Pace Law Review

Volume 20
Issue 1 *Fall 1999*

Article 8

September 1999

A More Convenient Crime: Why States Must Regulate Internet-Related Criminal Activity under the Dormant Commerce Clause

Laura Ann Forbes

Recommended Citation
Laura Ann Forbes, *A More Convenient Crime: Why States Must Regulate Internet-Related Criminal Activity under the Dormant Commerce Clause*, 20 Pace L. Rev. 189 (1999)
DOI: https://doi.org/10.58948/2331-3528.1266
Available at: https://digitalcommons.pace.edu/plr/vol20/iss1/8

Comment

A More Convenient Crime: Why States Must Regulate Internet-Related Criminal Activity Under the Dormant Commerce Clause

The powers delegated by the proposed Constitution to the federal government are few and defined. Those which are to remain in the State governments are numerous and indefinite. The former will be exercised principally on external objects, as war, peace, negotiation, and former commerce . . . . The powers reserved to the several States will extend to all the objects which, in the ordinary course of affairs, concern the lives, liberties, and properties of the people, and this internal order, improvement, and prosperity of the State.[1]

I. Introduction

Images of child pornography traded between co-workers.[2] A woman's life publicly threatened by an acquaintance.[3] A minor propositioned to engage in illicit sexual activity with an older stranger.[4] The states where these transactions occurred had every right to prosecute the offenders to the highest extent possible but for one thing. The incidents took place on the Internet. As a result, the situation was transformed. The federal government automatically assumed jurisdiction. A "common" crime was instantly morphed into a travesty of interstate commerce – a situation that, if not handled by the federal government, is claimed to have chilling and unconstitutional ramifications which echo off of every corner of the Information

1. THE FEDERALIST NO. 45 (James Madison).
2. *See* United States v. Anderson, 154 F.3d 1225 (10th Cir. 1998).
3. *See* United States v. Baker, 890 F. Supp. 1375 (E.D. Mich. 1995).
4. *See* United States v. Kufrovich, 997 F. Supp. 246 (D. Conn. 1997).

Superhighway. All of this occurred while the state was left with no way to protect its citizenry simply because the crime was not committed in a personally confrontational manner, but rather in the privacy of a home or office, a more convenient crime, if you will.

The Information Age has brought with it an expansion of criminal activity and a broadening of the exercise of the federal commerce power. The states are gradually losing their collective grasp on perpetrators to the federal government solely because modern criminals utilize technology to commit transgressions more quickly and inconspicuously than in previous times. This is clearly wrong. Technological advances should not afford a rationalization for the usurpation of states' rights to protect their citizenry from crime.[5] Congress enforces this usurpation by categorizing Internet communications as articles of interstate commerce[6] warranting Congress' exclusive regulation[7] via the Commerce Clause.[8]

The fact that Internet communications are articles of interstate commerce does not justify exclusive jurisdiction by the federal government over all related offenses. States originally were granted the power to enforce criminal statutes under the Dormant Commerce Clause,[9] and this power should be continued in light of the increased utilization of the Internet as a criminal instrumentality.[10]

The concept of Internet activity subjecting individuals to jurisdiction in a state court system is already established in the area of civil litigation.[11] Using traditional due process[12] notions

5. *But see* Dan L. Burk, *Federalism in Cyberspace*, 28 CONN. L. REV. 1095 (1996); *see also* Kenneth D. Bassinger, *Dormant Commerce Clause Limits on State Regulation of the Internet: The Transportation Analogy*, 32 GA. L. REV. 889 (1998).

6. *See infra* text accompanying notes 70-88.

7. *See infra* text accompanying notes 54-69.

8. *See infra* text accompanying notes 54-56.

9. *See infra* text accompanying notes 106-20.

10. Includes "any machinery, weapon, instrument, or tangible object that has played a significant role in a crime." CRIMINAL DIV., U.S. DEP'T OF JUSTICE. FED. GUIDELINES FOR SEARCHING AND SEIZING COMPUTERS 28 (1994).

11. For discussion, *see, e.g.*, Brian Covotta, *Personal Jurisdiction and the Internet: An Introduction*, 13 BERKELEY TECH. L.J. 265 (1998).

12. " No person shall . . . be deprived of life, liberty, or property, without due process of law." U.S. CONST. amend. V; "No State shall . . . deprive any person of life, liberty, or property, without due process of law." U.S. CONST. amend. XIV.

of "purposeful availment"[13] and "minimum contacts,"[14] it has become reasonable that a person can expect to be "haled into court"[15] where the Internet communications (either via the World Wide Web or electronic mail) were received. Through long-arm statutes,[16] state civil courts nationwide have successfully litigated claims regarding Internet-based activity.[17] This philosophy should be applied to (and in some states continue to be applied to) criminal liability, under the auspices of geographic jurisdiction subsections of state criminal procedure law.[18]

This article will advocate state jurisdiction over criminal activity which takes place on the Internet under the proviso of the Dormant Commerce Clause. This will be accomplished by journeying through a logical progression from the birth of both Congress' Commerce Power and the states' police power to their evolutions through the years in the face of emerging computer technology. Section II of this comment will briefly explain the concepts of Internet crime in general[19] and the development of the term "Information Superhighway."[20] Section III will explain the definition of the articles of commerce under the Commerce Clause[21] and how Internet communications have received such designation.[22] The subsequent case law, which stemmed

---

13. Burger King Corp. v. Rudzewicz, 471 U.S. 462, 475 (1985).

14. International Shoe Co. v. Washington, 326 U.S. 310, 316 (1945).

15. World-Wide Volkswagen Corp. v. Woodson, 444 U.S. 286, 287 (1980).

16. Various state legislative acts which provide for personal jurisdiction, via substituted service of process, over persons or corporations which are non-residents of the state and which voluntarily go into the state, directly or by agent, or communicate with persons in the state for limited purposes, in actions which concern claims relating to the performance or execution of those purposes, *e.g.*, transacting business in the state, contracting to supply services or goods in the state, or selling goods outside the state when the seller knows that the goods will be used or consumed in the state.

BLACK'S LAW DICTIONARY 942 (6th ed. 1990). *See, e.g.*, N.Y. C.P.L.R. § 302 (McKinney 1997).

17. *See, e.g.*, Bensusan Restaurant Corp. v. King, 937 F. Supp. 295 (S.D.N.Y. 1996), *aff'd*, 126 F.3d 25 (2d Cir. 1997); Maritz, Inc. v. Cybergold, Inc., 947 F. Supp. 1328 (E.D. Mo. 1996); Inset Systems, Inc. v. Instruction Set, Inc., 937 F. Supp. 161 (D. Conn. 1996).

18. *See, e.g.*, N.Y. CRIM. PROC. LAW Art. 20 (McKinney 1997).

19. *See infra* text accompanying notes 29-47.

20. *See infra* notes 48-53 and accompanying text.

21. *See infra* text accompanying notes 54-69.

22. *See infra* text accompanying notes 70-88.

from this designation and struck down state related statutes, will also be discussed in this section.[23] In Section IV, the Dormant Commerce Clause will be introduced,[24] and cases will be presented which support the exercise of police power over Internet crimes by the states in the face of earlier mentioned Commerce Clause case law.[25] The focus will be on federal and state courts in New York in this section since the majority of the Internet related criminal jurisdiction case law stems from this area.[26] These decisions will also be used to refute the federal legislative intent behind the Computer Fraud and Abuse Act,[27] under which the federal government brings most of its computer and Internet-related prosecutions. This article will then conclude in Section V with a summary of the tenets set forth throughout this comment and offer a prediction for the future of Internet prosecutions.[28]

II. A General Discussion About the Information Superhighway and Cybercrime

A. *Internet Crime: Different Instrumentality, Same Effect*

Many individuals have offered definitions of the Internet, and each definition incorporates a variety of unique aspects: lack of boundaries, speed, interactivity, and connectivity, among others. For legal uniformity however, both state and federal courts follow the definition provided in *American Civil Liberties Union v. Reno*.[29]

---

23. *See infra* text accompanying notes 89-105.
24. *See infra* text accompanying notes 106-32.
25. *See infra* text accompanying notes 126-28.
26. *See infra* text accompanying notes 145-213.
27. 18 U.S.C. § 1030 (1994); *see infra* text accompanying notes 133-46.
28. *See infra* text accompanying notes 214-30.
29. 929 F. Supp. 824 (E.D. Pa. 1996), *aff'd*, Reno v. ACLU, 521 U.S. 844 (1997). These cases struck down provisions of the Communications Decency Act of 1996 [CDA] which was codified as a sub-section of the Communications Act of 1934, 47 U.S.C. § 223. The Act was designed to avoid children's exposure to "indecent material" on the Internet and was struck down due to:

> the lack of legislative hearings;
> the use of different forms for 'indecent';
> the broad definition of indecent;
> the heightened level of review because of the criminal nature of the statute;
> the broad applicability of the statute to commercial and noncommercial speech;

> The Internet is not a physical or tangible entity, but rather a giant network that interconnects innumerable smaller groups of linked computer networks. It is thus a network of networks . . . . Many networks . . . are connected to other networks, which are in turn connected to other networks in a manner that permits each computer in any network to communicate with computers on any other network in the system. This global Web of linked networks and computers is referred to as the Internet.[30]

The Internet has three main functions: messaging, information, and entertainment.[31] "Messaging" includes common features such as electronic mail ("e-mail"), bulletin board services,[32] and "real-time" conversations ("chats"[33]).[34] "Information" encompasses all of the knowledge published digitally on the Internet, in both audio and visual formats, designed to benefit students, businesses, and any individuals in search of serv-

---

the failure of the government to consider less restrictive alternatives; and unreliable affirmative defenses.

