Fordham Intellectual Property, Media and Entertainment Law Journal

Volume 7 *Volume VII*
Number 1 *Volume VII Book 1*

Article 11

1996

Anonymity and International Law Enforcement in Cyberspace

Jonathan I. Edelstein
Fordham University School of Law

NOTES

Anonymity and International Law Enforcement in Cyberspace

Jonathan I. Edelstein*

INTRODUCTION

A. *A Plausible Scenario?*

It is the morning of April 11, 2000, on Grand Cayman Island.[1] Larry Smith,[2] having finished his breakfast, ambles

---

* J.D. Candidate, Fordham University School of Law, 1997; e-mail address jonathan@soho.ios.com. I would like to thank, first and foremost, Professor Abraham Abramovsky for his invaluable moral and scholarly assistance in the production of this Note. I also wish to thank Ruby Bradley, Guy Cohen, Cal Davis, Richard Dini, Gail Donoghue, Renee Farrell-Duval, Susan Finkenberg, Lyle Frank, Mike Geary, Doron Gopstein, Zena Johnson, Simon Kok, Sherrill Kurland, Denise McCracken, John McGowan, Jane Momo, Tom Nerney, Ken Reid, Linda Speranza, and David Steiner (in other words, the gang at the Corporation Counsel's office) for their unfailing encouragement.

1. Compare this scenario with the situation described in *Businesses Promote Fraud Tools on the Internet; Web Shows How to Hide One's Identity, Use Offshore Accounts for Secret Stocks*, AUSTIN AM.-STATESMAN, July 15, 1996, at D4 [hereinafter *Businesses Promote Fraud Tools*]. This article describes a corporation known as Privacy Tools Inc. ("Privacy Tools"), which:

> [W]ill sell a bogus passport imprinted with any name the customer selects. Claiming to be based in Estonia, it sells passports from a Web page in Anguilla, British West Indies. The company says its 'camouflage' passport ensures 'total anonymity' for tasks such as opening an offshore bank account. . . . The company also sells international driver's licenses and press cards 'issued by a bona fide European press agency' under any name a customer desires.

Id. Privacy Tools rents its Web site from an Anguilla-based Internet access provider called Offshore Information Services, operated by Vince Cate, a 32-year-old island entrepreneur. Cate has never met the owner of Privacy Tools and knows him only as "Richard." *Id.* Offshore Information Services, which advertises openly that it is "offshore and on-line," offers its customers "a new offshore identity over which [they] have total control," even allowing customers to provide the computer on which their offshore anonymous account will be established.

over to the small office he keeps in his home and boots up the waiting computer terminal.

Only a year before, the Cayman Islands had possessed only one Internet[3] access provider[4] of their own. Now, thanks to the Computer Privacy Act that the Cayman legislature had passed in December, there are 182 access services operating in the Caymans. Not entirely coincidentally, 179 of these are anonymous remailers—services which forward information to another destination while concealing the identity of its source.[5]

John Graham-Cumming, *Caught Up in a Web of Deceit*, GUARDIAN (LONDON), June 13, 1996, at 11. Incidentally, in a rare example of events occurring simultaneously with scholarship, Offshore Information Services opened shortly after the writing of the first draft of this Note.

2. All names used in this scenario are fictional.

3. The Internet "is a worldwide entity whose nature cannot be easily or simply defined. . . . [T]he Internet is the 'set of all interconnected I[nternetworking] P[rotocol] networks'—the collection of several thousand local, regional, and global computer networks interconnected in real time via the TCP/IP Internetworking Protocol suite. . . ." DANIEL P. DERN, THE INTERNET GUIDE FOR NEW USERS 16 (1994), *cited in* Religious Tech. Ctr. v. Netcom, 907 F. Supp. 1361, 1365 n.2 (N.D. Cal. 1995).

A 1995 magazine article also cited in *Netcom* describes the Internet in a more colloquial way as:

> [A] collection of thousands of local, regional and global Internet Protocol networks. What it means in practical terms is that millions of computers in schools, universities, corporations, and other organizations are tied together via telephone lines. The Internet enables users to share files, search for information, send electronic mail, and log onto remote computers. But it isn't a program or even a particular computer resource. It remains only a means to link computer users together. . . .
>
> No one pays for the Internet because the network itself doesn't exist as a separate entity. Instead various universities and organizations pay for the dedicated lines linking their computers. Individual users may pay an Internet provider for access to the Internet via its server.

David Bruning, *Blasting Along the InfoBahn*, ASTRONOMY, June 1995, at 74.

4. An Internet access provider is a computer connected to the Internet via dedicated telephone lines, through which members of the public can access the Internet, usually for a fee. *See* Bruning, *supra* note 3, at 76.

5. *See* Steve Harris, *E-Mail: No Names, No Pack Drill: Steve Harris Finds Out How You Can Send Untraceable Messages Over the Internet*, GUARDIAN (LONDON), Oct. 6, 1994, at 5. An anonymous remailer, or an "anonymous posting service," removes identifying information from electronic mail messages received from its users and replaces it with a numbered anonymous account identifier. *Id.* The messages are then forwarded in accordance with forwarding orders specified by

Smith, one of the Caymans' budding computer entrepreneurs, is the proprietor of four of these anonymous remailers, all run from his home. He has never met any of his clients face to face. Each of his services has approximately 1,000 accounts, of which all but four or five have never been used. The remainder provide him with an income of $1,000 per account per month,[6] plus a fee for each message forwarded. Of course, Smith only sees half of this money; the Cayman government levies a hefty tax on Internet accounts.

With the terminal booted up, Smith scans the previous day's activity on Caymanon, his oldest and most profitable remailer. There has been an unusual amount of mail received and forwarded to the holder of an active account; clearly, one of Smith's clients is doing business. What sort of business this may be, Smith neither knows nor wants to know. The less he knows, in fact, the better for his peace of mind. . . .

More than 1,500 miles away from Smith, Paul Anderson sits in his living room in New Jersey and checks his electronic mail.[7] His Caymanon account has been busy; seven requests from new clients anxious to purchase from his gallery of select photography, as well as a number of orders from established customers. The government may take a dim view of Anderson's business[8]—after all, some of the

---

the user. *Id.* Harris is the GUARDIAN's chief commentator on Internet issues.

6. Offshore Information Services' fees range from $20 per month for an offshore e-mail address to $300 per month for "a complete identity" over which the user has total control. Graham-Cumming, *supra* note 1, at 11. Considering the greater risk involved with an anonymous remailer service dedicated exclusively to criminal purposes, a fee of $1,000 per month does not seem unreasonable for an account on the hypothetical Caymanon service.

7. Electronic mail, or e-mail, is "a communications service for computer users wherein textual messages are sent to a central computer system, or electronic 'mailbox,' and later retrieved by the addressee. E-mail usually refers to private messages." WEBSTER'S NEW WORLD DICTIONARY OF COMPUTER TERMS 205 (5th ed. 1994).

8. *See* 18 U.S.C. §§ 2251-2257 (criminalizing the sexual exploitation of minors). According to 18 U.S.C. § 2252, any person who knowingly receives, transports, or distributes in interstate or foreign commerce any visual depiction in-

subjects of his photographs are under the age of consent and are shown in compromising positions—but Anderson sees himself as a businessman in the American tradition, filling an available market niche.[9] Certainly, none of his customers has ever complained.

Anderson switches to another file, and begins the process of filling orders. By the time his digitized photographs pass through Caymanon—and three other anonymous remailers—and reach his customers, the source of the photographs will be identified only by a numbered anonymous account. Even if the authorities find one of Anderson's customers, all the American court orders in the world would never suffice to obtain his name from Caymanon.[10] The Cayman com-

---

volving the use of a minor engaging in sexually explicit conduct may be imprisoned up to 10 years for a first offense. 18 U.S.C. § 2252. The statute specifically provides that transportation of such material by means of a computer is punishable under the law. 18 U.S.C. § 2252(a).

9. The availability of pornography over the Internet, including child pornography, has been widely commented upon. *See, e.g.*, *Hearing on Child Pornography on the Internet, before the Senate Judiciary Comm.*, 103d Cong., 2d Sess. (1995) (statement of Barry F. Crimmins, writer and child activist); 141 CONG. REC. S8310, S8329 (1995) (statements of Sen. James Exon in support of the Communications Decency Act of 1996); *Hearing on Encryption Legislation, before the Senate Commerce Comm.*, 104th Cong., 2d Sess. (1996) (testimony of FBI Director Louis J. Freeh, detailing an instance where child pornography was encrypted and transmitted via the Internet); Marty Rimm, *Marketing Pornography on the Information Superhighway: A Survey of 917,410 Images, Descriptions, Short Stories and Animations Downloaded 8.5 Million Times by Consumers in Over 2000 Cities in Forty Countries, Provinces and Territories*, 83 GEO. L.J. 1849 (1995); Anne Wells Branscomb, *Internet Babylon? Does the Carnegie Mellon Study of Pornography on the Information Superhighway Reveal a Threat to the Stability of Society?*, 83 GEO. L.J. 1935 (1995); *see also* David Connett et. al., *The Net Tightens on Child Abusers*, OBSERVER (LONDON), Sept. 1, 1996, at 18 (citing a study by Prof. Harold Thimbleby, Middlesex University, which concluded that nearly half of the 11,000 most repeated Internet search requests were for pornography and that the most visited Internet cites were pornographic); Angela Long, *Norwegians to "Police" Internet for Child Porn*, IRISH TIMES, Aug. 31, 1996, at 10 (detailing the activities of the Norwegian branch of Save the Children, an international child welfare organization, to monitor the Internet for child pornography); Charles Arthur, *How Porn Slipped the Net*, INDEPENDENT (LONDON), July 31, 1995, at 13-14 (describing the use of anonymous remailers in transmitting pornography over the Internet).

10. In the absence of a treaty, the "overriding primary rule of international law" is the sovereignty of the state. IAN BROWNLIE, PRINCIPLES OF PUBLIC INTERNATIONAL LAW 287 (4th ed. 1990). Among the principles which inhere from

puter privacy law, which protects the identity of Internet users from the prying eyes of law enforcement, is practically foolproof—as it very well should be; Anderson and others like him had certainly spent enough money making sure it would.

Money well spent, thinks Anderson as he adds the seven new addresses to his customer file. Doing business is so much easier now—not to mention the convenience of having his Internet provider on the same island as his checking account. . . .

B. *New Media, New Problems*

The Internet, the amalgamation of computer networks that carries an ever-increasing portion of the world's information traffic,[11] is at the forefront of both information technology and the law.[12] With the growth of the Internet to include access services in more than 150 countries,[13] the

---

the sovereignty of the state are prima facie exclusive jurisdiction over territory and population within the state, and the duty of non-intervention in other states' territory. *Id.* The first of these would provide, in the present scenario, that the courts of the Cayman Islands would have exclusive jurisdiction over Caymanon, and the second would preclude American courts from intervening in the legal procedures of the Cayman Islands.

11. *See supra* note 3 and accompanying text (defining the Internet).

12. For a sampling of the legal issues which have grown up around the Internet, see the Communications Decency Act of 1996, Pub. L. No. 104-104, § 502, 110 Stat. 56, 132-36 (amending 47 U.S.C. § 223 (1996)); *see also* Georgia Computer Systems Protection Act, GA. CODE ANN. § 16-9-90 through § 16-9-94 (1996); Shea v. Reno, 930 F. Supp. 916 (S.D.N.Y. 1996); ACLU v. Reno, 929 F. Supp. 824 (E.D. Pa. 1996) (challenging the constitutionality of the Communications Decency Act); Stratton Oakmont Inc. v. Prodigy Servs. Co., 23 Media L. Rep. 1794 (N.Y. Sup. Ct. 1995); Cubby, Inc. v. CompuServe Inc., 776 F. Supp. 135 (S.D.N.Y. 1991) (addressing the issue of Internet access services' liability as republishers for defamatory material carried on their networks); Religious Tech. Ctr. v. Netcom, 907 F. Supp. 1361 (N.D. Cal. 1995) (addressing Internet access providers' liability for violation of copyright by their users). It is also noteworthy that a recent search on LEXIS using the search term "Internet" turned up almost 600 law review articles. Search of LEXIS, LAWREV library, ALLREV file (Sept. 2, 1996).

13. *See* Peter H. Lewis, *Outlook 1995: Technology & Media Trying to Find Gold with the Internet*, N.Y. TIMES, Jan. 3, 1995, at C15 (indicating that Internet access is currently available from 159 countries).

exchange of ideas across international borders has become inexpensive and easy.[14] An ordinary person with a home computer can now reach an audience of millions,[15] a feat previously possible only for those with access to mass media.[16]

Along with its benefits to the international marketplace of ideas,[17] however, the spread of the Internet has also opened doors to new and sophisticated types of crime.[18] Since 1990, especially, the world has seen a proliferation of frauds,[19] data theft,[20] trafficking in pornography[21] and pi-

14. *See Businesses Promote Fraud Tools*, *supra* note 1, at D4 (quoting Rob Bertrum, chairman of the Internet fraud committee of the North American Securities Administrators Association, as saying that the Internet "lowers the barriers to entry for those people who would defraud"). Criminals might save the time and expense of such techniques as cold-calling prospective victims, mass mailings and publishing newsletters by using a World Wide Web ("WWW") site to solicit investors. *Id.* The World Wide Web is a network of Internet resources linked by "hypertext" messages which contain the Uniform Resource Locator ("URL") addresses of other related resources. By means of the WWW, it is possible to follow hypertext links through an unending chain of cross-referenced resources. *See* Douglas Dangerfield, *Web Surfing, or "The Internet for the Uninformed"*, AMER. BANKR. INST. J., Mar. 1996 at *5-*6.

15. *See* George P. Long III, *Who Are You?: Identity and Anonymity in Cyberspace*, 55 U. PITT. L. REV. 1177, 1180 (1994); *see also Shea*, 930 F. Supp. at 926 (indicating that Internet access was available to an estimated 40 million users as of early 1996, a figure which is expected to grow to 200 million by 1999). In considering a constitutional challenge to the Communications Decency Act, the Southern District in *Shea* made extensive findings of fact concerning the history of the Internet, its uses, and the availability of sexually explicit materials on-line. *See id.* at 925-34.

16. *See Businesses Promote Fraud Tools*, *supra* note 1, at D4.

17. The "marketplace of ideas" theory has its roots in the philosophy of the American Pragmatists, who proposed that truth will become apparent through the free exchange of ideas. *See* Byron V. Olsen, Rust *in the Laboratory: When Science is Censored*, 58 ALB. L. REV. 299, 315 n.117 (1994) It was first articulated as a key concept in American jurisprudence by Justice Oliver Wendell Holmes in his dissenting opinion in *Abrams v. United States*, 250 U.S. 616, 630 (1919). *See id.*

18. *See generally Businesses Promote Fraud Tools*, *supra* note 1, at D4.

19. *See id.* (detailing types of fraud that are common on the Internet); *Wireless Fraud Criminals Circulate Sensitive Data Via Internet, CTIA Fights Back with Internet E-Mail Hotline*, MOBILE PHONE NEWS, Sept. 2, 1996; Jeff Brown, *NASD Web Site Alerts Investors*, PHILA. INQUIRER, Aug. 27, 1996, at F1; Jerry Knight, *Regulator Goes On-Line to Foil Fraud*, WASH. POST, Aug. 24, 1996, at F1; Paula Squires, *Better Business Bureaus to Offer Approval of Web Sites*, RICHMOND TIMES DISPATCH, Aug.

rated software,[22] and copyright violation[23] on the global information network.

Two factors have combined to hinder law enforcement authorities' ability to battle Internet crime. The first of these is the international character of the Internet.[24] Even the simplest of Internet crimes may involve perpetrators, victims, and accessories in several countries, and require a level of international law enforcement cooperation formerly reserved for such crimes as international terrorism and drug trafficking.[25]

The second factor is the ease of concealing one's identity when using the Internet.[26] At any given time, twenty to twenty-five anonymous remailers—services established and maintained for the sole purpose of providing anonymity to Internet users[27]—are active on the Internet.[28] While anonym-

---

25, 1996, at E1 (indicating that "the Federal Trade Commission has settled about two dozen major cases of Internet fraud" and is investigating others).

20. *See generally* Clinton Wilder & Bob Violino, *Online Theft: Trade in Black-Market Data is a Growing Problem for both Business and the Law*, INFORMATIONWEEK, Aug. 28, 1995, at 30.

21. *See supra* note 9 and accompanying text.

22. *See* Wilder & Violino, *supra* note 20, at 30; Teddy C. Kim, *Taming the Electronic Frontier: Software Copyright Protection in the Wake of* United States v. LaMacchia, 80 MINN. L. REV. 1255, 1268-71 (1996); Andrea Sloan Pink, *Copyright Infringement Post Isoquantic Shift: Should Bulletin Board Services Be Liable?*, 43 U.C.L.A. L. REV. 587, 604-05 (1995).

23. *Id.*; *see also infra* notes 137-39 and accompanying text (discussing the dispute between the Church of Scientology and Johan Helsingius).

24. *See* Marc S. Friedman & Kenneth R. Buys, *'Infojacking': Crimes on the Information Superhighway*, COMPUTER LAW., Oct. 1996, at 1 (noting that "distance between the parties [on the Internet] is irrelevant—it is as easy for a Manhattanite to communicate with a Parisian as [with] someone in Brooklyn").

25. *See generally Businesses Promote Fraud Tools*, *supra* note 1, at D4 (quoting several securities enforcement and police sources as saying that the structure of the Internet and the ease of international access complicates law enforcement).

26. *See generally* Anne Wells Branscomb, *Anonymity, Autonomy and Accountability: Challenges to the First Amendment in Cyberspaces*, 104 YALE L.J. 1639 (1995); Long, *supra* note 15.

