anonymous communication without limits. Because Freenet is easier to use than Free Haven and Publius, and thus is the network that general users are most likely to adopt, it holds the most potential for growth of the three networks. But it also poses the greatest threat to law enforcement.[211]

Freenet consists of a network of "node operators"—the equivalent of Free Haven's and Publius's servers.[212] Its developers have attempted to engineer anonymity into the network primarily through the use of encryption and routing. They encourage authors and publishers to encrypt all files before inserting them onto the network—a strategy that not only provides anonymity, but that may also protect the network from liability because the developers do not have knowledge of the files' contents as the files are uploaded (this

---

fundamental to the operation of the system." Karen Heyman, *Napster, Round 2: Genie 1, Bottle 0*, L.A. Weekly, May 26–June 1, 2000, LEXIS, News &Bus. (quoting Ian Clarke).

211. For legal analyses of Freenet, particularly focusing on the threat it poses to the traditional copyright regime, see Ryan Roemer, *The Digital Evolution: Freenet and the Future of Copyright on the Internet*, 2002 U.C.L.A. J.L. Tech. 5 (examining the technology of Freenet in the context of efforts to develop p2p networks that withstand both legal and technological attack and considering how p2p technology tests the limits of copyright law and content owners' ability to restrict "full-fledged information anarchy" on the Internet); Jeffrey L. Dodes, Note, *Beyond Napster, Beyond the United States: The Technological and International Legal Barriers to On-Line Copyright Enforcement*, 46 N.Y.L. Sch. L. Rev. 279, 309–16 (2002–03) (concluding that the solution to the problem of online copyright infringement requires strengthening and broadening current copyright law, developing technological measures to counteract filesharing technologies, and cultivating new business models to offer legal digital music to the public).

212. Anyone who downloads and installs the Freenet software onto her computer may become a node operator. Each node operator donates bandwidth and space on her hard drive for the storage of files published on the network. Clarke et al., *supra* note 50, at 41. While an author wishing to publish a file on Free Haven must identify a publisher, an author wishing to publish a file on Freenet initiates publication simply by encrypting the file, assigning it a "globally unique identifier" (a unique identifying key in the form of a code), and then sending to his own node an insert request with the key and a "time-to-live" value signifying the number of copies of the file to store. *Id.* at 45. The node then checks its own data store to determine whether the key already exists. *Id.* If it does, the insert fails; if it does not, the node looks up the closest key and sends the request to the corresponding node. *Id.* The author then sends the file down the path forged by his initial insert request. *Id.* Then, each node on the path verifies the file against its key and stores the file. *Id.* To retrieve a file, a reader anonymously initiates a data request with the file's key. *Id.* at 44. The requesting node first checks itself to determine if it has the file. *Id.* If it does not, it forwards the request to another node in a "routing table" it maintains, which includes a list of other nodes and the keys it thinks they hold. *Id.* That node checks its own store. *Id.* If it does not have the file, it forwards the request to another node likely to have the file, and so on. *Id.* The chain ends when the request times out or when the file is found. *Id.* If the file is found, the system then retrieves the file. *Id.* It does not, however, send the file directly to the requester. *Id.* Instead, the file is forwarded randomly from the node where it was found through another chain; moreover, it is individually encrypted at each link. *Id.*

technology also protects individual servers from liability because they, too, do not have knowledge of the files on their computers; also, files migrate constantly from node to node).[213] In addition, the routing of insert and data requests through chains of nodes hinders anyone from tracing a request back to the initiating author, publisher, or reader.[214] In a routing chain, each node knows only its immediate predecessor or successor[215]—a structure that may evoke for critics the structure of some terrorist organizations, in which communication takes place through chains of cells that know only of the existence of the cells with which they immediately communicate. Moreover, the first node to which a request is sent does not know whether its predecessor initiated the request or is merely another link in the chain, and the next-to-last node does not know whether its successor is the request's ultimate recipient or merely another link.[216] Finally, the network is engineered so that it is virtually impossible for a node operator to know which files are being stored on her computer at any time.[217]

In contrast to Free Haven's and Publius's developers, Freenet's have not made the engineering of content accountability into the network a priority. Free Haven restricts the free flow of information on its network by requiring a server to identify a publisher who will publish a file before permitting the file to be published, and it allows servers to trade away shares of files they would prefer not to store.[218] Publius restricts the free flow of information on its network by limiting the size of files and choosing to list in its search directory only files it considers "interesting."[219] Freenet, by contrast, permits any node operator to insert any file under any circumstance onto its network.[220]

Nevertheless, to manage resources, Freenet gives storage priority to "popular" files—a criterion measured by the frequency of requests for the file.[221] When a new file is inserted onto a node and is waiting to be stored, the node will accommodate storage of the new file by deleting the least requested file in its storage area, should it lack sufficient storage space.[222] Although the developers hope node operators will donate sufficient storage space to the network to maintain all files indefinitely, the possibility that infrequently requested ones may be automatically deleted could be perceived as a form of censorship of the majority. Indeed, Freenet tells its node operators that because

213. *Id.* at 45.
214. Free Network Project, *supra* note 139.
215. Clarke et al., *supra* note 50, at 43.
216. *Id.*
217. *Id.*
218. *See supra* notes 166–70 and accompanying text.
219. *See supra* notes 199–205 and accompanying text.
220. *See supra* note 212.
221. Clarke et al., *supra* note 50, at 46.
222. *Id.*

content is available only as long as it is popular, they may help limit the popularity of information of which they disapprove by not requesting it and by instructing others not to request it.[223]

Ironically, assuming that most users are more interested in entertainment than politics, this instruction could mean Freenet will become a convenient storage service for popular music and pornography files at the expense of less popular political texts.[224] Indeed, one p2p expert who conducted an unscientific survey of Freenet's contents in 2000 found 1,075 files.[225] Analyzing these files, he developed this profile of the typical Freenet user: "[I]f we were to indulge ourselves and construct a demographic of the average Freenet user from Freenet content, he'd be a crypto-anarchist Perl hacker with a taste for the classics of literature, political screeds, 1980s pop music, Adobe software, and lots of porn."[226] This profile partially contradicts the image of the typical Freenet user as an earnest activist motivated solely by political concerns, as some of Clarke's statements seem to suggest.[227]

Freenet's decision to deemphasize accountability reflects its absolutist philosophy of anonymity. This philosophy derives from one central premise: the free flow of information is essential to the maintenance of democratic society.[228] In its purest form, it requires

---

223. Free Network Project, Freenet Frequently Asked Questions, *at* http://freenet.sourceforge.net/index.php?page=faq (last visited Oct. 14, 2003).

224. Dingledine et al., *supra* note 137, at 160.

225. Jon Orwant, *What's on Freenet?* (Nov. 21, 2000), *at* http://www.openp2p.com/pub/a/p2p/2000/11/21/freenetcontent.html. Orwant observed that of these files, 37.6% were text (including the entire texts of books such as Jean-Jacques Rousseau's *Confessions* and George Orwell's *1984*), 21.9% were audio (including entire albums by artists such as Sinead O'Connor and the Eurythmics); 14.3% were image (the vast majority of which seemed to be pornographic [he did not actually open any of the image files]); 11.3% were software; 3.6% were video (again, the vast majority seemed to be pornographic); and the rest, unknown. *Id.* Among all media, he made the following conclusion: "Overall porn: 15.6%. Overall sex, drugs, and rock and roll: 53.8%." *Id.*

226. *Id.*

227. *See, e.g.*, Free Network Project, The Philosophy Behind Freenet, *at* http://freenet.sourceforge.net/index.php?page=philosophy (last visited Oct. 14, 2003).

228. *Id.* The phrase "information wants to be free" has been a tenet among hackers, cypherpunks, and Internet advocates since the mid-1980s. *See* Roger Clarke, *Information Wants to Be Free*, *at* http://www.anu.edu.au/people/Roger.Clarke/II/IWtbF.html (last visited Oct. 14, 2003) (discussing the origins of the phrase "information wants to be free"). Roger Clarke suggests that Stewart Brand originally used the phrase at the first Hackers' Conference in 1984 and that it subsequently became an essential element of hacker ethics. *Id.* This phrase is most commonly associated with the philosophies of figures such as John Perry Barlow, co-founder of the Electronic Frontier Foundation, who argues that the Internet's characteristics as a medium demand the rejection of the conception of information as property. *See, e.g.*, John Perry Barlow, *The Economy of Ideas*, wired.com (Mar. 1994) (arguing that the emergence of the digital era requires developing a new framework for intellectual property), *available at* http://www.wired.com/wired/archive/2.03/economy.ideas_pr.html.

the rejection of the conception of information as property.[229] Nevertheless, for Clarke, the elimination of the traditional intellectual property regime is not an end in itself, but a consequence of the necessity to ensure total freedom of expression by protecting the free flow of information from surveillance and censorship of any kind—except, of course, the potential "censorship of the majority" that the network itself enables.[230]

In what amounts to Freenet's manifesto, its developers write that freedom of expression is one of the most fundamental individual rights: "So long as everything we see and hear is filtered, we are not truly free. Freenet's aim is to allow two or more people who wish to share information, to do so."[231] In contrast to First Amendment jurisprudence, which places limitations on freedom of expression, they are so committed to this belief that they reject all limitations. The only way to ensure freedom of expression, they argue, is to secure users' anonymity.[232] In this manner, they believe Freenet will play a critical role in promoting freedom of expression in totalitarian societies and protecting it in democratic ones.[233] Chinese dissidents, for example, have already used Freenet to publish an online library of human rights documents;[234] and should the "doomsday scenario" of a full-scale assault on freedom of expression occur in the United States, Freenet will be ready, Clarke insists.[235] Freenet's critics nevertheless claim that its ability to provide anonymity without accountability provides a haven for pirates, pornographers, terrorists, traitors, and disseminators of hate speech.[236] In this anarchist haven, such persons may operate with impunity beyond the reach of the law.[237]

This opposition between Freenet's "positive" and "negative" uses crystallizes the conflict that lies at the center of all anonymity-protecting p2p networks. Efforts to regulate these networks by prohibiting the distribution of illegal materials jeopardize the political expression that the networks attempt to protect by imposing systems of surveillance, control, and censorship. The implementation of these

229. *See* Barlow, *supra* note 228.