Child Online Protection Act, H.R. Rep. 105-775, 105th Cong. (1998). The Child Online Protection Act was subsequently passed in 1998 by Congress, as 47 U.S.C. § 231, to amend § 223. *See id.* This amendment was designed to be more narrowly tailored than its predecessor by including provisions for implementation of age verification protocols, application only to commercial web sites, and utilization of legislative hearings, among others. *See id.* However, on February 1, 1999, the Eastern District of Pennsylvania, the same court as in ACLU v. Reno "I", granted injunctive relief from the enforcement of the Act, which was originally slated for November 29, 1998. This injunction, as in *Reno I*, was again due to content-based restrictions on speech and excessive burdens on Internet users and businesses. See ACLU v. Reno, No. 98-5591 (E.D. Pa. filed February 1, 1999) ("*Reno II*").

30. ACLU v. Reno, 929 F. Supp. 824, 830-31 (E.D. Pa. 1996), *aff'd*, Reno v. ACLU, 521 U.S. 844 (1997).

31. *See* DANNY GOODMAN, LIVING AT LIGHT SPEED: YOUR SURVIVAL GUIDE TO LIFE ON THE INFORMATION SUPERHIGHWAY 19-22 (Random House 1994).

32. "A fancy name for an electronic message system running on a microcomputer. Call up, leave messages, read messages. The system is like a physical bulletin board. That's where the name comes from. Some people call bulletin board systems electronic mail systems." HARRY NEWTON, NEWTON'S TELECOM DICTIONARY 182 (10th ed. 1996).

33. A common name for a type of messaging done over a network, involving short, usually one or two line messages sent from one node to another. Usually a chatting facility is RAM-resident, meaning it can be 'popped up' inside an application program. Users are usually notified of an incoming chat by a beep and a message at the bottom of their screens.

NEWTON, *supra* note 32, at 248.

34. *See* GOODMAN, *supra* note 31, at 20.

ices.[35] "Entertainment" includes any music, videos, and games available over the Internet for leisure purposes.[36]

Although the Internet is an international phenomenon, American users comprise the overwhelming majority of the global online population.[37] Neilsen Media reported that in 1999, thirty-five million households, or approximately ninety-seven million people had Internet access.[38] This means that almost thirty-four percent of United States households have Internet access.[39] This figure has doubled from fifty-eight million users in September, 1997.[40] Of all the states, California has the highest Internet-using population, with 6.4 million people over age sixteen accessing the Internet by September, 1997.[41] New York State ranks second with 3.7 million users.[42] Together, California and New York accounted for fifty-eight percent of the country's Internet users in 1997.[43] Sixty percent of Internet users have utilized the World Wide Web to shop.[44]

---

35. *See id.* at 20-21.

36. *See id.* at 21-22.

37. The international total of Internet users is 171.25 million. The demographics are broken down as follows:

Africa:	1.14 Million
Asia/Pacific:	27 Million
Europe:	40 Million
Middle East:	.88 Million
Canada & U.S.:	92 Million
South America:	5.3 Million

CommerceNet Research Center, *Knowledge - Internet Statistics* (last visited Oct. 7, 1999) <http://www.commerce.net/research/stats/wwstats.html>.

38. *See* Nielsen Media Research, *New Internet Population Estimate of 97.1 Millions, 36% of the Total U.S. Population* (visited October 20, 1999) <http://www.nielsenmedia.com/newsreleases/releases/1999/netratings2.html>.

39. *See id.*

40. *See* Nielsen Media Research, *Number of Internet Users and Shoppers Surges in United States and Canada* (visited October 26, 1998) <http://www.nielsenmedia.com/news/commnet2.html>.

41. *See* Nielsen Media Research, *Florida Is Among Fastest-Growing Internet States; California Leads in Total Number of Internet Users* (visited October 26, 1998) <http://www.nielsenmedia.com/news/commnet1.html>.

42. *See id.*

43. *See id.*

44. *See* Nielsen Media Research, *Women Shoppers Head to the Web in Force as the Number of Internet Buyers Jumps 40% in Nine Months: New CommerceNet/Nielsen Media Research Study Also Shows Internet Users Top 92 Million in the U.S. and Canada* (visited October 20, 1999) <http:www.nielsenmedia.com/newsreleases/releases/1999/commercenet.html>.

With so many users accomplishing so many tasks online, it was inevitable that a criminal element would infiltrate the system. Experts have attempted to group the most common types of crimes which may be perpetrated on the Internet, either internally by individuals with legitimate access to networks or externally by unauthorized users.[45] Included in these groups of computer crimes are "unauthorized use of computer-related assets, introduction of fraudulent records or data into a computer system, alteration or destruction of information or files, and theft (by electronic means or otherwise) of money, financial instruments, property, services, or data."[46] Regardless of the classifications made by information technology experts, Internet crime has a less technical definition. Although there are crimes that are exclusive to the Internet, some crimes are merely physical crimes thrust into a virtual world. Although the aforementioned are the most common types of computer crimes, many other crimes may be accomplished online, including "theft, fraud, larceny, extortion, embezzlement, espionage, tampering, forgery, sabotage, piracy, smuggling, terrorism, pornography, pedophilia, impersonation, invasion of privacy, assault - even attempted murder."[47] These are the crimes with which states are most concerned, the "ordinary" crimes that target random citizens. Internet crime is no longer a crime affecting only the government, military computer networks, or the most complex of corporations. Unsuspecting private individuals are being shocked everyday as they become victimized by criminals using the Internet and computers as new weapons.

B. *The Internet as "The Information Superhighway"*

The Internet is appropriately nicknamed "The Information Superhighway."[48] "Early discussions about the Internet made use of the highway metaphor to compare the effort needed to wire America with that of paving America with interstate highways, begun in the 1950s."[49] As with paved highways, the vir-

45. *See* LAURA E. QUARANTIELLO, CYBERCRIME: HOW TO PROTECT YOURSELF FROM COMPUTER CRIMINALS 16 (Tiare Publications 1997).
46. *Id.*
47. QUARANTIELLO, *supra* note 45, at 12.
48. GOODMAN, *supra* note 31, at 1.
49. *Id.* at 2.

tual highway is extrinsically worthless, as is money, which is not extrinsically worth anything in comparison to its representation as currency. The significance of each highway is measured by what each accomplishes. One highway carries tangible items, while the other carries intangible electronic communications. Both modes encourage a proliferation of commercial activity, relationships, and travel, all of which directly affect the economy of the nation as a whole and those of its individual states.[50]

Despite the similarities, distinctions between actual and virtual highways are significant enough to demand notice by the courts. Paved highways are governmentally-funded projects, while the Internet's rapid expansion is due primarily to private individuals and organizations.[51] Furthermore, paved interstate highways connect main roads in contiguous states, but the Information Superhighway connects not only major thoroughfares, but "also provides access to the side streets and driveways leading straight to our doors."[52] Paved highways have signs for exits giving direction to towns, and then users are left to find their way to individual sites. However, Internet users are not simply directed where to go, but are instead led directly to web sites, requested information, or individual e-mail addresses.[53] This intimate connection with the daily lives of individuals should lessen the theory of federal stronghold over the Internet and place more penal authority into the hands of state governments.

