Destination Unknown: Does the Internet's Lack of Physical Situs Preclude State and Federal Attempts to Regulate It

Christopher S.W. Blake

Follow this and additional works at: https://engagedscholarship.csuohio.edu/clevstlrev

Part of the Jurisdiction Commons, and the Science and Technology Law Commons

How does access to this work benefit you? Let us know!

Recommended Citation

This Note is brought to you for free and open access by the Law Journals at EngagedScholarship@CSU. It has been accepted for inclusion in Cleveland State Law Review by an authorized editor of EngagedScholarship@CSU. For more information, please contact library.es@csuohio.edu.
DESTINATION UNKNOWN: DOES THE INTERNET'S LACK OF PHYSICAL SITUS PRECLUDE STATE AND FEDERAL ATTEMPTS TO REGULATE IT?

I. INTRODUCTION .................................. 129

II. MAPPING OUT THE INTERNET ....................... 131
    A. Internet Addresses ................................ 131
    B. Modes of Communication .......................... 132
    C. The Way Information Travels ...................... 134

III. PROBLEMS WITH PERSONAL JURISDICTIONAL .......... 134

IV. STATE REGULATION: LACK OF SITUS A STUMBLING BLOCK .... 138
    A. The Dormant Commerce Clause .................... 139
    B. Internet Characteristics Fit with Commerce
        Clause Violation .................................. 141
    C. American Libraries Association v. Pataki: Its
        Commerce Clause Application and Ramifications .. 142
    D. ACLU v. Miller: A Hypothetical Example ........... 144
    E. People v. Lipsitz: Limitations to Commerce
        Clause Application? .................................. 146

V. FEDERAL REGULATION: ZONING WITHOUT ZONES .......... 149
    A. ACLU v. Reno: Justice O'Connor's Prognosis
        for the CDA's "Zoning" Motive ...................... 150
    B. The First Amendment's Time, Place, Manner
        Analysis Applied to Internet Technology .......... 151
    C. Government's Hands-Off Approach .................. 155

VI. SELF-REGULATION: A THIRD VIABLE OPTION? ........... 156

VII. CONCLUSION ..................................... 157

I. INTRODUCTION

Between June 20 and June 27, 1997, federal and state courts handed down four decisions that could crucially impact the future of Internet content regulation.¹ The cases include the controversial United States Supreme Court case ACLU v. Reno, which struck down most of the federal government’s

Communications Decency Act. Three of the rulings invalidated laws that directly regulated the Internet, while one decision upheld use of a pre-existing law to regulate Internet activity.

In each case, the judges openly pondered how to harness the Internet or even whether to harness it, citing its geographical vagueness as a factor that complicates the question. Their opinions ran the gamut. In the stead of any consensus, state and federal legislators continue their attempts to restrain the world's "information superhighway." Should any governmental body be able to regulate the Internet? Due to its unorthodox ignorance of geography, a concept important to many court cases, can any such body regulate the Internet?

This Note summarizes recent tests of state and federal Internet content regulations and analyzes the impact the Internet's incompatibility with "real space" geography had or might have had on the courts' reasoning. To some extent, it posits what problems the incompatibility poses for impending legislation. In the midst of such discussion, this Note opines that state and federal regulations of the Internet could conceivably both fail Constitutional muster, due specifically to the "Net's" physical shortcomings.

Part II of this Note offers a background of the Internet's different communication capacities and describes its conflicts with geography. Part III summarizes the courts' problems in deciding whether they have personal jurisdiction over specific Internet activities.

Part IV briefly outlines arguments for and against state regulation of the Internet. First, it capsulizes the U.S. Supreme Court's dormant Commerce Clause standards. Second, it summarizes one federal court's application of those standards to invalidate a state Internet content law. Third, it applies the standards to another state law case. Finally, it uses a third case to weigh possible limitations to dormant Commerce Clause invalidations of laws that restrict content on the Internet.


3Reno, 117 S. Ct. at 2329; Pataki, 969 F. Supp. at 160; Miller, 977 F. Supp. at 1228. Lipsitz, 663 N.Y.S.2d at 468 (applied consumer fraud protection statute to Internet usage situation).

4See Reno, 117 S. Ct. at 2343, 2353; Pataki, 969 F. Supp. at 169; Miller, 977 F. Supp. at 1228; Lipsitz, 663 N.Y.S.2d at 474.

5"Information superhighway" is a term for the Internet often used by Vice President Al Gore. For an interesting branch-off on the highway, see LANCE ROSE, NETLAW: YOUR RIGHTS IN THE ONLINE WORLD 170-71 (1995).