230. Free Network Project, *supra* note 227. Clarke has described Freenet users' ability to circumvent copyright restrictions as a "side effect." *See* Godson, *supra* note 208.

231. Free Network Project, *supra* note 227.

232. *Id.*

233. *See* Godson, *supra* note 208.

234. *See* Lee, *supra* note 5, at G1.

235. "'Because of what's been happening legally, and the fact that a lot of the threats that only six months ago were theoretical are now becoming increasingly plausible, we're being forced to explore quite radical ideas . . . so that if the doomsday scenario should occur, we're ready for it.'" Borland, *supra* note 83 (quoting Clarke).

236. John Borland, *Free, Anonymous Information on the Anarchists' Net*, CNET news.com (April 26, 2000) (discussing the development of Freenet), *at* http://news.com.com/2100-1033_3-239756.html.

237. *See* Borland, *supra* note 130.

systems thus has the potential to destroy the very liberty the technology promises. As Lawrence Lessig has written, if the Internet continues to develop "along the lines it has taken so far, it will become a highly regulable space—not the locus of liberty, not a space of no control, but a technology of government and commercial power wired into every aspect of our lives."[238] In Part II, this Note examines through the lens of "Super-DMCA" legislation the difficulties that attempts to regulate anonymity-protecting p2p networks pose.

II. REGULATING ANONYMITY-PROTECTING P2P NETWORKS

As anonymity-protecting p2p networks attempt to resist the panoptic sort, the law has slowly begun to attempt to absorb them within this order. There has been no direct legislation or litigation against these networks yet, but since 2001 several states have proposed or passed "Super-DMCA" bills that might indirectly threaten the legality of anonymity-protecting p2p networks.[239] This part describes the threat that Super-DMCA legislation may pose to the provision of anonymous communication on anonymity-protecting p2p networks.[240] It then discusses the protectability of such communication under the First Amendment guarantees of the right to speak anonymously and the less explicitly articulated right to read anonymously.[241] Finally, it considers the advantages and disadvantages of protecting such communication.[242]

A. *Super-DMCA Legislation*

Since 2001, and with little fanfare, several states have proposed or enacted measures designed to criminalize the possession, use,

238. Lawrence Lessig, *supra* note 123, at 211. A development that occurred too recently to incorporate fully into this Note illustrates the central role that anonymity-protecting p2p networks may play in future conflicts between freedom of expression and alleged illegality. *See* John Schwartz, *File Sharing Pits Copyright Against Free Speech*, N.Y. Times, Nov. 3, 2003, at C1. In the fall of 2003, advocates published on various websites thousands of internal emails and other documents belonging to Diebold Election Systems, a company that manufactures electronic voting machines. *Id.* These documents include discussions of technological and security problems with the machines' software. *Id.* Arguing that unauthorized publication of the documents constitutes copyright infringement, Diebold has sent cease-and-desist letters to the publishers it has been able to identify—including Aviel D. Rubin, one of the developers of Publius. *Id.* In November, advocates published the documents on Freenet, where they cannot be censored. *Id.* As of this writing, Diebold has not filed a claim against Freenet.

239. Fred von Lohmann, Electronic Frontier Foundation, State "Super-DMCA" Legislation: MPAA's Stealth Attack on Your Living Room, *at* http://www.eff.org/IP/DMCA/states/200304_sdmca_eff_analysis.php (last visited Oct. 14, 2003).

240. *See infra* Part II.A.

241. *See infra* Part II.B.

242. *See infra* Part II.C.

development, and distribution of "unlawful communication and access devices."[243] Generally in the form of amendments to existing state laws that criminalize the theft of cable and satellite transmissions, most of these measures are based on a model bill drafted by the MPAA.[244] This bill provides that a person commits a criminal offense if she knowingly, and with the intent to defraud a communication service provider, engages in any of the following activities: first, possession, use, development, or distribution of a communication device to steal a communication service or to receive, disrupt, or transmit a communication service without the communication service provider's consent;[245] second, possession, use, development, or distribution of a communication device "to conceal or to assist another to conceal from any communication service provider, or from any lawful authority, the existence of the place of origin or destination of any communication, provided that such concealment is for the purpose of committing a violation" of the sort prohibited above;[246] third, modification of a communication device for any of the above purposes; fourth, possession, use, development, or distribution of any "unlawful access device;"[247] fifth, possession, use, development, or distribution of plans or instructions for making a communication or unlawful access for any of the above purposes.[248]

According to the MPAA, these measures are necessary to combat digital piracy because new hacking technologies have vitiated existing laws protecting cable and satellite transmissions from unauthorized use.[249] Critics, however, have condemned the measures as unjustified restrictions on the rights of computer users.[250] The Electronic Frontier Foundation ("EFF"), a nonprofit organization dedicated to the protection of digital rights, for example, has described the measures as a "stealth effort to dramatically expand the reach of the federal Digital Millennium Copyright Act."[251] These Super-DMCA bills, the

243. *See* von Lohmann, *supra* note 239. For the definition of "unlawful communication device," see *infra* note 256 and accompanying text.

244. Broadband & Internet Security Task Force, Draft Model Communications Security Legislation (April 11, 2003), *at* http://www.eff.org/IP/DMCA/states/sdmca_model_final.pdf [hereinafter *Draft Model Legislation*].

245. *Id.* at 2.

246. *Id.*

247. *Id.*

248. *Id.*

249. Declan McCullagh, *DMCA Critics Decry State-Level Proposals*, CNET news.com (Mar. 28, 2003) (discussing criticism of state bills designed to stop theft of cable and cellular phone services that are arguably broader in scope than the Digital Millennium Copyright Act), *at* http://news.com.com/2100-1028-994667.html.

250. *Id.*

251. von Lohmann, *supra* note 239; *see also* Mike Godwin, *A Brief Analysis of the Super "DMCA" (The Draft Model Communications Security Act)*, Public Knowledge, *at* http://www.publicknowledge.org/reading-room/documents/policy/super-dmca-analysis.html (last visited Oct. 14, 2003).

EFF maintains, are redundant as penalties for copyright infringement on the Internet and the theft of cable and satellite transmissions.[252] Moreover, they "represent an unprecedented intrusion into the living rooms of law-abiding citizens, giving communication service providers unilateral control over what you can connect to your home entertainment systems."[253]

Of particular concern for the purposes of this Note is the model bill's second provision, which prohibits communication devices that conceal the existence or place of origin or destination of any communication—provided that the person has the intent to defraud a communication service provider and that the purpose of the concealment is the theft of communication service. The MPAA added this limitation in response to criticism that the bill was too broad.[254] Nevertheless, the various state bills that have been proposed or enacted have incorporated this limitation "inconsistently or not at all."[255] Moreover, the model bill defines "communication devices" broadly as "[a]ny type of electronic mechanism, transmission lines or connections and appurtenances thereto, instrument, device, machine, equipment, technology or software which is capable of intercepting, transmitting, re-transmitting, acquiring, decrypting or receiving any communication service."[256] Because of the broad scope of this definition, the provision may criminalize a host of currently lawful technologies that enable the anonymous authoring, publishing, storing, and reading of files on the Internet. Affected technologies might include home-networking equipment because it contains firewall features that conceal the origin and destination of Internet communication, certain types of email and browsing encryption devices such as Anonymizer, virtual private networking software used by businesses to enable secured communication with offsite employees, and anonymity-protecting p2p networks.[257] In fact, in the spring of 2003, Freenet users posted messages to a Freenet chat room querying whether these statutes may make Freenet illegal—or whether they violate a constitutional "right to anonymity."[258]

---

252. von Lohmann, *supra* note 239.

253. *Id.*

254. Godwin, *supra* note 251.

255. *Id.* States that have proposed or enacted bills include: Arkansas, Colorado, Delaware, Florida, Georgia, Illinois, Massachusetts, Maryland, Michigan, Oregon, Pennsylvania, South Carolina, Tennessee, Texas, and Virginia. For a useful tabular summary of the bills and their current status, see Electronic Frontier Foundation, State-level "Super DMCA" Initiatives Archive, *at* http://www.eff.org/IP/DMCA/states (last visited Oct. 15, 2003). For a similar tabular summary, see Public Knowledge, *at* http://www.publicknowledge.org/reading-room/documents/policy/super-dmcas/super-dmcas-table.html (last visited Oct. 15, 2003).

256. *Draft Model Legislation*, *supra* note 244, at 5.