III. Interstate Commerce Meets the Internet

A. *The Origin of the Commerce Clause and Articles of Interstate Commerce*

The United States Congress is directly granted the power "[t]o regulate Commerce with foreign Nations, and among the several States."[54] This Commerce Clause must always be read in conjunction with the Necessary and Proper Clause,[55] which

50. *See id.*
51. *See id.* at 3.
52. *Id.*
53. *See* GOODMAN, *supra* note 31.
54. U.S. CONST. art. I, § 8, cl. 3.
55. U.S. CONST. art. I, § 8, cl. 18.

permits Congress "[t]o make all Laws which shall be necessary and proper for carrying into Execution the foregoing Powers."[56] Not all powers of Congress under the Commerce Clause are specifically enumerated; rather "[t]he powers delegated are of two classes: such as are expressly granted, and such as are implied, as 'necessary and proper' to carry into execution the powers expressly enumerated."[57]

Although the power is not specific, there are three broad areas of activities Congress can regulate under the Commerce Clause.[58] The clause is most often used to "regulate the use of the channels of interstate commerce[,] . . . protect the instrumentalities of interstate commerce, or persons or things in interstate commerce, even though the threat may come only from intrastate activities, . . . [and] regulate those activities having a substantial relation to interstate commerce."[59] These are hardly the clearest of guidelines. Anything, if argued persuasively, can become "an instrumentality of interstate commerce,"[60] which would then transform the item, no matter how innocuous, into something worthy of federal regulation.

"As a general rule, any article which has been recognized by custom or law as a fit subject for barter or sale – particularly if its manufacture has been made the subject of federal legislation and taxation – must be recognized as a legitimate subject of commerce."[61] In the past, this has covered the gamut of items from railroad cars[62] and ferries[63] to natural gas,[64] milk,[65] and even minnows.[66] The "article of interstate commerce" designa-

56. *Id.*; *see also* Gibbons v. Ogden, 22 U.S. 35 (1824).

57. Gibbons v. Ogden, 22 U.S. at 35; *see also* Heart of Atlanta Motel v. United States, 379 U.S. 241, 255 (1964); L.E. Service, Inc. v. State Lottery Comm'n of Indiana, 646 N.E.2d 334, 344 (Ind. 1995).

58. *See* United States v. Lopez, 514 U.S. 549, 558 (1995), discussed *infra* text accompanying notes 122-32.

59. *Id.*

60. *Id.*

61. 15A AMERICAN JUR. 2D *Commerce* § 36 (1976).

62. *See, e.g.*, Wabash, St. L. & P. Ry. Co. v. Illinois, 118 U.S. 557 (1886).

63. *See, e.g.*, Gloucester Ferry Co. v. Commonwealth, 114 U.S. 196 (1885).

64. *See, e.g.*, Manufacturers' Gas & Oil Co. v. Indiana Natural Gas & Oil Co., 58 N.E. 706 (Ind. 1900).

65. *See, e.g.*, Milk Control Bd. of Pennsylvania v. Eisenberg Farm Prod., 306 U.S. 346 (1939).

66. *See, e.g.*, Hughes v. Oklahoma, 441 U.S. 322 (1979).

tion is not necessarily a permanent or consistent one.[67] In fact, items may be stripped of this label[68] or be engaged in interstate commerce for only a limited purpose.[69]

B. *Internet Communications as Articles of Interstate Commerce*

The Internet and its communications may be considered articles of interstate commerce, based on the three main categories of interstate commerce over which Congress retains jurisdiction.[70] First, the Internet may be considered an "instrumentalit[y] of interstate commerce."[71] As mentioned previously, the Internet has been likened to a paved interstate highway,[72] which has been an article of interstate commerce for decades.[73] Just as highways assist in bringing products across borders for sale in other regions, so does the Internet.

Additionally, courts are currently considering Internet communications, such as any form of messaging,[74] a "thing[ ] in interstate commerce, even though the threat may come only from intrastate activities"[75] because of the technicalities in-

---

67. In view of the Supreme Court's refusal to fix an arbitrary rule as to what constitutes commerce subject to the power of Congress, ... [t]here is a possible conflict between earlier cases holding certain matters not to be subjects of interstate commerce and later cases holding related matters to be subjects of interstate commerce, although the earlier cases have not been specifically overruled.

15A AMERICAN JUR. 2D *Commerce* § 36 (1976).

68. *See, e.g.,* Oklahoma Tax Comm'n v. Jefferson Lines, Inc., 514 U.S. 175 (1995).

69. 15A AMERICAN JUR. 2D *Commerce* § 36 ("[W]hile advertising contracts entered into with the publisher of periodicals which are circulated throughout the country have been held not to constitute interstate commerce, national advertising originating throughout the nation and offering products for sale on a national scale has since been held to be interstate commerce." (discussing Times-Picayune Publ'g Co. v. United States, 345 U.S. 594 (1953) and Lorain J. Co. v. United States, 342 U.S. 143 (1951)).

70. *See* United States v. Lopez, 514 U.S. 549, 558 (1995), discussed *infra* text accompanying notes 122-32.

71. *Id.*

72. *See* GOODMAN, *supra* note 31, at 2.

73. "[I]nterstate roads and railroads are indispensable 'instrumentalities' in the carriage of persons and goods that move in interstate commerce." Alstate Constr. Co. v. Durkin, 345 U.S. 13, 15 (1953) (discussing Overstreet v. Northshore Corp., 318 U.S. 125, 129-30 (1943)).

74. *See* GOODMAN, *supra* note 31, at 20.

75. *Lopez*, 514 U.S. at 558.

volved in electronic mail message distribution and web page downloading. Due to the networked nature of Internet-accessible computers and a high priority for efficiency, any "communication sent over this redundant series of linked computers could travel any of a number of routes to its destination."[76] Internet communications are structured to utilize packet switching communication protocols,[77] which break messages down into packets[78] thus maximizing the efficiency of the travel time.[79] Because of this phenomenon, a message sent from one individual to another may travel one route, while a response to that communication or any future communications will follow a completely different path, depending upon the amount of Internet traffic at the time.[80] These routes do not differentiate between states. Because of this, an e-mail message sent from New York may go through Connecticut before reaching its final destination in New Jersey, but if that message were to be re-sent, the packets may travel through Maine or Delaware. The same holds true for any message sent from one state resident to another.[81]

Courts also have determined that Internet communications substantially affect interstate commerce.[82] Courts dealing with this issue have opined that inconsistent regulation by the states would have a chilling effect[83] on commerce, in that commercial

---

76. ACLU v. Reno, 929 F. Supp. 824, 831 (E.D. Pa. 1996).

77. Sending data in packets through a network to some remote location. The data to be sent is subdivided into individual packets of data, each packet having a unique identification and each packet carrying its own destination address. This way each packet can go by a different route. The packets may also arrive in a different order than how they were shipped. The packet ID lets the data be reassembled in proper sequence. Packet switching is a very efficient method of moving digital data around.

NEWTON, *supra* note 32, at 855.

78. "A bundle of data, usually in binary form, organized in a specific way for transmission. Three principle elements are included in the packet: 1. Control information – destination, origin, length of packet, etc., 2. The data to be transmitted, and 3. Error detection and correction bits." *Id.* at 854.

79. *See* ACLU v. Reno, 929 F. Supp. 824, 831 (E.D. Penn. 1997).

80. *See id.* at 831-32.

81. *See id.* at 832. *But see* United States v. Paredes, 950 F. Supp. 584 (S.D.N.Y. 1996), *aff'd on other grounds,* 162 F.3d 1149 (2d Cir. 1998), discussed *infra* notes 148-154 and accompanying text.

82. *See Lopez*, 514 U.S. at 558.

83. In constitutional law, any law or practice which has the effect of seriously discouraging the exercise of a constitutional right . . . . The deterrent

enterprises will resist expansion for fear of criminal liability in any state.[84] As a result, commerce (not only exclusively criminal activity) will be restrained, even in cases where "activities [are] undertaken without a profit motive"[85] because "many of those users who are communicating for private, non-commercial purposes . . . by virtue of their Internet consumption,"[86] via subscriptions to Internet Service Providers that charge for Internet access.[87] This is a difficult concept to accept, however, because "[t]his test, if taken to its logical extreme, would give Congress a 'police power' over all aspects of American life."[88]

C. *Court Opinions Declaring Internet Communications Subject Only to Federal Regulation*

The leading case advocating exclusive federal regulation is *American Library Ass'n v. Pataki*,[89] in which various organizations[90] challenged a New York state statute regarding dissemination of indecent material to minors,[91] based on facial

---

effect of governmental action that falls short of a direct prohibition against the exercise of First Amendment rights. To constitute an impermissible chilling effect the constrictive impact must arise from the present or future exercise or threatened exercise of coercive power.

BLACK'S LAW DICTIONARY 240 (6th ed. 1990) (citations omitted).

84. *See* American Library Ass'n v. Pataki, 969 F. Supp. 160, 174 (S.D.N.Y. 1997).

85. *Id.* at 172 (discussing Edwards v. California, 314 U.S. 160 (1940)).