6The "net" is a common slang name for the Internet, used so much that a 1994 movie of that name starring Sandra Bullock played off the double entendre. See also Lawrence Lessig, Constitution and Code, 27 CUMB. L. REV. 1, 10 (1990).
Part V looks at federal regulation of the Internet. It first details U.S. Supreme Court Justice Sandra Day O'Connor's concurring opinion in ACLU v. Reno, in which she hints at zoning the Internet. It then applies a First Amendment zoning test to the content prohibited by the Communications Decency Act and other states. The Note concludes in Part VI with details of a third type of regulation, the Internet industry's self-regulation, and earmarks the industry efforts as the best way for regulation to proceed.

II. MAPPING OUT THE INTERNET

The Internet is at its most basic an international "network of networks." Its "chaotic, random structure" of more than 500,000 independent network computers connect to nine million host computers in ninety countries, making the information housed on those computers rapidly available to anyone with the correct computer software, a modem and an "Internet service provider" ("ISP"). It is by nature an unregulated medium, and no one entity completely controls it.

Despite the fact that so many people can access the Internet from so many places, the Internet operates largely contrary to the idea of geography. It has no geographically fixed point and, at this point, no borders. To some commentators, the medium—known to most as "cyberspace"—"virtually transcends geography." In fact, most of the concepts which a person uses to communicate on the Internet make it almost impossible to determine the physical location of an accessed resource or another user.

A. Internet Addresses

Although Internet communications are based on a seemingly geographical concept—addresses—most do not consistently mirror a geographical location. Instead, they provide a "logical" framework in which the information can travel.

7 *Pataki*, 969 F. Supp. at 164.
8 *Id.; Reno*, 117 S. Ct. at 2336.
10 *Reno*, 117 S. Ct. at 2336.
11 *See Pataki*, 969 F. Supp. at 167, 169.
12 *Id.* at 167.
13 *Reno*, 117 S. Ct. at 2335.
15 *Pataki*, 969 F. Supp. at 165.
In their most general form, the addresses—also called "domain names"—describe the type of organization a user is contacting.\textsuperscript{16} Addresses have several tiers, starting from the end of the address, that increase in specificity.\textsuperscript{17} For example, the designations such as "-.com" and "-.gov" ends many addresses; "-.com" signifies a person or entity working through a commercial user, while the "-.gov" designation ends the addresses of networks associated with the federal government.\textsuperscript{18} The complete address "jsmith@omega.csuohio.edu"\textsuperscript{19} might hint to the location of the information received. However, the address "pixie@geocities.com" does not, especially once it is known that Geocities, an ISP, offers Internet access to people in practically every state.\textsuperscript{20}

B. Modes of Communication

Most of the ways a "cybernaut"\textsuperscript{21} can communicate on the Internet rely on Internet addresses, and many of the modes have their own devices that can blur the location of communicators even more. One example is electronic mail ("e-mail"). "E-mail" software lets any user transmit an electronic message—conceptually equivalent to instant mail—to anyone who has another Internet address.\textsuperscript{22} As stated before, the addressee's actual location or even identity is rarely known. Users can create an e-mail alias\textsuperscript{23} or employ an

\begin{itemize}
\item\textsuperscript{16}Hearst Corp. v. Goldberger, No. 96 Civ. 3620, 1997 WL 97097, at *2 (S.D.N.Y. Feb. 26, 1997).
\item\textsuperscript{17}Lockheed Martin Corp. v. Network Solutions, Inc., 985 F. Supp. 949, 952-53 (C.D. Cal. 1997). Under a contract with the National Science Foundation, a company called Network Systems Inc. manages domain name registrations. Other top-level domain names include "-.org," for non-profit organizations; "-.edu," for educational institutions; "-.net," for among other things, networks. Registration is affordable: $100 for a start-up two-year contract, and $50 per year thereafter. Id. at 953.
\item Most Internet addresses have two "fungible" addresses: an alphanumeric domain name and also a numeric "internet protocol" such as "123.45.123.12." While both work equally as well, domain names have been the subject of court cases because of the familiarity that the names can have with users and consumers. See Hearst, 1997 WL 97097, at *2.
\item\textsuperscript{18}Lockheed Martin Corp., 985 F. Supp. at 952, 953.
\item\textsuperscript{19}For a detailed explanation of domain names, see also MTV Networks v. Curry, 867 F. Supp. 202, 203-204 n.2 (S.D.N.Y. 1994).
\item A "cybernaut" is a slang term for an Internet user. See Dan Burk, Federalism in Cyberspace, 28 CONN. L. REV. 1095, 1099 (1996).
\item\textsuperscript{22}Reno, 117 S. Ct. at 2337 n.20.
\end{itemize}
anonymous remailer\(^{24}\) to make their identity and location even more difficult to discern.