27. *See supra* note 5 and accompanying text (defining anonymous remailers).

28. *See* Peter H. Lewis, *Anonymous Spoof Points Up Hazard in Information Highway*, DALLAS MORNING NEWS, Jan. 2, 1995, at 4D; *see also* Raph Levien, *Remailer List* (1996) (visited Sept. 14, 1996) <http://www.cs.berkeley.edu/~raph/

ity has legitimate purposes and enjoys a level of constitutional protection under American law,[29] it can also greatly hinder the ability of law enforcement authorities to determine the source of illegal materials.[30] In addition, anonymity poses even greater difficulties to owners of intellectual property seeking to assert their rights through civil action.[31]

The obstacles to law enforcement posed by anonymous remailers are especially apparent in cases where illegal materials are transmitted via a remailer in a foreign country.[32] In such cases, American law enforcement authorities would be unable to locate the source of the contraband without the cooperation of the courts in the nation where the remailer is located[33]—assistance which has proved difficult to obtain.[34]

When cooperation is obtained, moreover, the results to both society and the Internet community can be just as catastrophic as when it is not.[35] A recent court decision in Fin-

---

remailer-list.html> for a frequently-updated list of currently operating anonymous remailers.

29. *See infra* notes 70-80 and accompanying text (discussing the benefits of anonymous remailers; *infra* note 223 (discussion of the legal basis for constitutional protection of anonymity).

30. *See* I. Trotter Hardy, *The Proper Legal Regime for "Cyberspace"*, 55 U. PITT. L. REV. 993, 1050-51 (1994) (concluding that anonymous remailers should be banned because of the difficulties they impose upon law enforcement agencies).

31. *See id.*

32. *See* Douglas Lavin, *Cyber Dilemma: As Internet Widens, Free-Speech Debate Swirls Round a Finn*, WALL ST. J. EUR., July 10, 1995, at 1 (quoting a United States Senate staffer as saying that anonymous remailers located in foreign countries are "huge potential loopholes" to law enforcement on the Internet).

33. *See* BROWNLIE, *supra* note 10, at 287.

34. *See infra* notes 121-46 and accompanying text (discussing the Johan Helsingius affair); *see also* 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) (noting that "to the extent that foreign countries with good Internet connectivity . . . already have more permissive rules, those rules effectively undercut the United States' ability to enforce what rules it has"). Professor Froomkin's piece is a seminal article which discusses ethical, constitutional, and policy ramifications stemming from anonymity and privacy issues in cyberspace.

35. *See infra* notes 148-59 and accompanying text (discussing the consequences of the Helsinki District Court's decision in Church of Spiritual Tech. v. Helsingius.)

Finland, directing the operator of an anonymous remailer to divulge the identity of one of his customers to the police, resulted in the closing of the remailer service.[36] The operator of the remailer cited the uncertainty of the legal climate in his decision to close the service, stating that the ruling opened the possibility that he would have to "spend all his time in court" defending his customers' rights.[37] In the current legal atmosphere, where the rights of law enforcement agents and Internet service providers are equally undefined, law enforcement agencies and owners of intellectual property must walk a tightrope between failing to assert society's rights under the law and unintended chilling of the beneficial uses of the Internet.[38]

The majority of legal scholarship concerning the Internet thus far has focused upon the constitutional questions posed by the flow of information through an entirely new medium.[39] This is an important issue which must be resolved in

36. Church of Spiritual Tech. v. Helsingius (Helsinki Dist. Ct., Änestys, J., Aug. 22, 1996), *published in* HELSINGIN SANOMAT, Aug. 23, 1996 (on file with the author); *see also* Peter H. Lewis, *Behind an Internet Message Service's Close*, N.Y. TIMES, Sept. 6, 1996, at D2 (describing the decision of the Helsinki District Court). The Finnish Eduskunta (parliament) is also likely to reform Finland's telecommunications law in response to this court decision, and restore the strong protection of Finnish privacy law over electronic communications. Interview with Peter H. Lewis, Staff Reporter, N.Y. TIMES (Sept. 10, 1996).

37. Lewis, *supra* note 36, at D2.

38. *See infra* notes 220-46 and accompanying text (discussing practical issues in control of Internet anonymity).

39. For examples of articles dealing with constitutional issues on the Internet, especially those relating to encryption, free speech and anonymity, *see* Long, *supra* note 15; Branscomb, *supra* note 26; Hardy, *supra* note 30; Froomkin, *supra* note 34, Lee Tien, *Who's Afraid of Anonymous Speech? McIntyre and the Internet*, 75 OR. L. REV. 117 (1996); A. Michael Froomkin, *Anonymity and its Enmities*, 1995 J. ONLINE L., art. 4 (1996) (visited Sept. 14, 1996) <http://www.law.cornell.edu/jol/jol.table.html>; Timothy B. Lennon, *The Fourth Amendment's Prohibitions of Encryption Limitation: Will 1995 Be Like* 1984*?*, 58 ALB. L. REV. 467 (1994); Henry H. Perritt, Jr., *Tort Liability, the First Amendment, and Equal Access to Electronic Networks*, 5 HARV. J.L. & TECH. 65 (1992); A. Michael Froomkin, *The Metaphor Is the Key: Cryptography, the Clipper Chip, and the Constitution*, 143 U. PA. L. REV. 709 (1995); Michael Adler, *Cyberspace, General Searches and Digital Contraband: The Fourth Amendment and the Net-Wide Search*, 105 YALE L.J. 1093 (1996).

order to determine whether the increasing number of new laws and regulations[40] imposed upon Internet communication will pass constitutional muster, and to provide a framework within which future measures can be enacted. The increasing willingness of national governments to regulate the flow of information through cyberspace,[41] however, necessitates an examination of the practical difficulties law enforcement agencies face when trying to trace the perpetrators of electronic crime.

These difficulties promise to increase. Already, law enforcement agents have often found themselves stymied by the twin obstacles of anonymity and international transmission.[42] An even more sinister possibility exists in the future: the rise of anonymous remailers established and run, not by professors or civil libertarians, but by and for organized crime. Anonymous remailers have already been compared

---

40. *See, e.g.*, the Communications Decency Act of 1996 ("CDA"), Pub. L. No. 104-104, § 502, 110 Stat. 133 (amending 47 U.S.C. § 223 (1996)). Preliminary injunctions against the enforcement of the CDA have been issued by two Federal courts pending determination of the act's constitutionality. *See* Shea v. Reno, 930 F. Supp. 916 (S.D.N.Y. 1996); ACLU v. Reno, 929 F. Supp. 824 (E.D. Pa. 1996). Even if the CDA fails to pass constitutional muster, however, it seems inevitable that the United States government will pass further measures in an attempt to regulate communication on the Internet. A number of other countries have also recently begun to intensify their law enforcement efforts in cyberspace. *See* William Boston, *Germany Targets Compuserve in Child Porn Probe*, REUTER EUR. BUS. REP., Dec. 29, 1995 (regarding German anti-pornography measures and their affect on the U.S.-based Compuserve on-line network); Tom Standage, *Connected: Web Access in a Tangle as Censors Have Their Say: Singapore Wants to Regulate What is Broadcast on the Internet*, DAILY TELEGRAPH (LONDON), Sept. 10, 1996, at 3; James Kynge, *Electronic Undesirables: Southeast Asian States are Divided on How to Police the Internet*, FIN. TIMES (LONDON), Sept. 9, 1996, at 17; Gary Rodan, *Information Technology and Political Control in Singapore* (visited Nov. 11, 1996) <http://www.nmjc.org/jpri>; Mark Turner, *Labyrinth of Laws could Lead to a Net Loss*, INDEPENDENT (LONDON), Jan. 15, 1996, at 11 (mentioning recent measures taken by the UK and Germany).

41. Cyberspace is a popular term for the world of electronic communications over computer networks. Hardy, *supra* note 30 at 994. The term was coined in 1982 by the science fiction author William Gibson and popularized in his novel NEUROMANCER 51 (1984).

42. *See infra* notes 128-30 and accompanying text (discussing Finnish personal privacy laws).

to offshore banks,[43] and at least one commentator has predicted that the future of anonymous remailer services will follow a similar course.[44] The recent opening of an Internet access provider called "Offshore Information Services" on the Caribbean island of Anguilla, which provides anonymity and offshore data storage services to its customers, can hardly bode well for the future of law enforcement on the Internet.[45]

Accordingly, this Note will examine the practical difficulties posed by anonymous remailers to international law enforcement. Part I of this Note outlines the structure of anonymous remailers and the arguments for and against Internet anonymity. Part II considers several recent international law enforcement incidents, and the example of offshore banking, to determine the primary issues which police and prosecutors will face in tracing the perpetrators of Internet crime. Part III of this Note attempts to suggest solutions which clarify the rights of law enforcement agencies and Internet users, in order to preserve the right to anonymity and the free flow of information on the Internet while enabling law enforcement authorities to apprehend offenders and prevent the rise of "offshore databases." Finally, this

43. *See Businesses Promote Fraud Tools*, *supra* note 1, at D4; Douglas Lavin, *Anonymous Service an Internet Loophole: As Governments Try to Limit Content, Global Resistance Grows*, SAN DIEGO UNION TRIB., July 25, 1995, at 7 (referring to anon.penet.fi, an anonymous remailer located in Finland, as "the electronic publishing equivalent of offshore banking").

44. *See* Daniel Akst, *The Cutting Edge: The Helsinki Incident and the Right to Anonymity*, L.A. TIMES, Feb. 22, 1995, at D1 (offering the prediction that "little countries with a hankering for foreign exchange will step up to provide Internet secrecy, just as certain Caribbean islands now provide banking secrecy, for a fee."); *see also* Branscomb, *supra* note 26, at 1675-76 (predicting that "some nations might refuse to [cooperate in law enforcement on the Internet], offering instead a national data haven to attract the business of customers desiring to keep all of their activities on the global grid unidentified."); Canute James, *Barbados Ties Economy to Information Services*, J. OF COM., Mar. 20, 1996, at A5 (quoting Barbados Trade and Business Minister Phillip Goddard as saying that he wants to make Barbados "a center for offshore information services").

45. *See Businesses Promote Fraud Tools*, *supra* note 1, at D4.

Note concludes that an international convention concerning law enforcement on the Internet is necessary, and that national governments can strengthen their legal positions in the interim by establishing mutual legal assistance treaties ("MLATs")[46] with nations which pose problems to law enforcement in cyberspace.

I. ANONYMOUS REMAILERS: A TOOL FOR FREEDOM AND CRIME

The Internet has provided unprecedented ability to transmit and receive data internationally.[47] In addition, data transmission over the Internet can be accomplished with a great deal of secrecy and privacy through the use of identity-concealing devices such as anonymous remailers.[48] The ease of anonymity on the Internet has been a blessing for political dissidents, corporate whistle-blowers, participants in on-line therapy groups and others who depend on privacy to accomplish their goals in safety.[49] Nonetheless, anonymous remailers also create problems for law enforcement by making it difficult to trace individuals who break the law in cyberspace.[50] This section will outline the history and capabilities of anonymous remailers, describe their legitimate and beneficial uses, and conversely illustrate the ways in which anonymous remailers can be used to violate the law.

A. *The Rise of Anonymous Remailers*

By now, the Internet needs little introduction to much of

46. *See generally* James I.K. Knapp, *Mutual Legal Assistance Treaties as a Way to Pierce Bank Secrecy*, 20 CASE W. RES. J. INT'L L. 405 (1988) (discussing the nature and operation of MLATs).

47. *See Businesses Promote Fraud Tools*, *supra* note 1, at D4.

48. *See infra* notes 56-69 and accompanying text (discussing the operation of anonymous remailers).

49. *See infra* notes 70-80 and accompanying text (discussing beneficial uses of anonymity on the Internet).

50. *See infra* notes 81-118 and accompanying text (discussing obnoxious, tortious and criminal acts conducted with the aid of anonymous remailers).

the public. From obscure beginnings in the 1960s,[51] the Internet has expanded into an amalgam of more than 20,000 government, corporate, academic, and commercial networks[52] in 159 countries.[53] Recent estimates indicate that nearly twenty million users are connected to the Internet.[54]

Beginning in the late 1980s, as the Internet grew from a closed network primarily used by universities and governments into a public forum, large numbers of services sprang up in cyberspace to meet the needs of the growing population of users.[55] One of these needs—and one for which a large market existed—was anonymity; this need was filled by anonymous remailers.[56]

An anonymous remailer is essentially a conduit through which information is received, stripped of its identity, and forwarded to its final destination.[57] Electronic mail is sent to

---

51. The Internet grew out of an experimental project of the Department of Defense's Advanced Research Projects Administration ("ARPA"), designed to provide researchers with direct access to computers at key laboratories and to facilitate the transmission of vital national defense communications. *See Shea*, 930 F. Supp. at 925-26. ARPA supplied funds to link computers operated by the military, defense contractors, and universities conducting defense-oriented research over dedicated telephone lines. *Id.*

52. A network is a system of interconnected computer systems and terminals. WEBSTER'S NEW WORLD DICTIONARY OF COMPUTER TERMS, *supra* note 7, at 391-92.

53. *See* Lewis, *supra* note 13 at C15.

54. Long, *supra* note 15, at 1180; *see also Shea*, 930 F. Supp. at 925 (estimating that as many as 40 million users were connected to the Internet as of early 1996 and that as many as 200 million will have access by 1999).

55. *See generally* Long, *supra* note 15, at 1180-85 (outlining the history of the Internet, and describing many of the services that have grown up to meet the demands of Internet users).

56. *See id.* at 1185-86.

57. Harris, *supra* note 5, at 5. The function of anonymous remailers has been compared to a device called the "cheesebox," which was invented during the Prohibition era to prevent the tracing of telephone calls. *See* L. Detweiler, *Internet Anonymity FAQ*, § 1.6 (compiled May 9, 1993) <ftp://rtfm.mit.edu:/pub/ usenet/news.answers/net-anonymity> (quoting Phil Karn). The cheesebox connected two telephone lines on the premises of a third party, usually an uninvolved business, thus preventing law enforcement authorities from tracing bootleggers' calls. *Id.*

A FAQ file, or Frequently Asked Questions file, is a public file maintained

the remailer with forwarding orders.[58] Upon receiving the information, the remailer removes the source address and replaces it with identifying information indicating that the source of the mail is a numbered anonymous account.[59] Mail may be forwarded to a specific address or posted to a "Usenet newsgroup"—one of the more than 10,000 topical discussion groups that exist on the Internet.[60] Replies to messages sent via anonymous remailer are often anonymized, creating a "double-blind" situation in which a transaction can occur where neither party knows the identity of the other.[61]

The more sophisticated anonymous remailers contain custom features to ensure that forwarded messages remain anonymous.[62] Many electronic mail services automatically append the name or signature file[63] of the sender to the bot-

---

on the Internet to provide background and useful information in a specific area. *See* Long, *supra* note 15 at 1182 n.25. FAQs exist for a wide variety of topics and are maintained by Usenet newsgroups as well as private individuals. *Id.* Currently, two FAQs relating to the issue of anonymous remailers exist on the Internet. These are the Remailer FAQ (visited Sept. 14, 1996) <http://www.well.com/user/abacard/remail.html> and the Internet Anonymity FAQ. Many other FAQs and other World Wide Web sites dealing with anonymity and privacy issues exist on the Internet and can be found using public Internet search utilities.

58. Harris, *supra* note 5, at 5.

59. *Id.*

60. Usenet, which is one of the most popular and widely used Internet resources, has been defined as:

> [A] worldwide community of electronic B[ulletin] B[oard] S[ystems] that is closely associated with the Internet and the Internet community. The messages in Usenet are organized into thousands of topical groups, or "Newsgroups" . . . . As a Usenet user, you read and contribute ("post") to your local Usenet site. Each Usenet site distributes its users' postings to other Usenet sites based on various implicit and explicit configuration settings, and in turn receives postings from other sites. Usenet traffic typically consists of as much as 30 to 50 [megabytes] of messages per day. Usenet is read and contributed to on a daily basis by a total population of millions of people. . . . There is no specific network that is the Usenet. Usenet traffic flows over a wide range of networks, including the Internet and dial-up phone links.

Dern, *supra* note 3, at 196-97.

61. Froomkin, *Anonymity and Its Enmities*, *supra* note 39, at par. 38.

62. Harris, *supra* note 5, at 5.

63. A signature file, or ".sig file," is a file consisting of personal information,

tom of all outgoing mail; the operators of a number of anonymous remailers have responded to this automatic process by devising software that automatically deletes this identifying information.[64] Some remailers, in addition, allow users to specify custom "cutmarks," which instruct the remailer as to where and what to cut from each forwarded message.[65] In fact, some remailers introduce a random time delay prior to forwarding, so that the recipient of the message cannot draw any conclusions about the sender's location from the time the message was originally mailed.[66]

The first anonymous remailers appeared in 1988 for the convenience of Internet users who wished to post messages to certain sensitive Usenet newsgroups, such as alt.sexual.abuse. recovery, an on-line support group for survivors of sexual abuse.[67] The first "universal anonymous server"—a remailer through which users could post messages to a variety of newsgroups or send private e-mail—appeared in September 1992.[68] The majority of anonymous remailers in use today utilize variations of the software created for this original universal server by Carnegie-Mellon University research programmer Karl Kleinpaste.[69]

---

quotations and/or official disclaimers which is appended to the bottom of outgoing messages. *See* Judith H. Bernstein, *How to Handle Signature Files—Add Meaning*, *Add Snap*, *Add Another Message To Your Mail*, NET GUIDE, Feb. 1, 1996, at 85.