86. American Library Ass'n v. Pataki, 969 F. Supp. 160, 172 (S.D.N.Y. 1997).

87. *See id.* Such providers also include the plaintiffs in *American Library Ass'n*, who are small scale access providers or bulletin board operators.

88. United States v. Lopez, 514 U.S. 549, 584 (1995) (Thomas, J., concurring).

89. 969 F. Supp. 160 (S.D.N.Y. 1997); *but see infra* notes 172-76, 192 and accompanying text.

90. *See American Library Ass'n*, 969 F. Supp. at 161. Plaintiffs include "a spectrum of individuals and organizations who use the Internet to communicate, disseminate, display, and access a broad range of communications. All of the plaintiffs communicate online both within and outside the State of New York, and each plaintiff's communications are accessible from within and outside New York." *Id.* Plaintiffs' business and non-profit enterprises include library associations, bookstore trade organizations, literary, art, and software trade organizations, Internet service providers, and civil liberty organizations, including the ACLU. *See id.* at 161-62.

91. A person is guilty of disseminating indecent material to minors in the second degree when: . . . [k]nowing the character and content of the communication which, in whole or in part, depicts actual or simulated nudity, sexual conduct or sado-masochistic abuse, and which is harmful to minors, he intentionally uses any computer communications system allowing the input,

constitutional violations of the Commerce Clause and the First Amendment.[92] As the first court to consider Internet communications articles of commerce,[93] Judge Preska found that the statute[94] and its legislative intent[95] did not limit jurisdiction to intrastate conduct.[96] Consequently, New York State's regulation of indecent material unconstitutionally interfered with the free flow of interstate commerce.[97] This case stereotypes all Internet communications and users by presuming that an offender has no way of knowing the geographic location of the person with whom she is communicating.[98]

A more recent case, *United States v. Kammersell*,[99] further developed the *American Library Ass'n* decision and reinforced the interstate nature of the Internet. The defendant in *Kammersell* moved to dismiss his indictment[100] for making a threatening communication over the Internet in violation of 18 U.S.C.

---

output, examination or transfer, of computer data or computer programs from one computer to another, to initiate or engage in such communication with a person who is a minor. Disseminating indecent material to minors in the second degree is a class E felony.

N.Y. PENAL LAW § 235.21(3) (McKinney 1997).

92. Although First Amendment free speech concerns are legitimate in the face of Internet expansion and regulation, the issue far exceeds the scope of this comment, although some issues are intertwined with Commerce Clause considerations. For discussion, *see* Reno v. ACLU, 521 U.S. 824 (1997); *see also, e.g.*, James V. Dobeus, *Rating Internet Content and the Spectre of Government Regulation*, 16 J. MARSHALL J. COMPUTER & INFO. L. 625 (1998).

93. *See American Library Ass'n,* 969 F. Supp. at 167 ("While no one should lose sight of the inventiveness that has made this complex of resources available to just about anyone, the innovativeness of the technology does not preclude the application of traditional legal principles – provided that those principles are adaptable to cyberspace.").

94. *See id.* at 169-70 ("[T]he Act does not import any restriction that the criminal communication must take place entirely within the State of New York. By its terms, the Act applies to any communication, intrastate or interstate, that fits within the prohibition and over which New York has the capacity to exercise criminal jurisdiction.").

95. *See id.* at 170 ("Further, the legislative history of the Act clearly evidences the legislators' understanding and intent that the Act would apply to communications between New York and parties outside the State, despite the occasional glib references to the Act's 'intrastate' applicability.").

96. *See id.* at 171.

97. *See id.* at 172.

98. *See American Library Ass'n,* 969 F. Supp. at 170-72. *But see infra* text accompanying notes 163-71.

99. 7 F. Supp. 2d 1196 (D. Utah 1998).

100. *See id.* at 1197.

§ 875(c).[101] His contention that the federal court did not have jurisdiction was based on an e-mail transmission from himself, a Utah resident, to another Utah resident via the Internet Service Provider America Online. The fact that both the defendant and the victim were residents made it an entirely intrastate communication, and Kammersell's argument[102] relied on the Commerce Clause analysis provided in *United States v. Lopez*.[103] Kammersell argued that state criminal law is a more appropriate vehicle for prosecution of the type of crime that was committed.[104] Although the *Kammersell* court did not perform an analysis of Internet communications as articles of interstate commerce, it did say that a communication may be considered commerce although its intrinsic nature is not commercial or business related.[105]

IV. Dormant Commerce Clause as a Means of Exercising State Police Power Over Internet Crime

A. *Dormant Commerce Clause Generally*

The Dormant Commerce Clause[106] is the main precept on which the states rely for exercising jurisdiction over criminal activities within state borders. *Pike v. Bruce Church*[107] provides perhaps the most famous articulation of the Dormant Commerce Clause:

> Where the statute regulates even-handedly to effectuate a legitimate local public interest, and its effects on interstate commerce are only incidental, it will be upheld unless the burden imposed on such commerce is clearly excessive in relation to the putative local benefits. If a legitimate local purpose is found, the question

101. "Whoever transmits in interstate or foreign commerce any communication containing any threat to kidnap any person or any threat to injure the person of another, shall be fined under this title or imprisoned not more than five years, or both." 18 U.S.C. § 875(c) (1994).

102. *See Kammersell*, 7 F. Supp. 2d at 1198.

103. 514 U.S. 549 (1995).

104. *See Kammersell*, 7 F. Supp. 2d at 1200-01.

105. *See id.* at 1201.

106. The negative sweep of the Commerce Clause designed to restrict the states' regulatory interference with interstate commerce. *See* American Library Ass'n v. Pataki, 969 F. Supp. 160, 169 (S.D.N.Y. 1997); *supra* notes 86-98 and accompanying text.

107. 397 U.S. 137 (1970).

> becomes one of degree. And the extent of the burden that will be tolerated will of course depend on the nature of the local interest involved, and on whether it could be promoted as well with a lesser impact on interstate activities.[108]

State legislation will invariably be struck down in situations where the burdens placed on interstate commerce are economically protectionist[109] in nature or when there is preemptive federal regulation.[110] Nonetheless, a state's crimp on interstate commerce does not automatically render the legislation void. Rather, *Head v. New Mexico Board of Examiners in Optometry*[111] concisely articulates the basic premise set forth in *Pike v. Bruce Church,*[112] that "a state law may not be struck down on the mere showing that its administration affects interstate commerce in some way. 'State regulation, based on the police power which does not discriminate against interstate commerce or operate to disrupt its required uniformity, may constitutionally stand.'"[113]

The Federal Commerce Clause and states' limitations under the Dormant Commerce Clause are not necessarily competing interests. "It is perfectly settled, that an affirmative grant of power to the United States does not, of itself, devest [sic] the States of a like power."[114] Concurrency of legislation is a well-known, and well-founded, concept in our predominantly Federalist system.[115] "All powers . . . not expressly exclusive, or

---

108. *Id.* at 142.

109. "Economic protectionism" is defined as "regulatory measures designed to benefit in-state economic interests by burdening out-of-state competitors." New Energy Co. of Indiana v. Limbach, 486 U.S. 269, 273-74 (1988).

110. Where "state law is displaced only 'to the extent that it actually conflicts with Federal law.'" Dalton v. Little Rock Family Planning Servs., 516 U.S. 474, 476 (1996) (quoting Pacific Gas & Elec. Co. v. State Energy Resources Conservation and Dev. Comm'n, 461 U.S. 190, 204 (1983)).

111. 374 U.S. 424 (1963).

112. 397 U.S. 137 (1970).

113. *Head*, 374 U.S. at 428 (quoting Huron Portland Cement Co. v. City of Detroit, 362 U.S. 440, 448 (1960)).

114. Gibbons v. Ogden, 22 U.S. 35 (1824).

115. Federal jurisdiction should be asserted selectively based on such factors as the type of defendants reasonably believed to be involved and the relative ability of the Federal and state authorities to investigate and prosecute. For example, the apparent involvement of organized crime figures or the lack of effective local investigation because of the interstate features of the crime could indicate that Federal action was appropriate . . . . Cooperation and coordination between Federal and state officials should be utilized

clearly exclusive in their nature, ought to be deemed concurrent. All implied powers are, of course, concurrent."[116] This is true especially in the area of criminal law. Even though Congress has made an act criminal, the states are not necessarily precluded from legislating in that area.[117]

Under the dormant commerce power, the states exercise their police power via criminal statutory schemes designed to protect the health, safety and welfare of citizens.[118] The states possess primary authority for defining and enforcing the criminal law.[119] Therefore, though incidental burdens may be placed on interstate commerce during the course of enforcement, such burdens may be both permitted and inevitable when a state legislates in the name of the health and safety of its people.[120]

United States v. Lopez[121] is perhaps the most heavily relied upon case pertaining to the struggle between state and federal criminal jurisdiction. The case centered around the Gun Free Schools Act of 1990,[122] which made it a federal offense for any individual to knowingly possess a gun in what he knew, or had reason to believe, was a school zone.[123] Lopez argued that the

---

> to ensure that the new murder-for-hire statute is used in appropriate cases to assist the states rather than to allow the usurpation of significant cases by Federal authorities that could be handled as well or better at the local level.