257. *Id.*

258. *See* Free Network Project, [freenet-chat] New Law May Make Freenet Illegal,

B. *The Constitutional Right to Anonymity on the Internet*

Advocates ground their justifications for the legality of anonymity-protecting p2p networks in the face of threats such as Super-DMCA legislation in the claim that the First Amendment protects the "right to anonymity."[259] The First Amendment, however, does not explicitly guarantee a right to anonymity as such.[260] Nevertheless, the Supreme Court has interpreted its guarantees of freedom of expression and assembly to protect anonymous expression within certain limits.[261] A. Michael Froomkin, one of the most important legal scholars to have addressed this issue, has observed that the Court has often reiterated what it terms the "profound national commitment to the principle that debate on public issues should be uninhibited, robust, and wide-open," which would seem to protect anonymous expression.[262] But he goes on to observe that whether a right to anonymity exists in the First

---

at http://hawk.freenetproject.org:8080/pipermail/chat/2003-March/000305.html (last visited Oct. 15, 2003).

259. *See, e.g.*, Dingledine, *supra* note 157, at 37–44.

260. The First Amendment provides: "Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances." U.S. Const. amend. I. For surveys of the right to anonymity under the First Amendment, see A. Michael Froomkin, *Flood Control on the Information Ocean: Living With Anonymity, Digital Cash, and Distributed Databases*, 15 J.L. & Com. 395, 427–43 (1996) (arguing in part that given the importance of anonymity to free speech, electronic commerce, and privacy, the debate over anonymity on the Internet is a debate about the degree of political and economic freedom that will be cultivated, or tolerated, in a modern society); David W. Ogden & Joel A. Nichols, *The Right to Anonymity Under the First Amendment*, 49 Fed. Law. 44 (2002) (summarizing the anonymous expression doctrine); Michael H. Spencer, *Anonymous Internet Communication and the First Amendment: A Crack in the Dam of National Sovereignty*, 3 Va. J.L. & Tech. 1 (1998) (discussing the development of First Amendment jurisprudence as it relates to anonymous communication and whether the Constitution can adequately govern the coupling of anonymity and Internet communication); Jennifer B. Wieland, Note, *Death of Publius: Toward a World Without Anonymous Speech*, 17 J.L. & Pol. 589 (2001) (tracing the history of anonymous expression in the United States).

261. A. Michael Froomkin, *Legal Issues in Anonymity and Pseudonymity*, 15 Info. Soc'y 113, 117 (1999) (arguing that legal and constitutional constraints on anonymous communication should be considered along with policies motivating regulation, as well as regulation's effects).

262. Froomkin, *supra* note 260, at 428. This article is one of the comprehensive writings on the subject. Some of Froomkin's other related publications include: *The Constitution and Encryption Regulation: Do We Need a "New Privacy"?*, 3 N.Y.U. J. Legis. & Pub. Pol'y 25 (1999) (examining the regulation of cryptography); *The Death of Privacy?*, 52 Stan. L. Rev. 1461 (2000) (describing "privacy-destroying" technologies by governments and businesses to which the law has yet to respond effectively and discussing attempts to develop legal responses to the assault on privacy, including self-regulation, privacy-enhancing technologies, data-protection law, and property-rights based solutions); *habermas@discourse.net: Toward a Critical Theory of Cyberspace*, 116 Harv. L. Rev. 749 (2003) (analyzing Internet standards processes and offering preliminary speculations about how new technology might help widen, deepen, and enrich Habermasian discourse).

Amendment remains unclear as a general matter because the difficult cases are the ones in which the courts make exceptions to fit facts that do not sit comfortably within the rules that ordinarily apply.[263]

The scope of the right to anonymity in the context of anonymity-protecting p2p networks would qualify as one of the difficult cases of which Froomkin speaks. Advocates argue that these networks protect anonymity on the Internet against the threats posed by the expansion of the panoptic sort through the implementation of the online surveillance measures and initiatives discussed in Part I.[264] One might grid each manifestation of anonymity on these networks as the intersection of two axes: what one might call the "user axis" and the "content axis." First, as discussed previously, these networks serve at least four types of users: (1) the reader (a user who retrieves a file); (2) the server or node operator (a user on whose computer a file is stored); (3) the publisher (a person who inserts a file into the network, who may or may not be the author); and, (4) the author (the user who originally produces a file).[265] Second, these users engage with at least two types of files: files that may be classified as political content and files that may be classified as nonpolitical content.

To lay the foundation for this Note's conclusions regarding the regulation of anonymity-protecting p2p networks, it is necessary first to examine the constitutional scope of the right to anonymity. For this purpose, it is useful to define user functions in terms of the two categories defined by jurisprudence on the right to anonymity: the right to read anonymously[266] and the right to speak anonymously,[267] which encompasses author, server, and publisher anonymity. Woven into this discussion is another critical distinction in jurisprudence on the right to anonymity: the distinction between anonymous political speech, which courts accord the highest level of protection, and anonymous nonpolitical speech, which courts accord a lower degree of protection.[268]

---

263. Froomkin, *supra* note 260, at 428.

264. "The drive for absolute privacy online has bubbled up from several different sources in the past few years, as technology for tracing surfers online has improved, government monitoring tools such as Carnivore and Echelon have come to light, and file-trading services such as Napster have entered the spotlight." Borland, *supra* note 130.

265. *See* Dingledine et al., *supra* note 137, at 163. Note also that users may assume more than one function for the same transaction.

266. *See infra* Part II.B.1.

267. *See infra* Part II.B.2.

268. *See* Froomkin, *supra* note 261, at 117–19. On the rationale for according political speech the highest constitutional protection, see especially the work of Alexander Meiklejohn, including *Free Speech and Its Relation to Self-Government* (1948) and *Political Freedom: The Constitutional Powers of the People* (1965).

1. The Constitutional Right to Read Anonymously

The Supreme Court has not specifically recognized a right to read anonymously. Julie E. Cohen, who has developed a theory of the constitutional right to read anonymously, however, has persuasively argued that the most direct support for such a right exists in a series of cases decided during the Cold War period.[269]

In *United States v. Rumely*, for example, the Court held that the House Select Committee on Lobbying Activities was not authorized to request the names of purchasers of books published by a certain political organization.[270] "The finger of government leveled against the press is ominous. Once the government can demand of a publisher the names of the purchasers of his publications," Justice Douglas wrote in his concurrence, "the free press as we know it disappears. Then the spectre of a government agent will look over the shoulder of everyone who reads.... Some will fear to read what is unpopular, what the powers-that-be dislike."[271] The possibility that one's private reading habits may become public without one's consent, he concluded, has the potential to chill intellectual inquiry.[272]

Similarly, in *Lamont v. Postmaster General*, the Court held that a federal statute requiring the post office to detain and destroy unsealed mail that examiners classified as "communist political propaganda" from certain foreign nations—unless addressees returned a reply card indicating their desire to receive the mail—constituted "a limitation on the unfettered exercise of the addressees' First Amendment rights."[273] In his concurrence, Justice Brennan further concluded that

---

269. *See* Julie E. Cohen, *A Right to Read Anonymously: A Closer Look at "Copyright Management" in Cyberspace*, 28 Conn. L. Rev. 981, 1007–08 (1996) (discussing in part the sources and justifications for the individual right to read anonymously and arguing that reading is so closely connected with speech and freedom of thought that the First Amendment should be interpreted to guarantee this right) [hereinafter Cohen, *Right to Read*]. This Note's discussion of the right to read anonymously is indebted to this important and influential article. Some of Cohen's other major publications in this area include *DRM and Privacy*, 18 Berkeley Tech. L.J. 575 (2003) (identifying the privacy interests individuals enjoy in their intellectual activities, exploring how certain implementations of digital rights management technologies may threaten those interests, and considering the appropriate scope of legal protection for privacy in this context); *Examined Lives: Informational Privacy and the Subject as Object*, 52 Stan. L. Rev. 1373 (2000) (exploring the theoretical challenges to informational privacy protection and advocating the design of legal and technological tools for strong data privacy protection) [hereinafter Cohen, *Examined Lives*].

270. United States v. Rumely, 345 U.S. 41, 42 (1953) (holding that the House Committee authorized to investigate "lobbying" was not authorized to request the names of individuals who purchased books of "particular political tendentiousness" for further distribution and thus that the conviction of a witness who refused to produce these names could not be upheld).

271. *Id.* at 57 (Douglas, J., concurring).

272. *Id.*

273. Lamont v. Postmaster Gen., 381 U.S. 301, 305 (1965).

the "right to receive publications" is a fundamental right on the ground that the dissemination of ideas is meaningless if readers are not free to receive and thus engage with them.[274]

Finally, in *Stanley v. Georgia*, the Court struck down a state statute that criminalized the private possession of obscene materials on the ground that the First Amendment protects the right to receive information and ideas regardless of their social worth.[275] The Court held that the right that the defendant was asserting was the right to read or observe what he pleased to satisfy his intellectual and emotional needs in his own home.[276] It concluded that this right is not only well established, but fundamental to a free society:[277] "Our whole constitutional heritage rebels at the thought of giving government the power to control men's minds."[278] As in *Rumely* and *Lamont*, the Court suggested a connection between private or anonymous receivership and the encouragement of intellectual, emotional, or personal autonomy.[279]

As these and other opinions suggest, justification for the right to read anonymously is based on at least three grounds. First, it is integrally bound up with the right to speak anonymously, which enjoys explicit constitutional support.[280] Second, unauthorized disclosure of a person's reading choices may have a chilling effect on expression by leading to both censorship and self-censorship of controversial, questionable, or unpopular expression. In this respect, it may result in a "barren marketplace of ideas that [has] only sellers and no buyers," as Justice Brennan observed.[281] Third, a person's decision to withhold his name is just as expressive of his identity as his choices about what he reads.[282] In this respect, it can be interpreted as an important aspect of the process of self-definition and self-actualization.[283]

Yet, the right to read anonymously has been taken for granted as a discrete constitutional guarantee because the systematic monitoring of people's reading habits was technologically impractical until the development of the Internet. Surveillance technologies have enabled an unprecedented degree of intrusion into readers' private intellectual activities through the monitoring and analysis of their online browsing

274. *Id.* at 308 (Brennan, J., concurring).