A user who communicates by subscribing to a "listserv"\(^{25}\) has no way of knowing the e-mail addresses or locations of other subscribers. A listserv automatically compiles messages sent to it by its members and mails out a "list" at the end of a certain period.\(^{26}\) Contributors to "newsgroups" give only their e-mail addresses.\(^{27}\) Newsgroups are monitored discussion lists that a person accesses through a fixed link.\(^{28}\)

Internet relay chat ("IRC")\(^{29}\) and file transfer protocol\(^{30}\) do not use addresses. IRC users participate in real-time discussions and identify themselves with any name of their choosing upon entering the chat.\(^{31}\) File transfer protocol users contact a host computer network and download files anonymously.\(^{32}\)

On the World Wide Web, "surfers"\(^{33}\) use addresses to reach information destinations, but can also bypass addresses entirely by using sometimes nondescript links to move from information site to information site.\(^{34}\) The "Web"\(^{35}\) consists of an innumerable collection of information-filled pages written in compatible languages that a user accesses with web "browser" software.\(^{36}\) Besides using known addresses, Web surfers move from site to site with the help of "hypertext links"\(^{37}\) or highlighted text on a Web page that, in the background computer language, connects the user to another Web site. The Web also houses "search engines,"\(^{38}\) which search the entire Web for sites containing certain words or phrases, and create links to those pages.

\(^{24}\)Id.

\(^{25}\)Shea, 930 F. Supp. at 927.

\(^{26}\)Id.

\(^{27}\)Id. See also JONATHAN ROSENBERG, CYBERLAW: THE LAW OF THE INTERNET 13 (1997).

\(^{28}\)Shea, 930 F. Supp. at 928.

\(^{29}\)Id.

\(^{30}\)Id.

\(^{31}\)Id. See also ROSE, supra note 5, at 14, 15.

\(^{32}\)Shea, 930 F. Supp. at 929.

\(^{33}\)Traveling along the World Wide Web from site to site is commonly called "surfing." See Reno, 117 S. Ct. at 2335.

\(^{34}\)Shea, 930 F. Supp. at 929.

\(^{35}\)Id. The "web" is a slang term for the World Wide Web.

\(^{36}\)Id.

\(^{37}\)ROSENBERG, supra note 27, at 9-11. See also Miller, 977 F. Supp. at 1230, 1232.

\(^{38}\)Shea, 930 F. Supp. at 929.
The Web also is popular because of the ease with which users can set up their informational sites. However, once "content provider" posts their content on the Internet, they cannot prevent that content from being accessed by anyone.39

C. The Way Information Travels

The transmission of information on the Internet from address to address does not normally follow a straight line. Instead, information is broken into "packets"40 and transmitted through any number of routes, as the capacity of an intermediary network allows. It reassembles at the final address.41 For example, e-mail messages sent from the headquarters of Exchangenet, an ISP in Cleveland, Ohio, to the National Aeronautics and Space Administration Lewis Research Center located in the same city normally travel through a server in Atlanta, Georgia.

To summarize, even with domain names or addresses, Internet users might not accurately know from where information has come nor to where they have sent it. Such a system lies contrary not only to geography, but to courts and laws.43 The inability to predict the location of a site one might visit, coupled with the inability of the site to prevent one's visit, could cause conflicts of opinion in state's ability to pass laws and courts' abilities to apply such laws, as discussed below.

III. Problems With Personal Jurisdictional

In the past few years, judges, as much as users, have grappled with the problem of the Internet sites' lack of discernable location—most basically when they have questioned whether to grant personal jurisdiction over an Internet user. For example, court opinions cross the gamut on what contact is enough for "minimum contacts"44 and what action constitutes "purposeful availment."45 Although one federal district court recently offered a set of

39Reno, 117 S. Ct. at 2336.
40Shea, 930 F. Supp. at 926.
41Id.
42For example, a message sent on February 1, 1998 went through the following servers and addresses: from core1-hssi8.ds3. cleveland.en.net (204.89.181.210), to 901.Hssi1-0.GW1.CLE1.ALTER.NET (137.39.144.17), to Fddi000.CR2.CLE1.Alter.Net (137.39.37.100), to 119.Hssi60.CR2.CH1.Alter.Net (137.39.58.178), to 312.atm10.br1.chi1.alter.net (137.39.13.105), to core3-hssi3 0.WillowSprings.mci.net (206.157.77.81), to bordercore2.Atlanta.mci.net (166.48.48.1), to oarnet-c-omci.Atlanta.mci.net (166.48.49.254), to oeb1-atm20. columbus.oar.net (199.18.202.11), to nasa-si2-2.cleveland.oar.net (199.18.105.234)m to 198.118.128.1, and finally to fw01.lerc.nasa.gov (139.88.145.14).
guidelines, they might be premature, since recent opinions continue to greatly conflict.