64. Harris, *supra* note 5, at 5.

65. *Id.*

66. *Id.*; *see also* Andre Bacard, *Remailer FAQ* (compiled Apr. 12, 1995) (on file with author). According to Bacard, one of the characteristics of an "ideal" anonymous remailer is one that "[h]olds your messages for a RANDOM time before forwarding them. This time lag makes it harder for snoops to link a message that arrives at, say, 3:00 P.M. with a message that leaves your machine at, say, 2:59 P.M." *Id.*

67. John Byczkowski, *Online: Abuses v. Uses Stirs Anonymous Servers Controversy*, CINCINNATI ENQUIRER, June 12, 1994, at F10.

68. *Id.*; *see also* Joshua Quittner, *E-Mail Anonymity Eases Exchange of Secrets; Remailer Helps Protect Identities of Users*, EDMONTON J., Jan. 8, 1994, at G2.

69. *Id.* More advanced anonymity is also provided by "cypherpunk" and "Mixmaster" remailers. Mixmaster is the newest generation of anonymous remailer, relying on an encryption and anonymizing program installed in the original user's personal computer. *See* Arnoud Engelfriet, *Anonymity and Privacy on the Internet* (visited Sept. 14, 1996) <http://www.stack.urc.tue.nl/

B. *The Benefits of Anonymous Remailers*

Anonymous remailers have been staunchly defended by many civil-liberties advocates, who contend that public discussion on the Internet requires the protection of anonymity in certain cases.[70] For instance, anonymous remailers have been used by dissidents in Singapore to criticize the island's government without the risk of harassment or imprisonment.[71]

Other users of anonymous remailers include participants in on-line therapy groups, who often wish to remain

---

~galactus/remailers/index-anon.html>. Cypherpunk and Mixmaster remailers possess a disadvantage as compared to traditional "pseudonymous" remailers, in that the additional safeguards inherent in these systems make it impossible to reply to messages sent through these remailers. *Id.* Thus, anonymous two-way transactions over the Internet generally require the use of a pseudonymous remailer; however, more advanced remailers can be used for defamation, dissemination of copyrighted material, or "information terrorism." *See infra* notes 94-105 and accompanying text (discussing methods of using anonymous remailers for criminal acts). Engelfriet's web site provides detailed information on the current state of anonymity and privacy technology on the Internet, and offers links to other anonymity-related sites.

70. For example, the American Civil Liberties Union and the Electronic Frontiers Foundation have indicated that they will join anonymous-remailer operator Sameer Parekh and New York journalist Jonathan Wallace in challenging a recently enacted Georgia statute criminalizing the misrepresentation of identity on-line. Art Kramer & Elizabeth Lee, *On-Line Anonymity Lawsuit in Georgia Gets Extra Support*, ATLANTA CONST., Sept. 4, 1996, at 7C; Georgia Computer Systems Protection Act, GA. CODE ANN. §§ 16-9-90 through 16-9-94 (1996).

Discussions of the right to anonymity on the Internet are often couched in terms of civil liberties. *See* Detweiler, *supra* note 57, § 5.4 (quoting Stuart P. Derby as saying that "[t]hree of our [the U.S.'s] founding fathers, Madison, Hamilton, and Jay, seemed to think 'anonymous posting' was OK. The Federalist papers [sic] were originally printed in New York newspapers with authorship attributed to 'Publius.'"). Derby went on to speculate as to whether critics of Internet anonymity, such as the individual to whom he was replying, would find the Founding Fathers' purposes "legitimate." *Id. But see* McIntyre v. Ohio Elections Comm'n, 115 S. Ct. 1511, 1537 (1995) (Scalia, J., dissenting) (arguing that anonymity, although justifiable under extraordinary circumstances, is essentially dishonorable and undeserving of constitutional protection in that it "facilitates wrong by eliminating accountability, which is ordinarily the very purpose of the anonymity").

71. *See* Lavin, *supra* note 32, at 1; *see also* Standage, *supra* note 40, at 3 (discussing attempts by the government of Singapore to censor speech on the Internet).

anonymous while discussing sensitive personal issues in a public forum.[72] Participants in sexual discussion groups, which include many groups devoted to socially disapproved practices, also use anonymous remailers on a regular basis to prevent their sexual habits from becoming public knowledge.[73] Anonymity may be especially important to users who are public figures in their own right, and do not wish their psychological problems or sexual proclivities to become grist for the media.[74]

Privacy may be necessary for other reasons as well. Users of anonymous remailers include professionals who do not wish to be deluged with requests for free advice,[75] job-seekers who do not want their current employers to know that they are seeking work elsewhere,[76] corporate and government whistle-blowers who fear retaliation should their

---

72. Steve Harris, *Internet: Care in the Virtual Community: It's Easy to Find Social Support in Cyberspace*, GUARDIAN (LONDON), Mar. 16, 1995, at 4.

73. *See* Kenneth Li, *Where Nobody Knows Your Name*, VILLAGE VOICE, Aug. 15, 1995, Educ. Supp., at 28; *see also* Akst, *supra* note 39, at 1. An unidentified Alabama woman has been quoted as stating that:

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

Id. In addition, according to one court:

> Anonymity is important to Internet users who seek to access sensitive information, such as users of the Critical Path AIDS Project's Web site, the users, particularly gay youth, of Queer Resources Directory, and users of Stop Prisoner Rape (SPR). Many members of SPR's mailing list have asked to remain anonymous due to the stigma of prisoner rape.

ACLU v. Reno, 929 F. Supp. 824, 849 (E.D. Pa. 1996).

74. Li, *supra* note 72, at 28. Li explains: "[l]et's say you wanted to post a message to alt.transgender . . . and let's say . . . you were a congressman. Certainly, you wouldn't want your constituents, and certainly not the voters, to be aware of some of your idiosyncratic hobbies . . . ." *Id.*

75. Froomkin, *Anonymity and Its Enmities*, *supra* note 39, at par. 16. Professor Froomkin states that he has "posted messages to newsgroups and received a great deal of unwanted e-mail in reply because my e-mail signature identifies me as a law professor. One way to avoid getting requests for free legal advice is to delete the signature and route comments through a remailer." *Id.*

76. Bacard, *supra* note 66.

names become known,[77] refugees who fear retaliation against themselves or their families at home,[78] and participants in on-line dating services who prefer to remain anonymous during the initial stages of correspondence in order to minimize the risk of being victimized by a stalker.[79] Some Internet commentators have also recommended the use of anonymous remailers as a protection against receipt of unsolicited commercial e-mail.[80]

C. *The Dangers of Anonymity in Cyberspace*

Anonymous remailers, however, also have other, less legitimate uses, ranging from the annoying to the criminal. Anonymous remailers are often used for "spamming," which is excessive and unwanted advertising in inappropriate Internet forums.[81] Many Internet users have commented further on the high incidence of "trolling"—that is, public baiting of other users—by holders of anonymous accounts.[82]

---

77. *See* Peter H. Lewis, *Is Computer Anonymity a Constitutional Right?*, STATE J.-REG., Dec. 31, 1994, at 10.

78. Steve Harris, *E-Mail: Secret Service: Steve Harris on the Clash Between Anonymity and Accountability on the Internet*, GUARDIAN (LONDON), Mar. 2, 1995, at 7 (quoting physicist Dr. Bruce Scott as saying that "for many Iranians, an anonymous remailer of some sort is the only way they can contact their relatives and friends at all, since the mere appearance of their names is dangerous to their lives.").

79. *Id.*

80. Steve Creedy, *Internet Spawning Spammers: Unsolicited E-Mail a By-Product of On-Line Commercialization*, PITT. POST-GAZETTE, July 28, 1996, at C3. This article notes that many originators of commercial e-mail compile mailing lists by noting the e-mail addresses of Usenet posters. *See id.* Posting to Usenet anonymously is recommended as a means of insuring that on-line solicitors are unable to ascertain the user's actual e-mail address. *Id.*

81. Steve Harris, *Internet: A Plague that Travels by Post: Easy to Do and Often Tricky to Trace, Spamming is Sweeping the Net*, GUARDIAN (LONDON), July 6, 1995, at 4.

82. *See* Detweiler, *supra* note 57, § 1.5 (citing the example of "a poster [who] might describe ways of attacking cats on the cat-lovers group . . . these messages appeared long before the [anonymous remailer] services . . . but the servers tend to make it easier and almost encourage it. . . ."); *see also id.* § 2.1 (quoting Kleinpaste as saying that "even as restricted as it was, my system was subjected to abuses to the point where it was ordered dismantled by the facilities staff. . . . Such abuses started right after it was created").

Although the individuals who publish such messages are a small minority of anonymous-remailer users,[83] their presence has been significant and troubling enough to draw considerable attention from the Internet community.[84] In addition, a number of Internet hoaxes—such as the announcement, distributed in 1994 in the guise of an Associated Press news release, that Microsoft Corporation had acquired the Roman Catholic Church "in exchange for an unspecified number of shares of Microsoft common stock"—have also been transmitted via anonymous remailers.[85]

On a more sinister level, anonymous remailers can be used to harass or threaten other members of the on-line community without fear of retaliation.[86] Kleinpaste, the creator of the original universal anonymous server, shut his service down less than nine weeks after he opened it to the public.[87] This was in response to a rash of incidents, including a user who posted vulgar materials to Usenet newsgroups aimed at children and another who attempted to blackmail his former girlfriend by threatening to sell porno-

---

83. *See id.* § 5.5 (quoting Helsingius as saying that: "[t]he latest statistics from the service show 18203 registered users, 3500 messages per day on the average . . . . I have received complaints involving postings from 57 anonymous users, and, of these, been forced to block only 8 users who continued their abuse despite a warning from me. . . .").

84. *See generally id.* §§ 5.6, 6.1.

85. Peter H. Lewis, *Anonymous Spoof Points Up Hazard in Information Highway*, DALLAS MORNING NEWS, Jan. 2, 1995, at D4.

86. *See* Detweiler, *supra* note 57, § 2.3. Detweiler quotes a letter in opposition to anonymity by an unidentified Internet user, who argues that he is:

> [A] firm believer in privacy, but that is not the same thing as anonymity. Anonymity can be used to violate another's privacy. For instance, in recent years, I have had harassing anonymous notes and phone calls threatening XXX because of things I have said on the net . . . . I have seen neighbors and friends come under great suspicion and hardship because of anonymous notes claiming they used drugs or abused children. I have seen too many historical accounts of witch-hunts, secret tribunals, and pogroms—all based on anonymous accusations. I am in favor of defeating the reasons people need anonymity, not giving the wrong-doers another mechanism to use to harass others.

Id.

87. Byczkowski, *supra* note 67, at F10.

graphic pictures of her over the Internet.[88] Anonymous threats to the President of the United States have also been received via electronic mail.[89] In addition, anonymous remailers are also used regularly to post bigoted or hate-filled messages to Usenet newsgroups.[90]

Electronic vandalism, or on-line activities which damage or disrupt the flow of information over the Internet, is another common practice among anonymous Internet users.[91] Through a practice known as "pinging," users may temporarily disable an Internet address by bombarding it with thousands of messages.[92] This practice, also known as "mail bombing," temporarily disabled the Pipeline Internet access provider in New York City in November 1994.[93]

The greatest threats to law enforcement stemming from Internet anonymity, however, are large-scale data theft and financial crime,[94] copyright infringement,[95] international trafficking in pornography,[96] and "information terrorism."[97]

---

88. *Id.*

89. Lewis, *supra* note 77, at 10.

90. A recent spot check of the Usenet newsgroup soc.culture.jewish, for example, taken before the closing of anon.penet.fi, revealed that more than 20 percent of anti-Semitic messages posted to the newsgroup were posted through anonymous remailers. Search of soc.culture.jewish, Usenet newsgroup (May 12, 1996). A similar percentage of racist messages on soc.culture.african.american had been anonymized prior to being posted on the newsgroup. Search of soc.culture.african-american, Usenet newsgroup (May 12, 1996). A common complaint in many ethnic newsgroups, in the words of soc.culture.israel poster Roger Froikin, is that "the haters lack the guts to use their real names." *See also* Detweiler, *supra* note 57, § 5.6 (quoting various Internet users who describe "viciously offensive and scatological anti-Arab posts . . . in talk.politics.mideast" and "a rise in KTF ('Kill the Fags') in alt.sex from anonymous postings, as well as KTJ postings in soc.culture.jewish.")

91. Wilder & Violino, *supra* note 20, at 30.

92. *Id.*

93. Lewis, *supra* note 77, at 10.

94. *Id.*

95. *See id.*; *see also infra* note 135 (discussing the Church of Scientology's on-line intellectual property disputes).

96. *See supra* note 9 and accompanying text (discussing the availability of child pornography on the Internet).

97. *See* Paul A. Strassmann & William Marlow, *Risk-Free Access Into The*

Federal law enforcement estimates indicate that more than $10 billion in data is stolen annually in the United States.[98] In addition to pirated software and other copyrighted materials, stolen data includes credit-card and calling card numbers, and corporate trade secrets.[99]

Through the use of anonymous remailers, traders in stolen data are able to conceal both their identities and those of their customers.[100] Illegal data exchanges have sprung up on a number of Usenet newsgroups.[101] Typically, a transaction in stolen data begins with an anonymously posted message offering the contraband for sale.[102] Interested customers respond with encrypted messages indicating their interest in purchasing the data, following which the transaction "goes black"—that is, completely anonymous.[103] In one exceptionally large instance of data theft, MCI technician Ivy James Lay pled guilty in January 1995 on charges of selling more

---

Global Information Infrastructure Via Anonymous Re-Mailers, Harvard University, Kennedy School of Government, *Symposium on the Global Information Infrastructure: Information, Policy & International Infrastructure* (Jan. 28-30, 1996) (visited Nov. 16, 1996) <http://www.strassmann.com/pubs/anon-remail.html>. Strassmann and Marlow argue that the global government, financial, and telecommunications information infrastructure is vulnerable to disruption from computer-based assaults. *Id.* Strassmann is a member of the faculty of the U.S. Military Academy at West Point; Marlow is a senior vice president at Science Applications International Corporation ("SAIC"). *Id.*

Anonymous remailers have also been used to disseminate instructions on commission of more traditional acts of terrorism. *See Hearing on Terrorism, Technology and Government, before the Senate Judiciary Comm.*, 104th Cong., 2d Sess. (1995) (testimony of Robert S. Litt, Deputy Asst. Atty. General) (indicating that information regarding bomb construction had been disseminated via an anonymous remailer after the Oklahoma City bombing).

98. Wilder & Violino, *supra* note 20, at 30.

99. *Id.*; *see also* Froomkin, *Anonymity and Its Enmities*, *supra* note 39, at par. 49 (arguing that protection of intellectual property faces a great threat from anonymity on the Internet). Professor Froomkin cites the example of the recent disclosure on the Internet of the source code to a proprietary unpatented algorithm. *Id.* ("The proprietary value of that trade secret is now much less than it was a few months ago . . . .").

100. Wilder & Violino, *supra* note 20, at 30.

101. *Id.*

102. *Id.*

103. *Id.*

than 60,000 calling card and credit-card numbers under the cover of anonymity.[104] Lay, known in cyberspace as the "Knight Shadow," sold the stolen credit card numbers to end users in a number of European countries with the aid of a Spanish co-conspirator.[105]

Trafficking in pornography is also greatly facilitated by the use of anonymous remailers.[106] Dealers in child pornography often route their merchandise through anonymous remailers located in countries where child pornography is legal,[107] or where anti-pornography statutes have not yet expanded to cover electronic media.[108] Identity can be further

---

104. *Id.*

105. *Id.*

106. Arthur, *supra* note 9, at 13.

107. *See, e.g.*, United States v. Moncini, 882 F.2d 401, 403 (9th Cir. 1989) (defendant Moncini challenged his conviction for mailing child pornography from Italy to California on the grounds that distribution of child pornography was legal in Italy). A number of other countries have also not yet criminalized sale, possession or distribution of child pornography. *See Swedish Monarch, Nobel Laureates Urge War on Scourge of Child Abuse*, DEUTSCHE PRESSE-AGENTUR, Aug. 31, 1996 (sale and possession of child pornography legal in Sweden); Thomas Sancton, *Preying on the Young*, TIME, Sept. 2, 1996, at 22 (possession legal in Mexico); Angeline Oyog, *Cybercops Wanted to Police Information Highway*, INTER PRESS SERVICE, Aug. 30, 1996 (child pornography tolerated in Thailand). In many cases, the legality of child pornography in any given country is complicated by variations in the age of consent. *Id.* A recent study by Kathleen Mahoney of the University of Canada and Laura Lederer of the University of Minnesota, which surveyed child pornography laws in 162 countries, indicated that "the Philippines has all the right laws on the books, but the age of majority is 12." *Id.*; *see also* Roger J.R. Levesque, *Sexual Use, Abuse and Exploitation of Children: Challenges in Implementing Children's Human Rights*, 60 BROOK. L. REV. 959, 986 n.141 (1994) (regarding age of consent as an issue in determining the legality of child pornography).

