Loyola of Los Angeles
Entertainment Law Review

Volume 23 | Number 1 Article 3

6-1-2002

The Demise of Anonymity: A Constitutional Challenge to the Convention on Cybercrime

Albert I. Aldesco

NOTES & COMMENTS

THE DEMISE OF ANONYMITY: A CONSTITUTIONAL CHALLENGE TO THE CONVENTION ON CYBERCRIME

I. INTRODUCTION

The vertiginous growth of the Internet has vastly expanded the means of communication.[1] Cyberspace[2] enables people to share ideas over great distances and engage in the creation of an entirely new, diverse, and chaotic democracy, free from geographic and physical constraints.[3] While the demotic potential of cyberspace is well recognized,[4] less known is that individuals can reach audiences of thousands or even millions in ways that conceal their true identities.[5]

To be sure, there are legitimate reasons for individuals to interact anonymously on the Internet.[6] Anonymity allows whistle-blowers and political activists to express opinions critical of employers and the government; it enables entrepreneurs to acquire and share technical

1. *See* ACLU v. Reno, 929 F. Supp. 824, 844 (E.D. Pa. 1996) (describing the Internet as "a unique and wholly new medium of worldwide human communication"), *aff'd*, 521 U.S. 844 (1997).

2. NETLINGO DICTIONARY OF INTERNET WORDS: A GLOSSARY OF ONLINE JARGON WITH DEFINITIONS OF TERMINOLOGY, *at* http://www.netlingo.com/inframes.cfm (last visited Sept. 21, 2002) [hereinafter NETLINGO]. The term refers more generally to the digital medium constructed by computer networks. *Id.*; *see also* WILLIAM GIBSON, NEUROMANCER 51 (Ace Books 1984) (defining "cyberspace" as "[a] consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concepts . . . A graphic representation of data abstracted from the banks of every computer in the human system.").

3. *See* Ann Beeson, *Top Ten Threats to Civil Liberties in Cyberspace*, HUM. RTS., Spring 1996, at 10, 10 (stating that cyberspace is "probably the richest source of creative, diverse, empowering and democratizing communication ever to connect people across the globe").

4. *Reno*, 929 F. Supp. at 835. Participants exchange information and opinion on a wide variety of topics, leading the court to conclude that "the content on the Internet is as diverse as human thought." *Id.* at 842.

5. *See* MIKE GODWIN, CYBER RIGHTS: DEFENDING FREE SPEECH IN THE DIGITAL AGE 133 (Times Books 1998). Godwin explains that the Internet has the potential to turn anyone into a publisher with the reach of a newspaper or TV station. *Id.* at 10–12.

6. *See* Wendy M. Grossman, *Surveillance by Design*, SCI. AM., Sept. 2001, at 24.

information without alerting their competitors, and permits individuals to express their views online without fear of reprisals and public hostility.[7] Moreover, the right to speak anonymously is an important "aspect of the freedom of speech protected by the First Amendment."[8]

The technology underpinning online anonymity, however, has come under increasing scrutiny from law enforcement investigators who face unique technical and legal challenges from criminals operating online.[9] Principally, the same technology that allows individuals to communicate anonymously also enables criminals to hide their identities and evade detection in cyberspace.[10] Not surprisingly, investigators have been searching for a technical solution that would enable them to trace the perpetrators of computer crimes and expose their identities.[11]

The global nature of cybercrime[12] poses additional legal challenges to law enforcement.[13] Since cyberspace has no geographic boundaries, computer criminals are free to operate from anywhere in the world.[14] They can rest safe in the knowledge that targeted states cannot extend the jurisdiction of their courts to impinge upon the sovereignty of harboring nations.[15]

In effect, the infrastructure of cyberspace has made international cooperation a necessity, requiring "a universal legal framework equal to the worldwide reach of the Internet."[16] The Convention on Cybercrime (the "Convention") is the Council of Europe's response to these unique technical and legal challenges, the "first ever international treaty on

---

7. *See id.*

8. McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 342 (1995). The Court held that a ban on anonymity is a "direct regulation of the content of speech." *Id.* at 345.

9. *See* discussion *infra* Part II.B.

10. James K. Robinson, Assistant Attorney General, Internet as the Scene of the Crime, Remarks at the International Computer Crime Conference, *at* http://www.usdoj.gov/criminal/cybercrime/roboslo.htm (May 29–31, 2000) [hereinafter Robinson, Remarks].

11. *See id.*

12. *Id.* The umbrella term covers various computer crimes, including crimes in which computers are attacked, resulting in electronic theft or disruption of information or services, and crimes in which computers are used to carry out conventional offenses from manipulating stocks, to infringing of copyrights, and distributing child pornography. *See id.*

13. *See generally* A. Michael Froomkin, *Regulation of Computing and Information Technology: Flood Control on the Information Ocean: Living with Anonymity, Digital Cash, and Distributed Databases*, 15 J.L. & COM. 395, 445 (1996) [hereinafter *Flood Control*] (noting that countries with relaxed rules undercut the United States' ability to enforce its laws).

14. Robinson, Remarks, *supra* note 10.

15. *See id.*

16. *Id.* (quoting French President Jacques Chirac).

criminal offences [sic] committed against or with the help of computer networks such as the Internet."[17] The final draft of the Convention, approved in June 2001, is the outcome of four years of work by the European Committee on Crime Problems ("CDPC") and experts from the United States, Canada, Japan, and other countries.[18] The United States Department of Justice has been an active participant in the drafting process, and hails the Convention as a pioneer effort that "breaks new ground" by addressing the international nature of cybercrime, and as one that provides a "solid basis" for international cooperation in law enforcement investigations.[19]

Other reactions have not been as favorable.[20] Indeed, twenty-two associations in the United States and other nations have voiced concerns that the Convention embodies measures that are "disproportionate, destructive of liberty, and a threat to fundamental rights."[21] In particular, the treaty's provisions for government access to computer data and requirements compelling Internet providers to produce detailed logs of network activity undermine individual privacy and the right to communicate anonymously in cyberspace.[22]

---

17. Press Release, Council of Europe, 30 States Sign the Convention on Cybercrime at the Opening Ceremony, *at* http://press.coe.int/cp/2001/875a(2001).htm (Nov. 23, 2001) [hereinafter 30 States Sign the Convention]. The Convention was opened for signature on November 23, 2001, and was signed by twenty-six member states of the Council of Europe along with four non-member states: Canada, Japan, South Africa, and the United States. *Id.* "The Council of Europe is the continent's oldest political organiation [sic], founded in 1949." Press Release, Council of Europe, The CE in Brief, *at* http://press.coe.int/press2/Press.asp?B=30,0,0,0,0&M=http://press.coe.int/files/e-cebref.htm (June 30, 2001).

18. Press Release, Council of Europe, Council of Europe's Committee on Crime Problems Approves Final Draft of Cyber-crime Convention, *at* http://press.coe.int/cp/2001/456a(2001).htm (June 22, 2001) [hereinafter Final Draft].

19. U.S. DEP'T OF JUSTICE, FREQUENTLY ASKED QUESTIONS AND ANSWERS ABOUT THE COUNCIL OF EUROPE CONVENTION ON CYBERCRIME, *at* http://www.usdoj.gov/criminal/cybercrime/newCOEFAQs.html (last visited Sept. 20, 2002) [hereinafter FAQ ABOUT THE CONVENTION].

20. Press Release, Council of Europe, Big Brother or Free-for-All—How Can the Law Strike a Balance?, *at* http://press.coe.int/dossiers/107/E/e-bbfw.htm (last visited Oct. 7, 2001) [hereinafter Big Brother] ("Under the acronym GILC (Global Internet Liberty Campaign), 22 associations in nine European countries . . . the US, Japan, Australia and South Africa are campaigning against the draft Convention," because of their concern that the provisions on the interception of electronic communications may jeopardize the integrity of personal data and the right to anonymity.).

21. *Id.*

22. *See* Global Internet Liberty Campaign Member Letter on Council of Europe Convention on Cyber-Crime, to Council of Europe Secretary General, Walter Schwimmer, and COE Committee of Experts on Cyber Crime [sic], *at* http://www.gilc.org/privacy/coe-letter-1000.html (Oct. 18, 2000).

This Comment acknowledges that law enforcement has a legitimate interest in combating computer crimes and that international cooperation is essential to this effort. Nevertheless, providing the government with the means to pry into private communications and to track anonymous users on the Internet constitutes a radical curtailment of the freedom of speech protected by the First Amendment.

Part II of this Comment provides an overview of criminal law enforcement in cyberspace, the unique technical and legal challenges posed by electronic anonymity, and the drafting of the Convention designed to meet the global threat of cybercrime. Part III briefly discusses the development of constitutional law relating to anonymous speech. Part IV criticizes those specific provisions of the Convention that restrict truly anonymous speech on the Internet as being incompatible with the First Amendment. Finally, Part V concludes that the United States must not endorse the Convention in its current form, but instead must develop international agreements upholding First Amendment liberties and the precedence of the Constitution.

II. INTERNATIONAL LAW ENFORCEMENT IN CYBERSPACE

A. The Global Threat of Cybercrime

A worm may have unleashed the worst attack in history.[23] Admittedly, this was not an attack upon life, but rather upon computers. By the time accountants calculated the economic fallout, the "Love Bug" computer worm[24] had cost businesses worldwide an estimated $8.7 billion in damage.[25] To make matters worse, the college drop-out who confessed to have "accidentally" released the worm in the form of an email attachment got away with it because there were no applicable cybercrime laws in the Philippines with which to charge him.[26] The United States and

23. *See* Lynn Burke, *Love Bug Case Dead in Manila*, WIRED NEWS (Aug. 21, 2000), *at* http://www.wired.com/news/politics/0,1294,38342,00.html.

24. NETLINGO, *supra* note 2 (defining a "worm," also known as a "virus," as a small computer program that proliferates by attaching copies of itself to other programs, subsequently shutting down computers and networks.).

25. Kim Zetter, *Viruses: The Next Generation*, PC WORLD, Dec. 1, 2000, at 192 (citing research firm Computer Economics).

26. Burke, *supra* note 23 (noting that the suspect was charged with credit card fraud, but the charges were dropped due to insufficient evidence).

the Philippines had entered into a "Mutual Legal Assistance Treaty (MLAT),"[27] but to extradite him, a crime had to have been committed.[28]

The "Love Bug" and its "malicious code"[29] variants underscore the world's dependence on computers and concurrent vulnerability to computer attacks.[30] Credit card theft alone is estimated to cost banks and individuals some $400 million annually, while profits lost by firms from stolen patents and trademarks amount to $250 billion—nearly five percent of world trade.[31] Not surprisingly, with computer attacks doubling each year,[32] cybercrime has the capacity "to destabili[z]e a country's whole economy."[33]

The ease with which cybercrimes such as distributed "denial-of-service"[34] attacks can be carried out makes everyone a potential suspect.[35] Almost anyone can download malicious code toolkits from the Internet and unleash the computer equivalent of an Ebola virus.[36] Hackers[37] have hit a third of Great Britain's businesses and public authorities.[38] In the United States, nearly fifty percent of companies surveyed experienced attacks in

---

27. *Id.* By 1998, the United States had entered some twenty MLATs with foreign governments in order to facilitate criminal prosecutions abroad. United States v. Balsys, 524 U.S. 666, 715 (1998).

28. Burke, *supra* note 23.

29. Robert Lemos, *Year of the Worm: Fast-Spreading Code Is Weapon of Choice for Net Vandals*, CNET NEWS.COM (Mar. 15, 2001), *at* http://news.com.com/2009-1001-254061.html?legacy=cnet. Several types of destructive programs, such as worms, viruses, and Trojan horses, may be classified as malicious code. *Id.*

30. Robinson, Remarks, *supra* note 10.

31. Press Release, Council of Europe, Cyber-Crime—The Targets It Hits, the Damage It Does, *at* http://press.coe.int/dossiers/107/E/e-cibles.htm (last visited Aug. 21, 2002) [hereinafter Damage] (citing several studies carried out in Europe and the United States).

32. Robert Lemos, *Internet Attacks Seen Doubling in 2001*, CNET NEWS.COM (Oct. 15, 2001), *at* http://news.com.com/2100-1001-274435.html?legacy=cnet.

33. Damage, *supra* note 31 (quoting former FBI director Ronald L. Dick).

34. A distributed denial-of-service attack "flood[s] . . . Web servers with false requests for information, overwhelming the system and ultimately crashing it." *How a "Denial of Service" Attack Works*, CNET NEWS.COM (Feb. 9, 2000), *at* http://news.com.com/2100-1017-236728.html?legacy=cnet.

35. For example, in February 2000, a Canadian teen by the alias of MafiaBoy managed to shut down several of the Internet's largest sites; however, "it [was] widely agreed that MafiaBoy was neither ingenious or creative—he simply ran a computer script that clogged networks full of garbage data." *See* Michelle Delio, *The Greatest Hacks of All Time*, WIRED NEWS (Feb. 6, 2001), *at* http://www.wired.com/news/technology/1,1282,41630,00.html.