United States v. Paredes, 950 F. Supp. 584, 587-88 (S.D.N.Y. 1996), *aff'd on other grounds*, 162 F.3d 1149 (2d Cir. 1998).

116. Gibbons v. Ogden, 22 U.S. 35 (1824).

117. *See* S. REP. No. 99-432 (1986) *reprinted in* 1986 U.S.C.C.A.N. 2479, *infra* at notes 118, 120 ("S. 2281, as reported by the Committee, is a consensus bill aimed at deterring and punishing certain 'high-tech' crimes in a manner consistent with the States' own criminal laws in this area.").

118. The police power of a state was designed to:

> prescribe regulations to promote the health, peace, morals, education, and good order of the people, and to legislate so as to increase the industries of the state, develop its resources, and add to its wealth and prosperity . . . Regulations for these purposes may press with more or less weight upon one than upon the other, but they are designed, not to impose unequal or unnecessary restrictions upon any one, but to promote, with as little inconvenience as possible, the general good.

Barbier v. Connolly, 113 U.S. 27, 31-32 (1884).

119. *See* Engle v. Isaac, 456 U.S. 107, 128 (1982).

120. *See* City of Philadelphia v. New Jersey, 437 U.S. 617, 624-25 (1978).

121. 514 U.S. 549 (1995).

122. 18 U.S.C. § 922(q)(1)(A) (1994).

123. *See id.*

Act was an unconstitutional violation of the Commerce Clause and an overstepping of Congressional boundaries into the States' exercise of police power.[124] The Government unsuccessfully argued that the presence of guns on school grounds lead to violent crime on campus and a poor educational environment. Therefore, the students learn less, which results in poor jobs, and eventually, a depressed economy.[125] The majority disagreed,[126] despite the Government's attempt to articulate this tenuous connection between guns on school grounds and interstate commerce.[127] The Court held, "to uphold the Government's contentions here, we would have to pile inference upon inference in a manner that would bid fair to convert congressional authority under the Commerce Clause to a general police power of the sort retained by the States."[128]

The argument articulated in *Lopez* provides an excellent parallel for many criminal Internet communications. State regulation of the Internet raises fear of inconsistency from state to state which, "taken to its most extreme, could paralyze the development of the Internet altogether."[129] This, of course, is certainly the most extreme view. There are many forms of Internet usage,[130] and state regulation could never impact all of them. Is there not an assumption (regardless of the state) that denying access to a computer network and causing it to malfunction or even crash would be a crime?[131] Furthermore, is it

124. *See* United States v. Lopez, 514 U.S. 549 (1995).

125. *See id.* at 565.

126. *See id.* at 567.

127. *See id.* at 565.

128. *Id.* at 567.

129. American Library Ass'n v. Pataki, 969 F. Supp. 160, 169 (S.D.N.Y. 1997).

130. *See supra* notes 31-36 and accompanying text.

131. Generally, denial of service attacks [DoS attacks] bombard any networks and peripherals that have contact with the Internet with extra traffic, crippling them so that outside users (including customers of Internet Service Providers) cannot utilize the service. Such deliberate attacks can wreak havoc in a network and shut down operations across the board. Additionally, when Internet Service Providers are attacked, not only is the victim network disabled, but when a provider has any number of customers, the customers (both private individuals and businesses) also suffer. *See* Jeff Downey, *Can't Say No,* PC MAGAZINE, Apr. 21, 1998, at 203. *See also* CAL. PENAL CODE § 502(c)(5) (West 1997) ("[k]nowingly and without permission disrupts or causes the disruption of computer services or denies or causes the denial of computer services to an authorized user of a computer, computer system, or computer network."). *See, e.g.*, N.C. GEN. STAT. § 14-456 (1997);

not presumed per se illegal for a fifty-five year-old man to seduce a thirteen year-old girl, whether in real life or online, unless they are a married couple?[132] The relationship between total federal regulation of the Internet and the prevention of a chilling of all Internet commerce is as attenuated as the link in *Lopez* between guns near a school and the economy of the entire nation.

B. *The Federal Computer Fraud and Abuse Act versus State Jurisdiction Over Criminal Internet Activity via the Dormant Commerce Clause*

The thesis of this comment is not that states should be authorized to regulate *all* Internet activity without any federal involvement; rather, that states should have the authority to preside over cases where there is a substantial vested interest in protection of the state's citizenry. This authority may be asserted only by the state or together with the federal government when the offenses involved can be concurrently prosecuted by both the state and federal governments.[133] States should be empowered to retain jurisdiction when an element of a state crime is present during an Internet communication,[134] regardless of whether the state prosecutes alone or in conjunction with the federal government. In fact, states should not be permitted to

---

CONN. GEN. STAT. ANN. § 53a-252 (West 1994). These states have statutes criminalizing DoS attacks.

132. *See* People v. Barrows, 677 N.Y.S.2d 672, 685 (Sup. Ct. Kings County 1998); *see also infra* notes 169-96 and accompanying text.

133. The notion of dual sovereignty is not a foreign one in criminal law and may be utilized in the area of computer crimes. Double jeopardy does not attach when a federal action is brought against a defendant already convicted in a state for a violation of one of the state's laws. *See* Abbate v. United States, 359 U.S. 187 (1959) (double jeopardy principle not invoked when defendants were prosecuted under state law for conspiring to injure or destroy the property of another and subsequently under federal law for conspiring to destroy "coaxial repeater stations and micro-wave towers" by using dynamite to destroy telephone facilities); People v. Bryant, 699 N.E.2d 910 (N.Y. 1998) (concurrent jurisdiction principles apply in case of bank robbery where federal government prosecuted for bank robbery, use of weapons to place people in jeopardy, conspiracy, and use and possession of weapons and the state prosecuted for attempted murder of an on-duty police officer and knowing possession of defaced firearms). This concept has also been extended to successive prosecutions in multiple states. *See, e.g.*, Heath v. Alabama, 474 U.S. 82 (1985).

134. *See infra* text accompanying notes 159, 163-68.

regulate or impose jurisdiction over all Internet activity,[135] nor do states want such a responsibility. States do not want to become general "Internet police" because they have no vested interest in crimes that have both causation and consequences that take place outside their state borders.

The federal government has legislated in the area of computer and Internet crime for more than a decade for two main reasons: 1) the interstate nature or governmentally-related aspects of various computer-related crimes prompting exclusive federal action;[136] and 2) the discrepancy in ability between the state and federal sectors to prosecute technology-related crimes, resulting in primarily federal prosecutions.[137] In the Senate Report[138] for the Computer Fraud and Abuse Act,[139] the Judiciary Committee identified the crimes in which it has an interest and chose not to pursue all computer-related offenses. The Report specifically stated that the government "prefers instead to limit Federal jurisdiction over computer crime to those cases in which there is a compelling Federal interest, i.e., where computers of the Federal government or certain financial institutions are involved, or where the *crime itself* is interstate in nature."[140]

The second factor, the discrepancy between state and federal ability to prosecute, was addressed in the Senate Report, and the Committee discussed the opposing viewpoints. On one hand, the Committee considered "that[ ] because some States lack comprehensive computer crime statutes of their own, the Congress should enact as sweeping a federal statute as possible so that no computer crime is potentially uncovered."[141] This idea was rejected, however, and a more reserved approach was chosen. The Committee developed the Act instead, so that it

135. Taxation and gambling pose special problems that Congress is currently wrestling with. For discussion *see* Walter Hellerstein, *State and Local Taxation of Electronic Commerce: Reflections on the Emerging Issues*, 52 U. MIAMI L. REV. 691 (1998); John Edmund Hogan, *World Wide Wager: The Feasibility of Internet Gambling Regulation*, 8 SETON HALL CONST. L.J. 815 (1998).

136. *See* S. REP. No. 99-432, at 1 (1986), *reprinted in* 1986 U.S.C.C.A.N. 2479.

137. *See id.* at 2.

138. *See* S. REP. No. 99-432 (1986), *reprinted in* 1986 U.S.C.C.A.N. 2479.

139. 18 U.S.C. § 1030 (1994).