108. Arthur, *supra* note 9, at 13. A number of jurisdictions inside and outside the United States have thus far failed to modernize their child pornography statutes to include materials created or disseminated via electronic media. An instructive example is provided by Article 263 of the New York State Penal Law, which punishes the production, dissemination, purchase or possession of a "sexual performance" by a child. *See* N.Y. PENAL LAW § 263.00-.16. A "performance" is defined as "any play, motion picture, photograph or dance," and additionally as "any other visual representation exhibited before an audience." N.Y. PENAL LAW § 263.00(4). Any of the materials specifically listed in the statute is prohibited in New York, regardless of whether it is exhibited before an audience. People v. Gaito, 199 A.D.2d 615 (N.Y. App. Div.), *app. denied*, 83 N.Y.2d 805 (1993).

disguised, making the task of law enforcement officials even more difficult, by routing pornographic materials through a series of anonymous remailers.[109] In a related area of criminal activity, sexual predators may disguise their identity by means of anonymous remailers when communicating with underage victims via the Internet.[110]

An additional hazard to law enforcement may develop with the growth of "digital cash" or "e-cash."[111] Anonymous transmission of digital cash would greatly facilitate money-laundering, and might allow untraceable blackmail or even demands for ransom.[112]

However, materials not specifically listed in the statute—such as computer-generated images—must be shown before an audience in order to constitute a prohibited "performance" under the Penal Law. This gap in the Penal Law's protection against child pornography is especially problematic in cases where an image was altered or partially generated in the computer itself rather than being simply a digital representation of a photograph or motion picture.

109. Arthur, *supra* note 9, at 13. *Id.*; *see also* Peter H. Lewis, *Computer Jokes and Threats Ignite Debate on Anonymity*, N.Y. TIMES, Dec. 31, 1994, at A5 (indicating that messages mailed through multiple anonymous remailers can be remailed in a random sequence different from the order in which they arrive, making it impossible to trace messages by matching the routes taken by incoming and outgoing information); Dave Mandl, *Life After Penet: The Remailer is Dead, Long Live the Remailer*, VILLAGE VOICE, Oct. 8, 1996, at 23 (noting that an Oakland-based service, Community ConneXion, offers an interface that allows sending of anonymous E-mail through a chain of up to 10 remailers with the push of a button); Froomkin, *Anonymity and Its Enmities*, *supra* note 39, at pars. 22-25 (describing a process by which a message can be sent through a "chain" of anonymous remailers). The preservation of anonymity can be greatly facilitated if one of the remailers in the chain "either erases [the original sender's] logs or is outside . . . [the] jurisdiction" of the judge in whose court disclosure of the sender's identity is sought. *Id.* at par. 25.

110. *See* Friedman & Buys, *supra* note 24, at 15 (noting that a hypothetical child victim communicating with an anonymous predator "has no way of knowing that his or her e-mail 'friend' is really a convicted child abuser in the next town"). A number of pedophiles have gained access to minors by presenting themselves as minors on the Internet; in at least one case, a Florida man was arrested for kidnapping after he befriended a 13-year-old Chicago boy over the Internet, arranged a meeting, and brought the child to Louisville, Kentucky by bus. *See id.* at 14-15.

111. Froomkin, *Anonymity and Its Enmities*, *supra* note 39, at par. 41.

112. *Id.* at par. 46. Professor Froomkin describes a hypothetical kidnapping where:

> [I]nstead of demanding small unmarked bills, the extortionist demands

Perhaps the most disturbing consequence of Internet anonymity, however, is the possibility of "information terrorism" against national governments or corporations.[113] In developed nations, which are increasingly dependent upon information networks for crucial government and public utility functions, information-based assaults upon government, financial, power generation, or telecommunications computer systems have the potential for massive disruption.[114] If such an attack is conducted via anonymous remailers, the risk to the perpetrator is minimal.[115]

Law enforcement officials admit that they "are playing catch-up" in their efforts to combat electronic crime committed under cover of anonymity.[116] American authorities, however, may obtain court orders directing a remailer to reveal the source address of illegal materials that have been transmitted via an anonymous remailer located in the United States.[117] In cases where electronic contraband travels through one or more foreign countries before reaching its destination, though, the law enforcement agencies' task is often increased by orders of magnitude.[118]

> that the victims publish the digital signatures of a large quantity of e-cash in a newspaper. Because the payoff occurs via publication in a broadcast medium such as a newspaper [or] a Usenet group, the extortionist faces no danger of being captured while attempting to pick up the ransom. And because the e-cash is untraceable, the extortionist is able to spend it without fear of marked bills, recorded serial numbers, or other forms of detection.

Id.

113. Strassmann & Marlow, *supra* note 97.

114. *Id.*

115. *Id.*

116. Wilder & Violino, *supra* note 20, at 30.

117. *See* Froomkin, *Anonymity and Its Enmities*, *supra* note 39, at par. 15.

118. *See* Peter J. Vassalo, *The New Ivan the Terrible: Problems in International Criminal Enforcement and the Specter of the Russian Mafia*, 28 CASE W. RES. J. INT'L L. 173, 188-90 (1996) (discussing the difficult and time-consuming nature of traditional international criminal law enforcement).

II. A CASE IN POINT: L'AFFAIRE HELSINGIUS AND INTERNATIONAL LAW ENFORCEMENT IN CYBERSPACE

The difficulties of enforcing the law in an environment in which anonymity can be freely obtained is illustrated by several recent incidents involving stolen intellectual property. In these incidents, disputed intellectual property was published throughout the Internet by means of anonymous remailers. The most illustrative of these, and the incident with the most far-reaching effects, occurred recently in Helsinki, where Finnish police were persuaded to raid the offices of a local remailer operator in search of the identity of an alleged copyright violator.[119] The ramifications of the Helsinki incident, which are outlined below, are a graphic demonstration of the issues and balancing tests which face law enforcement agencies on the Internet and point up a comparison with another recent and growing international law enforcement problem—offshore banking.[120] This part discusses these ramifications, and describes measures taken in the regulation of offshore banking that may be of use in combating the similar problems posed by anonymity on the Internet.

A. *A Dispute in Finland*

Until recently, the world's largest anonymous remailer, anon.penet.fi,[121] operated in Helsinki, Finland.[122]

---

119. *See* Lavin, *supra* note 32, at 1; *see also infra* notes 134-42 and accompanying text (discussing the Helsingius affair).

120. A comprehensive discussion of offshore banking is beyond the scope of this Note. This Note will outline, in general terms, the issue of offshore banking and its analogies to the environment of the Internet, and describe measures taken to control offshore banking which might be adaptable to cyberspace. Readers are referred to the articles cited in this section for a more complete discussion of issues in international banking regulation.

121. An Internet address such as anon.penet.fi consists of a "user name" and a "domain name." The "user name" is an identifier unique to a particular user, while a "domain name" is assigned to a particular computer or set of computers. Shea v. Reno, 930 F. Supp. at 933. "Anon" is thus the user name assigned to the anonymous remailer service on the penet.fi computer network. The suffix "fi" indicates that the penet network operates in Finland. Each nation other than the

Anon.penet.fi, which processed and forwarded more than 8,000 messages each day,[123] contained more than 500,000 active accounts.[124] Approximately seventy-five percent of those accounts originated in the United States.[125] The proprietor of the remailer, Johan Helsingius, is the managing director and part owner of a Finnish Internet access provider, and a civil libertarian who operated anon.penet.fi as a labor of love.[126]

Finland is an ideal location for an anonymous remailer for several reasons. Finland leads the world in the number of Internet connections per capita, and contains the world's most comprehensive and sophisticated network of Internet access providers.[127] In addition, Finnish law includes stringent protections of personal privacy, including a constitutional provision which specifically protects the security of

---

United States has a distinctive identifying suffix which is attached to the domain names of its computer networks. Internet addresses additionally contain names or numbers identifying particular accounts. On anon.penet.fi, these account identifiers take the form anXXXXXX@anon.penet.fi. A numbered account on anon.penet.fi might be identified, for example, as an244354@anon.penet.fi.

122. Lavin, *supra* note 32, at 1.

123. Mandl, *supra* note 109, at 24.

124. Engelfriet, *supra* note 69.

125. Lavin, *supra* note 32, at 1.

126. Joshua Quittner, *Worldwide Anonymous Remailer Service Keeps Freedom of Expression On-Line*, PLAIN DEALER, Mar. 6, 1994, at 1G. Helsingius, the proprietor of the Oy Penetic Ab Internet access service in Helsinki, credits his commitment to on-line anonymity to his sensitivity "to the plight of political minorities; his parents, he explained, are part of Finland's Swedish-speaking minority." *Id.*; *see also* Bacard, *supra* note 66. Bacard quotes Helsingius as saying:

> Living in Finland, I got a pretty close view of how things were in the former Soviet Union. If you actually owned a photocopier or even a typewriter there you would have to register it and they would take samples of what your typewriter would put out so they could identify it later. That's something I find so appalling. The fact that you have to register every means of providing information to the public sort of parallels it, like saying you have to sign everything on the Net. We always have to be able to track you down.

Id.

127. Marc Ferranti, *Merita*, COMPUTERWORLD, Sept. 9, 1996, at 36. Finland has 24 people per Internet access server, compared to 59 per access point in the second and third ranking nations, Sweden and Australia. *Id.* In Finland, a nation of five million people, some 90,000 homes have access to the Internet. Katharine Stalter, *Scandinavia Wired for Growth*, VARIETY, Sept. 2, 1996, at 64.

confidential mail and telephone messages,[128] and laws ensuring that private communications and records in Finland will remain secure.[129] In fact, Finland's shield of personal privacy law has been breached on only one occasion.[130]

Anon.penet.fi weathered a number of scandals in its four years of operation. Detractors of Helsingius' service have "mailbombed" it on a number of occasions, disabling the service for hours or days.[131] In February 1995, a Swedish newspaper charged that pornographic pictures of children were being transmitted through anon.penet.fi.[132] Although

128. The Finnish Constitution Act of 1919 provides that "[t]he secrecy of postal, telegraphic, and telephonic communication shall be inviolable, except when otherwise provided by law." Constitution Act of 1919, art. 12 (Fin.). The Constitution Act of 1919 remains the current constitution of Finland. Interview with Nicholas Hill, Department of Scandinavian Studies, University of Wisconsin-Madison (Nov. 5, 1996).

129. The Personal Data File Act of 1987, for instance, forbids the collection, maintenance or disclosure of personal information without the consent of the person concerning whom records are maintained. *See* Personal Data File Act at § 18 (Fin. 1987). In general, disclosure of records is only possible under court order and under circumstances defined by statute. In addition, section 38(8) of the Finnish Criminal Code provides that unlawful opening of a sealed communication or unlawful interception of a telegram or telephone call is a criminal offense punishable by imprisonment for up to one year. Article 38(9a) of the Criminal Code further provides that the proprietor or employee of a telephone, radio, or telegraph service who unlawfully discloses the contents of communications or confidential information about his customers as provided in Article 40 of the Criminal Code may be imprisoned for up to two years. *See* Criminal Code, art. 38(9a), 40(15), 40(19a) (Fin.); *see also* Antti Suviranta, *Worker Privacy in Finland*, 17 COMP. LAB. L.J. 45, 45-46 (1995) (explaining that Finlanders are "traditionally regarded as valuing their privacy" and that the Finnish privacy laws have recently been made more stringent in response to the implementation of a national identification system); Lavin, *supra* note 32, at 1.

130. *See infra* notes 138-47 and accompanying text (describing the February 1995 Finnish police raid on the offices of anon.penet.fi.). It should be noted, however, that Helsingius is reported to have revealed the identity of a customer on one other occasion, in response to an ongoing American investigation of an alleged stalking incident. Thom Stark, *A Fine and Private Net: Anonymous Remailers Ensure Freedom of Thought, Dialogue*, LAN TIMES, Apr. 1, 1996, at 104.

131. Quittner, *supra* note 126, at 1G. "Mailbombing" is a common electronic vandalism practice wherein the target computer is deluged with electronic mail, causing the system to overload. Wilder & Violino, *supra* note 20, at 30.

132. *See* Harris, *supra* note 78, at 7 (referring to an article in the Swedish newspaper Dagens Nyheter); *see also* Strassman & Marlow, *supra* note 97 (claim-

the stories ultimately proved unfounded, they contributed to an atmosphere of suspicion that led to the breach of the service's secrecy by Finnish police later that month.[133]

The dispute, which led to a Finnish police raid on Helsingius' headquarters, stemmed from a long-running quarrel between the Church of Scientology and an estranged member, Dennis Erlich.[134] The Church of Scientology had frequently engaged in intellectual property disputes on the Internet and elsewhere, having accused former members of illegally distributing Church material on a number of occasions.[135] Scientologists have also released programs, known

---

ing that anon.penet.fi "is frequently used by the Russian (ex-KGB) criminal element").

133. Harris, *supra* note 78, at 7.

134. *Id.*

135. *See* Religious Tech. Ctr. v. Scott, 1996 U.S. App. LEXIS 16398 (9th Cir. 1996); Religious Tech. Ctr. v. Wollersheim, 971 F.2d 364 (9th Cir. 1992); Religious Tech. Ctr. v. F.A.C.T.NET, Inc., 907 F. Supp. 1468 (D. Colo. 1995); Religious Tech. Ctr. v. Lerma, 908 F. Supp. 1353 (E.D. Va. 1995); Religious Tech. Ctr. v. Netcom, 907 F. Supp. 1361 (N.D. Cal. 1995); Church of Scientology Int'l v. Elmira Mission of the Church of Scientology, 614 F. Supp. 500 (W.D.N.Y. 1985). The Religious Technology Center is the arm of the Church of Scientology responsible for protecting the Church's intellectual property. Lewis, *supra* note 36, at D2. The chairman of the Religious Technology Center's board of directors is David Miscavige, who is also the head of the Church of Scientology. *See* Robert Vaughn Young, *Scientology from Inside Out*, QUILL, Nov. 1993, at 38.

Lerma, *Netcom*, and *F.A.C.T.NET* are related cases, stemming from a long-running Internet copyright dispute involving works of the late L. Ron Hubbard, the founder of the Church of Scientology. *See* Alison Frankel, *Making Law, Making Enemies*, AM. LAW., Mar. 1996, at 68. These writings, known as the "Operating Thetans" or "Advanced Technology," were written by Hubbard during the period 1966-86, and were kept secret by his orders. *Id.* Portions of these writings, some of which had previously entered into the record of a California court case, were posted on the Internet by Erlich and Arnaldo Lerma, both ex-Scientologists and members of the board of F.A.C.T.NET, an anti-brainwashing organization. *See id.*

The *Netcom* case, involving a major California Internet access provider, is especially noteworthy, because Erlich was a co-defendant and because the *Netcom* court established the principle that an Internet access provider was not exempt from liability for copyright infringement as a "common carrier." *Netcom*, 907 F. Supp. at 1370. Thus, an Internet access service, including an anonymous remailer, may currently be held liable as a republisher for copyright violations or defamatory statements transmitted by its users. *See id.* at 1370, n.12; *see also Stratton Oakmont Inc. v. Prodigy Servs. Co.*, 23 Media L. Rep. 1794 (N.Y. Sup. Ct. 1996)

as "cancelbunnies" or "cancelbots," which seek out and delete on-line messages critical of the Church.[136]

In January 1995, anon.penet.fi became involved in the dispute between the Church of Scientology and Erlich, a former Scientology minister who had become an ardent opponent of Scientology after leaving the Church.[137] Erlich posted excerpts from the Church's sacred texts on a Usenet newsgroup, alt.religion.scientology, in order to highlight those aspects of the Church's teachings which he perceived to be absurd.[138]

On February 2, 1995, the Church of Scientology filed a complaint through Interpol with the Finnish police, charging that sacred texts, which the Church claimed were protected by copyright, had been stolen from the Church and transmitted through anon.penet.fi.[139] In the climate of suspicion which followed the Swedish newspaper accounts, the Church of Scientology was able to secure a search warrant from the Finnish courts.[140]

The Finnish authorities offered Helsingius a choice be-

(holding that an Internet access service may be held liable for defamatory statements on the part of its users).

The Church of Scientology has engaged in numerous other on-line copyright disputes, in one case attempting to shut down an entire Usenet newsgroup, alt.religion.scientology, by asserting an intellectual property right to the word "Scientology." Frankel, *supra*, at 68. Another on-line critic of the Church of Scientology, known as "Scamizdat," has thus far eluded detection through the use of a series of anonymous remailers. Kim, *supra* note 22, at 1267 n.59.

136. *See* Jim McClellan, *Cyberspace: Law of the Wires: Jim McClellan on an Almighty Row Over Net*, GUARDIAN (LONDON), Oct. 1, 1995, at 6.

137. *Id.*

138. *Id.*

139. *See* Andrew Brown, *Row Lifts Lid on Computer Giving User Anonymity*, S. CHINA MORNING POST, Mar. 5, 1995, at 10. The Church of Scientology was able to file its Interpol complaint through the FBI. *Flash Point 8 Finland—Identity Papers on the Internet*, COMPUTER FRAUD & SECURITY BULL., Jan. 1, 1996. At least one commentator has speculated that the Church of Scientology was able to obtain the assistance of the FBI because FBI director Louis Freeh favors an outright ban on anonymous remailers. *Id.*; *see also* Gary Chapman, *Net Gain*, NEW REPUBLIC, July 31, 1995, at 10 (stating that Freeh wants to outlaw anonymous remailers).

140. Harris, *supra* note 78, at 7.

tween revealing the source of the disputed messages or confiscation of his computer, which contained a comprehensive list of the source addresses for the 200,000 accounts then active on anon.penet.fi.[141] Rather than sacrifice the anonymity of his entire clientele, Helsingius released Erlich's identity to Finnish police, who passed the information on to the Church of Scientology.[142]

The raid on anon.penet.fi had hardly been completed when the Finnish police announced that they had made a mistake.[143] Finnish authorities stated that the national police department had been led to believe that a crime had occurred in Finland, but that Helsingius' service was actually a passive conduit through which material illegal in the United States had been distributed.[144] Under Finnish law, a search warrant cannot be obtained unless a crime has been committed in Finland.[145] Following the incident, the Finnish police promised to be more circumspect in piercing the privacy of anonymous remailers in the future.[146]

This incident, however, was not the end of the anon.penet.fi dispute. The Church of Scientology pursued a complaint against Helsingius in the Finnish courts, in connection with two other alleged copyright violators.[147] On

---

141. *Id.*

142. *See id.*

143. Lavin, *supra* note 32, at 1 (quoting Finnish Det. Sgt. Kaj Malmberg as stating that "we [the Finnish national police] really feel that we were being used").