36. *See* Lemos, *supra* note 32 (discussing the ease and speed with which virulent programs can proliferate through networks).

37. NETLINGO, *supra* note 2 (defining "hacker[s]" as "skilled programmers with the reputation of having a mischievous bent for breaking into secured systems").

38. Damage, *supra* note 31.

2001,[39] and the Pentagon's computer systems have been attacked more than 22,000 times in a single year.[40]

Despite the staggering cost of computer attacks, Internet fraud and the computer- facilitated theft of proprietary information are still the leading causes of financial loss due to computer use.[41] In addition, the human cost of cybercrime often tolls without a fixed dollar figure for crimes such as cyberstalking,[42] child pornography,[43] and identity theft.[44]

Computer security experts are also worried that a well-designed worm could crash or even demolish the Internet in times of war.[45] To underscore that those are not idle concerns, in October 2001, the White House appointed a cyberspace security presidential adviser to coordinate "efforts to safeguard critical [communication] infrastructures."[46] Similarly, in view of the disruptive potential of a cyberattack on the nation's critical infrastructures, a congressional commission raised hacking to "cyberterrorism," citing "the broad economic and operational consequences of a shut down."[47]

---

39. Sam Costello, *Survey: Web Attacks Doubled in Last Year*, INFOWORLD (Oct. 9, 2001), *at* http://www2.infoworld.com/articles/hn/xml/01/10/09/011009hnsurvey.xml (citing survey by security firm TruSecure). Among "primarily large corporations and government agencies," ninety percent of 503 respondents surveyed by the Computer Security Institute (CSI) detected computer security breaches within the previous twelve months, causing hundreds of millions of dollars in losses. Press Release, Computer Security Institute, Cyber Crime Bleeds U.S. Corporations, Survey Shows; Financial Losses From Attacks Climb for Third Year in a Row, *at* http://www.gocsi.com/press/20020407.html (Apr. 7, 2002) [hereinafter Losses from Attacks].

40. Damage, *supra* note 31.

41. *See* Losses from Attacks, *supra* note 39.

42. CRIMINAL DIVISION, U.S. DEP'T OF JUSTICE, 1999 REPORT ON CYBERSTALKING: A NEW CHALLENGE FOR LAW ENFORCEMENT AND INDUSTRY, *at* http://www.usdoj.gov/criminal/cybercrime/cyberstalking.htm (last updated Oct. 18, 1999).

43. CRIMINAL DIVISION, U.S. DEP'T OF JUSTICE, COMBATING CHILD PORNOGRAPHY ON THE INTERNET, *at* http://www.usdoj.gov/criminal/cybercrime/dagceos.html (last updated Dec. 3, 1999) (arguing that child pornography on the Internet is an issue of international concern).

44. CRIMINAL DIVISION, U.S. DEP'T OF JUSTICE, IDENTITY THEFT: THE CRIME OF THE NEW MILLENIUM, *at* http://www.usdoj.gov/criminal/cybercrime/usamarch2001_3.htm (last updated Apr. 13, 2001) (arguing that the crime's impact upon the victim can be devastating).

45. Carolyn Meinel, *Code Red for the Web*, SCI. AM., Oct. 2001, at 42.

46. Jennifer Jones, *White House Creates Cyberspace Security Post*, INFOWORLD (Oct. 9, 2001), *at* http://www.infoworld.com/articles/hn/xml/01/10/09/011009hnclarke.xml.

47. Patrick Thibodeau, *U.S. Commission Outlines Steps to Fight Cyberterrorism*, INFOWORLD (Oct. 18, 2001), *at* http://www.infoworld.com/articles/hn/xml/01/10/18/011018hncyberpanel.xml. *See generally*, Brian McWilliams, *Pakistani Group Strikes U.S. Military Web Site*, NEWSBYTES (Oct. 21, 2001), *at* http://www.infowar.com/hacker/01/hack_1022010_j.shtml (reporting defacement of government web sites by a Pakistani hacking group opposing U.S. military intervention in Afghanistan).

In the aftermath of the September 11, 2001 terrorist attack on the United States, Congress passed a series of laws designed to assist federal agents to combat terrorism by expanding the government's access to electronic data in cyberspace.[48] For example, the new legislation expands the list of identifying records that law enforcement may obtain with a subpoena,[49] and permits an Internet service provider (ISP) to "voluntarily consent" to disclosing its customers' communication records during an emergency.[50] While these measures differ from the Convention's broader provisions concerning the expedited preservation of data, they represent a similar legislative push to track communication data and Internet use for policing purposes.[51]

Ironically, the lives of ordinary Americans who are not suspected of having ties to terrorism will be affected by the government's expanded definition of "cyberterrorism,"[52] because, under the new laws, a link to suspected terrorism is not even necessary.[53] As people increasingly rely on computers and the Internet to engage in a wide variety of daily tasks, common expectations of privacy also increase. However, increased criminalization and employment of invasive technology to prevent crime and terrorism may infringe upon civil liberties without actually delivering

48. Congress introduced several provisions in the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, which authorize the government to conduct secret surveillance if foreign intelligence is a "significant purpose." USA PATRIOT Act of 2001, Pub. L. No. 107-56, §§ 209–12, 224, 115 Stat. 272, 283–85, 295 (2001) (codified in scattered sections of U.S.C.).

49. USA PATRIOT Act § 210. *See also* CRIMINAL DIVISION, U.S. DEP'T OF JUSTICE, FIELD GUIDANCE ON NEW AUTHORITIES THAT RELATE TO COMPUTER CRIME AND ELECTRONIC EVIDENCE ENACTED IN THE USA PATRIOT ACT OF 2001, *at* http://www.usdoj.gov/criminal/cybercrime/PatriotAct.htm (last updated Nov. 5, 2001).

50. USA PATRIOT Act § 212 (providing exception for civil liability of service providers that make "voluntary disclosures" of content and non-content communication records in emergencies).

51. *See* Julia Scheeres, *EU Law Turns ISPs into Spies*, WIRED NEWS (May 29, 2002), *at* http://www.wired.com/news/politics/0,1283,52829,00.html (comparing the European Communications Data Protection Directive with the USA PATRIOT Act as similar legislative efforts to track communications after the September 11 terrorist attack).

52. *See* USA PATRIOT Act § 814.

53. *See* Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (2001). For example, an amendment to the Computer Fraud and Abuse Act increases penalties for hackers who damage "protected computers" used in furtherance of national security and criminal justice; lowers the jurisdictional threshold damage to $5,000 in loss; and allows for aggregation of loss to meet that amount, but without requiring a link between the offender and a suspected terrorist group or organization. *See id.* § 1030(c)(2)(B)(ii).

any increased security.[54]

B. Tracking Criminals in Cyberspace

1. The Electronic Frontier

The advent of the Internet poses a serious threat to traditional rules of law because personal computers make it easier for criminals to evade detection and prosecution.[55] A single end-to-end transmission on the Internet may often pass through a dozen or more types of carriers—for example, telephone companies, satellite networks, and ISPs—in a number of different countries employing various technical capabilities and subject to different legal systems.[56] Because electronic information easily flows across territorial borders, the Internet is not as susceptible to traditional regulatory controls.[57] As a result, much of the Internet is free from the regulation of any sovereign nation.[58]

The globalization of crime impedes traditional investigative procedures in several ways.[59] First, deterring and punishing cybercriminals

54. Carnivore and Magic Lantern, respectively, are the FBI's latest eavesdropping tools capable of recording all the digital information associated with a specific person that passes through a computer network, and recording every keystroke on that person's computer. *See* Graham B. Smith, Comment, *A Constitutional Critique of Carnivore, Federal Law Enforcement's Newest Electronic Surveillance Strategy*, 21 LOY. L.A. ENT. L. REV. 481, 492, 499 (2001) (arguing that Carnivore is a threat to Fourth Amendment privacy rights). *But see* Christopher Woo & Miranda So, *The Case for Magic Lantern: September 11 Highlights the Need for Increased Surveillance*, 15 HARV. J.L. & TECH. 521, 521–22 (2002) (arguing that the use of Magic Lantern may be necessary to combat devious and sophisticated terrorists despite the risk of intruding on people's right of privacy).

55. CRIMINAL DIVISION, U.S. DEP'T OF JUSTICE, THE ELECTRONIC FRONTIER: THE CHALLENGE OF UNLAWFUL CONDUCT INVOLVING THE USE OF THE INTERNET, *at* http://www.usdoj.gov/criminal/cybercrime/unlawful.htm (last updated Mar. 2000) [hereinafter ELECTRONIC FRONTIER].

56. *Id.*

57. *See* Henry H. Perritt, Jr., *The Internet as a Threat to Sovereignty? Thoughts on the Internet's Role in Strengthening National and Global Governance*, 5 IND. J. GLOBAL LEGAL STUD. 423, 426–27 (1998) (discussing the difficulty of regulating Internet transactions by comparison to the telegraph, telephone, radio, and television technologies).

58. James Boyle, *Foucault in Cyberspace: Surveillance, Sovereignty, and Hardwired Censors*, 66 U. CIN. L. REV. 177, 179 (1997).

59. *See* Janet Reno, United States Attorney General, Keynote Address at the Meeting of the G8 Senior Experts' Group on Transnational Organized Crime, *at* http://www.usdoj.gov/criminal/cybercrime/agfranc.htm (Jan. 21, 1997) [hereinafter Reno, Keynote Address] (identifying four areas that international law enforcement must address: (1) inadequate laws to prosecute computer crimes; (2) poor technical ability to locate cybercriminals; (3) insufficient cooperation in the collection and sharing of evidence of the crimes; and (4) lack of

requires an international legal framework to investigate and prosecute computer offenses.[60] Because information can be transmitted through data networks that span the globe, an online offender can operate from a location outside the jurisdiction that proscribes his activities.[61] For example, although federal law prohibits the placing of wagers when either or both the sender and receiver are in states or countries where gambling is illegal,[62] an Internet gambling site operating within a jurisdiction where gambling is legal can still be accessed by persons residing in states or countries where gambling is illegal. Similarly, an obscenity law interpreted in light of local standards[63] may be evaded by an individual who publishes an offensive Web site on a computer server located outside the locality. Further, evidence stored on computers in remote or unknown locations takes the investigation of cybercrimes outside the "exclusive purview of any single jurisdiction"[64] and increases the chances that communication data will become unavailable or lost, especially when criminals weave communications through multiple countries.[65]

Second, because everything on the Internet—from email to an electronic heist[66]—is information, investigators must locate the true source of the communication to connect the cybercrime with a real person in the physical world.[67] The infrastructure of the Internet, however, does not provide a ready mechanism for tracing the "electronic trail" leading from the crime back to the perpetrator.[68] In the absence of actual fingerprints, the lack of identifying mechanisms on the Internet makes it especially easy for criminals to disguise themselves, thereby frustrating the ability of law enforcement to track them down.[69]

For example, a savvy criminal can routinely cover one's tracks by

---

resources and trained personnel to investigate and combat high-tech crimes).

60. Robinson, Remarks, *supra* note 10.

61. ELECTRONIC FRONTIER, *supra* note 55.

62. *See* 18 U.S.C. § 1084 (2001).

63. *See* Miller v. California, 413 U.S. 15, 24 (1973).

64. ELECTRONIC FRONTIER, *supra* note 55.

65. Robinson, Remarks, *supra* note 10.

66. Electronic thieves, for example, have broken into the networks of United States banks and carried out unauthorized electronic funds transfers to siphon amounts of up to $1 million out of the system. *See, e.g.*, Sandeep Junnarkar, *Can Your Bank Stop an E-stickup?*, ZDNET NEWS (May 1, 2002), *at* http://.zdnet.com.com/2102-1106-896101.html; Robert Lemos, *Western Union Data Heist: "Human Error,"* ZDNET NEWS (Sept. 10, 2000), *at* http://zdnet.com.com/2100-11-523769.html.

67. *See* Robinson, Remarks, *supra* note 10.

68. *Id.*

69. *See* ELECTRONIC FRONTIER, *supra* note 55.

providing false subscriber information when connecting to the Internet.[70] Even when online services maintain a log of the Internet Protocol (IP) number of the computer or the ISP from where the individual accessed the Internet,[71] the account used may have been hacked[72] and may not disclose the actual source of the communication.[73]

In addition, because the electronic trail of a crime may become untraceable once the criminal is offline, another obstacle arises due to the lack of communications data.[74] Carriers maintain far fewer phone lines than subscribers and often fail to retain the data necessary to link a customer with a specific incoming line.[75] The easy solution is to require carriers to retain access to user information for each link in the chain of transmission to be able to identify the source of every call.[76] This may not be accomplished, however, without infringing on users' legitimate ability to remain anonymous.[77]

Lastly, even if a foreign legal regime[78] does not hamper a local investigation, the "electronic trail" may go cold due to a slow response by foreign law enforcement in providing assistance and cooperation in the investigation of international computer crimes.[79] Operational challenges in coordinating the investigation of international crimes arise due to deficits in the "preservation of and quick access to electronic data;"[80] deficiencies in

---

70. *See* Robinson, Remarks, *supra* note 10.