The Internet complicates the issue because it does not mesh well with the normal conventions for personal jurisdiction. Traditional notions of export/import, sending/receiving, and traveling—concepts that in the real world are relied upon to assert jurisdiction—do not apply to the Internet.47

The main struggle has been how to classify the Internet medium. One option is to compare the Internet to a national magazine,48 because it is accessible by anyone anywhere in the country, and not targeted at any residents in particular. Another recommendation is to compare Internet sites to national television shows, since they do not target specific audiences, and like television, users must take affirmative steps to access it.49

Such classifications, however, would impart almost a per se availment upon the people who provide the Internet's content, and would make irrelevant what kind and extent of contact providers had with the forum state.50 As before stated, content providers cannot prevent anyone from accessing their information anywhere once they upload that information onto the Internet.51 Courts have split on whether the classifications apply and whether Internet existence is enough for defendants to be hauled into court.52

One state court recently reasoned in a case against a corporation that, by its invitation to United States users to download images, the company "is causing and contributing to ... distribution within the United States."53 Mere advertising without purposeful contacts with a certain state is enough for personal jurisdiction, because the appearance of the user’s information on the Internet "indicates a defendant's intent to serve the market in that state. . . . Defendants who know their message will be broadcast in this state are subject to suit here."54 A federal court ruled for personal jurisdiction merely on future contacts: "Defendant has obtained the website for the purpose of and in

47State Indictment of Internet Casino Highlights Online Jurisdiction, 66 USLW 2054, 2055 (1997) [hereinafter Internet Casino].
49Reno, 117 S. Ct. at 2336, 2345.
50See International Shoe, 326 U.S. at 316; see Hanson, 357 U.S. at 253.
51Reno, 117 S. Ct. at 2334.
52See infra notes 52-70.
54Id. (citing Asahi Metal Indus. Co. v. Superior Court of California, 480 U.S. 102, 112 (1987)). See also Quality Solutions, Inc. v. Henry Zupac, 993 F. Supp. 621 (N.D. Ohio 1997) (Defendants were subject to personal jurisdiction when they ran an Internet site accessible in Ohio and advertised in trade journal with large Ohio circulation).
anticipation that internet users, searching the internet for websites, will access the defendant's website and eventually sign up on the defendant's mailing list. Its intent is to reach all internet users, regardless of location.  

A seemingly larger number of courts, however, have decided to require more than an Internet content provider's "purposeful availment" to bring the provider into the court's jurisdiction.

A finding of personal jurisdiction in [a state] based on an Internet web site would mean that there would be nationwide (indeed, worldwide) personal jurisdiction over anyone and everyone who establishes an Internet web site. Such nationwide jurisdiction is not consistent with traditional personal jurisdiction case law nor acceptable to the Court as a matter of policy. Instead, the courts suggest that a ruling of personal jurisdiction should depend upon a showing of some kind of active pursuit of contacts with the forum in question. E-mail messages to an Internet service provider in the forum state satisfy the test. Other examples include providing a toll-free number with the Internet content in question; soliciting contributions; providing an e-mail address to which interested parties can write for more information; and providing a prompt connected to the site so that those interested parties can sign up for a mailing list subscribe to the service, or order merchandise. However, the line between passive and active availment blurred in a recent case, as evidenced by a Missouri state court's recent injunction against a gamb-

Missouri prohibits gambling anywhere other than at state-approved riverboat casinos. The ruling judge banned the Internet company from operating, marketing, offering or promoting a gambling establishment in the state, based on the fact that the company held two accounts opened by Missourians. Both accounts were opened by state investigators.

A Kansas federal district court recently posited a balancing rule to reconcile the conflicting cases. "[T]he likelihood that personal jurisdiction can be constitutionally exercised is directly proportionate to the nature and quality of commercial activity that an entity conducts over the Internet," its opinion said. "This sliding scale is consistent with well developed personal jurisdiction principles." While the balancing rule merits serious consideration, the Internet holds forth questions regarding personal jurisdiction that have yet to be evaluated. Courts have not discussed notions of unfairness and undue burden on novice internet content providers versus commercial providers, nor have they tested jurisdiction of Internet areas more vague than the Web, such as IRCs, newsgroups and listservs. Courts also have spoken little of personal jurisdiction in criminal trials, which could become a factor as more and more states pass legislation criminalizing some pornographic aspects of the Internet. Foremost, despite the conflicting talk and attempt at resolution, the question of exactly where transactions take place when they occur on the Web does not have a clear answer.

---

66 Id.
67 Id.
68 Id.
69 SF Hotel Co., 985 F. Supp. at 1034.
70 Id. "A passive Web site that does little more than make information available to those who are interested in it is not grounds for the exercise of personal jurisdiction." Id.
71 Id.
72 See Pataki, 969 F. Supp. at 171.
73 See Zeran v. America Online, Inc., 129 F.3d 327, 328 (4th Cir. 1997). AOL users can communicate publicly by posting messages on the ISP's "bulletin boards." Zeran filed a negligence suit against AOL based on information posted on one of the boards. Id.
75 Internet Casino, supra note 47, at 2055.
IV. STATE REGULATION: LACK OF SITUS A STUMBLING BLOCK

Without knowing the fixed boundaries of an Internet site, it would seem misconceived for legislators to write a law to regulate it within a fixed area. However, as of June 1997, at least thirteen states had passed legislation regulating the Internet since 1995, and many of them had additional legislation under discussion. While several of those states have created laws to tax commercial Internet activities, most of the new laws aim to regulate the content of transmissions across the Internet medium, such as an e-mail and its attachments, or access to Web pages or newsgroups with certain types of content. For example, a recently overturned Virginia law made illegal any use of state-owned computers to access "sexually explicit material."