144. *Id.*

145. *See id.*

146. *Id.* According to the Finnish police, "we are not going to just rush into someone's home on the basis of a complaint. It has to be a real crime." *Id.*

147. *See* Church of Spiritual Tech. v. Helsingius (Helsinki Dist. Ct., Änestys, J., Aug. 22, 1996), at 2. The Church of Scientology sought the identity of the holders of the accounts identified as an498608@anon.penet.fi and an545430@anon.penet.fi. *Id.* The primary plaintiff, the Church of Spiritual Technology, is a Scientology-affiliated organization which functions as the archivist for the works of L. Ron Hubbard. *See* Robert W. Welkos & Joel Sappell, *The Mind Behind the Religion: Church Scriptures Get High-Tech Protection*, L.A. TIMES, June 24, 1990, at A40. The Religious Technology Center and New Era Publications

August 22, 1996, the Helsinki District Court ruled that the Finnish personal privacy law did not protect electronic mail.[148] The court rejected Helsingius' analogies of his anonymous remailer service to protected trade secrets,[149] mass media,[150] protected telecommunications,[151] and mail,[152] holding that the provisions of Finland's Code of Court Operations required disclosure of the identities sought by the Church of Scientology.[153] The ruling of the District Court,

---

International, a Danish publisher connected to the Church of Scientology, were co-plaintiffs. Helsingius at 1. The complainant officially seeking the order for disclosure was Finnish Criminal Police Inspector Harri Pulkkinen. *Id.*

148. *Id.* at 4; *see also* Lewis, *supra* note 36, at D2.

149. *Helsingius* at 2-3. The legal definition of business or trade secrets in Finland has been read broadly to include customer lists such as Helsingius' customer file. *Id.* Nonetheless, the court found that the protection of trade secrets in Finland was primarily intended to prevent economic loss, and that there would be no economic loss to Helsingius from disclosure as he did not charge for the use of his service. *Id.* at 2-3 (citations omitted).

150. *Id.* at 3. Helsingius argued that the Finnish Constitution Act's protection of freedom of speech, combined with § 17(24) of the Finnish Code of Court Procedure (shielding the identity of mass media sources) protected the secrecy of his customer file. *Id.* However, the court held that "one could not legally draw a parallel [between the Internet and] mass media," because there is no individual on the Internet with editorial responsibility "who one could place in the place of the real writer" to answer for criminal or tortious material. *Id.*

151. *Id.* The court found that the provisions of Government Bill 309/93 (revising the Constitution Act of 1919) provided that the secrecy of confidential telecommunications may in some instances be subordinated to the needs of law enforcement. *Id.* The court also cited Chapter 17 of the Code of Court Procedure, which specifies that private documents or recordings may be subpoenaed for trial. *Id.* Furthermore, the court held that the Internet was not a broadcasting network within the meaning of Finnish law, and that the protections of section 29 of the Telecommunications Law thus did not apply to the Internet. *Id.* at 4.

152. *Id.* at 3-4. Helsingius argued that it would be a criminal offense for him, as the operator of a communications service, to disclose the contents of messages sent through his service, similar to the punishments provided for disclosure of confidential mail or telegraph communications. *Id.* at 3; *see also supra* note 129 (discussing the Finnish Criminal Code's protections of privacy). The court held that the protection of mail secrecy in Finnish law did not apply to Usenet posts which were meant to be read globally. Helsingius at 3. Thus, Helsingius would not be guilty of a criminal offense under the Criminal Code or the Personal Data File Act if he disclosed the identities of the users sought by the plaintiff. *Id.* at 3-4. Notably, the District Court left open the possibility that electronic mail sent privately from computer to computer, rather than posted on a public Internet forum, might be protected under Finnish law.

153. *Id.* at 2 (citing §§ 20, 23, 24, 25, 32, 37 of Chapter 17 of the Finnish Code

however, was based solely on the fact that electronic mail was not specifically included in the Finnish personal privacy statute, rather than any lack of sympathy to Helsingius' cause.[154]

As of this writing, Helsingius plans to appeal the ruling,[155] and at least one former Finnish appellate judge has expressed the opinion that the constitutional protection of privacy in Finland applies to e-mail communications.[156] In addition, the Finnish legislature has indicated that it will reform the personal privacy laws in the spring of 1997 to provide for the protection of electronic communications.[157] Thus, the window of opportunity for law enforcement agencies to obtain the identities of individuals who transmit messages through Finnish anonymous remailers is likely to be a narrow one.

In the meantime, however, Helsingius closed anon.penet.fi, citing a need for clarification of the rights of Internet users.[158] In the absence of a clearly defined regime

---

of Court Operations and § 27(1) of the Pretrial Investigation Law).

154. *Id.* at 4 (stating that "[w]hen the law has not now expressly regulated the circumstances which are in question, the interpretation cannot lead from this that [Finnish authorities] would have no right to get from Helsingius the [identities] of the senders"); *see also* Interview with Peter H. Lewis, Staff Reporter, N.Y. TIMES (Sept. 10, 1996).

155. Letter from Johan Helsingius to Jonathan I. Edelstein (Sept. 15, 1996, at 2) [hereinafter "Helsingius Letter"] (on file with author).

156. Suviranta, *supra* note 129, at 59. Suviranta is a retired President of the Supreme Administrative Court of Finland. *Id.* at 45, n.d. The Supreme Administrative Court has a parallel jurisdiction to the Supreme Court of Finland and is the court of highest jurisdiction in matters of administrative law. *See* JAAKKO UOTILA, THE FINNISH LEGAL SYSTEM 92-93 (2d ed. 1985). Administrative jurisdiction occupies an important position in Finnish law and has increased in importance in recent decades. *Id.* Administrative law courts in Finland handle a great many cases that would fall within the purview of Article III courts in the United States, and a member of the Supreme Administrative Court is a highly regarded jurist who carries considerable legal authority. *See id.*

157. Interview with Peter H. Lewis, Staff Reporter, N.Y. TIMES (Sept. 10, 1996); *see also* Helsingius Letter, *supra* note 155, at 2 (stating that Helsingius expects to see changes in Finnish law to accommodate the Internet, although these might be separate from the telecommunications regulations).

158. Lewis, *supra* note 36, at D2.

for disclosure of evidence in cyberspace, the anon.penet.fi affair has proved destructive both to Finnish civil society and to the Internet community.[159]

B. *Transnational Law Enforcement in Cyberspace*

The anon.penet.fi affair illustrates the difficulties faced by law enforcement agencies in combating electronic crime. Many, if not most, criminal acts committed over the Internet are international in scope, as evidenced by the high percentage of anon.penet.fi accounts held by American users.[160] If the Communications Decency Act of 1995,[161] or some similar measure, eventually passes constitutional muster in the United States, it is possible that many more Americans will choose to route potentially illegal messages through anonymous remailers in foreign countries. In countries such as

159. Another instructive incident involving the Church of Scientology occurred recently in the Netherlands. On September 5, 1995, the Religious Technology Center and its Dutch attorneys, the law firm of Nauta-Dutilh, prevailed upon the Dutch police to raid the offices of XS4ALL, an anonymous remailer service over which copyright-protected Scientology material was allegedly being sent. *Police and Members of Scientology Church Enter Offices of XS4ALL*, M2 PRESSWIRE, Sept. 6, 1995 [hereinafter *XS4ALL*]. The material at issue was included in a document called the F.A.C.T.NET Kit, which was published on the World Wide Web homepage of a user whose Internet address was fonss@xs4all.nl. *Id.* The Religious Technology Center filed for seizure of the assets of XS4ALL, following which the Dutch police recorded the serial numbers of XS4ALL's computers in accordance with standard Dutch procedure. *Id.*; *see also* Religious Tech. Ctr. v. F.A.C.T.NET Inc., 907 F. Supp. 1468 (D. Colo. 1995). The operation of the hacktic.nl Internet access service, which operated XS4ALL, has continued undisturbed, but hactic has shut down the XS4ALL remailer under pressure from the Church of Scientology. Lewis, *supra* note 36, at D2. In this instance as well, it is clear that the lack of clear parameters under which the anonymity of Internet users can be breached can result in the closing of beneficial services under pressure from organizations who use strong-arm tactics in their efforts to enforce the law. *XS4ALL*, *supra*; *see also supra* notes 134-58 and accompanying text (describing the Helsingius affair). The regulation of anonymous remailers would be better left to a well-defined international legal regime with clear procedures for obtaining the identities of individual users without imposing liability upon the operators of remailer services. *See* Turner, *supra* note 40, at 11.

160. *See* Lavin, *supra* note 32, at 1.

161. Pub. L. No. 104-104, 110 Stat. 133, § 502 (amending 47 U.S.C. § 223 (1994)).

Finland which have strong personal privacy laws, foreign courts' cooperation in determining the source of anonymous messages will not be easy to obtain. If, as seems likely, Finland's telecommunications law is reformed next year to protect the privacy of Internet communications,[162] the Finnish police and courts will be highly reluctant in light of the lessons learned from the Erlich incident to pierce the anonymity of anon.penet.fi's users.

Traffickers in pornography or stolen data can eliminate even more of the risk that their identity will be discovered by routing their merchandise through a series of remailers in several different countries.[163] A pornographic image might thus be encoded in a country where pornography is legal, and routed through a remailer in another nation with stronger privacy statutes to further ensure that the trafficker's identity will not be revealed.[164] If the image passes through several remailers, where merely one of these remailers is located in a nation with strong computer secrecy laws, the electronic trail of evidence will be broken.[165]

In the future, an even more disturbing possibility exists. At present, the majority of anonymous remailers are operated by civil libertarians who see themselves as protectors of free speech.[166] By and large, however, these remailer operators are opposed to their services being used in the commission of crimes, and often attempt to police their remailers.[167]

---

162. Interview with Peter H. Lewis, Staff Reporter, N.Y. TIMES (Sept. 10, 1996); *see also* Helsingius Letter, *supra* note 155, at 2.

163. Froomkin, *Anonymity and Its Enmities*, *supra* note 39, at par. 15.

164. *See id.*

165. Froomkin, *supra* note 34, at 400 ("If even one nation with extensive Internet connections chooses not to regulate the provision of anonymizing technology, the effect is to make anonymous communication possible by all persons connected to the Internet . . . .").

166. Lewis, *supra* note 77, at 10.

167. *See* Detweiler, *supra* note 57, § 4.1 (quoting a Usenet post by Helsingius in which he warns users that "anybody posting copyrighted material will be blocked from the server."). Detweiler also includes a guide to ethical operation of anonymous remailers in section 1.2 of his FAQ, suggesting that operators

Helsingius, for example, did not allow the transmission of photographs over anon.penet.fi, and sets a limit on message sizes sufficiently low to further ensure that no pornographic pictures are forwarded.[168] Information on how to report abuse of anonymous accounts is appended to every message transmitted via anon.penet.fi,[169] and Helsingius claims to have banned several hundred users for illegal activities or harassment.[170]

C. *The Specter of "Offshore Databases"*

The next logical step for electronic criminals, therefore, is to establish their own anonymous remailers for the sole purpose of conducting illegal activities.[171] Anonymous remailers are easy to set up: Kleinpaste's original universal remailer matured from concept to completion in a single afternoon.[172] The operation of an anonymous remailer has been described as "trivial[ly] easy" by Helsingius,[173] and is inexpensive by organized crime's standards: Helsingius spent approximately $500 to $700 monthly to maintain and operate his

---

"formulate a plan for problematic ethical situations" and create a published policy outlining the circumstances under which action will be taken against a user and the types of action that will be taken. *Id.* § 1.2. In the same section, Detweiler also warns users of anonymous remailers to "be prepared to forfeit [their] anonymity if [they] abuse the privilege." *Id.*

168. Akst, *supra* note 44, at 1.

169. A signature file automatically appended to every message that passed through Helsingius' remailer instructed that inappropriate use was to be reported to help@anon.penet.fi. *See supra* note 63 and accompanying text (discussing signature files).

170. Lavin, *supra* note 32, at 1.

171. Even Vince Cate, the proprietor of Offshore Information Services, has expressed "concern" that his service is being used for illegal ends and indicated willingness to investigate criminal uses of his Internet access server. *Businesses Promote Fraud Tools*, *supra* note 1, at D2. It is therefore logical that on-line criminals seeking maximum freedom of action would establish their own anonymizing devices in order to avoid contending with concerned system administrators who might investigate their activities or voluntarily cooperate with law enforcement authorities.

172. *See* Branscomb, *supra* note 26, at 1659.

173. Lavin, *supra* note 32, at 1. Helsingius adds that "any competent programmer could [set up an anonymous remailer] in a couple of days." *Id.*

service.[174]

The establishment of a dedicated anonymous remailer is thus well within the reach of traffickers in illegal information. All that is necessary is a compliant nation, willing to enact the necessary computer privacy laws.[175] There is clear historical precedent for this in the rise of "offshore banks" in Third World countries seeking to gain foreign exchange by providing a safe haven for money launderers.[176] If an impoverished nation can be persuaded in similar fashion to enact an airtight computer secrecy law, the door will be opened to the creation of "offshore databases" operated by local contacts for the benefit of organized crime.

D. *The Example of Offshore Banking*

The problem of international law enforcement in cyberspace, as previously stated, is similar to the growing problem posed by offshore banking.[177] Both problems are, at heart, technology-based; the rise of offshore banking was facilitated by the development of technologies that made it possible to complete "cross-border transactions . . . in a matter of seconds."[178] Both problems are international in scope, and have posed unprecedented problems for international law enforcement.[179] The problem of offshore banking is also

174. *Id.* Helsingius established his anonymous remailer on a computer equipped with an Intel 386 chip, which is two generations behind the current standard of personal computer design. Stark, *supra* note 130, at 104. Logically, it would be even easier to establish and operate an anonymous remailer service on a state-of-the-art personal computer.

175. *See* Akst, *supra* note 44, at D1.

176. In 1992, for example, the Cayman Islands, with a population of 13,000, contained 548 banking institutions with a total of $400 billion in assets, making this small Caribbean nation second only to Switzerland as a world banking center. *Where the Money Washes Us: Colony's Wealth Stems from the Rule that Money Flows to the Places that Regulate Least*, VANCOUVER SUN, Apr. 16, 1992, at A19.

177. *See* Lavin, *supra* note 43, at 7.

178. Bruce Zagaris & Scott B. MacDonald, *Money Laundering, Financial Fraud and Technology: The Perils of an Instantaneous Economy*, 26 GEO. WASH. J. INT'L L. & ECON. 62, 62 (1st ed. 1992).

179. *Id.* at 72-73. Zagaris and MacDonald note that:

[T]he very same instruments and markets that facilitate international fi-

exacerbated by the lack of binding, uniform laws in all countries with international banks.[180]

The rise of offshore banking occurred commensurately with the rise of international drug trafficking, and provided a convenient method for drug traffickers to safeguard and conceal the source of their profits.[181] Consequently, during the mid-1980s, the growing efforts by national governments to deal with the problem of drug trafficking led to the creation of an international legal regime to facilitate the control of offshore banks.[182] This took the form of international conventions,[183] multilateral agreements,[184] and bilateral treaties

---

> nance and make countries interdependent also represent potential threats to the international financial system. In particular, introducing increasingly new technology into the marketplace, and the resultant global financial integration, means that international borders represent less and less of an obstacle for both licit and illicit activities. Economist Richard O'Brien has called this the "end of geography," which he describes as "a state of economic development where . . . regulators no longer hold full sway over their regulatory territory; that is, rules no longer apply solely to specific geographical frameworks . . . ."

Id. (quoting RICHARD O'BRIEN, GLOBAL FINANCIAL INTEGRATION: THE END OF GEOGRAPHY 1 (1992)).

180. Thomas F. McInerney III, *Towards the Next Phase in International Banking Regulation*, 7 DE PAUL BUS. L.J. 143, 143-44 (1994).

181. Zagaris & MacDonald, *supra* note 177, at 63-64.

182. *Id.* A primary focus of anti-drug efforts since the 1980s has been money laundering, "based on the premise that attacking the profits of such activities is the best strategy against large, multinational criminal organizations." *Id.*

183. *See, e.g.*, Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, 28 I.L.M. 493 (1989) ("UN Narcotics Convention") at art. 3(1)(b), 3(1)(c)(i) (requiring signatory nations to criminalize money laundering). The Convention also set out specific enforcement procedures. *Id.* at art. 7. Sections 8 through 19 of Article 7 of the UN Narcotics Convention provide a standard format by which nations not bound by a functioning mutual legal assistance treaty may seek legal assistance in enforcing drug laws and investigating narcotics offenses. In general, Article 7 provides for a narrower scope of cooperation than is usual in the terms of a bilateral legal assistance treaty. *See id.* at art. 7(8)-(19).