71. An IP number is a unique identifier for every computer or user connected to the Internet. NETLINGO, *supra* note 2. In the case of a "dynamic IP," the number is assigned to a user for a particular session, and when the user signs off, it is assigned to a new user. CHRISTOPHER M.E. PAINTER, U.S. DEP'T OF JUSTICE, TRACING IN INTERNET FRAUD CASES: PAIRGAIN AND NEI WEBWORLD, *at* http://www.usdoj.gov/criminal/cybercrime/usamay2001_3.htm (last updated July 9, 2001) (By maintaining logs of IP numbers, dates, and exact times when the user logged on, it is possible to identify the user who made the logs.).

72. Some service providers maintain "radius logs," which indicate the telephone numbers from where the calls to the Internet were placed. *See* PAINTER, *supra* note 71.

73. Robinson, Remarks, *supra* note 10.

74. *See* ELECTRONIC FRONTIER, *supra* note 55.

75. *Id.* (The same identification number can be assigned to various users logging onto the network at different times.).

76. *See* Reno, Keynote Address, *supra* note 59.

77. *See* discussion *infra* Part IV.A. (arguing for the preservation of truly anonymous online communications coupled with user accountability).

78. *See* ELECTRONIC FRONTIER, *supra* note 55.

79. *See id.*

80. CRIMINAL DIVISION, U.S. DEP'T OF JUSTICE, COMMUNIQUE ANNEX: PRINCIPLES TO COMBAT HIGH-TECH CRIME, *at* http://www.usdoj.gov/criminal/cybercrime/principles.htm (last updated Feb. 18, 1998).

the "timely gathering and exchange of evidence;"[81] the lack of "transborder electronic access by law enforcement to publicly available . . . information;"[82] and the lack of international "forensic standards for retrieving and authenticating electronic data for use in criminal investigations."[83] A sufficient number of adequately trained and equipped law enforcement personnel allocated to assisting investigators from other countries is also essential to combat the global threat of cybercrime.[84]

2. Anonymous Communications

While experienced criminals know how to conceal their tracks in cyberspace, anonymous software makes it possible for anyone to completely erase the marks identifying the source of the communication, so that pinning a person down to a geographic location becomes technically impossible.[85] For example, anonymous remailers[86] enable users to send electronic mail to people or newsgroups[87] without revealing their names or email addresses to the recipients. By stripping the source IP address information from email messages, remailers leave carriers without the critical traffic data necessary to identify users, thereby posing an often insurmountable technical challenge for law enforcement and private industries.[88]

A second identity-cloaking technique, appropriately known as encryption,[89] reinforces users' ability to speak anonymously on the Internet

---

81. *Id.*

82. *Id.*

83. *Id.*

84. *See* Reno, Keynote Address, *supra* note 59.

85. Robinson, Remarks, *supra* note 10.

86. André Bacard, *Anonymous Remailer FAQ*, *at* http://www.andrebacard.com/remail.html (last updated Feb. 15, 2002). *See, e.g.*, ULTIMATE ANONYMITY, *at* http://ultimate-anonymity.com (last visited Aug. 20, 2002) (service provides tools and techniques enabling complete online anonymity from anonymous web browsing and email, anonymous participation in newsgroups and web based chat rooms); FILETOPIA: STRONG ENCRYPTION, CHAT & FILE SERVER, *at* http://www.filetopia.org/home.htm (last visited Aug. 22., 2002) (technology allows individuals to go online undetected, post anonymous messages, send scrambled messages, and block unwanted email).

87. NETLINGO, *supra* note 2 (defining a "newsgroup" as a discussion forum on the Internet which "allows users to post messages and reply to other users").

88. Dr. Fred Cohen, Center for Democracy & Technology, *Cyber Threats and the US Economy: Statement for the Joint Economic Committee*, *at* http://www.cdt.org/security/dos/000223senate/cohen.html (Feb. 23, 2000) ("The recent denial of service attacks could have been defeated if it weren't for the ease of anonymity in the Internet.").

89. *See* Junger v. Daley, 209 F.3d 481, 482 (6th Cir. 2000) (describing encryption as "the process of converting a message from its original form ('plaintext') into a scrambled form

by scrambling or encoding every message into an unreadable form that no one, except the intended reader, can decode within a reasonable time.[90] By routing a message through a series of remailers and employing encryption, the sender ensures that no one, not even the recipient, can identify the source of the message.[91]

Similarly, "anonymizing" proxies[92] permit users to surf the web incognito. Anonymizing proxies act as a "gateway" between the user's workstation and the Internet by encrypting web content, hiding the user's address identifier, and blocking "cookies" from being stored on the user's hard drive.[93] Because the content of one's sessions is scrambled, unauthorized parties cannot obtain any identifying information, thus ensuring one's privacy while surfing the web.[94]

Anonymous technology and encryption pose a considerable threat to government and private institutions by enabling criminals to operate surreptitiously, without fear of being detected.[95] However, because online anonymity consists of the ability to control the electronic information used to identify oneself,[96] in the context of telecommunications, criminals are indistinguishable from legitimate users of anonymous technology. Clearly, this brings individuals who wish to remain anonymous on the Internet in direct conflict with government, which would like to know exactly who is accessing the network at any given time. However, regulating anonymous technology by uniformly defeating the service providers' technical guarantees of privacy is not a good solution, and, furthermore, constitutes a ban on legitimate anonymous speech. The critical challenge for governments is to control the new technology *without* eliminating its legitimate uses.

('ciphertext').").

90. GODWIN, *supra* note 5, at 137.

91. By routing messages through a series of anonymous remailers, a technique known as "chained remailing," neither the recipient nor any of the remailers in the chain can identify the sender of the message without the cooperation of every prior remailer in the chain. *Flood Control*, *supra* note 13, at 418. Further, remailer services usually refuse to retain subscriber information. *See id.* at 415–18.

92. *See, e.g.*, *Anonymous Surfing Accelerator*, Megaproxy, *at* http://www.megaproxy.com/_anonymous/_surfing/_services/ (last modified Aug. 25, 2002).

93. *Id.*

94. *Id.*

95. *See* ELECTRONIC FRONTIER, *supra* note 55.

96. Perrin Beatty, Canadian Minister of Department of Communications, Privacy Protection in Telecommunications, *at* http://www.ifla.org/documents/infopol/canada/privacy.txt (last visited Oct. 2, 2001).

C. The International Convention

Governments have confronted the dangers of cyberspace by devoting significant resources towards formulating a legal framework that addresses the technical and operational challenges of computer crime.[97] The Convention on Cybercrime (the "Convention") is the most comprehensive response to date.[98] Considered "one of the most important legal instruments elaborated within the Council of Europe,"[99] the Convention was approved by the Committee of Ministers of the Council of Europe (COE),[100] and on November 23, 2001, the Convention was signed by twenty-six member states of the COE along with four non-member states—Canada, Japan, South Africa, and the United States.[101] Although only two countries have ratified the treaty,[102] the Convention will go into effect "three months after the date on which five States, including at least three member States of the Council of Europe," have ratified it.[103]

1. Measures to Be Taken

The main objective of the Convention, as defined in the preamble, is to pursue "a common criminal policy aimed at the protection of society against cybercrime, *inter alia* by adopting appropriate legislation and fostering international co-operation."[104] The final draft of the Convention covers three main topics: (1) harmonization of the national laws defining substantive criminal offenses; (2) definition of investigative and procedural provisions to cope with global networks; and (3) establishment of

97. *See* Robinson, Remarks, *supra* note 10.

98. *See Final Draft*, *supra* note 18.

99. *Id.* (quoting Hans Christian Krüger, Deputy Secretary General of the Council of Europe).

100. 30 States Sign the Convention, *supra* note 17.

101. *Id.*

102. Council of Europe, Convention on Cybercrime, European Treaty Series (ETS) no. 185, Ratification Status, *at* http://conventions.coe.int/Treaty/EN/searchsig.asp?NT=185&CM=1&DF=21/11/02 (last visited Nov. 21, 2001). The Council of Europe is also working on the First Protocol, which criminalizes "hate speech," and on a Second Protocol to address how to identify, filter, and trace communications between suspected terrorists. Declan McCullagh, *Beefed-Up Global Surveillance?*, WIRED NEWS (Feb. 20, 2002), *at* http://www.wired.com/news/politics/0,1283,50529,00.html.

103. Council of Europe, Convention on Cybercrime, European Treaty Series (ETS) no. 185, *at* http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm (last visited Nov. 21, 2002) [hereinafter Cybercrime Convention].

104. *Id.* pmbl.

procedures to create an effective system of international cooperation.[105]

The Convention defines substantive criminal laws to be legislatively adopted by all signatory states. It covers crimes in four main categories: (1) "offenes [sic] against the confidentiality, integrity and availability of computer data and systems;"[106] (2) computer-related offenses;[107] (3) content-related offenses (for example, child pornography);[108] and (4) "offences [sic] related to infringements of copyright and related rights."[109] In addition, signatory nations must criminalize attempting and aiding or abetting of the offenses defined in accordance with Articles 2 through 10 of the Convention;[110] provide for criminal corporate liability;[111] and ensure that criminal offenses are "punishable by effective, proportionate and dissuasive sanctions, which include deprivation of liberty."[112] To take into account the different legal systems of the signatory nations, the crimes are broadly defined, and an explanatory memorandum[113] describes the crimes in more detail to ensure that parties enforce the Convention in a consistent manner.[114]

The Convention also seeks to harmonize new procedures and rules of "mutual assistance" to aid law enforcement in the investigation of cybercrimes.[115] Signatory countries are required to ensure that certain measures are available under their national law: "[e]xpedited preservation of stored computer data;"[116] expedited preservation and disclosure of traffic data;[117] the ability to order a person to provide computer data and to order an ISP to provide subscriber data under its control; "[r]eal-time collection

105. *See* Final Draft, *supra* note 18.

106. Cybercrime Convention, *supra* note 103, arts. 2–6.

107. Computer offenses include those committed with the intent to falsify computer data and those causing the loss of property by computer-related fraud. *Id.* arts. 7–8.

108. *Id.* art. 9.

109. *Id.* art. 10.

110. *Id.* art. 11.

111. *Id.* art. 12.

112. Cybercrime Convention, *supra* note 103, art. 13(1).

113. Council of Europe, Convention on Cybercrime, European Treaty Series (ETS) no. 185, Explanatory Report, *at* http://conventions.coe.int/Treaty/en/Reports/Html/185.htm (Nov. 8, 2001) [hereinafter Explanatory Report].

114. FAQ ABOUT THE CONVENTION, *supra* note 19.

115. Press Release, Council of Europe, Main Lines of the Convention, *at* http://press.coe.int/dossiers/107/E/e-grdlignes.htm (last visited Oct. 7, 2001) [hereinafter Main Lines].

116. Cybercrime Convention, *supra* note 103, art. 16.

117. *Id.* art. 17.

of traffic data;"[118] and interception of content data.[119]

The Convention provides that signatory countries must adopt measures to establish jurisdiction over any offenses committed in their respective territories or by their nationals.[120] Moreover, the Convention empowers legal authorities and police in one country to collect evidence of cybercrimes for police in another country, and establishes a "24/7 network"[121] operating around the clock, seven days per week, to provide immediate assistance with ongoing investigations.[122]

2. Privacy Concerns

If ratified, the Convention will be the first international treaty to allow police in one country to request that their counterparts abroad collect an individual's computer data, have the individual arrested and extradited to serve a prison sentence abroad.[123] Given the unprecedented exchange of personal data between participating countries, some of which may have lesser standards of privacy and due process, individuals should be concerned about the collection and monitoring of their personal information. While the Convention makes a passing reference to a number of international instruments which provide protection for personal data,[124] it does not, however, specify what safeguards must apply.[125]

Article 15 of the Convention, which deals with "conditions and safeguards," states that the "establishment, implementation and application of the powers and procedures provided for in [Section 2 of the Convention pertaining to procedural law] are subject to conditions and safeguards" provided under the domestic law of each signatory country,[126] but it does

---

118. *Id.* art. 20.

119. *Id.* art. 21.

120. *Id.* art. 22.

121. *Id.* art. 35.

122. *See* Main Lines, *supra* note 115.

123. *See generally* Mike Godwin, *International Treaty on Cybercrime Poses Burden on High-Tech Companies*, IP WORLDWIDE (Apr. 4, 2001), *at* http://www.law.com (explaining that this treaty would permit extradition of computer users in other countries).