140. S. REP. No. 99-432, *reprinted in* 1986 U.S.C.C.A.N 2479.

141. S. REP. No. 99-432, at 2 (1986), *reprinted in* 1986 U.S.C.C.A.N. 2479 (emphasis added).

"strikes the appropriate balance between the Federal Government's interest in computer crime and the interests and abilities of the States to proscribe and punish such offenses."[142]

This balance is no longer at issue in today's criminal legal system, and as such, the Computer Fraud and Abuse Act cannot legitimately be used by the federal government to assert jurisdiction over just any computer crime. The government would rather "limit federal jurisdiction over computer crime to those cases in which there is a compelling federal interest."[143] The federal government should limit itself to situations where computers of the federal government or certain financial institutions are involved, or where the crime itself is interstate in nature.[144] The crime itself should be interstate in nature, rather than a crime that only involves an interstate instrument during the course of the crime's commission. "[T]he manner in which the communication facility operates does not determine the outcome. In evaluating the assertion of federal jurisdiction, the focus should be on the location of the communicating parties."[145] This would reduce the number of federal prosecutions significantly and allow states to prosecute crimes which they prosecuted prior to the use of technology in criminal acts.

In addition to the number of crimes that can be turned over to the states because of decreased federal interest, states now also have the ability to investigate and prosecute Internet offenses. Currently, all states except Vermont have penal statutes specifically targeting computer crime, and prosecution of technology crimes by state agencies has become more commonplace.[146] As a result, the lack of experience in technology-related prosecution is no longer a valid reason for the federal government to retain exclusive possession of the right to proceed against such offenders. Based on the legislative statement of the Computer Fraud and Abuse Act, the federal government should rely on the Act only to assert jurisdiction in the very limited situation where a federal computer is affected. The two

142. *Id.* at 2.

143. S. REP. NO. 99-432, at 1 (1986), *reprinted in* 1986 U.S.C.C.A.N. 2479.

144. *See id.* at 2.

145. United States v. Paredes, 950 F. Supp. 584, 589 n.8 (S.D.N.Y. 1996). *See* discussion *infra* notes 147-57 and accompanying text.

146. *See, e.g.*, CAL. PENAL CODE § 502 (Deering 1999); TEX. PENAL CODE ANN. § 33.01-.05 (West 1998); VA. CODE ANN. § 18.2-152.1-.15 (Michie 1998).

main reasons stated in the legislative intent, including lack of state resources and greater federal interest, are now moot. Therefore, the states should satisfactorily rely upon the Dormant Commerce Clause to prosecute Internet and computer related offenders.

C. *New York State as a Model for State Jurisdiction*

States are now able to successfully prosecute Internet-related crimes on their own, and the courts in New York are paving the way. The state that brought *American Library Ass'n v. Pataki* to the forefront of Internet-related criminal law softened the effect of the case since both federal district courts and state supreme courts are now straying from the idea of exclusive federal dominion in this area. These courts currently acknowledge that as computer and Internet technology expand, the federal government's exclusive grip on regulation of related criminal activity must be loosened. Therefore, the courts in New York should be looked to as a model for future Internet prosecution. The expansion of technology should take our present existence and make it easier. However, the federal government, by deeming most forms of modern technology interstate in nature, has assumed control over crimes which otherwise would have been completely within state jurisdiction. The New York courts are now taking the rights of the state back into their own courtrooms.

Ironically, a federal district court in the Southern District of New York was the first to become aware of the potential problem with federal dominion over a case which, but for a technological facet, would be in state court. In *United States v. Paredes*,[147] the defendant appealed his indictment under the federal murder-for-hire statute[148] by questioning the interstate

147. 950 F. Supp. 584 (S.D.N.Y. 1996), *aff'd on other grounds*, 162 F.3d 1149 (2d Cir. 1998); *but see* United States v. Stevens, 842 F. Supp. 96 (S.D.N.Y. 1994) (intent to have communication be interstate in nature is not necessary for federal prosecution for criminal activities requiring interstate nexus).

148. *See Paredes*, 950 F. Supp. at 585 (quoting in pertinent part):

> Whoever . . . uses or causes another (including the intended victim) to use the mail or any facility in interstate or foreign commerce, with intent that a murder be committed in violation of the laws of any State or the United States . . . shall be fined under this title or imprisoned for not more than ten years, or both.

nature of communications via a paging system.[149] The district court held that a statutory interstate nexus requirement was not satisfied in this situation because the communications in question between government agents and the defendant all took place within the jurisdictional confines of New York State,[150] regardless of the fact that the paging system has the capability of locating individuals in other states.[151]

This holding is most relevant in situations where the sending and receipt of Internet communications are solely intrastate. However, Judge Scheindlin issued a broader statement which is applicable to any offense which, but for the technology used as an instrumentality, would have been an offense against the state and not the federal government.[152] Judge Scheindlin warned that if the current trend of technological evolution continues, the federal government would be able to prosecute types of crimes from which it was barred in recent years, thus expanding the jurisdiction of the federal government to surpass that originally contemplated by the framers of the Constitution, who feared an excessively centralized government.[153]

> The spread of innovative interstate communications technology, combined with this interpretation of the interstate nexus requirement, sweeps within the province of federal jurisdiction crimes previously considered to be entirely local in nature. In enacting § 1958, [the Federal murder-for-hire statute], Congress's expressed intent was to provide a statutory mechanism for prosecuting "crimes with interstate features." That a defendant who never traveled from one state to another, conducted an interstate transaction, or communicated across state lines could now be prosecuted under this Act because of the evolution in communications technology runs against the grain of the statute's legislative history.[154]

Judge Scheindlin further stated that decisions such as *Paredes* must always be decided mindful of both the precedent

---

18 U.S.C. § 1958 (1994).

149. *See Paredes,* 950 F. Supp. at 586.

150. *See id.* at 590.

151. *See id.*

152. *See id.*

153. *See* 18 U.S.C. § 1958 (1994).

154. United States v. Paredes, 950 F. Supp. 584, 588 (S.D.N.Y. 1996), *aff'd on other grounds,* 162 F.3d 1149 (2d Cir. 1998).

regarding state police power as set forth in *United States v. Lopez*,[155] and the influx of modern technology's usage in both peaceful and criminal endeavors.[156] In very insightful dicta, the court noted that:

> Intrastate communications have taken on an interstate quality because of the means by which beepers, cellular phones, *email* [sic] and telephones function. It is very likely that in the near future all electronic forms of communication will be transmitted across state lines regardless of the location of the communicating parties. As the original role of federal criminal jurisdiction was intended to be limited in nature, it is troubling to permit technological innovation to significantly expand its scope without a specific expression of Congressional intent. The weakest link in the government's argument is its failure to set reasonable bounds on federal criminal jurisdiction. Under the government's theory, an email [sic] sent from the kitchen to the office down the road might implicate federal jurisdiction simply because the electronic message was transmitted from a computer in New York to a computer in New Jersey before reaching its final destination.[157]

With *Paredes* as a breakthrough, the state courts began to preside over litigation of Internet related crimes via its authority under the Dormant Commerce Clause. Although the Internet has no geographic boundaries,[158] states like New York have exercised, and should continue to successfully exercise, jurisdiction via criminal jurisdiction statutes because of the states' interest, and in some cases, better ability,[159] to apprehend and prosecute Internet criminals who choose to commit

---

155. 514 U.S. 549 (1995).

156. *See Paredes*, 950 F. Supp. at 589.

157. *Id.* (emphasis added).

158. This is of debate in the courts, however, as they struggle with the notion of jurisdiction. In *American Library Ass'n v. Pataki*, 969 F. Supp. 160, 169 (S.D.N.Y. 1997), Judge Preska stated, "Typically, states' jurisdictional limits are related to geography; geography, however, is a virtually meaningless construct on the Internet." This directly contradicts the earlier decision in *Reno v. ACLU*, 521 U.S. 844 (1997), which, while discussing the fundamental differences between the real and virtual worlds in terms of limiting access to certain web sites deemed harmful to children, asserts that "[c]yberspace undeniably reflects some form of geography: chat rooms and Web sites, for example, exist at fixed 'locations' on the Internet." *Id.* at 890.

159. Local officials may have a better rapport with local Internet Service Providers and other investigatory resources because of their involvement with community outreach programs or frequent assistance with investigations and prosecutions.

some element of an actual or attempted crime which has significant ramifications affecting the citizenry of a state.