184. *See, e.g.*, Council of Europe, Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime, 30 I.L.M. 148 (1991); Model Regulations Concerning Laundering Offenses Connected to Illicit Drug Trafficking and Related Offenses, OEA/ser. L./XIV.2/CICAD/INF58/92 (May 23, 1992) (promulgated by CICAD, an anti-drug-abuse organization within the Organization of American States).

between national governments.[185]

These agreements, as well as purely national laws, have sought to enforce a number of measures designed to make it easier to trace illicit transactions. The task of law enforcement was complicated by the long-standing tradition of secrecy in the financial world, and the recognition that banking secrecy has legitimate uses—for example, a corporation might wish to hide a financial transaction from a competitor in order not to lose a business advantage. Thus, the regulation of offshore banking had to balance a legitimate need for financial privacy with the necessity of enforcing the law in an "instantaneous economy."[186]

Among the measures taken to accomplish this have been the increased use of reporting regulations to establish an audit trail for sophisticated transactions,[187] "know your customer" requirements which obligate financial institutions to make inquiries and maintain files as to the identities of account holders,[188] mandatory reporting of complex, unusual and large transactions,[189] and increased supervision of banks to insure that they police themselves for illicit financial transactions.[190] These regulations, while preserving banking secrecy for legitimate users, have the effect of creating a system of vigilance and record-keeping that makes it easier to spot illicit transactions and trace them once they are identified.[191]

---

185. *See infra* notes 191-207 and accompanying text (discussing MLATs and the U.S.-Venezuela banking regulation agreement).

186. Zagaris and MacDonald use the term "instantaneous economy" to describe an environment in which financial transactions are not limited by time. *See id.* at 62.

187. Zagaris & MacDonald, *supra* note 178, at 82-83.

188. *Id.* at 85.

189. *Id.* at 85-86 (citing Financial Action Task Force ("FATF") and CICAD regulations). FATF is a creation of the Group of Seven Leading Economic Countries (G-7). *Id.* at 64.

190. *Id.* at 88.

191. *See generally id.* at part I (discussing emerging financial technologies and their legitimate and illegitimate uses).

A landmark in law enforcement cooperation in the area of offshore banking was the bilateral agreement entered into by the United States and Venezuela in 1990.[192] This was the first agreement between two nations to exchange currency transaction information, recorded by financial institutions in each country, for use in law enforcement.[193] The agreement contained specific reporting requirements and outlined a formal procedure for making requests.[194] Requests for assistance could be denied only if deemed likely to prejudice the security, public policy or essential interests of the requested party.[195]

Since then, the United States has entered into agreements with other countries requiring a minimal level of regulatory supervision and information sharing, including customer and transaction reporting requirements.[196] The focus of offshore banking regulation has been on reliable record-keeping and on measures which would allow law enforcement agencies to pierce banking secrecy under circumstances where a violation of the law is suspected.[197]

One of the key methods by which international enforcement of money laundering regulations has been enhanced is the use of mutual legal assistance treaties, or MLATs.[198] An MLAT is a bilateral treaty which creates binding obligations between the treaty partners to assist each other in criminal investigations.[199] An MLAT combines enforcement and co-

192. Agreement Regarding Cooperation in the Prevention and Control of Money Laundering Arising from Illicit Trafficking in Narcotic Drugs and Psychotropic Substances, Nov. 5, 1990, U.S.-Venez., Hein's No. KAV 2802, 30 I.L.M. 250 (entered into force Jan. 1, 1991).

193. Zagaris & MacDonald, *supra* note 178, at 94.

194. *Id.* at 95.

195. *Id.* The requested party may also postpone granting a request if it will interfere with an ongoing investigation, prosecution or other administrative proceeding taking place in that country. *Id.*

196. *See id.* at 93.

197. *See id.*

198. *See generally* Knapp, *supra* note 46.

199. *Id.* at 405. Most MLATs contain a standard list of forms of assistance

operation in criminal matters by first identifying a specific area or areas where the signatory nations have agreed to cooperate, and then creating legal mechanisms to facilitate the transfer of information regarding these areas.[200] In addition, MLATs can allow foreign intrusion into areas that are traditionally the preserve of domestic courts and legislatures.[201] For instance, the MLAT between the United States and Switzerland, designed to combat bank frauds, provides that the terms of treaty take precedence over any inconsistent provisions of the law of the contracting states.[202]

MLATs are a relatively recent addition to international legal procedure,[203] and represent a considerable advance

---

available to requesting parties, including:

(a) locating or identifying persons or items;
(b) serving documents;
(c) taking the testimony or statements of persons;
(d) transferring persons in custody for testimony or other purposes;
(e) providing documents, records and articles of evidence;
(f) executing requests for searches and seizures;
(g) immobilizing assets;
(h) assisting in proceedings related to forfeiture and restitution; and
(i) any other assistance consistent with the objects of this Treaty mutually acceptable to the Central Authorities of the Contracting Parties.

Treaty with Austria on Mutual Legal Assistance in Criminal Matters, S. Treaty Doc. No. 104-21, art. 1.2 (1995) ("Austrian-American MLAT").

200. *See* Vassalo, *supra* note 118, at 188.

201. *See id.*

202. *Id.* (citing Treaty of Mutual Legal Assistance in Criminal Matters, May 25, 1973, U.S.-Switz., art.9, 27 U.S.T. 2019, 2035 ("Swiss-American MLAT")).

203. The Swiss-American MLAT, which entered into force officially in 1977, was the first major MLAT to be entered into by the United States. Vassalo, *supra* note 119, at 189. As of 1994, the United States had functioning MLATs with 17 foreign jurisdictions. These are Jamaica, Uruguay, Spain, Argentina, Bahamas, Mexico, Canada, Switzerland, Belgium, the United Kingdom, Italy, Colombia, Thailand, Turkey, the Netherlands, and Morocco. McInerney, *supra* note 179, at 148 n.27. The MLAT between the United States and the United Kingdom was expanded to include the Cayman Islands, a British colony, in 1986. Treaty Concerning the Cayman Islands and Mutual Legal Assistance in Criminal Matters, 26 I.L.M. 536 (1987) ("Cayman Islands MLAT"). The Cayman Islands MLAT was further extended to include Anguilla, the British Virgin Islands, and the Turks and Caicos Islands in 1990 and Montserrat in 1991. *See* 30 I.L.M. 250 (1991); 30 I.L.M. 1147 (1991) (describing agreements to expand the Cayman Islands MLAT, effected by exchange of notes between the United States and the United Kingdom). Most recently, the United States concluded an MLAT with the Russian

over previous international evidence-gathering procedures[204] in that they allow requests for information to be processed by central authorities established by the signatory nations rather than being sent through diplomatic channels.[205] In the specific areas delineated in an MLAT as being subject to cooperation,[206] a great many procedural barriers which exist under the traditional regime of letters rogatory are eliminated.[207]

Multilateral conventions such as the UN Narcotics Convention[208] may also function as means of obtaining legal assistance in money laundering investigations.[209] Although international conventions are not directly enforceable in the member states of the United Nations,[210] signatories to the Narcotics Convention are required to adopt legislation which will aid in identifying and freezing assets which are

---

Federation, which entered into force on Feb. 5, 1996. *See* Agreement Between the United States and Russia on Cooperation in Criminal Law Matters, State Dept. No. 96-38, KAV No. 4518 (1996) ("Russian-American MLAT"). A proposed MLAT with Austria received its first reading in the Senate on Sept. 6, 1995. *See* Austrian-American MLAT, *supra* note 198, Letter of Transmittal.

204. The traditional method of requesting evidence from a foreign jurisdiction is through "letters rogatory," which are requests issued by the court system of the requesting nation and delivered through diplomatic channels to the courts of the foreign jurisdiction. Vassalo, *supra* note 118, at 188. This procedure was time-consuming and often costly due to the precise drafting necessary to insure that the letter would comply with the procedures of the foreign jurisdiction and be considered by its courts. *Id.*

205. *Id.*

206. The Russian-American MLAT contains an annex delineating specific criminal offenses in connection with which cooperation will be rendered, including organized crime activity, money laundering, trafficking in nuclear weapons, drug trafficking, fraud, violent crimes against individuals, and sexual offenses against children. *See* Annex to Russian-American MLAT, *supra* note 202; Russian-American MLAT, art. 2.1. The Cayman Islands MLAT defines the area of cooperation more broadly to include, in addition to the offenses enumerated in the treaty, "any conduct punishable by more than one year's imprisonment under the laws of both the Requesting and Requested Parties." Cayman Islands MLAT, *supra* note 202, art. 19.3(a).

207. *Id.*

208. Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, 28 I.L.M. 493 (1989).

209. McInerney, *supra* note 180, at 165.

210. *Id.*

the proceeds of drug activities,[211] and are forbidden from denying legal assistance to other signatory nations because of local banking secrecy laws.[212]

The bilateral and multilateral treaty relationships developed to control offshore banking provide a model approach to the problem of international law enforcement in an atmosphere where cross-border transactions and secrecy are made easy by technology and conflicting national law. A similar set of solutions may be effective in protecting liberty but controlling secrecy in the analogous environment of cyberspace.[213]

The analogy between international banking regulation and the Internet is further demonstrated by the use of emerging technologies and institutions by law enforcement agencies to monitor international financial activities. By means of computerized payment systems such as the Society for Worldwide Interbank Telecommunications ("SWIFT") and the Clearing House for International Payments Systems ("CHIPS"), agencies can create an electronic trail through which they may monitor transactions, thus turning emerging banking technologies to the service of law enforcement as well as crime.[214] Law enforcement agencies may also put he growing technology of the Internet to use; for example, the United States and British governments have already debated the use of the "Clipper chip," which would allow law enforcement agencies, pursuant to a court order, to decode and analyze encrypted data.[215]

---

211. UN Narcotics Convention, *supra* note 183, art. 5.

212. *Id*. at art. 7(5).

213. *See infra* notes 247-303 (discussing law enforcement measures to control Internet anonymity).

214. McInerney, *supra* note 180, at 147 ("[CHIPS and SWIFT] may provide an additional fulcrum for domestic regulators to apply when seeking to uncover illegal and destabilizing transfers of funds . . . . Moreover, the fact that these systems are located in the United States creates some leverage over other countries seeking to use the system").

215. For a more thorough analysis of the legal issues involved with the

In addition, the banking industry engages in a great deal of self-regulation through organizations and supervisory banks.[216] At least one authority has suggested that the Internet be constituted, in a similar manner, as an independent and self-governing jurisdiction with its own courts, laws, and law enforcement mechanisms.[217] Such a jurisdiction would have its own legislative bodies which would be empowered to define and enforce community standards on the Internet.[218] This would, in many ways, be similar to the pri-

---

Clipper chip and the system of key escrow (a program under which decoding information for all marketed encryption devices is placed in an "escrow account" to which law enforcement agents may have access under certain circumstances), *see* Froomkin, *supra* note 39; Henry R. King, *Big Brother, The Holding Company: A Review of Key Escrow Encryption Technology*, 21 RUTGERS COMPUTER & TECH. L.J. 224 (1995); Christopher E. Torkelson, *The Clipper Chip: How Key Escrow Threatens to Undermine the Fourth Amendment*, 25 SETON HALL L. REV. 1142 (1995). *See also* Robert Uhlig, *Ministers Seek Net Codebuster: Technology Minister Ian Taylor Backs a System That Lets the State Read Our Private E-Mail Reports*, DAILY TELEGRAPH (LONDON), Apr. 23, 1996, at 2 (discussing the issues surrounding the implementation of the Clipper chip in the UK).

216. *See* Zagaris & MacDonald, *supra* note 178, at 88. Law enforcement authorities often work through regulatory and supervisory agencies internal to the banking industry and encourage such agencies to share information with each other and with investigators. *Id.*

217. Branscomb, *supra* note 26, at 1666-69. Earlier in her article, Branscomb offers several examples of Internet communities enforcing community standards through mail-bombing, massive censure or expulsion from a particular Internet service. *Id.* at 1656-63. At least one of these incidents, involving a participant in a virtual community who was ousted for committing a "virtual rape" on a female character, turned into a formal debate over community standards and ended in a referendum on expulsion among registered members of the community. *Id.*

218. *See id.*; *see also* David G. Post, *Virtual Magistrates, Virtual Law*, AM. LAW., July/Aug. 1996, at 104, describing Tierney v. Email America, VM Docket # 96-0001 (May 20, 1996) (decision available at http://vmag.law.vill.edu:8080 on the World Wide Web). *Tierney* was the first case to be decided by the "Virtual Magistrate." *Id.* The Virtual Magistrate is an on-line arbitration system established by the Cyberspace Law Institute, the American Arbitration Association, Villanova Law School, and the National Center for Automated Information Research. *Id.* A complete description of the Virtual Magistrate project, including a concept paper, rules, and procedures for submitting a complaint, can be found at http://vmag.law.vill.edu:8080. The Virtual Magistrate is an on-line arbitration project designed to resolve disputes involving users of on-line systems, those who claim to be harmed by wrongful messages, and complaints or demands for remedies directed at system operators. *Id.*

Tierney, which was decided by N.M. Norton Jr. of Wright, Lindsey & Jen-

vate securities and banking regulatory organizations which police their industries against illicit financial transactions.[219]

III. ANONYMITY AND PUBLIC ORDER: A PROPER BALANCE IS NECESSARY

Anonymous remailers will be a part of the Internet for the foreseeable future. With the constitutional protection enjoyed by anonymity in many Western countries, and the professed desire of certain other nations to act as "data havens," it is unlikely that private data transmission over the Internet will be universally banned or even seriously curtailed.[220] Nonetheless, just as with the similar problem of offshore banking, common-sense measures can be agreed upon between nations that would minimize the potential for violation of the law through anonymous transmission of data.[221] This section will examine several proposals which may be taken to ease the task of law enforcement on the Internet. These include a technology-based approach similar to the "key escrow" encryption technology which has been debated by American and European governments, a self-governing Internet jurisdiction with the power to resolve disputes in cyberspace, an international convention on Internet crime, and the use of MLATs to assist in gathering evidence and prosecuting international cybernetic crime.

A. *Practical Issues Must Be Considered in Control of Anonymity*

It is clear that the combination of readily obtained anonymity and easy transmission of information across national borders creates an environment hostile to law enforcement

---

Jennings (Little Rock), involved a complaint about deceptive advertising sent in bulk to subscribers of America Online. *Tierney*, VM Docket # 96-0001 (May 20, 1996). Norton ruled that America Online should delete the offending advertisement. *Id.*

219. *See generally* Zagaris & MacDonald, *supra* note 178, at part III.

220. *See* Strassmann & Marlow, *supra* note 97.

221. *See supra* notes 187-216 and accompanying text (discussing measures that have been taken to combat the dangers of offshore banking).

and extremely friendly to crime.[222] Any attempt by national or international agencies to control the traffic of information through anonymous remailers, however, must walk a fine line between privacy and public order. Anonymity enjoys a limited degree of constitutional protection in the United States;[223] in addition, information privacy is vital in a medium as open to public access as the Internet.[224] There are a large number of legitimate reasons why Internet users might seek to protect their anonymity.[225] A complete ban on anonymous remailers, as some authorities have advocated[226] and as the State of Pennsylvania has recently enacted,[227] would have a drastic chilling effect on legitimate political, therapeutic, and recreational uses of the Internet.[228] Some

222. *See supra* notes 81-120 and accompanying text (discussing illegitimate uses of anonymous remailers).

223. *See, e.g,* McIntyre v. Ohio Elections Comm'n, 115 S. Ct. 1511 (1995) (permitting the distribution of anonymous political leaflets). *McIntyre* is currently regarded as the leading case in this area. *See also* Whalen v. Roe, 429 U.S. 589 (1977) (establishing a balancing test for determination of the right to informational privacy, setting public interest against the individual's interest in protecting himself from disclosure); Talley v. California, 362 U.S. 60 (1960) (overturning a municipal ban on distribution of anonymous pamphlets); Gilbert v. Allied Chem. Corp., 411 F. Supp. 505, 508 (E.D. Va. 1976) (holding that journalists possess "a privilege from revealing their confidential news sources in civil proceedings that may be abrogated only in rare and compelling circumstances."). For an excellent discussion of the constitutional right to anonymity on the Internet, especially in the wake of the *McIntyre* decision, see generally Tien, *supra* note 39.

224. *See supra* notes 70-80 and accompanying text (discussing the benefits that flow from privacy on the Internet).

225. *See supra* notes 71-80 and accompanying text (discussing beneficial uses to which anonymous remailers have been put).

226. *See* Hardy, *supra* note 30, at 1050-51; *see also supra* note 139 and accompanying text (stating that FBI Director Louis Freeh favors a ban on anonymous remailers). In addition, at least one commentator has noted that if anonymous remailers are banned in the United States, "they will undoubtedly proliferate overseas." Chapman, *supra* note 139 at 10.

227. PA. SESS. LAW ACT 1995-8 (amending 18 PA. C.J.A. 910 (a)(1)(ii)) makes it a crime to create, possess, or use a device which can be used to "conceal or assist another to conceal . . . the existence of place of origin or of destination of any telecommunication." *See also* GA. CODE ANN. § 16-9-93.1 (criminalizing the use of "misleading" identities on the Internet).

228. Professor Tien argues, in his cogent defense of the constitutional right to anonymity on the Internet, that "online anonymity is also used innocuously.

features of Internet anonymity, however, such as anonymous transfer of digital cash, might be prohibited with little damage to the legitimate uses of Internet anonymity.[229]

Any measures taken to lower the hurdles faced by law enforcement in piercing the secrecy of anonymous remailers must thus preserve intact all the legitimate uses of anonymity.[230] First, any remedies available to law enforcement should preserve the free flow of political and religious discussion over the Internet.[231] This argues in favor of absolute protection of anonymity in messages which express political or religious opinions. The confidentiality of persons participating in on-line self-help or therapy groups should also be preserved.[232]

Another issue is raised by requirements, such as those contained in Finnish law, that a crime must be committed in the anonymous remailer's host country, or that an offense must be committed which would constitute a crime in the host country, before a search warrant or disclosure order can be issued.[233] Care must be taken when confronting this re-

---

There is something fundamentally misguided about basing any analysis of anonymity on the anonymous threat or libelous message—extremes in the universe of social interaction." Tien, *supra* note 39, at 120 (citing numerous beneficial uses of anonymity on the Internet). I agree with Professor Tien insofar as the benefits of anonymous communication on the Internet should be preserved and that an outright ban on anonymizing devices would be misguided. From a law enforcement perspective, any analysis of the proper regime for regulating anonymity on the Internet must necessarily take into account those individuals who abuse the ability to communicate anonymously and suggest means by which they may be brought under control.