124. Cybercrime Convention, *supra* note 103, pmbl.

125. *See* Center for Democracy & Technology, *Comments of the Center for Democracy and Technology on the Council of Europe Draft "Convention on Cyber-crime" (Draft No. 25)*, *at* http://www.cdt.org/international/cybercrime/010206cdt.shtml (Feb. 6, 2001) [hereinafter *CDT Comments*] (criticizing the Council of Europe, a governmental body created to promote human rights, for not specifying what privacy protections should limit government authority).

126. Cybercrime Convention, *supra* note 103, art. 15.

not require such provisions to be actually instituted.[127] Instead, the Convention merely hints at vague procedural safeguards,[128] while granting broad powers to government investigators in countries such as Romania and Albania,[129] former Soviet bloc nations that have a less than robust tradition of checks and balances on police power.[130]

What would also change under the Convention is that in addition to complying with requests submitted by U.S. law enforcement officials, ISPs and telephone companies would have to respond to warrants and court orders from forty-three Council of Europe nations.[131] Because the Convention mandates "mutual assistance" and extradition between nations without requiring "dual criminality,"[132] a U.S. citizen or corporation may be prosecuted abroad for crimes that do not exist in the United States.[133] The lack of dual criminality is a special problem when considering the vast differences in punishment for similar offenses and the considerable lack of adequate due process and human rights protections in various countries.[134]

Not surprisingly, the Convention has met with vigorous opposition.[135] Both corporate interests, such as AT&T, as well as civil liberties groups, such as Privacy International and the Center for Democracy & Technology, have decried the financial and privacy costs of the Convention.[136] In particular, civil liberties groups and ISPs have voiced a common objection to the requirement that ISPs and network administrators keep detailed logs of network activity.[137] ISPs have also opposed the Convention on the

---

127. *See id.*

128. *See id.*

129. Albania and Croatia are the only member states of the Council of Europe so far to have ratified the treaty. Council of Europe, Convention on Cybercrime, European Treaty Series (ETS) no. 185, Ratification Status, *at* http://conventions.coe.int/Treaty/EN/searchsig.asp?NT=185&CM=1&DF=21/11/02 (last visited Nov. 21, 2002).

130. Godwin, *supra* note 123.

131. *See id.*

132. United States courts hold that dual criminality is satisfied if the offense charged is "considered criminal under the laws of both surrendering and requesting nations." Murphy v. United States, 199 F.3d 599, 602 (2d Cir. 1999) (quoting Clarey v. Gregg, 138 F.3d 764, 765 (9th Cir. 1998)).

133. *See* Godwin, *supra* note 123.

134. *See* Ellen Goodman, *The Hidden Suffering of Women in Afghanistan*, BOSTON GLOBE, Dec. 6, 1998, at D7 (demonstrating the value of dual criminality by analogizing to the protection of human rights in the case of women).

135. *See* Big Brother, *supra* note 23.

136. *See* Godwin, *supra* note 123; *see also CDT Comments*, *supra* note 125.

137. Lesley Stones, *Forty Nations Unite to Define Cybercrime and Fight Net Bandits*, BUS. DAY (South Africa), Nov. 2, 2000, at 20 (reporting that "[m]any service providers believe that such clauses would breach the confidentiality agreements they sign with their customers").

ground that it does not provide reimbursement for the increased costs of surveillance and storage of information.[138] The U.S. Chamber of Commerce, the world's largest business federation representing more than three million members, has warned that the Convention would impose "unworkable and possibly unlawful restrictions" on U.S. firms.[139]

The requirement that signatory nations enact measures to "obtain the expeditious preservation of specified [stored] computer data," including traffic data,[140] directly impacts providers of anonymous technology, and may defeat the ability of individuals to send and receive anonymous messages over the Internet.[141] The requirement that each signatory adopt "legislative and other measures as may be necessary" to compel service providers to disclose subscriber information under their control[142] has a concurrent effect. The stored data includes the "subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement."[143]

While the text of the Convention does not explicitly state that a provider, such as an anonymous remailer, must collect and keep information to identify its customers, any electronic data already stored in the provider's computer network must be turned over to the appropriate authorities.[144] Ironically, the recent Communications Data Protection Directive passed by the European Parliament[145] has affirmed the concern that after signing the treaty governments would be prompted to enact legislation forcing service providers to be able to always identify their customers.[146]

---

138. *See* Privacy International, *Comments of the American Civil Liberties Union, the Electronic Privacy Information Center and Privacy International on Draft 27 of the Proposed CoE Convention on Cybercrime, at* http://www.privacyinternational.org/issues/cybercrime/coe/ngo_letter_601.htm (June 7, 2001) [hereinafter *ACLU Letter*].

139. Press Release, U.S. Chamber of Commerce, U.S. Chamber Opposes European Cyber Crime Treaty, *at* http://www.uschamber.com/Press+Room/2000+Releases/December+2000/00-229.htm (Dec. 8, 2000).

140. Cybercrime Convention, *supra* note 103, arts. 16–17.

141. *See CDT Comments*, *supra* note 125.

142. Cybercrime Convention, *supra* note 103, art. 18.

143. *Id.* art. 18(3)(b).

144. *See id.* art. 18.

145. The directive, which faces approval by the fifteen European Union member countries, mandates that telecommunications companies keep detailed records of customers' data. Julia Sheeres, *Europe Passes Snoop Measure*, WIRED NEWS (May 30, 2002), *at* http://www.wired.com/news/politics/0,1283,52882,00.html.

146. *CDT Comments*, *supra* note 125.

Lastly, Article 19 requires that signatory parties adopt laws that compel "any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein" to disclose the "necessary information"[147] required to retrieve any stored data, which effectively bans encryption.[148] In view of the Convention's broad requirements for data preservation, divulgence of subscriber information, and compelled disclosure of encryption code, the treaty is certain to have a chilling effect on anonymity online.

III. A BRIEF HISTORY OF ANONYMITY

A. Anonymous Speech and the First Amendment

"Congress shall make no law . . . abridging the freedom of speech, or of the press . . . ."[149] The First Amendment does not specifically mention anonymous speech,[150] but considering that the authors of the Federalist Papers concealed their identities when writing in support of the Constitution, anonymity may be essential to political freedom itself.[151]

The Supreme Court has interpreted the First Amendment "to prevent the majority, through acts of Congress, from silencing those who would express unpopular or unconventional views."[152] A primary function of the amendment is to ensure political discourse.[153] The Court has repeatedly endorsed a "profound national commitment to the principle that debate on public issues should be uninhibited, robust, and wide-open."[154] Presumably, such openness affirms anonymous political speech, but while political speech "occupies the core of the protection afforded by the First

147. Cybercrime Convention, *supra* note 103, art. 19(4).

148. *See ACLU Letter*, *supra* note 130 (explaining that both the encryption code and the plain text of the encrypted files must be turned over to the authorities).

149. U.S. CONST. amend. I.

150. *See id.* Nor is there a "record of discussions of anonymous political expression either in the First Congress, which drafted the Bill of Rights, or in the state ratifying conventions." McIntyre v. Ohio Elections Comm'n, 514 U.S. 334, 360 (1995) (Thomas, J., concurring).

151. *See* Talley v. California, 362 U.S. 60, 65 (1960). Justice Black noted that persecuted groups throughout history have been able to challenge oppression "either anonymously or not at all." *Id.* at 64. Anonymous publishing was so widespread during the Revolutionary period that only two Federalist essays appear to have been signed by their authors. *McIntyre*, 514 U.S. at 368 (Thomas, J., concurring).

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

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

154. N.Y. Times Co. v. Sullivan, 376 U.S. 254, 270 (1964).

Amendment,"[155] anonymity has strong detractors on the Court.[156]

Indeed, on first impression, anonymity seems deviant, positively anarchical. Why would people want to hide their true identity? For some, this is cause for immediate suspicion.[157] It is not surprising, therefore, that even though anonymous authors have long been acknowledged as having made invaluable contributions to civilization,[158] the courts have only recently regarded anonymous speech as a right protected by the First Amendment.[159]

1. Freedom of Association and Inviolable Privacy

It is well established that the people may advocate their political beliefs without state scrutiny.[160] In *NAACP v. Alabama ex rel. Patterson*,[161] the Supreme Court upheld the NAACP's refusal to disclose its membership list in accordance with a court order because compelled disclosure would have curtailed the members' ability to promote their common beliefs.[162] The NAACP showed that such prior disclosures of its members' identities subjected them to economic reprisals and public hostility.[163]

In effect, the state was unable to demonstrate that the membership list was essential to a governmental purpose.[164] Against the efforts of the state to compel the NAACP to cease its activities in Alabama, the Court recognized that the "inviolability of privacy" might be "indispensable to preservation of freedom of association, particularly where a group espouses

155. *McIntyre*, 514 U.S. at 346.

156. *See id.* at 385 (Scalia, J., dissenting) (claiming that the "very purpose" of anonymity is to facilitate wrongs by "eliminating accountability.").

157. *See* Cohen, *supra* note 88 ("I find that the ability to act with relative anonymity in the Internet is primarily being used for criminals to avoid attribution and to hide their crimes.").

158. *Talley*, 362 U.S. at 64 ("Anonymous pamphlets, leaflets, brochures and even books have played an important role in the progress of mankind.").

159. *McIntyre*, 514 U.S. at 357 (stating that anonymity "exemplifies the purposes behind the Bill of Rights, and of the First Amendment in particular: to protect unpopular individuals from retaliation—and their ideas from suppression—at the hand of an intolerant society.").

160. *See* NAACP v. Alabama *ex rel.* Patterson, 357 U.S. 449, 462 (1958). Political expression receives the broadest protection "to assure the unfettered interchange of ideas for the bringing about of political and social changes desired by the people." Roth v. United States, 354 U.S. 476, 484 (1957).

161. 357 U.S. 449 (1958).

162. *Id.* at 462–66.

163. *Id.* at 462.

164. *Id.* at 466.

dissident beliefs."[165]

The nexus between privacy, anonymity, and political expression was expanded in later decisions.[166] In the landmark case, *Talley v. California*,[167] the Court upheld one individual's interest to remain anonymous when distributing handbills advertising a boycott against certain employers accused of discriminating against minorities.[168] *Talley* recognized that "anonymity has sometimes been assumed for the most constructive purposes."[169] In *Talley*, the Supreme Court extended its earlier decision in *Lovell v. City of Griffin*[170] that the freedom to distribute information is essential to the freedom of expression, and that an "identification requirement" would tend to restrict that freedom.[171]

2. Strict Scrutiny and Content-Based Restrictions

Both *Patterson* and *Talley* recognized that only a compelling governmental interest could impinge on the freedom of speech and association, advancing significant protection for anonymous speech.[172] However, the ordinance at issue in *Talley* was deemed void on its face because it was overbroad, barring all anonymous handbills "under all circumstances anywhere."[173] By contrast, in *Buckley v. Valeo*,[174] by employing the same "strict standard of scrutiny" to evaluate an ordinance that curtailed anonymous political speech, the Court reached a different conclusion.[175] The *Buckley* court held that while disclosure requirements,

---

165. *Id.* at 462.

166. *See* Brown v. Socialist Workers '74 Campaign Comm., 459 U.S. 87, 91 (1982) (noting that the "Constitution protects against the compelled disclosure of political associations"); Shelton v. Tucker, 364 U.S. 479, 480, 490 (1960) (holding invalid a statute that compelled teachers to disclose associational ties); Bates v. City of Little Rock, 361 U.S. 516, 529 (1960) (holding that the NAACP did not have to disclose its membership list at the peril of its freedom of assembly).

167. 362 U.S. 60 (1960).

168. *Talley*, 362 U.S. at 63–65 (invalidating a flat ban on the distribution of handbills).

169. *Id.* at 65.

170. 303 U.S. 444, 450–52 (1938) (holding that a municipal ordinance prohibiting the distribution of literature without a permit was an unconstitutional infringement on First Amendment freedom of speech and of the press).

171. *Talley*, 362 U.S. at 64.

172. *See id.* at 66 (Harlan, J., concurring) (citing the holding in *Patterson*, 357 U.S. at 463, 464).

173. *Id.* at 64.

174. 424 U.S. 1 (1976).