State legislators have made pornographic images and writings their main content target, and opponents responded in 1997 by challenging several of the statutes on First Amendment grounds. In the past two years, however, commentators, opponents and courts have started to use the United States Constitution’s Commerce Clause as another—and perhaps initial—test to determine the validity of state Internet regulations. In the words of commentator Glenn Harlan Reynolds: "[o]nly where regulations pass the Commerce Clause test is it even necessary to address First Amendment issues." In cases involving a New York law and a New Mexico law, a federal district court ruled them unconstitutional on Commerce Clause grounds. An analysis of the clause’s applicability to the Internet’s geographically vague nature demonstrates that most state regulations are ill-suited to the cyberspace medium.


77Id.


79http://www.aclu.org/, supra note 74.

80http://www.aclu.org/, supra note 74; Miller, 977 F. Supp. at 1228; Pataki, 969 F. Supp. at 183. The Pataki court bowed to the U.S. Supreme Court’s then impending determination on the issue.


82Reynolds, supra note 81, at 536.

83Pataki, 969 F. Supp. at 160 (as practically predicted by Burk, supra note 81); ACLU v. Johnson, 4 F. Supp. 2d 1029 (D.N.M. 1998).
A. The Dormant Commerce Clause

The United States Supreme Court ("the Court") and other courts historically have used a loose definition for the concept of interstate commerce, holding that even situations such as driving people across state lines fall under the category.\(^{84}\) Using the Court’s rulings as a guideline, lower courts have determined that Internet communication, specifically electronically mailing images through the Internet, qualifies as interstate commerce.\(^{85}\) The decisions suggest that the Internet like all interstate commerce, should be regulated by the federal government.\(^{86}\)

Few federal Internet laws currently exist that can preempt state regulation because it conflicts with the federal right to regulate under the Clause. In June 1997, the Court ruled unconstitutional most of the federal government’s Communications Decency Act ("the Act," "the CDA"), affirming the earlier judgment of a special three-judge district court panel.\(^{87}\) Still, even when Congress has not regulated an area, state laws must survive scrutiny under the clause’s negative or "dormant" use, which "limits the ability of states to impede the flow of interstate commerce and to legislate in that area deemed reserved for federal legislation."\(^{88}\)

Commentators have adopted one of two approaches to analyze the Internet regulation for "dormant" conflicts: the dormant analysis\(^{89}\) and the tax analysis.\(^{90}\) Theorists on each side admit problems with state regulation of the Internet stem in part from a lack of firm physical presence for the medium’s activities.\(^{91}\)

Under the dormant analysis, any state regulations that "purposely discriminate" against interstate commerce are practically invalid per se without extraordinary justification.\(^{92}\) Ordinarily, a court must first identify a local

\(^{84}\)Edwards v. California, 314 U.S. 160 (1941); see also Camps Newfound Owatonna, Inc. v. Town of Harrison, 520 U.S. 564 (1997).


\(^{86}\)See infra notes 114-69 and accompanying text.

\(^{87}\)Reno, 117 S. Ct. 2329. Some of the regulations within the Act still pass muster, such as the ISP’s immunity from liability as a publisher of defamatory material that appears on their service. See Zeran, 129 F.3d at 328.

\(^{88}\)Burk, supra note 81, at 1123-24.

\(^{89}\)Id. at 1123.

\(^{90}\)Reynolds, supra note 81, at 539. Logistically speaking, the analyses could both fall under the dormant analysis heading.

\(^{91}\)Burk, supra note 81, at 1126; Reynolds, supra note 81, at 539.

public interest benefited by the regulation and determine its legitimacy. If the state interest is deemed legitimate, the court must then balance it against the federal interest in maintaining an unburdened interstate commerce. The weight of the burden allowed hinges on the local interest's nature and the option of reasonable alternatives to the legislation that would cause "less of an impact" on interstate commercial activities.

Local health and safety measures have been accorded leeway in their impingement on interstate commerce. However, the Court drew a line even there in a 1981 case over an Iowa transportation regulation that conflicted with all of its neighboring states.

Regulations that touch upon safety, especially highway safety, are those that 'the Court has been most reluctant to invalidate'. But incantation of a purpose to promote the public health or safety does not insulate a state law from Commerce Clause attack. Regulations designed for that salutary purpose nevertheless may further the purpose so marginally, and interfere with commerce so substantially, as to be invalid under the Commerce Clause.