229. *See* Froomkin, *Anonymity and Its Enmities*, *supra* note 39, at par. 69 (noting that, as "money equals speech in some political contexts, but . . . money can nonetheless be regulated in that context, it seems likely that anonymous money could be regulated more generally").

230. *See supra* notes 70-80 and accompanying text (discussing the legitimate uses of anonymity on the Internet).

231. *See supra* note 71 and accompanying text (discussing use of anonymous remailers by political dissidents).

232. *See supra* note 72 and accompanying text (discussing the benefits that anonymous remailers provide to on-line self-help and therapy groups).

233. *See supra* note 145 and accompanying text (discussing Finnish law regarding search warrants).

quirement to avoid assigning criminal responsibility to operators of anonymous remailers which carry illegal traffic. Placing criminal responsibility on providers of electronic anonymity, such as that imposed on Internet access providers by the recent Communications Decency Act,[234] would have the same practical effect as an outright ban on anonymous remailers. It would be impossible for a the operator of a remailer such as anon.penet.fi, which had a daily traffic in excess of 8,000 messages,[235] to completely prevent illegal materials from being routed through the service.[236] Requiring operators of anonymous remailers to take certain commonsense safeguards, such as the regulations imposed by anon.penet.fi, might not be out of place.[237] In contrast, a legal regime which places vicarious criminal liability on operators whose services are abused by criminals would make operation of anonymous remailers impractical, if not impossible. Rather than imposing criminal liability on the operators of anonymous remailers, international evidence gathering should be made available even in the absence of a crime committed in the host country.[238]

Establishment of mandatory safeguards should also be a

234. Communications Decency Act of 1996, Pub. L. No. 104-104, 110 Stat. 133, § 502(e)(3).

235. *See supra* note 123 and accompanying text (discussing anon.penet.fi's traffic volume).

236. *See* Shea v. Reno, 930 F. Supp. 916, 950 (S.D.N.Y. 1996) (concluding that "current technology provides no feasible means for most content providers to avail themselves" of the two affirmative defenses provided in the Communications Decency Act for access services which carry prohibited communications); *see also* 47 U.S.C.A. § 223(e)(5) (West Supp. 1996) (providing that Internet access providers may assert, as a defense to a prosecution under the CDA, they have "taken . . . reasonable, effective, and appropriate actions . . . to restrict or prevent access by minors" to communications prohibited by the act, or that they have "restricted access to such communication by requiring use of a verified credit card, debit account, adult access code, or adult personal identification number.")

237. *See supra* notes 168-69 and accompanying text (discussing regulations imposed by anon.penet.fi.).

238. *See supra* notes 192-95 and accompanying text (discussing the information-sharing requirements of the U.S.-Venezuelan anti-money-laundering agreement).

basis for limiting the civil liability of Internet access providers for materials transmitted over their services. Liability could ideally be limited to failure to comply with the safeguards set forth in the international legal solution that is taken. In light of the conclusion in *Religious Technology Center v. Netcom*,[239] in which the court held that an Internet access provider is not a common carrier which is absolutely immune from liability under 17 U.S.C. § 111(a)(3),[240] care should be taken to limit the circumstances under which operators of remailers can be held civilly liable for tortious or criminal materials transmitted over their services.

Imposition of broadly based civil liability on operators of anonymous remailers would have a chilling effect almost as great as if criminal liability were imposed.[241] Service providers would be tempted to censor the messages they carry in order to avoid liability. Even worse, some might be forced to close due to damages imposed for failure to police their networks.[242] Because the *Netcom* court's holding that Internet access providers could be held liable for their message traffic was based largely upon the determination that the message traffic was under the access provider's indirect control,[243] it would only be fair to limit the access provider's li-

239. 907 F. Supp. 1361 (N.D. Cal. 1995).

240. *Id*. at 1369 n.12 (citing 17 U.S.C. § 111(a)(3) (1994)).

241. *See supra* notes 158-59 (concerning the closure of the anon.penet.fi and XS4ALL remailers due to pressure from the Church of Scientology's civil lawsuits).

242. *See Netcom*, 907 F. Supp. at 1370 (holding that Internet access providers may be held liable for tortious messages posted on the networks they manage). As so many Internet access providers operate in the United States, American law is disproportionately influential on the environment of the Internet. In addition, other nations such as Germany are considering, or have already implemented, legislation or regulations holding Internet access providers liable for messages transmitted over their networks. *See Germany Targets Compuserve*, *supra* note 40.

243. *Netcom*, 907 F. Supp. at 1369 n.12. The *Netcom* court gave great weight to the doctrine that a common carrier "must not have any direct or indirect control over the content or selection of the primary transmission." *Id.*; *see also* Stratton Oakmont Inc. v. Prodigy Inc., 23 Media L. Rep. 1794 (N.Y. Sup. Ct., Nassau Co. 1995) ("[T]he critical issue to be determined by this Court is whether the foregoing evidence establishes . . . that PRODIGY exercised sufficient editorial

ability to failure to comply with the controls mandated by law. It is important, in any international legal solution to the problem of law enforcement in cyberspace, to insure that an anonymous remailer which complies with the measures mandated to ease the task of law enforcement authorities should not be infringed further in its ability to transmit anonymous messages for legitimate purposes.[244]

Finally, any international solution to the law enforcement problems posed by anonymity must avoid inhibiting the growth of information technology.[245] A legal regime, whether created by statute or treaty, that bans technologies or freezes technology at its current level would prevent information technology from achieving its full potential.[246]

B. *Law Enforcement Solutions on the Internet are Possible*

For better or for worse, the Internet has become one of the primary means of transmitting data in the modern

---

control over its computer bulletin boards to render it a publisher with the same responsibilities as a newspaper."); Cubby Inc. v. Compuserve Inc., 776 F. Supp. 135, 140 (S.D.N.Y. 1991) (noting that "[w]hile CompuServe may decline to carry a given publication altogether, in reality, once it dies decide to carry a publication, it will have little or no editorial control over that publication's contents.")

244. *See supra* notes 158-59 and accompanying text (discussing the unintended consequences of law enforcement efforts regarding anonymous remailers).

245. *See, e.g.*, David Ward, *Sisyphean Circles: The Communications Assistance for Law Enforcement Act*, 22 RUTGERS COMP. & TECH. L.J. 267, 282 (1996) (stating that "[t]he [Communications Assistance for Law Enforcement] Act . . . operates as a disincentive for technological innovation and will likely retard competition. The Act impedes technological innovation by allowing governmental needs to be a determinative factor in the research and development decisions of telecommunications carriers"); *see also* Ted Bunker, *Is It 1984*, LAN TIMES, Aug. 1994 (quoting Roy Neel, President of the United States Telephone Association, as saying that "our nation cannot be held hostage to inexpert analysis of telecommunications technology as we move into the information age").

246. The effect of curtailment of research upon technological innovation, especially in the medical field, has often been commented upon. *See, e.g.*, *Arizona: 4 w/Parkinson Challenge State Fetal Tissue Ban*, ABORTION REP., May 1, 1996 (quoting Planned Parenthood executive director Virginia Yrun as saying that Arizona's ban on fetal tissue research "retard[s] the discovery and application of new lifesaving techniques").

world, and will become more so in the future.[247] With the growth of the Internet, privacy technologies such as anonymous remailers will no doubt also come into wider use, leaving national governments with the difficult task of enforcing the law in an environment of widespread secrecy.[248] Fortunately, the example of offshore banking is available as a guide to developing law enforcement strategies for the Internet.[249]

The problem of anonymous remailers is not strictly analogous to that of offshore banking. For one thing, it is much easier to establish an anonymous remailer than it is to set up a financial institution,[250] and the "paper trail" of an anonymous message is much easier to hide.[251] In addition, the legal regime governing cyberspace communications in most countries is not nearly as well-defined as that governing banking, which has traditionally been one of the most regulated areas of the business world.[252] Thus, any agreements or conventions relating to control of computer crime

---

247. *See supra* notes 51-54 and accompanying text (discussing the growth of the Internet).

248. Strassmann and Marlow argue that, because anonymous remailers cannot be banned outright in the context of a free society:

> The best one can do is to start treating the pathologies inherent in the Internet in the same way as we have learned to deal with infectious epidemics. That calls for constructing new institutions and processes that are analogues to inoculation, immunization, prophylactics, clean water supply, sewers, hygiene, early detection of outbreaks of diseases, quarantine, the offices of health examiners, the Center for Disease Control and the World Health Organization.

Strassmann & Marlow, *supra* note 97. This Note attempts to suggest means by which some or all of these goals can be accomplished without killing the metaphorical patient.

249. *See supra* notes 187-216 and accompanying text (discussing law enforcement measures taken to control offshore banking).

250. *See supra* notes 187-91 and accompanying text (discussing the ease of establishing an anonymous remailer).

251. *See supra* note 109 and accompanying text (discussing means of increasing the difficulty of tracing e-mail messages).

252. *See supra* notes 185-88 and accompanying text (describing a small portion of the regulations that have been imposed on banking transactions). Equivalent regulations have not been enacted with regard to Internet access providers.

would have to define their terms, and the circumstances under which they could be invoked, in even more detail than those governing financial crime.

Nevertheless, the problems posed by offshore banking and by Internet anonymity are remarkably similar. Both are based upon technologies which allow inexpensive, easy and secret transmission of information across international borders,[253] both pose problems in law enforcement because of the privacy haven provided by certain nations,[254] and both have legitimate uses but are widely used illegitimately.[255] Thus, some or all of the solutions which have proven effective in controlling offshore banking might be adapted for use in regulating anonymous communication on the Internet.[256] These include the use of technologies which ease the task of locating and tracing illicit data, increased self-regulation by the Internet itself, an international convention on Internet crime, and MLATs designed to combat trafficking in illegal data.[257]

1. A Technology-Based Approach?

It may be possible to circumvent international law enforcement difficulties by utilizing technologies which facilitate data tracing by police agencies. In a manner similar to the "Clipper chip" or to emerging technologies used to trace

253. *See supra* notes 57-69 and accompanying text (regarding anonymous remailers); notes 178-80 and accompanying text (regarding offshore banks).

254. *See* Akst, *supra* note 44, at D1.

255. *See supra* notes 70-120 and accompanying text (discussing beneficial and criminal uses of anonymous remailers); *supra* notes 178-86 and accompanying text (discussing offshore banking).

256. *See* Froomkin, *supra* note 34, at 447-48. Professor Froomkin argues that:

> Governments have demonstrated that they are capable of acting in concert to seek to control activities such as money laundering which they perceive as a common threat . . . . As yet, there appears to be no equivalent movement to control anonymous remailers, but it is not inconceivable.

Id.

257. *See supra* notes 187-216 and accompanying text (discussing law enforcement measures relating to offshore banking).

financial transactions,[258] the federal government could mandate the inclusion in all new computers of technology which creates a unique and indelible signature on each outgoing message. This would enable the information to be traced to its original source no matter what steps are taken to ensure anonymity en route.[259] Presumably, messages would be traceable only by court order upon a prima facie showing that a criminal act has been committed over the Internet.[260]

This proposal, while attractive in its simplicity, has a number of drawbacks. For example, the privacy of individuals or services whose computers carried an encoded message en route to its destination might be compromised.[261] Moreover, any technological solution is vulnerable to being superseded by superior technology. A technology which stamps a mandatory data signature on electronic mes-

---

258. *See supra* note 215 and accompanying text (discussing the "Clipper chip").

259. *See supra* notes 64-66 and accompanying text (discussing the customized anonymity provided by sophisticated remailers).

260. This requirement has a parallel in the Federal wiretapping statute. *See* 18 U.S.C. § 2510-2521. 18 U.S.C. § 2518(3) provides that the interception of wire, oral, or electronic communications may be authorized if:

> (a) there is probable cause for belief that an individual is committing, has committed, or is about to commit a particular offense . . .
>
> (b) there is probable cause for belief that particular communications concerning that offense will be obtained through such interception;
>
> (c) normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous;
>
> (d) . . . there is probable cause for belief that the facilities from which, or the place where, the wire, oral, or electronic communications are to be intercepted are being used, or are about to be used, in connection with the commission of such offense, or are leased to, listed in the name of, or commonly used by such person.

18 U.S.C. § 2518(3)(a)-(d). This statute could very easily be adapted to allow the investigating judge or magistrate to order the disclosure of an anonymous user's identity under similar circumstances. *See* Long, *supra* note 15, at 1205-06.

261. An electronic message might pass through several computers or networks before reaching its destination. Many of these may be merely carriers or relay stations through which the message passes on the way from source to destination, and have nothing to do with the production, processing or publication of the message.

sages could potentially be defeated by another technology which erases or masks that signature. Short of curtailing entire lines of research in the field of encryption, which would inhibit the growth of information technology and endanger corporate data security,[262] any technological edge gained by law enforcement could not be made to last forever.

A more serious drawback, however, is the possibility that the veil of privacy might be breached by parties other than those authorized to penetrate it. Thus far, computer "hackers" have shown themselves able to break codes thought unbreakable by their creators.[263] A strong possibility exists that an ingenious hacker could devise a way to trace anonymous messages illegally, with possibly catastrophic consequences to the person or persons whose anonymity has been violated.

2. The Option of Self-Government: Is It Viable?

As previously noted, a number of commentators have proposed that the Internet be constituted as a self-governing jurisdiction with its own laws and courts.[264] Although this highly idealistic solution may eventually be possible, it would probably be unworkable at the present time. Aside from the overriding question of where an Internet jurisdiction would derive its power, the Internet is at present not a single community, but thousands of discrete communities with highly varying standards and norms.[265] It is highly unlikely, therefore, that the diverse users of the Internet would be able to agree on a constitution or construct a workable

262. *See supra* notes 245-46 and accompanying text (discussing the effect of excessive regulation on technological advance).

263. *See, e.g.*, Dr. Marcus du Sautoy, *Search for a Code that Breakers Can't Crack: Mind and Matter*, TIMES (LONDON), Dec. 11, 1995 (dealing with the solution of RSA-129, a hitherto secure code based on a 129-digit number arrived at through the multiplication of two prime numbers).

264. *See supra* notes 216-17 and accompanying text (discussing self-regulation).

265. *See generally* Branscomb, *supra* note 26.

workable legislature.[266]

Problems would also arise concerning the remedies available to an independent Internet jurisdiction. As there are no "virtual jails," the remedies available to an Internet court acting on its own resources would be limited to censure or expulsion from the Internet. The latter remedy would be especially ineffective because of the ease of obtaining a new Internet account under a pseudonym from another of the thousands of competing Internet access providers.[267]

An Internet jurisdiction might be workable in certain areas, especially those which involve offenses consisting solely of violation of Internet community standards, or which occur entirely on the Internet.[268] Such a jurisdiction might also

---

266. *See generally* Detweiler, *supra* note 57, providing excerpts from an ongoing and passionately argued Internet debate over standards of behavior and the proper uses of anonymity. The contentious nature of community standards on the Internet is especially apparent in sections 4.5, 6.1 and 7.3. *But see* Branscomb, *supra* note 26, at 1665-70 (describing informal community regulation by Internet users in which a general consensus has developed over standards of "netiquette" or proper on-line behavior). Informal "netiquette" standards have been established by Internet communities consisting of users from a number of cultures and nations. *Id.*; *see also* Hardy, *supra* note 30, at 1019-21 (comparing "netiquette" to the medieval "law merchant," which provided a unified system of laws for merchants from varying countries who met at trade fairs).

267. *See supra* note 3 and accompanying text.

268. Professor Post argues that Internet-based arbitration services might be an ideal forum to adjudicate complaints of violation of the Internet's developing community standards, and that their decisions, available on a worldwide database, might constitute a "common law of cyberspace." Post, *supra* note 216, at 104-05. He additionally predicts that the deliberations of on-line courts might be accompanied by real-time commentary by observers in cyberspace, and that amicus briefs might be submitted by clicking a button at the arbitrator's World Wide Web page. *Id.*

Professor Post has also argued in connection with the Helsingius-Scientology debate that Internet law should take precedence over national law in areas involving dissemination of information, including copyright protection. David G. Post, *New World War: Critics of Scientology*, REASON, Apr. 1996, at 28. He argues that "it is the inhabitants of cyberspace, after all, who are in the best position to determine the varying shapes of a copyright law that can truly take account of the strange features of this new informational landscape." *Id.* Professor Post acknowledges, however, that "the inhabitants of cyberspace, too, must develop

be an adequate forum to resolve disputes concerning on-line copyright infringement.[269] A panel of authorities recently suggested the establishment of on-line arbitration boards empowered to make instant decisions as to whether a publicly posted message violated a copyright.[270] If the board determined that a message was an infringement, it could order a commercial Internet provider to delete the offending message.[271]

Although this tribunal might be effective in curtailing publicly posted infringements, especially if its authority were backed by enabling legislation from a national government, it would still be ineffective in preventing the trafficking of stolen data from computer to computer. Although such a board might be able to make inroads into the stolen data market if it were empowered to delete advertisements offering stolen data for sale, it would be powerless to curtail such traffic entirely because much of it occurs privately and without advertisement.[272]

In addition, although a message in this scenario would be subject to Internet law while traveling in cyberspace, it would still be subject to national law before it is introduced into the Internet and after it is received and downloaded.[273] The creation of an Internet jurisdiction, without further measures, would not solve the problem of tracing an anonymous message which violates national law to its source.