275. Stanley v. Georgia, 394 U.S. 557, 563–64 (1969) (holding that the First and Fourteenth Amendments prohibit making mere private possession of obscene materials a crime).

276. *Id.* at 565.

277. *Id.* at 564.

278. *Id.* at 565.

279. *See supra* notes 270–74 and accompanying text.

280. *See* Froomkin, *supra* note 261, at 121.

281. Lamont v. Postmaster Gen., 381 U.S. 301, 308 (1965); *see also* Cohen, *Right to Read*, *supra* note 269, at 1010.

282. Cohen, *Right to Read*, *supra* note 269, at 1012.

283. Froomkin, *supra* note 261, at 121.

activities.[284] Until the development of these technologies, however, it was not cost-efficient for interested parties to monitor readers' reading choices. Indeed, as Justice Thomas states in his concurrence in *McIntyre v. Ohio Elections Commission*, a case examined in detail in Part II.B.2., "[i]t is only an innovation of modern times that has permitted the regulation of anonymous speech."[285] For example, marketers compile user profiles for the very reason that they are expressive of the user's identity.[286] Similarly, intelligence agencies assume that what a user reads offers valuable insight into her political motivations. As a result, as Cohen suggests, First Amendment doctrine must be reshaped to ensure that the new surveillance technologies do not vitiate free speech protections.[287]

Toward this end, one state supreme court recently built on the foundation supplied by some of the previously mentioned Supreme Court cases to recognize explicitly the constitutional right to read anonymously. In *Tattered Cover, Inc. v. City of Thornton*, a bookstore sought to restrain a municipal police department from executing a search warrant for its customer purchase records.[288] Denying the warrant in an *en banc* decision, the Supreme Court of Colorado concluded that the city failed to establish that its need for the records was sufficiently compelling to outweigh the constitutional harm that the execution of the warrant would have caused.[289] Citing *Stanley* and *Lamont*, among other cases, the court held that the First Amendment protects a wide range of activities, including the right to receive information and ideas.[290] Anonymity is often essential to the exercise of this right because of the chilling effects that the disclosure of identity can induce.[291] Thus, the First Amendment protects "the individual's right to purchase and read whatever books she wishes to, without fear that the government will take steps to discover which books she buys, reads, or intends to read."[292] To date, other state courts have not recognized the constitutional right to read anonymously so boldly.

2. The Constitutional Right to Speak Anonymously

In contrast to the right to read anonymously, the Supreme Court has recognized explicitly the right to speak anonymously. In *McIntyre*

284. Cohen, *Right to Read*, *supra* note 269, at 1015.
285. McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 367 (1995) (Thomas, J., concurring), *cited in* Froomkin, *supra* note 261, at 121.
286. Cohen, *Right to Read*, *supra* note 269, at 1012.
287. *Id.* at 1015.
288. Tattered Cover, Inc. v. City of Thornton, 44 P.3d 1044, 1050 (Colo. 2002).
289. *Id.* at 1063.
290. *Id.* at 1051–52.
291. *Id.* at 1052.
292. *Id.* at 1053.

v. Ohio Elections Commission, the plaintiff was fined for distributing anonymous handbills in violation of an Ohio statute prohibiting the distribution of anonymous campaign literature.[293] The state argued that its overriding interest in preventing fraudulent or libelous conduct justified the statute. The plaintiff countered that the contested statute violated the First Amendment. The Court held that the statute contained no limiting language and that other statutes principally protected against fraud and libel.[294] Thus, the state's interest in preventing fraud and libel was insufficient to justify an additional statutory prohibition.[295]

More broadly, the Court recognized a right to speak anonymously that protects anonymous political and literary expression.[296] Indeed, in two long footnotes, it sketched an honorable history of political and literary figures who have published texts anonymously or pseudonymously.[297] It established at minimum two basic propositions regarding anonymous expression.[298] First, anonymity may be justified by legitimate reasons, including fear of economic or political retaliation, apprehension about social ostracism, and a wish to protect one's privacy.[299] Second, a speaker may not be compelled to identify herself absent a strong justification.[300] Nevertheless, even under a broad interpretation of *McIntyre*, the right to speak anonymously does not protect fraudulent or other illegal conduct.[301] Toward this end, Justice Ginsburg emphasized in her concurrence that the Court left open the possibility that a state may impose identification requirements in certain limited circumstances.[302] She did not, however, specify what those circumstances might be.

In *Buckley v. American Constitutional Law Foundation, Inc.*, the

293. McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 337–38 (1995). For analyses of *McIntyre*, *see, e.g.*, Caroline E. Strickland, *Applying* McIntyre v. Ohio Elections Commission *to Anonymous Speech on the Internet and the Discovery of John Doe's Identity*, 58 Wash. & Lee L. Rev. 1537, 1583 (2001) (concluding that *McIntyre*'s protection of anonymous speech has limits demanding a thorough consideration of interests of plaintiffs who have been defamed on the Internet); Lee Tien, *Who's Afraid of Anonymous Speech?* McIntyre *and the Internet*, 75 Or. L. Rev. 117, 126–28 (1996) (concluding that because a substantial amount of expressive activity on the Internet is associational, broad regulation of Internet anonymity is likely to be unconstitutional); *see also* Amy Constantine, Note, *What's in a Name?* McIntyre v. Ohio Elections Commission*: An Examination of the Protection Afforded to Anonymous Political Speech*, 29 Conn. L. Rev. 459 (1996) (analyzing *McIntyre* and its implications).

294. *McIntyre*, 514 U.S. at 350–53.

295. *Id.* at 349.

296. *Id.* at 342–43.

297. *Id.* at 341 n.4, 343 n.6.

298. Tien, *supra* note 293, at 126.

299. *Id.*

300. *Id.*

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

302. *Id.*

Court reaffirmed the right to speak anonymously.[303] It held that a Colorado statute that required persons who were circulating ballot initiative petitions to wear a name identification badge violated the First Amendment.[304] The state argued that the badge requirement enabled the public to identify, and the state to apprehend, petition circulators who violated the law.[305] The Court, however, concluded that the requirement restrained speech even more than distributing anonymous campaign literature did because it compelled identification at the very moment the circulator's interest in anonymity was the greatest.[306] Thus, the requirement was not the type of limited identification requirement that *McIntyre* left open.[307]

The Court has not explicitly extended the right to speak anonymously that it affirmed in *McIntyre* and *Buckley* to expression on the Internet. Lower federal courts, however, have done so.[308] Most Internet anonymity cases have involved plaintiffs who request subpoenas to obtain from ISPs the identity of Internet users who anonymously made allegedly defamatory statements or posted allegedly infringing content online. As the district court observed in *Columbia Insurance Co. v. seescandy.com*, the Internet is a medium in which users can commit tortious acts like defamation or copyright or trademark infringement without revealing their identities.[309] Thus, it may be particularly difficult for injured parties to seek redress for the harms they have suffered.[310] Nevertheless, the court must balance this need with the "legitimate and valuable right to participate in online forums anonymously or pseudonymously."[311] This right not only fosters communication and debate, but it also enables users to obtain information about potentially sensitive topics without the fear of harassment or embarrassment.[312] The court adopted a four-factor balancing test to determine whether a plaintiff seeking to obtain the identity of an anonymous Internet user during the discovery process is permissible.[313] Under this test, the plaintiff must: (1) identify the targeted user with enough specificity to enable the court to determine

303. Buckley v. Am. Constitutional Law Found., 525 U.S. 182 (1999).
304. *Id.* at 200.
305. *Id.* at 198.
306. *Id.* at 199.
307. *Id.* at 199–200.
308. *See, e.g.*, Doe v. 2TheMart.com, 140 F. Supp. 2d 1088, 1095–97 (W.D. Wash. 2001) (adopting a four-factor balancing test to determine whether plaintiff is permitted to seek to obtain the identity of an anonymous Internet user during the discovery process); Columbia Ins. Co. v. seescandy.com, 185 F.R.D. 573, 578–80 (N.D. Cal. 1999) (adopting a four-factor balancing test to determine whether plaintiff is permitted to obtain the identity of an anonymous Internet user during the discovery process).
309. *Columbia Ins. Co.*, 185 F.R.D. at 578.
310. *Id.*
311. *Id.*
312. *Id.*
313. *See id.* at 578–80.

whether the user is an entity amenable to suit; (2) identify all previous efforts it has taken to locate the user; (3) establish that its claim could withstand a motion to dismiss; and (4) file a discovery request justifying its need for the information it seeks.[314]

Similarly, in *Doe v. 2TheMart.com*, an Internet company requested a subpoena of an ISP that operated a website for investors.[315] The company's purpose was to obtain the identity of certain Internet users.[316] The website included bulletin boards on which users could anonymously post messages about various companies.[317] On the bulletin board devoted to the plaintiff company, certain users anonymously had posted unflattering messages about the company's policies and its officers.[318]