Although *Paredes* is most significant as a precedent for New York courts in situations where both the criminal and the victim are located in the same state, later New York case law has also established jurisdictional sufficiency when the alleged criminal activity has only one element - a cause, effect or intent of either - within the boundaries of the state. Like many other states, New York has several statutes encompassing Internet-related crimes, including the most controversial pedophilia[160] and child pornography[161] statutes, the focus of the most significant and recent Internet-related litigation.[162] These statutes are fundamentally based on two areas of New York's criminal procedure law, one pertaining to general geographic jurisdiction of offenses,[163] and one asserting jurisdiction over Internet and computer related crimes.[164] Under New York Criminal Procedure Law § 20.20, the state generally retains jurisdiction over offenses in which:

(1) Conduct occurring within a state establishes an element of the offense, an attempt, or a conspiracy to commit the offense;[165] or
(2) no conduct occurred in the state, but the offense's result was in-state, the effect was intended to be felt in the state, or attempt of conspiracy was meant to be in-state;[166] or
(3) there was a crime of omission with effect in the state, whether or not the offender is physically present in the state.[167]

Under § 20.60 "[a] person who causes by any means the use of a computer or computer service in one jurisdiction from another

160. *See* N.Y. PENAL LAW § 235.20-.24 (McKinney 1997).
161. *See* N.Y. PENAL LAW § 263.00-.25 (McKinney 1997).
162. *See* N.Y. PENAL LAW § 156.00-.50 (McKinney 1997) (identifying additional computer and Internet related statutes, i.e., unauthorized use of a computer, unlawful duplication of computer related material, computer possession of computer related material, computer tampering, and computer trespass).
163. *See* N.Y. CRIM. PROC. § 20.20 (McKinney 1997).
164. *See* N.Y. CRIM. PROC. § 20.60 (McKinney 1997).
165. *See* N.Y. CRIM. PROC. § 20.20-.20(1) (McKinney 1997).
166. *See* § 20.20(2).
167. *See* § 20.20(3).

jurisdiction is deemed to have personally used the computer or computer service in each jurisdiction."[168] This statute takes computer and Internet crime out of the virtual world, and places it in a tangible location.

One year after *Paredes*, *People v. Barrows*[169] was decided in Kings County, New York, upholding the indictment of James Barrows. Barrows, a Connecticut resident, was indicted on one count of promoting an obscene sexual performance by a child[170] and two counts of first-degree attempted dissemination of indecent material to minors,[171] after he used the Internet to arrange a meeting with an undercover agent whom Barrows believed to be a thirteen year-old girl.[172] On appeal, the indictment was upheld and the court directly rejected Barrow's contention that the statute was a violation of the First Amendment[173] and the Commerce Clause.[174]

The Commerce Clause argument was rejected because the defendant purposefully attempted to lure a child for sexual acts within New York State.[175] The *Barrows* court examined the *American Library Ass'n v. Pataki* decision[176] and distinguished the *Barrows* fact-pattern. In striking down a portion of the New York Penal Law, the plaintiffs in *American Library Ass'n* did

168. N.Y. CRIM. PROC. § 20.60-.60(3) (McKinney 1997).

169. 664 N.Y.S.2d 410 (Sup. Ct. Kings County 1997).

170. N.Y. PENAL LAW § 263.10 (McKinney 1997).

171. N.Y. PENAL LAW § 235.22 (McKinney 1997). This is only an attempt crime since the recipient was not a minor, but an investigator posing as one.

172. *See* People v. Barrows, 664 N.Y.S.2d 410, 411-12 (Sup. Ct. Kings County 1997). Defendant James Barrows, a Connecticut resident, aged 39, was a subscriber of America Online, an Internet Service Provider, and used the screen name (Internet alias) "Captain Jack." With this alias, he "met" "Tori 83," a male undercover agent posing as a thirteen year-old female, and sent "her" an instant message asking her if she preferred "older men." The two engaged in several such "real time" chats and also exchanged e-mail that had attachments containing obscene images. The conversations were sexually explicit in nature, even though Barrows frequently acknowledged that what he was engaging in was illegal. The Internet contacts and a telephone call culminated in a meeting at a boat marina in Brooklyn, New York, where Barrows was arrested. A search of his car resulted in seizure of various pornographic magazines and computer diskettes, in addition to various items that were revealed by Barrows to be used to tie up a sexual partner.

173. *See id.* at 412. The First Amendment free speech challenge was rejected because "[s]tates are entitled to greater leeway in the regulation of pornographic depictions of children." New York v. Ferber, 458 U.S. 747, 756 (1982).

174. *See Barrows*, 664 N.Y.S.2d at 412-13.

175. *See id.*

176. *See* discussion *supra* text accompanying notes 93-97.

not challenge the portions of the statute which penalize those who transmit obscene material to children or lure children for sexual acts.[177] Instead, the plaintiffs only argued that the statute as it existed unconstitutionally subjected residents of other states to New York State laws, even when these other residents do not interact with any state residents.[178] This distinction meant that the *Barrows* court was not compelled to follow *American Library Ass'n* and could uphold Penal Law § 235.22 as constitutional under a Commerce Clause analysis.[179] New York's police power ultimately prevailed. In the court's opinion, "[t]he State of New York should have the power to punish anyone who sends sexually explicit material over the Internet to a minor in New York and then seeks to lure that child to perform a sexual act within the State."[180] However, the regulation of Internet communications alone would not have withstood the court's scrutiny under the tenets established in *American Library Ass'n.*[181]

The *Barrows* indictment led to a jury conviction which was reversed in part on First Amendment grounds and Commerce Clause violations.[182] Count Seven, involving the defendant's graphic descriptions of acts he desired to perform on the undercover agent and explicit instructions for acts the undercover agent was to perform on herself,[183] was dismissed under a free speech analysis.[184] The court felt that the suggestions made by the defendant constituted "mere words" and "pure speech" and was therefore subject to *Reno*.[185] This analysis rendered § 235.22 vague, as it has the potential to limit the speech between adults on the Internet, an article of interstate commerce.[186] The count was therefore dismissed and the statute was deemed unconstitutional via a First Amendment and Commerce Clause analysis.

177. *See* American Library Ass'n v. Pataki, 969 F. Supp. 160, 179 (S.D.N.Y. 1997); *see also* Barrows, 664 N.Y.S.2d at 413.
178. *See American Library Ass'n*, 969 F. Supp. at 177.
179. *See Barrows*, 664 N.Y.S.2d at 413.
180. *Id.*
181. *See id.*
182. *See* People v. Barrows, 677 N.Y.S.2d 672 (Sup. Ct. Kings County 1998).
183. *See id.* at 676.
184. *See id.* at 685.
185. *See id.*
186. *See Barrows*, 677 N.Y.S.2d at 685.

Count Eight, entering New York to engage in sexual activity with a minor, was also dismissed on First Amendment grounds.[187] The court emphasized that although there were First Amendment violations, the count was *not* in violation of the Commerce Clause, and in fact "the constraints of [the] Commerce Clause do not apply."[188] Barrows' purposeful act evinced his intent to commit a sexual offense[189] within the State of New York[190] under Article 130 of the Penal Law,[191] so neither preemption nor Commerce Clause/extraterritoriality[192] violations existed.[193] "Defendant's repeated concerns that he would 'go to jail' for engaging in such activity indicates that he was well aware that what he was proposing to [the undercover agent] was illegal, as well as immoral."[194]

Even though Barrows' conviction under Counts Seven and Eight were reversed,[195] the Commerce Clause violations were hand-in-hand with the First Amendment violations. Despite the reversal, *Barrows* is still significant under a Dormant Commerce Clause analysis. What has still survived is the proposition that states may regulate Internet activities in conformance with their police power if they do not burden free speech while doing so. The continued belief that Barrows was subjected to New York laws based on his intentional targeting of a New York citizen is chipping away at the credibility of *American Library Ass'n v. Pataki.*[196]

---

187. *See id.* at 686.

188. *Id.* at 685-86.

189. "Had Tori 83 actually been a thirteen-year-old girl, the probable outcome of Defendant's meeting with her requires little speculation." *Barrows*, 677 N.Y.S.2d at 681.

190. *See id.* at 685.

191. *See* N.Y. PENAL LAW § 130.00-.85 (McKinney 1997).

192. *See Barrows*, 677 N.Y.S.2d at 686.

193. *See id.*

194. *Barrows,* 677 N.Y.S.2d at 685.

195. *See Barrows*, 677 N.Y.S.2d at 685. Count One was upheld for "Promoting an Obscene Sexual Performance by a Child" under Penal Law § 263.10.

196. 969 F. Supp. 160 (S.D.N.Y. 1997). *See supra* notes 89-98 and accompanying text. Additionally, People v. Gilmour, 678 N.Y.S.2d 436 (Sup. Ct. Richmond County 1998), distinguished itself from *American Library Ass'n* when it held that the Internet is a satisfactory investigative tool within the parameters of the Dormant Commerce Clause. *See id.* at 441.