175. *Id.* at 75. The Court upheld mandatory disclosure of campaign-related expenditures to the Federal Election Campaign Act, because the requirement was "narrowly limited to those

by themselves, "can seriously infringe on privacy of association and belief guaranteed by the First Amendment,"[176] governmental interests can be "sufficiently important to outweigh the possibility of infringement."[177]

More recently, in *McIntyre v. Ohio Elections Commission*,[178] the Court struck down as unconstitutional Ohio's prohibition on the distribution of anonymous campaign literature.[179] In this case, Mrs. McIntyre distributed leaflets that communicated opposition to a proposed school tax levy, to people attending a public meeting at a middle school in Westerville, Ohio.[180] The Ohio Tax Commission charged Mrs. McIntyre with violating a state statute prohibiting the distribution of "unsigned documents designed to influence voters in an election"[181] because some of Mrs. McIntyre's handbills purported to express the views of "Concerned Parents and Tax Payers."[182]

The state argued that the prohibition prevented "the dissemination of untruths" intended to influence the electoral process.[183] Rejecting this argument, the Court noted that the Ohio statute contained "no language limiting its application to fraudulent, false, or libelous statements."[184] As in *Patterson* and *Talley*, the *McIntyre* Court was concerned that a ban on anonymity "places a more significant burden on advocates of unpopular causes than on defenders of the status quo."[185] As such, the ban could be viewed as retaliation against an unpopular point of view—as an outright and "direct regulation of the content of speech."[186]

Principally, *McIntyre* illustrates that "our society accords greater weight to the value of free speech than to the dangers of its misuse."[187] However, the case may likewise be interpreted as being limited to protecting political speech, which "by its nature will sometimes have

---

situations where the information sought has a substantial connection with the governmental interests sought to be advanced." *Id.* at 81.

176. *Id.* at 64.

177. *Id.* at 66.

178. 514 U.S. 334 (1995).

179. *Id.* at 357.

180. *Id.* at 337.

181. *Id.* at 338.

182. *Id.* at 337.

183. *Id.* at 344.

184. *McIntyre*, 514 U.S. at 344.

185. *Id.* at 345 n.8.

186. *Id.* at 345.

187. *Id.* at 357.

unpalatable consequences."[188] Indeed, the Court indicated that even in the context of political speech, which occupies the "core of the protection" granted by the First Amendment, it would uphold a statute "narrowly tailored" to serve a clear and important government objective.[189] Thus, despite *McIntyre*'s rhetoric about the "tradition of anonymity in the advocacy of political causes,"[190] the Court recognized that "a State's enforcement interest might justify a more limited identification requirement."[191]

Because of its narrow holding, *McIntyre*'s significance to the regulation of non-political anonymous speech is uncertain in situations where the government's objective in the regulation is substantial.[192] Nevertheless, *McIntyre* marks a significant departure from the Court's jurisprudence culminating with *Talley*, holding that the "identity of the speaker is no different from other components of the document's content that the author is free to include or exclude."[193] By suggesting that the author's decision to remain anonymous is a decision "concerning omissions or additions to the content of a publication,"[194] the Court implied that regulations of anonymity should be subject to the same exacting scrutiny that applies to content-based restrictions on speech.[195] Further, recent decisions by lower courts upholding anonymous authorship on the Internet indicate that *McIntyre*'s holding may be generalized to non-political speech in the electronic media as well as in print.[196]

B. Anonymity on the Internet

Speech on the Internet enjoys the same level of protection from governmental interference as does speech in traditional public forums.[197]

---

188. *Id.*

189. *Id.* at 346–47.

190. *McIntyre*, 514 U.S. at 343.

191. *Id.* at 353; *but see* Buckley v. Am. Constitutional Law Found., 525 U.S. 182, 188–89, 199 (1999) (invalidating a Colorado requirement that petition circulators be registered voters, wear identification badges, disclose their names, addresses, and the total amount they were paid).

192. *McIntyre*, 514 U.S. at 358 (Ginsburg, J., concurring) ("We do not thereby hold that the State may not in other, larger circumstances require the speaker to disclose its interest by disclosing its identity.").

193. *Id.* at 348.

194. *Id.* at 342.

195. *Id.* at 346.

196. *See* Doe v. 2TheMart.com, Inc., 140 F. Supp. 2d 1088, 1097 (W.D. Wash. 2001); *see also* ACLU v. Miller, 977 F. Supp. 1228, 1232 (N.D. Ga. 1997).

197. ACLU v. Reno, 929 F. Supp. 824, 842 (E.D. Pa. 1996).

Indeed, as "the most participatory form of mass speech yet developed,"[198] the Internet has enjoyed relatively greater immunity from government supervision and regulation than other media.[199] While the Supreme Court has yet to weigh the constitutionality of a restriction on anonymous Internet speech, several federal courts have upheld the right of individuals to remain anonymous online.[200]

1. Unmasking John Doe

In *ACLU v. Miller*,[201] a federal district court enjoined a Georgia statute that prohibited fraudulent transmissions on the Internet.[202] Specifically, the statute made it illegal to falsely identify oneself while transmitting information over the Internet.[203] The court concluded that the statute was not drafted precisely enough to avoid proscribing protected speech.[204] Citing *McIntyre*, the court determined that Georgia's online identification requirement constituted "a presumptively invalid content-based restriction."[205] Further, the statute was not narrowly tailored to only prohibit "fraudulent" transmissions, as defined in the criminal code.[206] Even though the legislation could be used to prosecute persons who falsely identify themselves in order to defraud the public, the statute was constitutionally invalid because it targeted a "substantial category of speakers" who employ deception and anonymity to avoid being ostracized or harassed, to prevent being discriminated against, or to protect their privacy.[207]

Similarly, in a precedent-setting case dealing with online defamation, a federal district court in Washington quashed a subpoena issued by a private corporation seeking to force an ISP to disclose the identity of persons who spoke anonymously on a message board.[208] Specifically, the

198. *Id.* at 883.

199. Reno v. ACLU, 521 U.S. 844, 868–69 (1997).

200. *See, e.g.*, Dendrite Int'l, Inc. v. Doe No. 3, 775 A.2d 756, 771 (N.J. Super. Ct. App. Div. 2001); *2TheMart.com*, 140 F. Supp. 2d at 1097; Columbia Ins. Co. v. Seescandy.com, 185 F.R.D. 573, 578 (N.D. Cal. 1999); *Miller*, 977 F. Supp. at 1232 (N.D. Ga. 1997).

201. 977 F. Supp. 1228 (N.D. Ga. 1997).

202. *Id.* at 1231, 1235.

203. *Id.* at 1230.

204. *Id.* at 1233 (holding that the Georgia statute was "not readily susceptible to a limiting construction and . . . not narrowly tailored to promote a compelling state interest").

205. *Id.* at 1232.

206. *Id.*

207. *Id.* at 1233.

208. *2TheMart.com.*, 140 F. Supp. 2d at 1098. The court said that "[a]court order, even

court considered several factors in determining whether a subpoena should issue and concluded that when First Amendment rights are at stake, only information "directly and materially relevant" to a core claim or defense can outweigh the individual's right to speak anonymously.[209] The court emphasized that "[p]eople who have committed no wrongdoing should be free to participate in online forums without fear that their identity will be exposed."[210]

2. Encrypted Content

Encryption technology is crucial to sending and receiving truly anonymous communication on the Internet.[211] Rather than preventing the disclosure of the "non-content" source of the message, such as the address header, which is erased by the remailer, encryption ensures that the actual "content" of the electronic message remains anonymous.[212] A discussion regarding encryption and the various government proposals to regulate it is beyond the scope of this Comment.[213] Attempts to ban encryption have been unsuccessful, however, and the nature of the technology is such that the most severe laws could not completely curtail its use.[214] Current U.S. policy allows consumers access to privacy-enhancing encryption.[215] This is the outcome of both a long debate in Washington over improving privacy online[216] and judicial recognition of the connection between the regulation of cryptography and people's ability to communicate privately and anonymously in "an increasingly monitored world."[217]

---

when issued at the request of a private party in a civil lawsuit, constitutes state action and as such is subject to constitutional limitations." *Id.* at 1091–92.

209. *Id.* at 1095.

210. *Id.* at 1092 (citing *Seescandy.com*, 185 F.R.D. at 578).

211. *See Flood Control*, *supra* note 13, at 418–20.

212. *See id.*

213. *See* A. Michael Froomkin, *The Metaphor Is the Key: Cryptography, the Clipper Chip, and the Constitution,* 143 U. PA. L. REV. 709 (1995) (giving a comprehensive discussion of encryption).

214. *See* HENRY B. WOLFE, CATO INSTITUTE BRIEFING PAPERS NO. 42, THE MYTH OF SUPERIORITY OF AMERICAN ENCRYPTION PRODUCTS, *available at* http://www.cato.org/pubs/briefs/bp42.pdf (Nov. 12, 1998).

215. Press Release, Center for Democracy & Technology, New U.S. Encryption Regulations a Major Step Forward for Online Privacy, *at* http://www.cdt.org/press/000113press.shtml (Jan. 13, 2000).

216. *Id.*

217. *See* Michael Froomkin, *Statement on the* Bernstein *Decision*, *at* http://www.law.miami.edu/~froomkin/bernstein99.htm (May 7, 1999) (describing the Ninth Circuit's decision upholding encryption source code as protected speech as a major victory for

Although the U.S. government continues to impose restrictions on the export of encryption, in three separate lawsuits[218] cryptographers have argued that the requirement to obtain an export license before publishing encryption source code[219] on the Internet constitutes censorship of protected First Amendment speech. In one of the cases, *Bernstein v. Dep't of State*,[220] a district court held that encryption software is "expression" for First Amendment purposes and is entitled to protection against an order that precludes a person from speaking in advance.[221] Although district courts in two other cases rejected similar challenges and upheld the federal export regulation,[222] a more recent decision on this matter issued by the Sixth Circuit reaffirmed that "the First Amendment protects computer source code."[223] By designating source code as expressive speech, the court ensured that a ban on encrypted computer code would be subject to the same exacting scrutiny that applies to all content-based restrictions on speech.[224]

IV. THE BIG CHILL: THE CONVENTION'S EFFECTS ON SPEECH

A. Privacy, Anonymity, and Expression

As the Internet exceeds 200 million users worldwide,[225] individuals increasingly must contend with the "information wants to be free" imperative of cyberspace.[226] The digitization of information ranging from

---

privacy and the First Amendment).

218. *See* Junger v. Daley, 209 F.3d 481 (6th Cir. 2000); Bernstein v. Dep't of State, 922 F. Supp. 1426 (N.D. Cal. 1996); Bernstein v. Dep't of State, 945 F. Supp. 1279 (N.D. Cal. 1996); Bernstein v. Dep't of State, 974 F. Supp. 1288 (N.D. Cal. 1997), *aff'd*, Bernstein v. Dep't of State, 176 F.3d 1132 (9th Cir. 1999) (opinion withdrawn pending *en banc* review); Karn v. U.S. Dep't of State, 925 F. Supp. 1 (D.D.C. 1996).

219. *Karn*, 925 F. Supp. at 3 n.1 (explaining that source code expresses a cryptographic algorithm, which is a precise set of programming operating instructions that enables a computer to transform data into an unintelligible form).

220. 974 F. Supp. 1288 (N.D. Cal. 1997).

221. *Id.* at 1305–06.

222. Junger v. Daley, 8 F. Supp. 2d 708, 712 (N.D. Ohio 1998); Karn v. Dep't of State, 925 F. Supp. 1 (D.D.C. 1996).

223. Junger v. Daley, 209 F.3d 481, 482 (6th Cir. 2000).

224. *See* Sable Communications of California, Inc., v. FCC, 492 U.S. 115, 126 (1989) (holding that the state may impose a content-based restriction to promote a "compelling state interest" and only through "the least restrictive means to further the articulated interest").

225. Stephen E. Arnold, *Internet Users at Risk: The Identity/Privacy Target Zone*, SEARCHER, Jan. 1, 2001, at 24.

226. *See* Vin Crosbie, *Information Wants to Be Free (or Does It?)*, CLICKZ TODAY (July 2,

records of telephone calls and surfing habits, to medical history and financial statements, allows governments and private interests to assemble composite "profiles" of Internet users without their knowledge, and to create an electronic picture of the relationships that exist among events and people.[227] Although the concept of a constitutionally-protected "zone of privacy"[228] is beyond the scope of this Comment, two facets of privacy are germane to anonymity, and concern (1) the right of the individual "not to have [one's] private affairs made public by the government,"[229] and (2) the right to remain free from governmental compulsion when making certain kinds of important decisions.[230] Both of these aspects are implicated by a requirement to compel individuals to identify themselves whenever they log online.

1. A Web of Associations

A requirement to identify oneself in order to gain access to the Internet poses a serious burden on autonomy and "spontaneous expression."[231] Indeed, the decision to remain anonymous can be seen as a decision "to preserve as much of one's privacy as possible."[232] For some time, the court has been aware of "the threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks" and the potentially embarrassing and harmful effects of unwarranted disclosure.[233] The aggregation of personal information from diverse sources enables others to form opinions about the user and to target the user for marketing or discrimination based on one's profile, which has been turned into a public commodity.[234]

2002), *at* http://www.clickz.com/design/freefee/print.php/137889.

227. Arnold, *supra* note 225, at 28–29.

228. The Supreme Court has recognized that the Constitution protects a right of privacy and personal autonomy. Whalen v. Roe, 429 U.S. 589, 598–600 & nn. 23–26 (1977) (discussing diverse aspects of privacy that are "implicit in the concept of ordered liberty," such as the right to be let alone, and a woman's decision whether or not to terminate her pregnancy).