The court adopted a four-factor balancing test similar to the one adopted in *Columbia Insurance Co.* Under this test, (1) the plaintiff must have issued the subpoena in good faith and for a proper purpose; (2) the information the plaintiff seeks must relate to an essential core claim or defense; (3) the identifying information must be directly relevant to the claim or defense; and (4) the plaintiff must have been unable to obtain information sufficient to establish or to disprove the claim or defense from another other source.[319] Applying the test to the facts of the case, the court granted the users' motion to quash the subpoena.[320]

Moreover, citing *McIntyre* and *Buckley*, the *Doe* court held explicitly that the First Amendment protects the anonymity of Internet expression.[321] The First Amendment guarantee of free speech extends to the Internet, and the right to speak anonymously is a component of this guarantee.[322] Online anonymity benefits society because it encourages the "rich, diverse, and far ranging exchange of ideas."[323] If plaintiffs could strip Internet users of this anonymity, the result would be a chilling effect on online speech and thus on fundamental First Amendment rights.[324] In this regard, the court emphasized that although *McIntyre* and *Buckley* hold that the state's interest in enforcing the law may justify the imposition of limited identification requirements, and thus demarcate the outer boundaries

314. *Id.*
315. Doe v. 2TheMart.com, 140 F. Supp. 2d 1088, 1090 (W.D. Wash. 2001).
316. *Id.*
317. *Id.*
318. *Id.*
319. *Id.* at 1095–97.
320. *Id.* at 1095–98.
321. *Id.* at 1091–92.
322. *Id.* at 1092.
323. *Id.*
324. *Id.* at 1093.

of the right to speak anonymously, this right remains after speech because it would otherwise hold little practical value.[325]

In contrast to these opinions, in 2003 the D.C. District Court issued two decisions that define the contours of the right to speak anonymously more narrowly, but that nevertheless may protect expression on anonymity-protecting p2p networks dedicated to the distribution of political content. In both decisions, the court distinguished anonymous political expression, which it held was potentially protectable, from anonymous nonpolitical expression, which it suggested was less protectable. In *In re Verizon Internet Services, Inc.* ("*Verizon I*") the court ordered an ISP to disclose to the plaintiff, the RIAA, the identity of a user who had anonymously downloaded over six hundred copyrighted songs from the p2p filesharing network Kazaa without the copyright holders' permission.[326] The court concluded that "this is not a case where Verizon's customer is anonymously using the Internet to distribute speeches of Lenin, Biblical passages, educational materials, or criticisms of the government—situations in which assertions of First Amendment rights more plausibly could be made."[327] It justified this conclusion by noting that "the Supreme Court [has] explained . . . the purpose of protecting anonymous expression is to safeguard those 'who support causes anonymously' and those who 'fear economic or official retaliation,' 'social ostracism,' or an unwanted intrusion into 'privacy.'"[328]

After the court issued this decision, the RIAA served another subpoena on Verizon. In *In re Verizon Internet Services, Inc.* ("*Verizon II*"), the court denied Verizon's motion to quash the subpoena.[329] In a more lengthy discussion of the right to anonymity, it acknowledged that the Supreme Court has recognized the right to speak anonymously in *McIntyre* and *Buckley* and that lower courts

325. *Id.*

326. *In re* Verizon Internet Servs., Inc., 240 F. Supp. 2d 24, 26 (D.C. Cir. 2003) (granting the RIAA's motion to enforce a subpoena served pursuant to the Digital Millennium Copyright Act on an ISP and seeking to identify the alleged infringer on the ground that the Act's subpoena authority extended to ISPs with limited liability); *see also* Katyal, *supra* note 17.

327. *Verizon I*, 240 F. Supp. 2d at 43. Note that *Verizon I* involved a question of apparent anonymity, in which the system enables the identification of a user, not true anonymity, in which the system does not permit such identification. Thus, the decision would be unenforceable if applied to anonymity-protecting p2p networks like Free Haven, Publius, or Freenet, which allow true anonymity.

328. *Id.* (citing Watchtower Bible & Tract Soc'y of N.Y., Inc. v. Vill. of Stratton, 536 U.S. 150, 166 (2002)).

329. *In re* Verizon Internet Servs., Inc., 257 F. Supp. 2d 244, 247 (D.C. Cir. 2003) (denying an ISP's motion to quash a subpoena served on it under the subpoena power authorized by the Digital Millennium Copyright Act on the ground that such subpoena power did not violate the case or controversy requirement of Article III and provided sufficient safeguards and judicial supervision to protect Internet users' First Amendment rights).

have extended this right to expression on the Internet.[330] It concluded, however, that when the Court has held that the First Amendment protects the right to speak anonymously, it has done so in cases that involve "core First Amendment expression"—that is, political expression.[331] Developing a regulatory regime applicable to anonymity-protecting p2p networks that would prevent the anonymous distribution of unprotected expression, without restraining the anonymous distribution of protected expression, and that would also survive judicial scrutiny—especially the "exacting scrutiny" afforded to core political expression—is a daunting task.[332]

C. *Arguments For and Against the Protection of Anonymous Communication*

Because of the difficulty in distinguishing for the purposes of regulation protected from unprotected anonymous expression on anonymity-protecting p2p networks, formulating a normative vision on which to build a regulatory regime is imperative. This section consequently considers the two most important arguments against and for the provision of anonymity on these networks.[333]

First, critics argue that anonymous communication on p2p networks vitiates the quality of debate. Because one cannot know the identity of an anonymous speaker, it is difficult to identify her self-interests and to analyze her arguments fully.[334] Moreover, the absence of identification encourages texts to become "louder" in order to be heard. Discourse will become more distorted, shrill, and simplistic, and the lack of any kind of gatekeeping will encourage the proliferation of rumor, disinformation, and hate speech.[335]

By contrast, others argue that anonymity-protecting p2p networks may actually enrich the quantity and quality of expression. They enable users who wish to express their viewpoints without disclosing

---

330. *Id.* at 258–59.

331. *Id.* at 259–60. Even though this conclusion is true, *McIntyre* did not, in fact, restrict protection of anonymous expression to anonymous political expression. Indeed, after the Court's recitation of the facts, it began its analysis by emphasizing the social benefits of anonymous literary expression. *See* McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 341–42 (1995). Thus, with respect to this issue, the court read *McIntyre* too narrowly.

332. The Court applies "exacting scrutiny" to a statute that regulates core political expression, and it will uphold such a statute only if it is "narrowly tailored" to serve an "overriding state interest." *McIntyre*, 514 U.S. at 347.

333. Marx's article, *What's in a Name? Some Reflections on the Sociology of Anonymity*, provides an excellent, concise introduction to the rationales for and against anonymous communication. *See* Marx, *supra* note 148, at 99. For another summary focusing on arguments in favor of anonymous communication, see Mike Godwin, Cyber Rights: Defending Free Speech in the Digital Age 154–57 (2003).

334. Froomkin, *supra* note 260, at 402–03.

335. *See* Eli Noam, *The Web Is Bad for Democracy* (Aug. 29, 2002), *at* http://www.mail-archive.com/do-wire@tc.umn.edu/msg00529.html.

their identities to speak, and they similarly enable users who wish to retrieve information without revealing their identities the opportunity to do so. These users may include whistleblowers afraid of losing their jobs, political dissidents fearful of being persecuted for expressing their beliefs, journalists wary of publishing investigative reports because they are concerned about being forced to reveal sources, persons seeking information about socially sensitive subjects such as alcohol or drug abuse, or users who simply prefer that their communications remain private.[336]

In addition to enhancing the quantity of expression, anonymity may enhance its quality in certain circumstances. First, anonymity encourages users to speak and read with confidence because they can do so without fear or embarrassment.[337] As the Court held in *McIntyre*, a person may choose to remain anonymous out of fear of economic or official retaliation, concern about social ostracism, or a desire to preserve her privacy: "Whatever the motivation may be . . . the interest in having anonymous works enter the marketplace of ideas unquestionably outweighs any public interest in requiring disclosure as a condition of entry."[338] Second, anonymity prevents others from judging users on the basis of their race, gender, sexual orientation, disability, class, or other identifying characteristics, and subjecting them to dismissal on the basis of stereotyping. Instead, they must be judged on the basis of their expression.[339] This argument finds support in *First National Bank of Boston v. Bellotti*, in which the Court held that the "inherent worth of . . . speech in terms of its capacity for informing the public does not depend upon the identity of its source, whether corporation, association, union, or individual."[340] This argument also finds support in *McIntyre*. As the Court held, "an

336. Declan McCullagh, *Technology as Security*, 25 Harv. J.L. & Pub. Pol'y 129, 136 (2001) (discussing how technology has begun to supplant law and arguing that this may be a positive and inevitable development); *see also* Cohen, *Examined Lives*, *supra* note 269, at 1425 ("A realm of autonomous, unmonitored choice, in turn, promotes a vital diversity of speech and behavior. The recognition that anonymity shelters constitutionally-protected decisions about speech, belief, and political and intellectual association—decisions that otherwise might be chilled by unpopularity or simple difference—is part of our constitutional tradition."). For documentation of concrete efforts by governments to stifle journalists, see Julia Scheeres, *Online Journalists Jailed in Cuba*, wired.com (Mar. 20, 2003) (discussing the Cuban government's imprisonment of journalists, most of whom publish on the Internet, as part of a larger crackdown against political opposition), *at* http://www.wired.com/news/politics/0,1283,58128,00.html.

337. *Cf.* Godwin, *supra* note 333, at 155–56.

338. McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 341–42 (1995); *see also* Talley v. California, 362 U.S. 60, 64 (1960) ("Anonymous pamphlets, leaflets, brochures and even books have played an important role in the progress of mankind. Persecuted groups and sects from time to time throughout history have been able to criticize oppressive practices and laws either anonymously or not at all.").

339. *See McIntyre*, 514 U.S. at 342–43; *see also* Lessig, *supra* note 123, at 33; Froomkin, *supra* note 260, at 410.

340. First Nat'l Bank of Boston v. Bellotti, 435 U.S. 765, 777 (1978).

advocate may believe her ideas will be more persuasive if her readers are unaware of her identity. Anonymity thereby provides a way for a writer who may be personally unpopular to ensure that readers will not prejudge her message simply because they do not like its proponent."[341] And third, anonymity may promote the public interest by facilitating the process of autonomous self-development and consequently the development of democratic society. Anonymity encourages autonomous self-development by permitting users to liberate themselves from the identities with which they are born. In this respect, it expands the possibilities of expression.[342] Citing *Roth v. United States*, the *McIntyre* Court seemed to endorse such expansion by underscoring the importance of ensuring the "unfettered interchange of ideas for the bringing about of political *and* social changes desired by the people."[343] Toward this end, the court in *Miller* struck down a state statute that restricted anonymous and pseudonymous communication on the Internet on the ground that it chilled protected expression.[344] The chilling effect resulted from the plaintiffs' "self-censorship": their alteration of what they thought was legitimate behavior—the use of online pseudonyms to communicate about sensitive topics to avoid subjecting themselves to social ostracism and embarrassment.[345] Broadly read, this holding might stand for the principle that the opportunity to expand the possibilities of identity by experimenting with self-definition nurtures robust debate on issues of public concern, which in turn nurtures democratic society.[346]

This last point is particularly important because the debate over the provision of anonymity in anonymity-protecting p2p networks maps the tension between the individual and the collective, the private and the public. Cohen's argument, which others have made as well, helps deconstruct these oppositions. As Gandy so eloquently observes, the rationales for guaranteeing the private (read anonymous) are not necessarily antagonistic to the public interest: "[T]he operation and survival of a vibrant democracy may be specified as a goal that defines active, informed participation by its citizens as a necessary prerequisite. The autonomous development of that citizenry can be argued to depend on the protections of personhood and individuality privacy [read anonymity] describes."[347] In this respect, he collapses the opposition between individual and collective, private and public

341. *McIntyre*, 514 U.S. at 342.
342. Katyal, *supra* note 17.
343. *McIntyre*, 514 U.S. at 346 (emphasis added).
344. ACLU v. Miller, 977 F. Supp. 1228, 1234 (N.D. Ga. 1997).
345. *Id.*
346. Cohen, *Examined Lives*, *supra* note 269, at 1426–27.
347. Gandy, *supra* note 19, at 179.

that has shaped the debate over the role of anonymous communication in the political economy.

Second, critics contend that anonymity-protecting p2p networks facilitate wrongdoing by eliminating accountability.[348] Holding users accountable for their actions becomes more difficult in the absence of real-world signs of identity. Lack of accountability strips users of the civility that face-to-face encounters encourage, facilitates dissemination of false or misleading information that may harm others, and prevents potential plaintiffs from seeking redress for their injuries.[349] In his dissent in *McIntyre*, Justice Scalia concludes: "I can imagine no reason why an anonymous leaflet is any more honorable . . . than an anonymous phone call or an anonymous letter. It facilitates wrong by eliminating accountability, which is ordinarily the very purpose of the anonymity."[350] The government in particular has the concern that the elimination of accountability inhibits law enforcement.[351] Without the knowledge that they are being watched, some users may be tempted to publish confidential information that compromises national security, disclose trade secrets, distribute child pornography, pirate intellectual property, and defame their enemies.[352] The harm caused by engaging in such activities over such networks is magnified because Internet communication is global, instantaneous, and infinitely reproducible.

By contrast, although some users may use anonymity-protecting p2p networks to engage in illegal activities without accountability, there is no evidence that these networks have become hotbeds of illegality.[353] Moreover, as Freenet's developers argue, "While most people wish that child pornography and terrorism did not exist, humanity should not be deprived of their freedom to communicate just because of how a very small number of people might use that freedom."[354] This argument echoes the Court's holding in *McIntyre* that even though the right to anonymity may be abused when it shields illegal conduct, the value of free speech is greater than the dangers of its misuse.[355]

---

348. Marx, *supra* note 148, at 105–06.

349. Anne Wells Branscomb, *Anonymity, Autonomy, and Accountability: Challenges to the First Amendment in Cyberspaces*, 104 Yale L.J. 1639, 1645 (1995) (examining how the cultural behavior developing on the Internet is challenging the First Amendment and how intrusion by real-world communities may inhibit the free flow of information in cybercommunities, threatening the value of electronic communication as a vehicle for democratic discourse).

350. McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 385 (1995) (Scalia, J., dissenting).

351. *See* Godwin, *supra* note 333, at 149.

352. Froomkin, *supra* note 260, at 402.

353. This is not to say that no users ever engage in illegal activities, however.

354. Free Network Project, *supra* note 223.

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

III. CODE IS LAW

Even if one accepts the constitutionality of anonymous communication on anonymity-protecting p2p networks and agrees that the benefits of protecting anonymity in this forum outweigh the costs, one must acknowledge that the potential harms are real. Nevertheless, whether it is possible to draft legislation that effectively mitigates these harms without violating the First Amendment and whether it is possible to enforce such legislation is questionable. In view of the limitations of legal regulation, regulation by computer code may be preferable. Indeed, in his influential book *Code and Other Laws of Cyberspace*, Lawrence Lessig argues that "code is law"—that computer code may have regulatory effects analogous to those of law.[356] From this perspective, the limitations of Super-DMCA bills as means of regulating anonymity-protecting p2p networks, in comparison to self-regulation by code, become apparent.

A. *The Limitations of Legal Regulation*

Whether Super-DMCA bills effectively target the harms posed by the provision of anonymous communication on anonymity-protecting p2p networks without violating the First Amendment is contestable.[357] Because these networks' primary purpose is to protect anonymous political expression, and because they do serve this purpose,[358] the networks would be expected to argue that a court should apply the "exacting scrutiny" standard set forth in *McIntyre* to statutes like Super-DMCA bills, which have the potential effect of regulating anonymous communication, including anonymous political expression, on anonymity-protecting p2p networks. To the extent that Super-DMCA bills regulate anonymous communication on these networks, a court should hold that under the *McIntyre* standard, the bills are not narrowly tailored and should be struck down.

Legislators may be able to demonstrate that statutes like Super-DMCA bills that burden core political expression serve an overriding state interest.[359] Drafting a statute that meets the "narrowly tailored" requirement, however, may be more challenging. The *raison d'être* of non–anonymity-protecting p2p networks like Kazaa is to enable users to distribute nonpolitical content—that is, to share music, video, and software files, some of which may be copyrighted. By contrast, the *raison d'être* of anonymity-protecting p2p networks like Freenet, Free

356. *See* Lessig, *supra* note 123, at 89.
357. *See supra* Part II.A.
358. *See supra* Part I.C.
359. Courts have held that preventing fraud and libel is a compelling state interest. *See McIntyre*, 514 U.S. at 349; *see also* ACLU v. Miller, 977 F. Supp. 1228, 1232 (N.D. Ga. 1997). Courts have also held that the First Amendment does not protect copyright infringement, for example. *See* Eldred v. Ashcroft, 123 S. Ct. 769, 788 (2003).

Haven, and Publius is to distribute political content. Indeed, the latter networks justify their existence on the ground of "safeguard[ing] those 'who support causes anonymously' and those who 'fear economic or official retaliation,' 'social ostracism,' or an unwanted intrusion into 'privacy,'" to borrow the words of *McIntyre* via *Verizon I*.[360] The difficulty arises when these networks distribute political and nonpolitical content. When a user attempts to upload a file, the technology cannot distinguish between a constitutionally protected political file, such as a speech by Lenin, to borrow the *Verizon I* court's example, and an unprotected nonpolitical one, such as a copyrighted song by Metallica.[361] As currently structured, p2p Networks cannot accept the protected file and reject the unprotected one.

Yet, pursuant to the First Amendment, a statute that seeks to regulate anonymous communication on anonymity-protecting p2p networks must be able to distinguish constitutionally protected from constitutionally unprotected expression. As Justice Harlan concluded in his concurrence in *Talley*, "it will not do for the State simply to say that the circulation of *all* anonymous handbills must be suppressed in order to identify the distributors of those that may be of an obnoxious character."[362] In *McIntyre*, for example, the Court struck down the contested statute on the ground the state's interest in preventing fraud and libel was principally protected by other laws and thus did not justify the additional statutory prohibition against the distribution of anonymous campaign literature, which applied regardless of whether the materials were false or misleading.[363] And most recently, in *Miller*, the court found that the contested statute prohibiting anonymous and pseudonymous communication on the Internet applied regardless of whether a speaker had an intent to deceive or any actual deception occurred.[364] Clarke points to the dilemma legislators face in drafting statutes that effectively regulate anonymous communication on anonymity-protecting p2p networks without violating the narrowly tailored requirement when he stated: "[T]he freedom to communicate is a fundamental value in a democratic society. There is no way to deny it to the 'bad guys' without also denying freedom to the 'good guys.'"[365] The latter may include civil rights activists, minority religious sects, and even ordinary individuals who merely desire to protect their privacy.[366]

360. *In re* Verizon Internet Servs., Inc., 240 F. Supp. 2d 24, 43 (D.D.C. 2003).
361. *Id.*; *see also* Froomkin, *supra* note 261, at 119.
362. Talley v. California, 362 U.S. 60, 66 (1960) (emphasis added).
363. *McIntyre*, 514 U.S. at 349–52.
364. *Miller*, 977 F. Supp. at 1233 (discussing the overbreadth of the statute).
365. Clarke et al., *supra* note 50, at 41. Clarke also writes: "The fundamental underlying principle behind Freenet is that a third person should not be able to prevent two other people from communicating." McCullagh, *supra* note 336, at 137.
366. Clarke et al., *supra* note 50, at 41.