In general, the Court has determined that such state regulations, especially those deemed inconsistent with the policies of surrounding states, cause an inordinate burden on the commercial activities between them. "The menace of inconsistent state regulation invites analysis. . . because that clause represented the framers' reaction to overreaching by the individual states that might jeopardize the growth of the nation and in particular, the national infrastructure of communications." Such statutes may also cause an extraterritorial effect in the areas they were created to regulate, adversely affecting interstate commerce. For example, a Connecticut law requiring beer

93Id. at 142.
95Pike, 397 U.S. at 142. But see Bendix Autolite Corp. v. Midwesco Enters., Inc., 486 U.S. 888, 897 (1988) (Justice Antonin Scalia stated that "[w]eighing the governmental interests of a state against the needs of interstate commerce is . . . a task squarely within the responsibility of Congress.").
96Pike, 397 U.S. at 142.
98Id. at 670 (quoting Raymond Motor Transp. Inc. v. Rice, 434 U.S. 429, 443 (1978)).
100Patak, 969 F. Supp. at 169 (referring to Quill Corp. v. North Dakota, 504 U.S. 298, 312 (1992)).
distributors to post their wholesale prices in the state to affirm they were no
higher than those charged in the four states bordering was invalidated on the
grounds of its extraterritorial effect.\textsuperscript{101} "While a State may seek lower prices for
its consumers, it may not insist that producers or consumers in other States
surrender whatever competitive advantages they may possess."\textsuperscript{102} Finally,
state legislators may overstep their bounds—invalidating their legislative
work—if the interest they seek to regulate transcends state boundaries; in other
words, one that demands national uniformity or that is part of a national
market.\textsuperscript{103}

In the tax analysis, commentators analogize Internet regulation with the
Court's \textit{Quill Corp. v. North Dakota} decision to strike down a state's attempt to
tax interstate mail orders.\textsuperscript{104} In \textit{Quill Corp.}, the Court determined that
"unexceptional" procedures of state authority become unauthorized when
multiple standards would create a large burden for those organizations who
operate in more than one state.\textsuperscript{105} As logic might suggest, "if this 'interstate
burden' analysis is sufficient to bar state action in the extremely important area
of taxation, then it is difficult to see why it should not apply with equal force
in the area of obscenity law."\textsuperscript{106}

\textbf{B. Internet Characteristics Fit with Commerce Clause Violation}

A simple comparison of the characteristics of the Internet medium to the tests
set out by the Court finds that a generic state law regulating Internet content
would likely run afoul of the federal government's dormant Commerce Clause.
As a medium accessible by anyone from practically anywhere, the Internet
transcends state boundaries.\textsuperscript{107} By design, it is a national, if not worldwide,
transportation device for communication.\textsuperscript{108} Because Internet users generally
cannot prevent their communications or content from being accessed by a
geographical section of the country,\textsuperscript{109} any state law that regulates Internet
content or communications within a state runs the risk of having an extraterri-

\textsuperscript{101}Healy v. Beer Institute, 491 U.S. 324 (1989).
\textsuperscript{102}Brown-Forman Distillers Corp. v. New York State Liquor Auth., 476 U.S. 573, 580
\textsuperscript{103}Southern Pac. Co. v. Arizona ex. rel. Sullivan, 325 U.S. 761, 767 (1945). \textit{See also} Pataki,
969 F. Supp. at 161 (in which Judge Preska analogizes the Internet to a highway or a
railroad).
\textsuperscript{104}504 U.S. at 298.
\textsuperscript{105}Reynolds, \textit{supra} note 81 at 539.
\textsuperscript{106}Id. at 539-40.
\textsuperscript{107}Reno, 117 S. Ct. at 2335.
\textsuperscript{108}Southern Pac. Co., 325 U.S. at 767; Pataki, 969 F. Supp. at 160.
\textsuperscript{109}Reno, 117 S. Ct. at 2336.
itorial effect on Internet sites outside that area.\textsuperscript{110} The inability to prevent access also puts content providers at risk to host of inconsistent regulations in different jurisdictions.\textsuperscript{111} To compensate, non-profit and profit content providers would be forced to censor their content to satisfy the "lowest common denominator" state law, creating an undue burden on interstate commerce that would outweigh the local benefit that may have spawned the legislation.\textsuperscript{112}

A finding of economic benefit discrimination would most likely be limited to a specific case. For example, potential regulation in New York that hopes to ban internet sales of alcohol might be struck down under dormant Commerce Clause scrutiny because its outward motive is to help the sales of in-state wholesalers.\textsuperscript{113}

\textbf{C. American Libraries Association v. Pataki:\textsuperscript{114} Its Commerce Clause Application and Ramifications}