People v. Lipsitz[197] illustrates how New York State, using an approach similar to those in *Barrows* and *Paredes,* minimizes the interstate character of Internet communications for prosecution of consumer fraud cases.[198] *Lipsitz* involved a consumer fraud prosecution by the New York State Attorney General's Office.[199] In that case, Lipsitz utilized e-mail solicitations for the online sale of magazine subscriptions and either never delivered the subscriptions or began delivering them halfway through the subscription period.[200] Lipsitz was convicted on an *in personam* jurisdiction theory since he himself solicited the sales from a business in Staten Island, New York,[201] and utilized "an independent 'host' source" to target New York customers.[202]

By engaging in an *in personam* jurisdiction analysis of "minimum contacts" paralleling other types of civil litigation, the state maintained jurisdiction notwithstanding the Internet communications.[203] The *Lipsitz* court held that "for Internet consumer fraud claims, the Internet medium is essentially irrelevant, for the focus is primarily upon the location of the mes-

197. 663 N.Y.S.2d 468 (Sup. Ct. N.Y. County 1997).

198. In October 1998, Congress enacted "The Children's Online Privacy Protection Act of 1998." This Act, designed to protect the identity and safety of children who use the Internet, was drafted to permit the States' Attorney General, under section 1305, in cases in which he or she

> has reason to believe that an interest of the residents of that State has been or is threatened or adversely affected by the engagement of any person in a practice that violates any regulation of the Commission prescribed under section 1303(b), the State, as *parens patriae*, may bring a civil action on behalf of the residents of the State in a district court of the United States of appropriate jurisdiction, to –
>
> (A) enjoin that practice;
>
> (B) enforce compliance with the regulation;
>
> (C) obtain damage, restitution, or other compensation on behalf of residents of the State; or
>
> (D) obtain such other relief as the court may consider to be appropriate."

H.R. CONF. REP. 105-825, 105th Cong. (1998).

199. *See Lipsitz*, 663 N.Y.S.2d at 472 (noting that New York's consumer protection laws are modeled after the Federal Trade Commission Act and "are similar to consumer fraud, deceptive sales practices and consumer protection law of other states."). *See also* N.Y. GEN. BUS. LAW Art. 22-A (McKinney 1998 & Supp.1999).

200. *See Lipsitz*, 663 N.Y.S.2d at 471.

201. *See id.*

202. *See id.* at 474.

203. *Id.*

senger and whether the messenger delivered what was purchased."[204] There, the court emphasized that the "entire enterprise was firmly based in New York State."[205] In *Paredes*, the court acknowledged that a paging system may be interstate in nature at times, as is true with the Internet.[206] However, *Lipsitz* also acknowledged the intrastate nature of the Internet when, in that case, there was a New York resident targeting residents of the same state.[207]

The court further held that actions brought by the New York State Attorney General are not limited to prosecutions for harm inflicted upon residents of New York State.[208] Out-of-state complainants victimized by New York State residents are also offered recourse because the Attorney General has the authority to "restrain illegal business practice by a local business . . . notwithstanding that these practices occur on the Internet."[209] In this respect, the concept of interstate commerce is deemed irrelevant for consumer protection claims against a New York State resident by the Attorney General.

The *Lipsitz* court analyzed how its decision impacts interstate commerce, given the designation of Internet communications as articles of interstate commerce by *American Library Ass'n v. Pataki*,[210] and it rejected any contention that the Internet aspect of this case affected the decision.[211] The court examined the role of consumer protection laws as a regulator of local businesses, not as a prosecutor of businesses which act outside of the state borders, even in an indirect fashion.[212] By looking at the case from this perspective, the court saw no different issues presented in the *Lipsitz* fact-pattern.[213]

> There is no compelling reason to find that local legal officials must take a "hands off" approach just because a crook or con artist is technologically sophisticated enough to sell on the Internet. Invo-

204. *Id.*
205. *Lipsitz*, 663 N.Y.S.2d at 474.
206. *See Paredes*, 950 F. Supp. at 587-88.
207. *See id.*
208. *See Lipsitz*, 663 N.Y.S.2d at 474.
209. *Id.*
210. *See supra* text accompanying notes 89-98.
211. *See Lipsitz*, 663 N.Y.S.2d at 474-75.
212. *See id.* at 475.
213. *See id.*

> cation of "the Internet" is not the equivalent to a cry of "sanctuary" upon a criminal's entry into a medieval church. It should be sufficient that the laws sought to be applied, even if they might tangentially implicate interstate commerce, are "media neutral" and otherwise pass constitutional muster.[214]

The cases from New York State since *American Library Ass'n*, including *Paredes*, *Barrows*, and *Lipsitz,* are defying the federal government and giving jurisdictional power back to the states. These courts do not let the particulars of technology detract from the cases presented before them. There are actual victims who, but for the modern criminal and his methods, would not be in federal court.

V. Conclusion

Internet communications are labeled by the federal government as articles of interstate commerce,[215] and as such, must be regulated by Congress under the Commerce Clause.[216] The Information Superhighway is likened to a paved highway,[217] which is unquestionably regulated by the federal government.[218] However, the Information Superhighway offers valuable distinctions[219] and blurs the analogy sufficiently to justify reanalyzing the federal government's exclusive dominion and control over the implementation of related penal laws and ensuing prosecutions. Internet crime is only going to rise in the coming years as technology becomes even more involved in our daily lives. If the federal courts continue to claim exclusive jurisdiction based on a Commerce Clause theory over any crime in which the Internet is utilized, there will be a significant reduction in the prosecutorial ability of the states and a weakening of their police power, leaving states virtually paralyzed as crimes increasingly involve technology.

The federal government, at this point in time, is overstepping the very authority it granted to itself. Congress stated in

---

214. *Id.*
215. *See supra* text accompanying notes 70-88.
216. *See supra* text accompanying notes 54-59.
217. *See supra* notes and accompanying text at 48-50.
218. *See supra* notes 72-73 and accompanying text.
219. *See supra* text accompanying notes 51-53.

the Computer Fraud and Abuse Act[220] that the federal government does not want to prosecute all computer crimes;[221] rather it is only interested in pursuing those that affect the government specifically[222] for crimes where the state is unable to prosecute because of a lack of resources.[223] This is no longer a problem,[224] and yet, under a Commerce Clause theory, the federal government continues to pursue Internet criminals which would otherwise be subject to state prosecutions. The federal government must loosen its grasp, re-evaluate its rationale for pursuing crimes of this nature, and permit states to prosecute either alone or jointly with it.[225] The states must be given latitude under the Dormant Commerce Clause to develop their own methods for exercising police power over Internet activities.

United States v. Paredes[226] offers a valid warning of the dangers of federal prosecution of technology-related crimes,[227] and New York State provides a chain of cases[228] offering viable solutions for state jurisdiction that comport with the Commerce Clause and Due Process. In *Paredes*, a federal court realized the flaws in the very statutes it is meant to enforce,[229] and it was only a matter of time before state courts followed suit. This trend may very well continue into the future, and in time, the impact of *American Library Ass'n* will be lessened even more as the states learn to more effectively utilize the Dormant Commerce Clause and the police power it confers.

There is nothing intrinsically wrong with federal legislation. In fact, in certain situations, it is vital.[230] However, technology is advancing so rapidly that if the federal government continues to prosecute any crime with a technological aspect,

220. 18 U.S.C. § 1030 (1994).

221. *See supra* text accompanying notes 138-40.

222. *See supra* text accompanying notes 136, 140.

223. *See supra* text accompanying note 137.

224. *See supra* text accompanying note 146.

225. *See supra* text accompanying notes 133-35.

226. 950 F. Supp. 584 (S.D.N.Y. 1996); *see supra* notes 147-57 and accompanying text.

227. *See supra* text accompanying note 157.

228. *See supra* text accompanying notes 169-214.

229. *See supra* text accompanying notes 152-54.

230. *See* Computer Fraud and Abuse Act, discussed *supra* at notes 136-40 and accompanying text, which is designed primarily to protect computers belonging to the federal government and financial institutions.

and therefore interstate features, the states will have no police power left. Consequently, the United States could become the centralized society from which the colonists fled and upon which the Framers reflected when they established a government composed of federal and state systems. The line must be drawn clearly before this occurs. States cannot lose police power while a criminal commits crimes more conveniently and covertly under the guise of a domain name or e-mail address.

*Laura Ann Forbes**

* The author is a member of the Class of 2000 from Pace University School of Law in White Plains, New York. She extends gratitude to her family for their support, the staff of PACE LAW REVIEW for encouragement, guidance, and editing, and the prosecutors and investigators of the High Technology Crimes Bureau of the Office of the District Attorney, Westchester County, New York, for their dedication to the cause of state prosecution and inspiration for this article.