Super-DMCA bills are not sufficiently narrowly tailored to distinguish between the "good" and "bad" guys. The broadest of these bills prohibit possession, use, development, or distribution of any communication device to conceal or to assist another to conceal from any communication service provider, or any lawful authority, the existence of the place of origin or destination of any communication.[367] The effect of these bills would be to ban devices that enable anonymous communication, including the technologies that anonymity-protecting p2p networks use.[368] In response to criticisms of overbreadth, other Super-DMCA bills are more narrowly tailored. These prohibit communication devices used to conceal the origin or destination of communications provided that such concealment is for the purpose of knowingly and intentionally defrauding a communication service provider.[369]

But even these more narrowly tailored Super-DMCA bills may be constitutionally infirm. Indeed, without sufficient procedural safeguards, they run the risk of prohibiting protected anonymous expression—especially political expression. In this respect, they may function as indirect or secondary prior restraints, which are presumptively unconstitutional.[370] Although the prohibition of prior restraints on expression is subject to certain exceptions, including expression that threatens national security when the nation is at war, incitements to acts of violence, and obscenity,[371] justifying prior restraints on anonymity-protecting p2p networks on the basis of these exceptions is complicated by the fact that the nature of the technology makes drafting a prior restraint that targets prohibited expression, such as obscenity, without restricting protected expression, such as political speech, seemingly impossible.[372] As the Court held in *Speiser*

---

367. *See supra* notes 243–48 and accompanying text.

368. von Lohmann, *supra* note 239.

369. *Id.*

370. *See* Near v. Minnesota, 283 U.S. 697, 713–14 (1931) (holding prior restraints particularly suspect under the First Amendment). There are four major types of prior restraints: administrative preclearances, preliminary injunctions, legislative prior restraint statutes, and indirect or secondary prior restraints. See Note, Richard Favata, Filling the Void in First Amendment Jurisprudence: Is There a Solution for Replacing the Impotent System of Prior Restraints?, 72 Fordham L. Rev. 169, 176–77 (summarizing Thomas I. Emerson's typology of prior restraints). Pursuant to this typology, Super-DMCA bills might be classified as indirect or secondary prior restraints because the restraint of protected expression on anonymity-protecting p2p networks would create the indirect or secondary effect of criminalizing the use of unlawful communication and access devices.

371. *Near*, 283 U.S. at 716.

372. Note in this regard that *Verizon II* held that the statute involved in the case does not involve the prior restraint of potentially restricted expression. Instead, it simply permits a copyright holder to obtain an alleged copyright infringer's identity to protect copyright. The statute, the court concluded, "does not regulate protected expression or otherwise permit prior restraint of protected speech. It only requires production of the identity of one who has engaged in unprotected conducts—haring [*sic*] copyrighted material on the Internet." *In re* Verizon Internet Servs., Inc., 257 F.

v. Randall, the line between unconditionally guaranteed expression and expression that may legitimately be regulated is subtle, and distinguishing between the two calls for "sensitive tools."[373] Because Super-DMCA bills as currently drafted cannot make this distinction with respect to expression on anonymity-protecting p2p networks, they do not qualify as the sensitive tools of which the Court speaks.

Even if legislators could draft a Super-DMCA bill or other statute that accounted for this distinction, enforcing it would be challenging to say the least. Clarke, for example, has stated: "Anarchy means without a ruler and that sums up the architecture of Freenet.... It does not have any kind of centralized control. In fact, it is designed in such a way that it is impossible to control."[374] As suggested previously, anonymity-protecting p2p networks like Free Haven, Publius, and Freenet differ from p2p networks like Napster in that they lack a central server that can be shut down, terminating the circulation of files.[375] Instead, control is distributed across the multitude of nodes that comprise the network. Even if a plaintiff successfully argued for an injunction against one of these networks, the "company" might cease operation, but the network of nodes would persist.[376] Copies of the network software may continue to circulate; nodes may continue to emerge; files may continue to be inserted, stored, and retrieved. Seemingly, the only way to shut down such a network would be to shut down the vast majority of the nodes

---

Supp. 2d 244, 261 (D.D.C. 2003).

373. Speiser v. Randall, 357 U.S. 513, 525 (1958) (holding in part that when a state seeks to restrain unlawful advocacy, it must provide procedures sufficient to protect against infringement of constitutionally protected rights, and because only considerations of greatest urgency may justify restrictions on speech, and because the validity of restraints on speech depends on careful analysis of particular circumstances, procedures by which each case's facts are adjudicated are especially important and restraints' validity may turn on the safeguards they afford).

374. Jennifer L. Schenker, *The Infoanarchist: Could This 23-Year-Old Irish Programmer Begin to Unravel the Web?*, Time Int'l, July 17, 2000, LEXIS, News & Bus.

375. *See supra* Part I.C.

376. *See* Miller, *supra* note 116, at 77. Jane C. Ginsburg, among others, has recognized the likelihood of this post-*Napster* phenomenon: "But even if some new technologies, including Napster, can be policed into copyright compliance, will not other, more copyright resistant modes of communication arise to retrieve and redistribute the excluded content? ... Self-styled 'cyber anarchists' invite us," she continues, "to 'copyright's funeral,' proclaiming that no protective measures that copyright owners devise will withstand the efforts of hackers who will, moreover, avail themselves of pervasive yet untraceable means of file sharing." Jane C. Ginsburg, *Copyright and Control Over New Technologies of Dissemination*, 101 Colum. L. Rev. 1613, 1642 (2001) (concluding that greater author control enhances moral appeal of exercise of copyright and may offer the public increased quantity and variety of works of authorship because authors whom the traditional intermediary-controlled distribution system has excluded may directly propose to the public and be compensated for their creations).

that comprise it or to disable every copy of network software. Both options are technologically impractical at this time.[377]

In addition, the developers of anonymity-protecting p2p networks have engineered their systems to minimize liability for themselves and for node operators. The case of copyright infringement is instructive in this respect. In *Napster*, the court held Napster liable for contributory infringement on the ground that Napster had actual knowledge that specific infringing files were available to users, could have blocked access to the system by users who supplied those files, failed to remove them, and provided a site and facilities for direct infringement.[378] It also held Napster liable for vicarious infringement in part on the ground that Napster had a limited right and ability to police its system, but failed to exercise that right to prevent the exchange of infringing files.[379] By contrast, the fact that no one can monitor and control users' activities in anonymity-protecting p2p networks protects not only the users from liability for direct infringement, but the developers from contributory and vicarious infringement, even under the diluted knowledge requirement the *Napster* court established.[380] Indeed, in *Metro-Goldwyn-Mayer Studios, Inc. v. Grokster, Ltd.*, the Central District of California held that a decentralized p2p network that enables users to exchange files directly was not liable for contributory copyright infringement, even if it was aware that users were using the network to infringe copyrighted works, on the ground that there were substantial noninfringing uses for the network and that the network operators had no material involvement in the users' conduct.[381] Similarly, the court held that the

377. *See* Miller, *supra* note 116, at 77. To be sure, the struggle between the agents and the subjects of surveillance is a cat-and-mouse game. *See* Marciniak, *supra* note 82. Just as quickly as programmers develop technologies that resist surveillance, the agents of surveillance develop more powerful surveillance mechanisms. *Id.* For example, in 2001, it was revealed that the FBI was developing "Magic Lantern," a program that can allegedly record every keystroke a user makes on her computer keyboard. *Id.* Encryption and anonymizing technologies would be useless because investigators could implement the program before the user activated these shielding services. *Id.* The FBI has confirmed the program's existence, but it has not revealed whether it has ever used it. *Id.*

378. A & M Records, Inc. v. Napster, Inc., 239 F.3d 1004, 1019–22 (9th Cir. 2001).

379. *Id.* at 1023–24.

380. *See* Fred von Lohmann, Electronic Frontier Foundation, IAAL: Peer-to-Peer File Sharing and Copyright Law After *Napster*, (Jan. 2003), *at* http://www.eff.org/IP/P2P/20010227_p2p_copyright_white_paper.html. In this set of guidelines for p2p developers, von Lohmann suggests that p2p developers can reduce the possibility of liability for copyright infringement by engineering their networks for "total control" or "total anarchy." *Id.* The developers of Free Haven, Publius, and Freenet have gravitated toward the latter option.