3. An International Convention on Electronic Crime:

---

mechanisms to recognize and respect the legitimate interests of individuals outside their borders." *Id.*

269. Rory J. O'Connor, *Cyberspace Experts Suggest Ways to Make On-Line Copyrights Secure*, AUSTIN AM.-STATESMAN, Oct. 9, 1995, at D8.

270. *Id.*

271. *Id.*

272. *See supra* notes 100-05 and accompanying text (discussing anonymous trafficking in stolen data on the Internet).

273. *See supra* note 40 and accompanying text (discussing attempts by national governments to regulate the Internet).

The Ultimate Solution

Anonymity over the Internet has been compared to offshore banking: useful in the secrecy it provides, but dangerous in the convenience it offers to criminals.[274] It might be useful, therefore, to consider a similar solution: an international convention on Internet law enforcement similar to the treaty recently adopted by the United Nations to combat drug trafficking and money laundering.[275]

An international convention, accompanied by a multilateral treaty,[276] would be well within the accepted bounds of international law[277] and would be a powerful tool to combat Internet crime. An international convention on computer crime would require signatory nations to take certain measures to combat criminal activity on the Internet.[278] These might include, for example, a provision requiring signatory nations to order disclosure of the sources of messages transmitted via anonymous remailers upon a prima facie

274. *See* Lavin, *supra* note 32, at 1.

275. *See supra* note 183 and accompanying text (discussing the UN Narcotics Convention). Mark Turner, a partner at the London law firm Garrett & Co., has recently advocated an international convention on Internet regulation in order to clarify the conflicts of rights created by differences in national law and prevent a drift toward the "highest common denominator" of regulation by Internet access providers in an effort to avoid liability. *See* Turner, *supra* note 40, at 11.

276. The convention, adopted by the United Nations or some other international body, would form the framework for the multilateral treaty. Without a multilateral treaty, a United Nations convention would not be binding on the signatory nations under the doctrine of dualism; that is, that states are not automatically subject to the constraints of international law in the absence of implementing legislation. *See* McInerney, *supra* note 180, at 167-68.

277. *See id.* at 168 n.163 (citing the Vienna Convention on the Law of Treaties, U.N. Doc. A/Conf. 39/27, and Restatement (Third) of the Foreign Relations Law of the United States §§ 102(1)(b), 122(3), in support of international recognition of the right of nations to consent to binding treaties).

278. Arguably, with the rise of "digital cash" and other means of conducting financial transactions over the Internet, it will soon be necessary to expand existing international conventions governing financial offenses into cyberspace. A new convention on electronic crime could take in the offenses covered by prior conventions on money laundering and fraud, and also encompass new offenses unique to cyberspace. *See generally* Froomkin, *Anonymity and Its Enmities*, *supra* note 39, at par. 41-43.

showing that a crime had been committed in the requesting nation.[279] Such an order for disclosure would not be contingent upon a finding that a crime had been committed in the host nation; thus, the requesting nation could investigate crimes under its law without the necessity of criminal responsibility being imposed upon the operator of the anonymous remailer.[280] In fact, a convention might make disclosure available for a strictly defined list of torts such as copyright infringement, allowing the victims of such torts to apply to the courts of their home nations for assistance in determining the identity of the illicit distributors of their property.[281]

Such a convention could also close the loopholes through which child pornography is often transmitted over the Internet by mandating that signatory nations include electronic media in their anti-pornography statutes.[282] Much as the UN Convention on Narcotics Trafficking requires signatory nations to criminalize money laundering,[283] a convention on

279. *See* UN Narcotics Convention, *supra* note 183, at art. 7(10) (setting forth information that must be provided when requesting legal assistance under the terms of the convention).

280. *See supra* note 145 and accompanying text (discussing Finnish law relating to the February 1995 police raid on anon.penet.fi.).

281. No known international law would limit the application of international conventions or MLATs to criminal matters only. *See* Vassalo, *supra* note 118, at 192, n.139. Access by private parties to procedures established under international conventions or MLATs could be limited by a requirement that such parties apply to the courts or to a central law enforcement authority in their country of residence for approval of their requests for information.

282. *See supra* note 109 and accompanying text (noting that certain jurisdictions do not prohibit child pornography carried over electronic media).

283. UN Narcotics Convention, *supra* note 183, art. 3 (1)(b)(ii). It should be noted, however, that each signatory nation to the convention is required to criminalize certain drug and money-laundering-related activities "subject to its constitutional principles and the basic concepts of its legal system." *Id*. at art. 3 (1)(c) This creates a loophole under which a number of signatory nations, such as Israel, have failed to enact anti-money-laundering statutes. *See* Abraham Abramovsky, *Partners Against Crime: Joint Prosecutions of Israeli Organized Crime Figures by U.S. and Israeli Authorities*, 19 FORDHAM INT'L L.J. 1903, 1910 (1996). The negotiators of a convention against computer crime would have to take care, as far as possible, to eliminate such loopholes from the draft treaty, although this

Internet crime could similarly mandate the criminalization of such offenses as data theft, possession of stolen data,[284] and electronic vandalism.[285]

Finally, an international convention on computer crime could regulate the use of anonymous remailers by mandating that signatory nations enact certain regulations limiting the right to anonymity. Such regulations might include common-sense measures such as those already enforced by many remailer operators,[286] including a maximum message size.[287] A strict size limit would inhibit the transmission of pornographic materials or pirated software, while allowing the use of anonymous remailers for legitimate purposes such as political discussion or therapy.[288]

An international convention, if ratified and strengthened

---

may not be entirely possible due to fundamental differences in the criminal justice systems of the various member states of the United Nations.

284. "Stolen" data can be defined to include not only data protected by copyright but also credit card or similar account numbers and confidential corporate or legal material. One model for such a definition might be the definition of "secret scientific material" contained in Section 155.00(6) of the New York State Penal Law. This statute defines "secret scientific material" as property or records which "[are] not, and [are] not intended to be available to anyone other than the persons rightfully in possession thereof" and "accord or may accord such rightful possessors an advantage over competitors or other persons who do not have the knowledge or benefit thereof." N.Y. PENAL LAW § 155.00(6) (McKinney 1996).

285. A multilateral treaty on international crime could be drafted, like most multilateral treaties, by a congress of technical experts from the negotiating countries. *See* McInerney, *supra* note 180, at 167 n. 161. A conference of Internet and legal experts drawn from the courts, corporations, and universities of the member states of the United Nations, could draft a treaty specifically tailored to the needs of law enforcement and Internet users, and define in concrete terms the acts which must be criminalized in order to create a lawful society in cyberspace.

286. *See supra* notes 165-66 and accompanying text (discussing regulations set by Helsingius for anon.penet.fi).

287. Johan Helsingius is of the opinion that codification of a message size limit for anonymous remailers would be "too arbitrary," but would support an international convention which clearly delineates the rights and obligations of Internet users and service providers. Helsingius Letter, *supra* note 155, at 2.

288. *See supra* notes 71-72 and accompanying text (discussing political and therapeutic uses of Internet anonymity).

by bans on sales of encryption technologies to non-signatory nations, would assist in easing law enforcement in cyberspace and managing the right to anonymity in a rational manner while promoting full use of the Internet's resources. Care would have to be taken to include a strict political offense exception in any such convention,[289] insuring that democratic nations could not be forced to disclose the identity of dissidents wanted for criticizing dictatorial governments.[290] Any international convention on cybernetic crime would have to recognize not only the need for law enforcement to trace illegal messages across national boundaries, but also the basic human right of free expression.

4. An Interim Approach: MLATs as a Means of Facilitating International Law Enforcement Cooperation

The creation of an international convention on Internet crime will understandably take time; even more time will pass before enough nations ratify the convention to make its implementation comprehensive.[291] In the meantime, the United States might increase its ability to enforce the law in cyberspace by establishing mutual legal assistance treaties

289. The principle of the political offense exception, which is traditional in the law of extradition, permits a state to refuse an extradition request from another state if the offense charged in the request is of a purely political nature. *See* Louis Rene Beres, *The Legal Meaning of Terrorism for the Military Commander,* 11 CONN. J. INT'L L. 1, 18 n.63 (1995). This principle could be adapted from the law of extradition to provide that disclosure of the identity of an anonymous user could be refused if the offense charged by the nation requesting disclosure was solely political in character.

290. *See supra* note 71 and accompanying text (discussing use of anonymous remailers by political dissidents).

291. The UN Narcotics Convention, for example, was in force in 89 nations as of January 15, 1990. Bruce Zagaris, *Developments in International Judicial Assistance and Related Matters*, 18 DENV. J. INT'L L. & POL'Y 339 (1990). Since then, it has only been ratified by one other nation, bringing the total to 90. *Government Asks Parliament to Ratify Accords*, MTI ECONEWS, Jan. 19, 1996. *See also* Scott Sultzer, *Money Laundering: The Scope of the Problem and Attempts to Combat It*, 63 TENN. L. REV. 143, 209 (1995) (indicating that only Chile had fully ratified the Organization of American States' model rules to combat money laundering).

("MLATs") with the host nations of anonymous remailers.[292]

Much as MLATs governing money laundering enable law enforcement authorities to override local banking secrecy laws,[293] an MLAT governing investigations of electronic crimes would enable police agencies to override host nations' computer privacy laws when pursuing Internet criminals. This cooperation, however, would be limited to the offenses delineated in the terms of the MLAT, thus providing a clear outline of when an Internet user's right to anonymity may or may not be compromised.[294]

Furthermore, MLATs need not require a showing of dual criminality[295] to be invoked. For instance, the MLAT concluded in 1989 between the United States and Nigeria al-

---

292. *See supra* notes 196-205 and accompanying text (discussing the history and structure of MLATs).

293. Knapp, *supra* note 46, at 407.

294. MLATs commonly contain provisions limiting the circumstances under which assistance can be requested or under which information gained pursuant to the treaty can be used. *See* Cayman Islands MLAT, *supra* note 202, Articles 3, 7. These may include requirements that information gained under the terms of the treaty be kept confidential and/or limiting the use of such information in additional prosecutions or civil forfeiture proceedings. *Id.* at Articles 3(2), 3(4).

295. The principle of dual criminality requires a state to demonstrate that the offense charged in a request for extradition or legal assistance constitutes a crime both in the requesting and the requested nation. *See* John G. Kester, *Some Myths of United States Extradition Law*, 76 GEO. L.J. 1441, 1461 (1988). Existing MLATs treat the dual criminality principle in various ways. *See* Cayman Islands MLAT, *supra* note 202, articles 3.2, 19.3(a) 26 I.L.M. at 538 (containing no requirement of dual criminality unless assistance is sought in connection with an offense not specifically enumerated in the treaty); Russian-American MLAT, *supra* note 202, art. 3.1(2) (providing that the requested party may deny assistance if "the conduct under which the request is received would not constitute an offense under the laws of the Requested State"); Austrian-American MLAT, *supra* note 198, art. 1.3 (providing that the requested party shall provide assistance regardless of whether the conduct which is the subject of the request is a criminal offense in the requested nation, but that "the Requested State may refuse to comply in whole or in part with a request for assistance to the extent that the conduct would not constitute an offense under its laws and the execution of the request would require a court order for search and seizure or other coercive measures."). Because of the wide variation in national laws regarding financial crime, trafficking in pornography and copyright, any MLAT dealing with computer crime should follow the pattern of the Cayman Islands MLAT.

lowed American authorities to call upon their Nigerian counterparts for assistance in the investigation of money laundering offenses, even though money laundering was not then a crime in Nigeria.[296] An MLAT between the United States and Finland governing investigations of Internet crime would, if properly crafted, allow American law enforcement agencies to request Finnish authorities to order a remailer such as anon.penet.fi to disclose the source of an illegal message even though no crime had been committed in Finland.[297] This would enable the United States to enforce its laws while eliminating the possibility of another Erlich incident[298] which would pose a threat to the privacy of anon.penet.fi's entire clientele.[299]

In addition, due to the frequency of civil litigation stemming from alleged copyright infringement in cyberspace, MLATs dealing with law enforcement on the Internet could be extended to a limited range of civil matters for the resolution of the specific problem of anonymity.[300] Under such a treaty, a civil litigant might apply to the courts of his home nation for an order directing that the identity of the distributor of his allegedly protected materials be disclosed. If he could show that he would be likely to prevail in litigation against the anonymous distributor, the court order would be transmitted for execution to the nation in which the anonymous remailer operated. The standard of proof necessary for disclosure in civil matters would have to be relatively

296. *See* Treaty of Mutual Legal Assistance in Criminal Matters between the Federal Republic of Nigeria and the United States of America (Sept. 13, 1989). Money laundering was criminalized in Nigeria in 1990 by the Nigerian Drug Law Enforcement Act. It should be noted that the Nigerian-American MLAT has not been ratified by the United States Senate.

297. *See supra* note 145 and accompanying text (outlining Finnish law regarding disclosure in the context of the Helsingius affair).

298. *See supra* notes 134-42 and accompanying text.

299. *See supra* notes 138-47 and accompanying text (describing the Finnish police raid on anon.penet.fi in February 1995).

300. *See supra* note 281 (stating that no known principle of international law prevents the use of legal assistance treaties in civil matters).

high, in order to protect the privacy rights of Internet users in situations where no crime is present. If owners of intellectual property are unable to determine the identity of those who violate their rights, however, those rights will become meaningless.[301]

In civil matters, however, the scope of assistance available under the MLAT should be limited to disclosure of the identity of the putative defendant. Once the aggrieved party's right to know the identity of his opponent has been vindicated, further proceedings should be conducted according to customary methods of civil procedure. The disclosure process should also be strictly supervised by the courts of the requested nation, which should have the right to deny disclosure if, in their estimation, the allegations of tortious conduct were frivolous.

The great majority, if not all, of the anonymous remailers currently in existence operate in Western Europe, the United States and Canada.[302] Thus, the United States would be able to create a viable basis for evidence gathering in cyberspace by concluding MLATs with a few key nations.[303] Although a

---

301. *See* Church of Spiritual Tech. v. Helsingius (Helsinki Dist. Ct., Ânestys, J., Aug. 22, 1996), at 4 (acknowledging that the matter of copyright violation alleged by the Church of Scientology could only be resolved if the identity of the alleged violator was released by Helsingius).

302. Raph Levien's list of anonymous remailers includes one in Canada, one in Germany, one in Finland and 22 in the United States. Levien, *supra* note 28. A search on the Internet search utility Alta Vista revealed an additional remailer, "Sven's Remailer," operating in Belgium.

303. The United Kingdom, rather than Finland, might be the first priority for the United States in concluding an MLAT targeted at investigation of computer crime. Many of the nations which are emerging as "data havens," including Barbados and Anguilla, are British colonies or members of the British Commonwealth. An MLAT is already in force between the United States and the United Kingdom which pertains to the Cayman Islands, Anguilla, Montserrat, the Turks and Caicos Islands and the British Virgin Islands, all of which are known centers of offshore banking and potential or actual locations of offshore databases. The MLAT between the United States and the United Kingdom might easily be expanded to include provisions for disclosure of the identities of Internet users suspected of crime. Other priorities in concluding MLATs include nations where anonymous remailers are known to operate and nations where the

comprehensive solution to the problem of anonymity and law enforcement in cyberspace will require a multilateral treaty, the United States would be able to go a long way towards securing its law enforcement position by establishing binding treaty relationships with significant jurisdictions such as Finland.[304]

CONCLUSION

Anonymity in cyberspace is a controversial and vehemently debated issue. Proponents of the right to anonymity point to the legitimate and compelling reasons why Internet users might want or need to maintain their privacy in a public forum. Critics of anonymity, however, argue that the ease with which identities can be hidden in cyberspace, combined with the ability to transmit information across international borders with impunity, facilitates crime and hinders law enforcement.

This conflict is particularly difficult to settle, largely because both sides are right. Any solution to the problem of anonymity on the Internet must balance the right to privacy against the difficulties of international law enforcement.

---

transmission, possession or sale of child pornography or other black-market data is legal. Internet access services in nations meeting any of these conditions possess a high potential for illicit use. *See supra* notes 81-120 (discussing the criminal potential of anonymous remailers).

304. MLATs, combined with the previously-mentioned concept of a self-governing Internet, may also provide an intriguing long-term solution to the problems posed by information transmitted through anonymous remailers. If the Internet is recognized as a sovereign nation, it will possess the right to enter into treaties in the same manner as other nations. It might therefore be possible to conclude an MLAT *with the Internet itself*, allowing anonymity to be pierced at any location on the Internet without regard to the national jurisdiction in which a remailer's host computer is located. Similarly, it would be possible for a sovereign Internet to become a signatory to an international convention governing computer crime. It would thus be possible to obtain disclosure from multiple anonymous remailers, even if their host computers are located in several different countries. In addition, law enforcement agencies would then be able to trace the electronic trail of contraband information from start to finsih without the necessity of obtaining warrants from several jurisdictions.

A number of idealistic but impractical suggestions, such as a self-governing Internet, have been offered as solutions to this problem. In reality, there is no way that Internet crime can be completely curtailed, any more than money laundering or drug trafficking can be entirely eliminated. An environment can be created, however, which greatly facilitates the ease of international evidence gathering in cyberspace while protecting the rights to privacy and free flow of information.

The most comprehensive means of accomplishing such an environment would be a multilateral convention on computer crime which specifies areas of cooperation in investigation, closes loopholes which allow traffickers in child pornography and stolen data to operate with impunity in certain nations, and regulates the right to anonymity. Before such a treaty is ratified, however, the United States can still strengthen its ability to enforce its laws by entering into bilateral treaty relationships with key nations which share with it a common interest in combating computer crime.