229. *Whalen*, 429 U.S. at 599 n.24 (quoting with approval Philip B. Kurland, *The Private I*, U. CHI. MAG. 7, 8 (1976)) (outlining three aspects of privacy, and drawing a distinction between the right to be free from governmental surveillance, which is protected by the Fourth Amendment, and two aspects of privacy, which are implicated by an identification requirement).

230. *Id.*

231. *See* Rosen v. Port of Portland, 641 F.2d 1243, 1249 (9th Cir. 1981).

232. McIntyre v. Ohio Elections Comm'n., 514 U.S. 334, 342 (1995).

233. *Whalen*, 429 U.S. at 605.

234. *See* Arnold, *supra* note 225, at 36–37.

In this respect, anonymity on the Internet works as a "firewall"[235] against unwanted intrusions on privacy from larger and faster machine networks that continually record and compile the online habits, personal preferences, and identifiable transactional data[236] of millions of unsuspecting users.[237] Electronic anonymity safeguards the individual's interest in selectively revealing oneself to others, which is a function of the "ability independently to define one's identity that is central to any concept of liberty."[238] On the Internet, where much of the detailed collection of data takes place within "virtual communities,"[239] the ability to remain anonymous is part of the autonomy that is indispensable to defining oneself and forming associations online.[240]

The Internet may be a computer network, but it is really a "community of people."[241] Seemingly countless electronic forums, mailing lists, and "meeting places"[242] have proliferated in cyberspace, promoting written exchanges, information, and support for individuals on a wide

---

235. Anonymizers and firewalls work in the same way. A firewall is a security device that "stands" between a computer or private network and the Internet. CONSUMER PRIVACY GUIDE.ORG, GLOSSARY OF INTERNET PRIVACY TERMS, *at* http://www.consumerprivacyguide.org/glossary (last visited Aug. 20, 2002) [hereinafter GLOSSARY OF IPT]. By relaying web traffic through an intermediary server, the security system keeps the computer from being accessible to others. *Id.*

236. Transactional data, which describes information revealed in the normal course of using the Internet, differs from the *content* of a communication since it is not the actual substance of the message, but rather the information about the communication. *See* GLOSSARY OF IPT, *supra* note 235.

237. *See* Press Release, Federal Trade Commission, Young Investor Web Site Settles FTC Charges, *at* http://www.ftc.gov/opa/1999/9905/younginvestor.htm (last visited Oct. 29, 2001) (discussing how Web site promised that information collected from users, who were children, would be held anonymously, but maintained the information in a way that linked it with each child); *see also* Adam Clayton Powell III, *E-Privacy Complaint Filed with FTC*, FREEDOM FORUM, *at* http://www.freedomforum.org/templates/document.asp?documentID=11676 (last visited Aug. 20, 2002).

238. Roberts v. United States Jaycees, 468 U.S. 609, 619 (1984) (citations omitted).

239. Anne W. Branscomb, *Anonymity, Autonomy, and Accountability: Challenges to the First Amendment in Cyberspaces*, 104 YALE L.J. 1639, 1640 (1995) (The Internet is "designed to bring together like-minded individuals, regardless of where they live, work, or play . . . unbounded by geographical, temporal, or other physical barriers.").

240. *See Roberts*, 468 U.S. at 620. The Court recognized a constitutional protection for "the formation and preservation of certain kinds of highly personal relationships." *Id.* at 618.

241. *Praise for 'Caring' Chatroom Community*, BBC NEWS (Mar. 22, 2002), *at* http://news.bbc.co.uk/1/hi/sci/tech/1883939.stm.

242. Jerry Finn, *An Exploration of Helping Processes in an Online Self-Help Group Focusing on Issues of Disability*, 24 HEALTH & SOC. WORK 220, 221 (1999) (discussing online self-help and mutual aid groups that use the Internet and electronic bulletin board systems as places to meet).

variety of topics ranging from general health and dieting, to pregnancy, sexual addiction, and physical disability, to name a few.[243]

Individuals who participate in those and similar online associations find it easier to express themselves by "talking" alone at the keyboard, and often rely on their anonymity to be able to interact with others.[244] Research supports findings that "computer-mediated communication" promotes social interaction and relationships.[245] By contrast, concerns about privacy and messages that can be traced back to specific users may inhibit people from sharing material that might be considered "taboo" and lead to self-censorship.[246] Indeed, in a recent study, inner-city teenagers who were given Internet access wrote hundreds of messages to their friends on topics from rap music to sexual behavior, but suddenly and drastically quit speaking online when project officials informed them that messages would be monitored.[247] The generalized concern arising from such accounts is that an online identification requirement will result in self-censorship and place a substantial burden on the speech and freedom of association of persons who wish to participate in online communities.

History has shown that anonymity gives a voice to individuals who have reason to fear that disclosure of their identities will subject them to ostracism and public hostility.[248] For individuals who are political activists under a repressive regime or whistle-blowers speaking against a corrupt government agency, anonymity may be a necessity.[249] While the whistle-blower may not be an honored figure in our culture,[250] recent high-profile scandals in the corporate world, the FBI, and the Catholic Church

243. *See* Daniel Bubbeo, *Help Is on Hand Online*, NETGUIDE, Dec. 1996, at 109, 109–10, 115; *see also* Tim McLellen, *An Introduction to Usenet News*, *at* http://www.islandnet.com/~tmc/html/articles/usentnws.htm#Newsgroups (last visited Nov. 21, 2002) (describing what a Usenet newsgroup is and how it works). A search by the author using Yahoo! (a search engine for locating content on the Internet) found 49,500 matches for the topic "sexual identity discussion group," *at* http://google.yahoo.com/bin/query?p=sexual+identity+discussion+group&hc=0&hs=0 (last visited June 19, 2001).

244. See Finn, *supra* note 242, at 222.

245. *Id.* at 220.

246. *Id.* at 221.

247. Yitzchak M. Binik et al., *Ethical Issues in Conducting Sex Research on the Internet*, 36 J. SEX RES. 82, 86 (1999).

248. *See generally* Elizabeth Pennisi, *Challenger's Whistle-Blower: Hero and Outcast*, THE SCIENTIST (Jan. 20, 1990), *at* http://www.the-scientist.com/yr1990/jan/pennisi_p1_900120.html (discussing how Roger Boisjoly's testimony regarding the dangers in design of a space vehicle's booster rockets caused him to be ostracized by his community).

249. Grossman, *supra* note 6, at 24.

250. *See* Pennisi, *supra* note 248.

demonstrate that informers willing to unmask insidious insiders can play a crucial part in the process of social and political reform.[251]

Anonymity is especially valuable in the context of online communication, which "promises to become one of the most powerful democratic tools ever devised."[252] Both the disgruntled employee and the unpopular critic prefer publishing their views online without running the risk of being fired or raising the eyebrows of their neighbors. As such, anonymity insulates individuals from self-censorship and gives a voice to people who would otherwise not dare speak in a public forum. More importantly, anonymous speech serves the long-standing goals of preserving pluralism in a democratic society and challenging bigotry and stereotyping by allowing persons to be judged solely on the merits of their ideas without consideration of their personal characteristics.[253]

2. Permission to Speak?

If ratified by the Senate,[254] the proposed treaty will have a dismal effect on anonymous speech and privacy in cyberspace by imposing the online equivalent of an identification requirement. This is because the treaty fails to draw a distinction between computer criminals and legitimate users of online anonymity, or between a criminal investigation and the government's ability to compel people who have not been accused of wrongdoing to identify themselves while surfing in cyberspace.

First, by requiring signatory nations to adopt legislative measures to obtain the "expeditious preservation" of data stored by any computer system,[255] including traffic data,[256] and by requiring providers to disclose subscriber information under their control,[257] the treaty adduces threats of

---

251. *See* Lynn Smith, *Are Women Indeed the Fairer Sex? Prominent Whistle-Blowers Give Rise to Speculation About Gender and Ethics*, L.A. TIMES, June 28, 2002, at E1 (discussing the role of women, particularly FBI agent Coleen Rowley and Enron vice-president Sherron Watkins, in exposing government incompetence and corporate greed).

252. Branscomb, *supra* note 239, at 1640.

253. *See* GODWIN, *supra* note 5, at 13–18.

254. International treaties are subject to approval by two-thirds of the votes in the Senate. U.S. CONST. art. 2, § 2.

255. Cybercrime Convention, *supra* note 103, art. 16(1).

256. *Id.* art. 17(1). Traffic data is "any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service." *Id.* art. 1(d).

257. *Id.* art. 18(3)(b).

disclosure and legal intimidation, chilling to anonymous online speech.[258] The concern is that anonymous remailers, who generally refuse to maintain "server log files"[259] or lists linking their anonymous clientele with corresponding identifying customer information,[260] will be required to "preserve" such lists in the aftermath of the treaty.[261]

Second, the drafters of the Convention have placed a fatal constraint on "chained remailing,"[262] the practice that anonymous remailers use to erase the header identifying the sender and source of the message received. Specifically, Article 16 of the Convention singles out traffic data for "expeditious preservation," as well as any data that "is particularly vulnerable to loss or modification."[263] Likewise, Article 17 ensures that such "data is available regardless of whether one or more service providers were involved in the transmission of that communication."[264] Because the treaty does not define "stored computer data," if traffic data such as the identifying header is stored merely for the duration of the connection, arguably the government could request that it be preserved for an additional ninety days.[265] In addition, the treaty requires providers to disclose the information necessary to retrieve "any stored computer data," including encrypted data,[266] rendering ineffective the use of cryptographic messages and threatening individuals with the loss of their anonymity.

Government actions that restrict or preclude persons from speaking in

---

258. *See* Press Release, American Civil Liberties Union, In Two Significant Cases, ACLU Seeks to Protect Anonymous Online Speakers from Legal Intimidation, *at* http://www.aclu.org/news/2001/n022601b.html (Feb. 26, 2001) (discussing how the threat of disclosure of identity inhibits online speech).

259. Kurt Thumlert, *E-Metrics: Understanding Your Website's Traffic Data*, SITEPOINT (Feb. 21, 2001), *at* http://www.ecommercebase.com/article/354. When someone visits a Web site, data communicated between the visitor's computer and the site, such as the visitor's computer identity and IP address, the length of the visit, and the pages accessed on the site, is recorded in the Web site's server log file, and can provide a scientific understanding of how Internet users behave. *Id.*

260. *See Flood Control*, *supra* note 13, at 415–18.

261. *See* FAQ ABOUT THE CONVENTION, *supra* note 19. The Justice Department distinguishes between "data retention," which would "require providers to collect and keep all or a large portion of a provider's traffic as a routine matter," and "data preservation," which only enables law enforcement to "instruct a service provider to set aside specified data that is already in the service provider's possession until law enforcement procures the proper documents to require the data's disclosure." *Id.*

262. *See Flood Control*, *supra* note 13, at 415–18.

263. Cybercrime Convention, *supra* note 103, art. 16(1) (explaining that stored data with a short life would be particularly vulnerable to both loss and modification).

264. *Id.* art. 17(1)(a).

265. *See id.* art. 16(2).

266. *Id.* art. 19(3).

advance are constitutionally disfavored and presumptively invalid.[267] The unintended outcome of the Convention might then be to give governments the authority to hold people accountable not only for what they speak, write, or publish on the Internet, but also for identifying themselves each time they log on to the Internet *before* they speak, write, or publish. To do so will deprive persons of even the most rudimentary anonymity they enjoy in the physical world.

As such, these specific provisions of the Convention impose substantial "burdens on individual rights"[268] and raise serious problems of vagueness—"particularly treacherous" where the fear of incurring criminal sanctions will likely "deter those who seek to exercise [their] protected First Amendment rights."[269] Given the treaty's vague procedural safeguards,[270] which permit United States citizens to be extradited to face charges abroad for crimes that do not exist in the United States, and that one could not reasonably have known to be proscribed, the treaty provokes serious misgivings regarding due process.[271] Accordingly, if the provisions of the Convention are at odds with constitutional standards of substantive and procedural due process, federal courts cannot give the treaty full force and effect.[272]

B. Conflicts with Current Law

The Cybercrime Convention is intended as a "self-operating" treaty, requiring no legislation by either Congress or the states to be enforceable.[273] Although specific provisions of the Convention may require additional legislative action by Congress to regulate the details of a process or right specified in the treaty,[274] this requirement would not affect

---

267. Org. for a Better Austin v. Keefe, 402 U.S. 415, 419 (1971) ("Any prior restraint on expression comes to this Court with a 'heavy presumption' against its constitutional validity." (citations omitted)).

268. Buckley v. Valeo, 424 U.S. 1, 68 (1976).

269. *Id.* at 76–77.

270. *See* Cybercrime Convention, *supra* note 103, art. 15.

271. *See* United States v. Harriss, 347 U.S. 612, 617 (1954) (holding that due process requirements must provide adequate notice to a person of ordinary intelligence that contemplated conduct is illegal).