381. Metro-Goldwyn-Mayer Studios., Inc. v. Grokster, Ltd., 259 F. Supp. 2d 1029, 1036–37, 1046 (C.D. Cal. 2003) (finding that a filesharing network whose users distributed copyrighted films was not liable for contributory infringement absent a showing that the network had any material involvement in the users' conduct and was not liable for vicarious infringement absent a showing that it had any right or ability

network was not liable for vicarious copyright infringement, even though it derived financial benefit from enabling users' direct infringement, without establishing that it had the right or ability to supervise the users' conduct.[382]

In view of these challenges, the best approach from the perspective of legal regulation may be to rely on preexisting laws against end-users accused of copyright infringement, child pornography, fraud, and so on to regulate anonymity-protecting p2p networks. Indeed, the *McIntyre* Court seemed to endorse this approach by holding that a state may not punish a crime by "indirectly or indiscriminately" prohibiting a category of expression based on its content when there is no "necessary relationship" to the harm that the state seeks to prevent.[383] In addition, though criticized by some civil liberties organizations, another way of discouraging illegality may be the DSEA's proposal to enhance penalties for persons convicted of federal felonies who have knowingly or willfully used encryption.[384] This proposal would punish users who use anonymizing technologies for illegal purposes without prohibiting the technologies themselves.

B. *The Regulatory Effects of Code*

Because of the limitations of legal regulation of anonymous communication in anonymity-protecting p2p networks poses, self-regulation by code may be preferable. The difficulty of regulating anonymity-protecting p2p networks through legislation exemplifies the extent to which disruptive anonymous technologies have begun to contest the enforceability of the law in the Internet context.[385] But in a recent article building on Lessig's theory of "code as law," Tim Wu persuasively argues that the disruptive effect of technology on law is best understood not as a process of supplantation, but as "a change in power dynamics among and within regulated groups."[386] Laws impose certain costs on regulated groups, which strive to minimize these costs by choosing between mechanisms of change (such as lobbying), which "decrease the sanction attached to certain conduct and tend to require collective action," and mechanisms of avoidance (such as tax evasion), which "decrease the probability of detection and typically do not require that groups act collectively, but depend on specific vulnerabilities in the law."[387] Like tax lawyers, code designers search

to supervise the users' conduct). For discussion of this decision, see Tim Wu, *When Code Isn't Law*, 89 Va. L. Rev. 679 (2003) (proposing a new way of understanding the relationship between code and compliance with law by studying code design as an aspect of interest group behavior).

382. *Grokster*, 259 F. Supp. 2d at 1043–46.

383. McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 357 (1995).

384. *See supra* note 79 and accompanying text.

385. McCullagh, *supra* note 336, at 139.

386. *See* Wu, *supra*, note 381, at 686.

387. *Id.* at 684.

for areas in which the law's stated purposes differ from its practical limits and then redesign behavior to avoid legal sanctions.[388] In this respect, code design could be understood as "an alternative means of regulation" by which the regulated avoid a regulatory scheme to which they object by drafting and enacting a scheme that embodies their own values.[389] This mode of self-regulation offers several advantages over regulation by law.

1. The Advantages of Regulation by Code

First, anonymity-protecting p2p networks are discrete communities that struggle against the threats that the expansion of Internet surveillance poses by implementing—in effect, drafting and enacting—systems that effectively and efficiently protect the constitutionally defined right to anonymity. The developers of Free Haven, Publius, and Freenet, for example, have perceived a threat to individual liberty catalyzed by the development and implementation of powerful new online surveillance technologies.[390] Informed by First Amendment jurisprudence, they have sought to avoid this threat by identifying and defining a right to anonymity on the Internet and by using code design to develop an alternative mode of regulation that protects this right.[391] This approach reflects the one adopted by the participants in the AAAS's Internet anonymity project.[392] Online communities should have the freedom to develop, adopt, and implement their own policies regarding the use of anonymous communication.[393] Such an approach would encourage a range of networks offering different frameworks for anonymous communication, thus enriching the proverbial "marketplace of ideas."

Second, participation in these networks is consensual, not coercive. Users who do not subscribe to Freenet's policy that freedom of expression entails the toleration of expression one may not personally endorse, for example, may choose not to "opt in" to the network in the first place. And if they do choose to opt in, they still have the option to work within the network's norms to limit the distribution of files to which they object.

Third, in this respect, these networks have implemented systems of anonymity-supportive accountability that attempt to encourage normative and discourage transgressive behavior. Publius discourages the distribution of child pornography and copyrighted music, video, and software files by limiting the size of files users may publish to

388. *Id.* at 708.
389. *Id.* at 687–88.
390. *See supra* Part I.
391. *See supra* Part I.C.2.
392. *See* Teich et al., *supra* note 149, at 73.
393. *Id.*

100K.[394] In addition, to minimize further the distribution of such files, it declines to list them in its search directory on the ground they are "not interesting," thus making it more difficult for users to locate them.[395] Free Haven has attempted to engineer accountability through the implementation of reputation systems.[396] Finally, Freenet supports accountability by permitting an author to sign files cryptographically—a technique that enables him to prove he is the author without revealing his identity. In this manner, he may develop an anonymous reputation for reliability.[397] To be sure, these systems are imperfect.

Fourth, these networks may further encourage accountability by developing codes of conduct for users analogous to the code of conduct recently developed by P2P United. P2P United is a trade association whose membership includes major p2p networks, including Bearshare, Blubster, eDonkey2000, Grokster, Limewire, and Morpheus (but not Kazaa).[398] In September 2003, it issued a Member Code of Conduct in which the charter members pledged to meet a series of obligations.[399] With respect to the issue of compliance with the law, each network pledged to inform users prominently that using the network for illegal activities, especially copyright infringement, is strictly forbidden and may subject the user to liability; to provide links to responsible sources of information regarding the nature and scope of copyright laws; and to comply with the Children's Online Privacy Protection Act while cooperating with governmental agencies to prosecute trafficking in child pornography and related crimes.[400] Anonymity-protecting p2p networks could consider adopting similar codes of conduct.[401]

And fifth, anonymity-protecting p2p networks seem to demand what Joel R. Reidenberg has termed a new "network governance paradigm" that recognizes the extent to which this technology has eroded the viability of traditional territorial and substantive borders

394. *See supra* note 199 and accompanying text.

395. *See supra* note 203 and accompanying text.

396. *See generally* Dingledine et al., *supra* note 166, at 306–28.

397. Free Network Project, *supra* note 223.

398. *See* P2P United, P2P United Members, *at* http://www.p2punited.org/members.php (last visited Oct. 15, 2003).

399. *See* P2P United, Member Code of Conduct (Sept. 29, 2003), *at* http://www.p2punited.org/modules.php?op=modload&name=News&file=index&catid=&topic=9&allstories=1.

400. *Id.*

401. Other industry initiatives might include industry-wide procedures for addressing copyright infringement complaints; industry-wide commitments to assuring a right of reply in defamation cases; the inclusion of assumption-of-the-risk clauses in user agreements that warn users that if they use the network, they may encounter files of which they disapprove; and other nonmonetary tort remedies. *See* Godwin, *supra* note 333, at 157.

as paradigms for regulatory policy and enforcement.[402] As Reidenberg has observed, regulatory authority has been defined in terms of territorial borders (sovereignty, regulatory authority, and enforcement are predicated on the existence of territorially distinct political and social entities) and substantive borders (governance relies on clear distinctions and borders in substantive law).[403] The Internet erodes both types of borders.[404] Moreover, it has resulted in the emergence of networks that achieve the status of semi-sovereign entities.[405] The sovereignty of these entities is grounded in their capacity to establish rules of participation that form visible borders—rules that define users' rights and responsibilities, that determine the norms governing their conduct, that are enforceable, and that ultimately may supplant substantive governmental rules.[406] According to Reidenberg, a new network governance paradigm that recognizes this development "must emerge to recognize the complexity of regulatory power centers, utilize new policy instruments such as technical standardization to achieve regulatory objectives, accord status to networks as semi-sovereign entities, and shift the role of the state toward the creation of an incentive structure for network self-regulation."[407] From this perspective, recognizing the semi-sovereign status of anonymity-protecting p2p networks and encouraging the attempts they made to regulate themselves may ultimately serve the government's own regulatory interests.

2. The Disadvantages of Regulation by Code

In spite of the advantages of regulation by code, the technological solution nevertheless poses a risk that goes beyond obstructing the efforts of law enforcement. As code designers assume primary responsibility for regulating anonymity-protecting p2p networks and thus creating alternative regimes of regulation that apply only to the technologically savvy, the state cedes its sovereignty over them. As Lessig has remarked, this sovereignty in cyberspace competes with "real-space" sovereignty; yet, "control of that sovereign is essential if we are to achieve democratic control over an extraordinarily important aspect of real-space life. *Real-space* life, not just cyberspace life, since in the end, and in the beginning, life there is always also life here."[408] This is the danger of permitting one First Amendment regime to operate inside the networks and another, outside. In this

402. *See* Joel R. Reidenberg, *Governing Networks and Rule-Making in Cyberspace*, 45 Emory L.J. 911, 930 (1996).
403. *Id.* at 914–16.
404. *Id.*
405. *Id.* at 930.
406. *Id.* at 919.
407. *Id.* at 930.
408. Lessig, *supra* note 123, at 190.

mode of ordering, the networks constitute "a First Amendment *in code* more extreme than our own First Amendment *in law*."[409] By providing greater constitutional protections than the law does, anonymity-protecting networks may ironically accelerate the migration of deliberative discourse to the safety of the networks themselves, ironically undermining in "real-space life" the very democratic values their developers strive to promote. This tendency, rather than the alleged free haven they may provide for copyright infringement, defamation, and other horribles, may be the real "specter . . . haunting the modern world, the specter of crypto anarchy" of which Tim May warned.

409. *Id.* at 167.