Still in its youth, Internet law as of yet has a dearth of case law with actual Internet Commerce Clause application. Perhaps the first case that directly applied the Commerce Clause to an Internet regulation involved a national association that successfully sued the State of New York in federal court, claiming the state's 1996 law outlawing adult Internet contact of a sexual nature with minors was unconstitutional on First Amendment and Commerce Clause grounds.\textsuperscript{115} On June 20, 1997, United States District Court Judge Loretta A. Preska permanently enjoined any state action under the law after analyzing the statute under commerce clause scrutiny:

I find... that the Internet is analogous to a highway or railroad. This determination means that the phrase 'information superhighway' is more than a mere buzzword; it has legal significance, because the similarity between the Internet and more traditional instruments of interstate commerce leads to analysis under the Commerce Clause.\textsuperscript{116}

Specifically, Judge Preska ruled that the criminal statute under scrutiny had extraterritorial effects and placed a burden on interstate commerce that clearly exceeded its benefit to its local interest.\textsuperscript{117} Generally, however, Preska found it

\begin{itemize}
\item \textsuperscript{110}See \textit{Healy}, 491 U.S. at 324.
\item \textsuperscript{111}See \textit{Bibb}, 359 U.S. at 520.
\item \textsuperscript{112}\textit{Internet Casino}, supra note 47, at 2055.
\item \textsuperscript{114}\textit{Pataki}, 969 F. Supp. at 160. Pataki is governor of New York.
\item \textsuperscript{115}Id. Many other groups joined as plaintiff, including American Booksellers Foundation for Free Expression, Bibliobytes, Magazine Publishers of America, Art on the Net and the ACLU.
\item \textsuperscript{116}Id. at 161.
\item \textsuperscript{117}Id. at 169. See also N.Y. PENAL LAW § 235.21 (McKinney 1984).
\end{itemize}
difficult to determine how a state could fashion an internet content regulation without violating a prong of dormant Commerce Clause scrutiny.\textsuperscript{118}

The New York statute in question, section 235.21 of the New York Penal Law, made it a crime to "intentionally use... any computer communication system allowing the input, output, examination, or transfer, of computer data or computer programs from one computer to another, to initiate or engage" in communication with a minor that "in whole or in part depicts actual or simulated nudity, sexual conduct or sadomasochistic abuse, and which is harmful to minors."\textsuperscript{119} Preska determined that the law contained no language that required the criminal activity to occur solely in New York, nor, as evidenced by its legislative history, was it intended to apply only to New York residents making contact with other New York residents.\textsuperscript{120} The benefit to the local interest the law seeks to protect—the possible prosecution of New York sexual predators who attempt to entice New York children—is arguably small, considering the amount of pornographic material and conversation sent to U.S. Internet computer servers from sites outside the country.\textsuperscript{121} Its size is especially small when compared to the possible chilling effect the law could have on anyone whose Internet communication might be accessed by a New Yorker and might be criminally liable.\textsuperscript{122}

Moreover, Preska determined, the nature of the Internet effectively precludes the possibility that the New York lawmakers could avoid dormant Commerce Clause scrutiny with any statute that limits its effect to interstate communication because "no [intrastate] communications exist."\textsuperscript{123} Limited by technology and a lack of fixed locational situs to specifically target, an Oklahoma artist who showcases his wares on a Web page cannot close his site to New Yorkers any more than he can close it to countries outside the United States.\textsuperscript{124} Most times, the Internet user may be ignorant as to where his message has arrived, and even if not, the user may be misled about the location.\textsuperscript{125} On the flip side, a New York e-mail may well pass through computer servers in any number of locations outside the state before it arrives at the computer of another New Yorker, turning intrastate transmissions into interstate mails, and

\textsuperscript{118}\textit{Pataki}, 969 F. Supp. at 170.

\textsuperscript{119}\textit{Id.} at 163.

\textsuperscript{120}\textit{Id.} at 169.


\textsuperscript{122}\textit{See Pataki}, 969 F. Supp. at 173.

\textsuperscript{123}\textit{Id.} at 171.

\textsuperscript{124}\textit{Id.} at 173.

\textsuperscript{125}\textit{Id.} at 170.
involving the sender or service provider in a potential myriad of inconsistent laws. Food "Further development of the Internet requires that users be able to predict the results of their Internet use with some degree of certainty," Preska cautioned in her opinion. With no certainty of locational effect by state laws, the Internet should receive uniform, predictable national treatment in the form of federal regulations.

D. ACLU v. Miller: A Hypothetical Example

A recently overruled Georgia law attempted to regulate the Internet at its lack-of-location core: domain names and e-mail addresses. Although the federal district court in ACLU v. Miller did not use a dormant commerce clause analysis, instead opting to rule only on the plaintiffs' First Amendment claim, the case seemed ripe for review under the clause. Had that court applied the dormant clause test, it would have found a different but compelling argument to enjoin enforcement of the statute.