272. *See* Reid v. Covert, 354 U.S. 1, 7 (1957) (holding that treaties and executive agreements must comply with existing constitutional standards).

273. Amaya v. Stanolind Oil & Gas Co., 158 F.2d 554, 554 (5th Cir. 1946), *cert. denied* 331 U.S. 808 (1947), *reh'g denied* 331 U.S. 867 (1947). Implementing legislation is not "required for the United States to become a party." *See* FAQ ABOUT THE CONVENTION, *supra* note 19.

274. *See* Cybercrime Convention, *supra* note 103, arts. 2–14, 16–22, 27–35. The

"the legal force of the treaty per se."[275] "Treaties between the United States and other nations are [considered to be] the supreme law of the land," and when there is a conflict between a treaty and a homegrown statutory provision, the treaty supersedes it.[276]

The Department of Justice claims on its Web site that it does not "currently anticipate that implementing legislation" will be required for the United States to become a party to the Convention.[277] This assurance rests on the contention that "the U.S. delegation has worked hard to balance attentiveness to the suggestions of other countries with respect for the strengths of current U.S. law."[278] Nevertheless, there are significant differences between the Convention's requirements for the expedited preservation of traffic data and disclosure of identifying information, and analogous "data preservation" and disclosure requirements under U.S. law.

Federal law concerning "data preservation" is found in the Electronic Communications Privacy Act of 1986 (ECPA).[279] The ECPA also provides how the government can obtain both email communications and subscriber or transactional records held by a provider of electronic communication.[280] Despite similarities to the ECPA, Articles 16 and 29 of the Convention are far more sweeping[281] and apply to any type of computer data,[282] including traffic data that has been "stored by means of a computer system."[283] Under the Convention, data preservation may include any kind of personal and business records, as well as traffic data, such as Web surfing information that "reveals a large amount of detail of—and perhaps a comprehensive profile on any individual."[284] Merely by visiting various

---

Convention addresses enforcement by requiring that each signatory nation "shall adopt such legislative and other measures as may be necessary" to carry out its various provisions. *Id.* art. 18(1).

275. Copyright Convention with Great Britain, 6 Op. Att'y Gen. 292, 293 (1854).

276. Mizugami v. Sharin West Overseas, Inc., 583 N.Y.S.2d 577, 579 (N.Y. App. Div. 1992), *appeal granted* 602 N.E.2d 233 (N.Y. 1992), *aff'd* 615 N.E.2d 964 (N.Y. 1993).

277. FAQ ABOUT THE CONVENTION, *supra* note 19.

278. *Id.*

279. *See generally* 18 U.S.C. §§ 2701–2705 (2002) (setting forth the legal standards regarding access to stored communications as well as the requirements for evidence preservation).

280. 18 U.S.C. § 2703(c)(1).

281. *See* Cybercrime Convention, *supra* note 103, arts. 16, 29.

282. *Id.* art. 1(b) (broadly defining "computer data" as "any representation of facts, information or concepts in a form suitable for processing in a computer system, including a program suitable to cause a computer system to perform a function").

283. *Id.* arts. 16, 29.

284. Privacy International, Privacy International Comments to Working Paper on Data Retention, EU Forum on Cybercrime, *at* http://www.privacyinternational.org/issues/cybercrime/eu/pi-euforum-retention.html (Nov. 27, 2001) [hereinafter Working Paper

Web sites for a few minutes, users can unwittingly "reveal a wide and detailed spectrum of their personal situation," including medical, financial, and "other highly personal information."[285] By contrast, the ECPA's "data preservation" provision is limited to customer communications or records[286] and may only require a service provider "to preserve records and other evidence in its possession pending the issuance of a court order or other process."[287]

Traffic data holds special significance to anonymous remailers who erase message traffic to ensure untraceable online anonymity for their customers.[288] By requiring the preservation of "a sufficient amount of traffic data in order to identify th[e] service provider and the path through which the communication was transmitted,"[289] and "regardless of whether one or more service providers were involved in the transmission,"[290] the Convention places a new burden on providers to be able to trace every anonymous message, record every Web site visited, and in effect, be able to capture "a full profile of an individual's personal and professional associations and activities."[291] By contrast, there is no analogous provision under the ECPA.[292]

Similarly, there is a concern that governments who have signed a treaty requiring them to enact laws on the disclosure of subscriber identifying information[293] will compel service providers to *always* be able to identify their customers.[294] Under such an international regime, anonymous remailers who refuse to keep logs of message traffic[295] would no longer be able to operate. Nevertheless, the Department of Justice insists that the Convention makes a distinction between data *retention* requirements, "which would require providers to collect and keep all or a large portion of a provider's traffic as a routine matter, and *preservation*

Comments].

285. *Id.*

286. *See* 18 U.S.C. §§ 2703(c)(1)(B)–2703(c)(1)(C).

287. *Id.* § 2703(f).

288. *See Flood Control*, *supra* note 13, at 416.

289. Cybercrime Convention, *supra* note 103, art. 30(1).

290. *Id.* art. 17(1)(a).

291. *CDT Comments*, *supra* note 125.

292. *See generally* 18 U.S.C. § 2703 (The ECPA requires providers to preserve the contents of electronic communications as well as information regarding a customer's or subscriber's identity, but does not require tracing of anonymous messages or tracking of Internet traffic.).

293. Cybercrime Convention, *supra* note 103, art. 18(1)(b).

294. *CDT Comments*, *supra* note 125; *see* Scheeres, *supra* note 51.

295. *Flood Control*, *supra* note 13, at 416.

requirements, which enable law enforcement authorities . . . to [instruct] a service provider to set aside *specified* data that is *already in the service provider's possession.*"[296]

The distinction cannot assure providers of anonymous services that they will not be required to retain any data beyond whatever data is otherwise retained by them for business purposes, such as billing.[297] Moreover, it is not relevant whether a service provider needs only to collect data "within its existing technical capability"[298] because providers continuously filter, store, and process copious amounts of traffic data. As the price of communication becomes less dependent on distance or destination and there is no longer any need to store data for billing purposes, enforcement authorities may request that a minimum amount of data be kept for a sufficient time necessary to facilitate the criminal investigations envisioned by the treaty.[299]

Lastly, unlike the ECPA, which contains some protection for the service provider, even allowing a court order to be quashed "if the information or records requested are unusually voluminous in nature or compliance with such order otherwise would cause an undue burden on such provider,"[300] there is no comparable provision under the Convention. To the contrary, Articles 29 and 30— pertaining to mutual assistance between nations—limit a party's ability to refuse a request for expedited preservation or disclosure of data.[301]

C. De Facto Identification Requirement

In examining the Convention's identification requirements from the perspective of the First Amendment, the first issue to be determined is what level of scrutiny is applicable.[302] "[T]he appropriate level of scrutiny is initially tied to whether the statute distinguishes between prohibited and permitted speech on the basis of content."[303] Government regulation of speech is content-neutral if it is "justified without reference to the content of the regulated speech."[304]

---

296. FAQ ABOUT THE CONVENTION, *supra* note 19.

297. *See id.*; *see also* Explanatory Report, *supra* note 113, paras. 151–52.

298. Cybercrime Convention, *supra* note 103, arts. 20–21.

299. *See* Working Paper Comments, *supra* note 284.

300. 18 U.S.C. § 2703(d).

301. *See* Cybercrime Convention, *supra* note 103, arts. 29–30.

302. *See* Turner Broad. Sys., Inc. v. FCC, 512 U.S. 622, 637 (1994).

303. Frisby v. Schultz, 487 U.S. 474, 481 (1988).

304. Virginia State Bd. of Pharmacy v. Virginia Citizens Consumer Council, Inc., 425 U.S.

At first glance, exacting scrutiny appears to be the applicable standard by which to examine a restriction on the ability to communicate anonymously over the Internet.[305] Because the identity of the speaker is no different from other components of a document's contents that the author is free to include or exclude,[306] the Convention's provisions mandating the preservation of traffic data and disclosure of the subscriber's identity constitute presumptively invalid content-based restrictions.[307] Thus, in order to overcome the presumption of invalidity, the Convention's specific provisions must further an "overriding state interest" and be "narrowly tailored" to achieve the articulated interest.[308]

Nevertheless, despite some scholarly suggestions that exacting scrutiny should apply to all restrictions on speech,[309] it may be argued that the Convention's provisions do not aim at prohibiting anonymous communication,[310] but rather aim at the "secondary effects"[311] of such communication.[312] In this respect, the Supreme Court's decision in *City of Renton v. Playtime Theatres, Inc.*,[313] is relevant, as it supports the proposition that "an otherwise content-based restriction on speech can be recast as 'content neutral' if the restriction 'aims' at 'secondary effects' of the speech."[314]

748, 771 (1976).

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

306. *McIntyre*, 514 U.S. at 342.

307. *See* R.A.V. v. City of St. Paul, 505 U.S. 377, 382 (1992) (holding content-based regulations presumptively invalid).

308. *McIntyre*, 514 U.S. at 347.

309. *See, e.g.*, Alex Kozinski & Stuart Banner, *Who's Afraid of Commercial Speech?*, 76 VA. L. REV. 627, 628 (1990).

310. *See* Explanatory Report, *supra* note 113, para. 62.

> The modification of traffic data for the purpose of facilitating anonymous communications (e.g., the activities of anonymous remailer systems), or the modification of data for the purpose of secure communications (e.g. encryption), should in principle be considered a legitimate protection of privacy and, therefore, be considered as being undertaken with right.

Id.

311. *See* City of Renton v. Playtime Theatres, Inc., 475 U.S. 41, 47 (1986) (emphasis omitted).

312. *See* Explanatory Report, *supra* note 113, para. 62 (explaining that the Convention aims to criminalize abuses related to anonymous communications, such as where the identifying information is altered in order to conceal the identity of the perpetrator committing a crime).

313. *City of Renton*, 475 U.S. at 46–47 (holding that a zoning ordinance barring adult movie theatres from locating within 1000 feet of a residence, school, church, or park was a valid content-neutral restriction because it aimed not at the content of the movies, but at the "secondary effects" of the theatres on the surrounding community).

314. Boos v. Barry, 485 U.S. 312, 334 (1988) (Brennan, J., concurring in part and

Content-neutral regulations "that have an incidental effect on First Amendment rights will be upheld if they further an important or substantial governmental interest."[315] For example, in *American Library Ass'n v. Reno*,[316] the District of Columbia Circuit Court of Appeals found that the Child Protection and Obscenity Enforcement Act of 1988,[317] which required producers of sexually-explicit materials to determine and maintain records of the identities of performers, was a content-neutral statute having only an incidental effect on the rights of performers to remain anonymous.[318] The court held that Congress enacted the statute not to regulate the content of speech, but "to prevent the use of underage performers in the production of sexually explicit materials."[319] Further, the court rejected the district court's contention that the statute invaded the privacy of adult performers, discouraged them from engaging in protected expression, and made it exceedingly difficult, if not impossible, for performers to remain anonymous.[320]

Notwithstanding the decisions in *City of Renton* and *American Library Ass'n*, the limits on anonymous speech placed by the Convention may be distinguished from the restrictions on speech in those cases. Whereas in both *City of Renton* and *American Library Ass'n* the restrictions incidentally burden a predominantly salacious category of speech, the provisions of the Convention burden anonymous speech, whose primary function is the communication of "unpopular or unconventional views."[321] Further, as the *McIntyre* Court recognized, because anonymous speech "exemplifies the purposes behind the Bill of Rights, and of the First Amendment in particular,"[322] the applicable standard of constitutional review deserves the most exacting scrutiny.

Moreover, the provisions of the Convention do not incidentally burden anonymous speech, but rather directly undermine the technical ability of remailers to assure the anonymity of their users, thus disabling

---

concurring in judgment).

315. Walsh v. Brady, 927 F.2d 1229, 1235 (D.C. Cir. 1991) (citations omitted).

316. 33 F.3d 78 (D.C. Cir. 1994).

317. Pub. L. No. 100-690, § 7501, 102 Stat. 4181, 4485–4503 (1988), *amended by* The Child Protection Restoration and Penalties Enhancement Act of 1990, Pub. L. No. 101-647, § 301, 104 Stat. 4789, 4816–17 (1990) (codified as amended at 18 U.S.C. § 2257(b)(1) (2000)).

318. *See* Am. Library Ass'n v. Reno, 33 F.3d 78, 87 (D.C. Cir. 1994).

319. *Id.*

320. *See id.* at 94.

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

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

the only vehicle for truly anonymous speech in cyberspace.[323] Unlike the zoning regulations at issue in *City of Renton*, which allowed for "reasonable alternative avenues of communication" by permitting theatres to locate on the farther outskirts of town,[324] the provisions of the Convention do not provide any alternative means for persons to communicate anonymously in cyberspace. In the aftermath of the treaty, remailers will not be able to offer untraceable anonymity.

Whereas anonymous speakers use remailers and anonymizers because they have reason to fear that disclosure of their identities will subject them to ostracism and public hostility, the adult performers in *American Library Ass'n*, who had to disclose their identities to producers, were not likely to be subjected to stigmatization, harassment, and ridicule by the very producers they helped enrich.[325] Lastly, neither *City of Renton* nor *American Library Ass'n* involved the abridgment of one's freedom to associate for social or political reasons. "Although associations formed for the pursuit of private economic interests have received some [F]irst Amendment protection," that protection does not receive the same exacting standard of review as provided to those who communicate for political and social reasons.[326]

D. The Treaty's Provisions Fail Exacting Scrutiny

The Supreme Court applies "exacting scrutiny"[327] to determine whether the subordinating interests of the state have a "substantial relation"[328] to the information required to be disclosed. If the government demonstrates a compelling interest substantially related to the disclosure, the Court then weighs the interest against the "burdens on individual rights."[329] To find an intrusion on First Amendment liberties, the Court demands a showing of "reasonable probability" that requiring disclosure of individuals' "names [and identities] will subject them to threats, harassment, or reprisals from either Government officials or private

323. *See Flood Control*, *supra* note 13, at 418–24. Remailers are the primary vehicles for untraceable anonymous and pseudonymous speech. *Id.* Users using pseudonyms can always be identified by their online identities, but cannot be traced to their true identities in the physical world. *Id.*

324. *City of Renton*, 475 U.S. at 53.

325. *Am. Library Ass'n*, 33 F.3d at 94.

326. Trade Waste Mgmt. Ass'n v. Hughey, 780 F.2d 221, 238 (3d Cir. 1985).

327. *Buckley*, 424 U.S. at 64.

328. Gibson v. Fla. Legis. Investigation Comm., 372 U.S. 539, 546 (1963).

329. *Buckley*, 424 U.S. at 68.

parties."[330]

Arguably, the government has a compelling interest to combat crime and, therefore, may require providers to preserve data stored in any computer service,[331] including traffic data,[332] as well as disclose subscriber information under their control.[333] Similarly, government investigators may have a compelling need to obtain the information necessary to unlock the encrypted data,[334] without which it is not possible to identify the sender and routing information detailing the electronic path of the chained remailing.[335] But such a compelling interest can only apply on a case-by-case basis, not as a blanket requirement that affects all legitimate providers and users of online anonymity resulting in a *de facto* ban on electronic anonymity.

Although the government interest may be substantially related to the data requested on a case-by-case basis, the provisions of the Convention are not narrowly tailored to achieve that end through the use of "the least restrictive means."[336] Instead, the regulations sweep innocent, protected speech within their scope. Specifically, Article 16 applies to any data that is stored within a computer system.[337] An anonymous remailer, a bulletin board, or a Usenet service may be ordered to preserve information that it would not ordinarily keep during the course of its business.[338] Not only does the information have the potential of exposing unwary customers to a breach of their anonymity, it is also capable of revealing their entire "personal and professional associations and activities.[339]

Furthermore, the Convention formulates procedures giving police the authority to seize entire computer systems and to "render inaccessible or remove those computer data in the accessed computer system."[340] Thus, police will be able to seize computer information from legitimate service providers and users who have no connection with the crime. Such activities not only place substantial "burdens on individual rights,"[341] but

330. *Id.* at 74.
331. Cybercrime Convention, *supra* note 103, art. 16.
332. *Id.* art. 17.
333. *Id.* art. 18(3)(b).
334. *See id.* art. 19(4).
335. *Flood Control*, *supra* note 13, at 415–18.
336. *Sable Communications*, 492 U.S. at 126.
337. Cybercrime Convention, *supra* note 103, art. 16.
338. *See CDT Comments*, *supra* note 125.
339. *Id.*
340. Cybercrime Convention, *supra* note 103, art. 19(3)(d).
341. *Buckley*, 424 U.S. at 68.

unfairly target those individuals who are most likely to experience "threats, harassment, or reprisals from either Government officials or private parties"[342] because they are the persons most likely to use anonymous remailers and encryption in the first place.[343]

E. Diminished Expectations

Under current United States law, an individual does not have a reasonable expectation of privacy in a record or other information pertaining to one's communication service or remote computer service.[344] Some telecommunications providers, however, such as remailers and anonymizer services, do not regularly keep identifying records, and are not required to keep them under United States law.[345] By requiring providers to retain such data, the Convention will alter these expectations.

The ability of remailers to maintain the anonymity of their customers will be foreclosed by the requirement that every provider supply authorities with any information stored in its computer system, or otherwise risk being shut down.[346] Further, without an expectation of anonymity in the traffic data that can be retained by remailers, individuals' ability to communicate on the Internet, without disclosing their identities, will be severely curtailed.

Given the broadly written Article 16, which does not limit preservation of data to communication data,[347] remailers will face the difficult prospect of refusing to comply with authorities by not maintaining information to identify their customers, such as billing and transactional data. Paradoxically, the attempt by governments to trace every call may only motivate users to become more untraceable, and drive legitimate remailers out of business, while encouraging others to start operating in locations beyond the jurisdiction of the Convention.

---

342. *Id.* at 74.

343. *See* Nadine Strossen, *Protecting Privacy and Free Speech in Cyberspace*, 89 GEO. L.J. 2103, 2108–09 (2001) (discussing the connection between privacy and freedom of speech for individuals researching sexual orientation).

344. *See* 18 U.S.C. § 2703(c)(1)(A); *see also* United States v. Hambrick, No. 99–4793, 2000 U.S. App. LEXIS 18665, at *11 (holding that a person does not have an expectation of privacy in the account information given to the internet service provider in order to establish an account).

345. *See* 18 U.S.C. § 2703(c); *see also* 18 U.S.C. § 2510(15) (defining "electronic communication service" as "any service which provides to users thereof the ability to send or receive wire or electronic communications").

346. *See* Cybercrime Convention, *supra* note 103, art. 19(3).

347. *Id.* art. 16.

Because the provisions of the treaty are drafted in very broad terms,[348] a final consideration is that United States corporations and Internet users may also find themselves liable for crimes that they were not even aware existed.[349] By contrast, due process requires that a criminal statute provide adequate notice to a person that his contemplated conduct is illegal.[350] Given that an even "greater degree of specificity" is required when First Amendment rights are involved,[351] the Convention fails to pass constitutional muster.

Proponents of online identification point out that "true anonymity,"[352] which allows users to become untraceable online, is unlike anything that could be tolerated in the physical world simply because one cannot possibly go completely unnoticed outside of cyberspace.[353] In the physical world, so goes the argument, something is always left behind, be it fingerprints at the scene of the crime, the distinctive markings of a particular typewriter used to print a ransom note, or some "nonanonymous action sufficient to allow [one] to be identified and charged with the offense."[354] The argument is that truly anonymous communication is beyond the reach of the law because it poses an insurmountable problem of enforcement, so that prohibition is "the only effective deterrent."[355]

But even if the physical world were an Orwellian utopia where no crime went unsolved because everyone's identity was sufficiently known, such an argument runs into the paradox that full accountability places a complete ban on anonymity.[356] Thus, even if one were to accept at face value the requirement that something about the identity of the user must be

348. *CDT Comments*, *supra* note 125; *see also* FAQ ABOUT THE CONVENTION, *supra* note 19.

349. *See* Cybercrime Convention, *supra* note 103, art. 29(3) ("[D]ual criminality shall not be required as a condition to providing such preservation.").

350. *Harriss*, 347 U.S. at 617.

351. *Buckley*, 424 U.S. at 77.

352. Branscomb, *supra* note 239, at 1641. A truly anonymous communication insulates the speaker's identity from disclosure but also invites the danger inherent in foreclosing detection. *See id.* at 1641–42.

353. *See* David G. Post, *Pooling Intellectual Capital: Thoughts on Anonymity, Pseudonymity, and Limited Liability in Cyberspace*, 1996 U. CHI. LEGAL F. 139, 146 (1996) (arguing Mrs. McIntyre's actions were not anonymous at all and that the absence of anonymity is a precondition for all enforcement).

354. *Id.*

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

356. *See* Branscomb, *supra* note 239, at 1641–42 (suggesting that providers "must grapple with the propriety of anonymity").

made available to ensure some *de minimis* authentication, the answer to what that something should be differs depending on whether governments, business interests, or civil liberties advocates provide the answer.

Indeed, a persistent criticism has been "the non-transparent manner in which this Convention has been developed,"[357] and the lack of interest on the part of the Council of Europe to "substantially incorporate the views and concerns"[358] of non-governmental groups on the issues of privacy and civil liberties. In the United States, critics have accused the Department of Justice and the FBI of using a foreign forum to install an international police regime that predominantly advances law enforcement interests over those of ordinary citizens and businesses, and then "bring it back to the U.S. as an international treaty—which obliges Congress to enact it,"[359] a practice described as "policy laundering."[360] However, this closed approach to regulating the Internet can only chill speech, limit consumer choices and privacy, and provide a disincentive for the development of technological solutions to cybercrime.[361]

By contrast, proposals by non-governmental groups and experts regarding cyber-security emphasize technological developments and fixes.[362] Not surprisingly, the same technology that allows cybercriminals to hide their identities can also prevent them from reaching their potential victims.[363] A lawless cyber-frontier is not the sole alternative to an Internet identification requirement and expanded government powers. Rather, greater preventive measures by the private sector and technical innovation are needed to improve security in cyberspace.[364]

To ensure user accountability[365] while preserving avenues for

357. *ACLU Letter*, *supra* note 138.

358. *Id.*

359. David Banisar, *Love Letter's Last Victim*, SECURITY FOCUS ONLINE (May 22, 2000), *at* http://online.securityfocus.com/news/39.

360. *Id.*

361. Declan McCullagh, *White House Defends Cybersecurity Plan*, CNET NEWS.COM (Sept. 20, 2002), *at* http://news.com.com/2100-1023-958775.html (citing cautionary statement of Orson Swindle, one of the Federal Trade Commission's five commissioners, regarding "attempts to enact a broad privacy law to regulate the data collection practices of Internet companies").

362. *See* Emma Ogilvie, *Cyberstalking*, TRENDS AND ISSUES IN CRIME AND CRIM. JUST., Sept. 2000, at 4–5, *available at* http://www.aic.gov.au/publications/tandi/ti166.pdf (discussing that many of the solutions to cyberstalking are more likely to come from "technological fixes" than from legislation).

363. *Id.*

364. *See* McCullagh, *supra* note 361.

365. *See* Branscomb, *supra* note 239, at 1641–42 (discussing lack of user accountability as a negative aspect of untraceable anonymity).

anonymous online communication, the Internet can be zoned for various uses that offer individuals varying degrees of anonymity or privacy, while simultaneously requiring accountability by some means of authentication.[366] For example, online retailers, banks, content providers, and the panoply of personal and professional cyber-associations can readily establish authentication requirements commensurate with the type of services they offer. Such a voluntary system ensures that users can choose how much information to disclose and to whom, depending on the specific transaction. Just like in the real world, such a system allows persons a greater degree of anonymity when browsing through a catalogue or when sending a letter than when purchasing a plane ticket or conducting a banking transaction.

V. CONCLUSION

Absent evidence linking anonymous servers to any criminal or terrorist conspiracy,[367] the Convention's broad identification requirement is overblown. While much can be done about security on the Internet, putting an end to untraceable anonymity is not the way to do it. The Convention's broad requirements for data preservation, and provisions for the disclosure of subscriber information and encryption code pose a chilling effect on anonymous online speech. To enact this Convention, lawmakers must introduce such legislative and other measures that preserve online anonymity, or reject the treaty in its entirety. While the United States has a strong interest to prosecute and punish individuals who misuse computers

366. *See* Scott Charney, Prepared Witness Testimony, On-line Fraud and Crime: Are Consumers Safe?, Hearing Before the Subcomm. on Commerce, Trade, and Consumer Protection (May 23, 2001), *at* http://energycommerce.house.gov/107/hearings/05232001Hearing235/Charney357.htm (discussing three ways of authenticating an unknown buyer's identity on the Internet). Mr. Charney is a Principal of Digital Risk Management and Forensics at PricewaterhouseCoopers. *Id.*

367. Matthew Fordahl, *Anonymous E-Mail Services May Have Increased Since Sept. 11*, DETNEWS.COM (Dec. 9, 2001), *at* http://www.detnews.com/2001/technews/0112/09/technology-362425.htm.

by committing crimes that have an effect in this country, those aims should be pursued without compromising time-honored First Amendment liberties.

*Albert I. Aldesco**

* I would like to thank the editors and staff of Loyola of Los Angeles Entertainment Law Review, particularly Kent F. Lowry, Christopher P. Campbell, Jeremy A. Lane, Lauren Katunich, Dara Tang, Shannon McWhinney, and Jennifer L. Grace for their generous contributions and diligent efforts. I dedicate this Comment to my parents, the rest of my family, and to Jacqueline, whose unwavering support and love inspires me.