On June 23, 1997, Senior District Judge Marvin H. Shoob of the Federal Northern District of Georgia ruled that the law's restrictions were vague and overly broad, so much that Internet users would have a difficult time determining what actions would constitute a violation. In his analysis, Judge Shoob pointed to (1) the law's lack of necessity of intent to defraud and (2) the questionable definition of the word "use," as parts of the legislation that might

126 See supra notes 40–47 and accompanying text.

127 Pataki, 969 F. Supp. at 183.

128 Id. at 80, 183. Judge Preska's determination made quick, albeit limited, impact on state Internet regulation elsewhere. Little more than a year after Pataki, a New Mexico federal judge ruled on almost identical commerce clause analysis to enjoin action under an Internet content-related criminal statute. Johnson, 4 F. Supp. 2d at 1029.

The law, adopted in 1998, prohibited "dissemination" on-line to a minor of content "harmful to a minor," such as nudity or sexual conduct. Violation of the law was punishable by imprisonment of one year and/or a $1,000 fine. N.M. STAT. ANN. § 30-37-3.2(A) (1978). See also Johnson, 4 F. Supp. 2d at 1029 (complaint), available on <http://www.aclu.org/court/acluvjohnson_complaint.html>.

Citing Pataki in his brief opinion, District Court Judge Hansen determined that the statute violated the federal commerce clause because it regulated conduct outside New Mexico, placed an unreasonable and undue burden on interstate commerce and subjected Internet users to inconsistent state regulations. Johnson, 4 F. Supp. 2d at 1033-34. Hansen also said that the statute's defenses—use of mandatory age or credit card notification software—were cost prohibitive to Internet context providers. Id.


130 Miller, 977 F. Supp. at 1228, GA. CODE ANN. § 16‐9‐93.1 (1996). The statute made it unlawful for an entity to knowingly transmit data through the Internet or other computer transmission facilities if such data "uses any individual name, trade name, registered trademark, logo, legal or official seal, or copyrighted symbol to falsely identify the person, organization or representative transmitting such data" or to state or imply that the entity has permission to use such symbol, etc., when the entity has not obtained such permission. GA. CODE ANN. § 16‐9‐93.1(a).
make innocent people think they were in violation, and allow the state to selectively prosecute who it wanted.\textsuperscript{131} Shoob said he expressed concern that the law would chill legal speech.\textsuperscript{132} The Georgia statute made it criminal for "any person to knowingly transmit any data by a computer network" for purposes such as "exchanging data with an electronic information storage bank or point of access to electronic information" if those people "use" a name to falsely identify themselves, or if they use a trade name or logo in their identification that would falsely imply they had permission for its use.\textsuperscript{133}

By attacking the sometimes deceptive domain names and e-mail addresses of Internet users, Georgia lawmakers might have eliminated possibilities for confusion over location, and helped to prevent Internet fraud or misrepresentation. The state contended that the law aimed to prevent fraud which it claimed as the local interest it was aiding with the legislation in question.\textsuperscript{134} However, as Judge Shoob alluded to in his opinion, the law had an extraterritorial effect that burdened interstate commerce and outweighed the benefit it gave to the state of Georgia.\textsuperscript{135} Specifically, it restricted Internet content providers' use of World Wide Web "links" to lead or connect a viewer from their Web site to another site run by a person in Georgia or somewhere else.\textsuperscript{136} The law's authors, like in \textit{Pataki}, could not partition its effect to intrastate communication because of the vaguity of the domain names or addresses they were limiting, causing a chill in Internet communication.

A fair reading of the clause, as written, is that it prohibits the current use of web page links. The linking function requires publishers of web pages to include symbols designating other web pages which may be of interest to a user. This means that an entity or person's seal may appear on hundreds or thousands of other web pages, just for the purpose of enabling the linking system.\textsuperscript{137}

Shoob amplified the burden on interstate commerce when he discovered a variety of less restrictive Georgia statutes already in place to address fraud and misrepresentation, such as statutes criminalizing computer theft by deception, unauthorized and deceitful use of name or seal of another and unfair and

\textsuperscript{131}Id. at 1232-34.

\textsuperscript{132}Id. at 1234.

\textsuperscript{133}\textit{GA. CODE ANN.} § 16-9-93.1 (1996).

\textsuperscript{134}\textit{Miller}, 977 F. Supp. at 1232.

\textsuperscript{135}\textit{See Pike}, 397 U.S. at 137.

\textsuperscript{136}\textit{Miller}, 977 F. Supp. at 1233, n.5.

\textsuperscript{137}Id. "The appearance of the seal, although completely innocuous, would definitely 'imply' to many users that permission for use had been obtained. Defendants have articulated no compelling state interest that would be furthered by restricting the linking function in this way." Id.
deceptive consumer trade practices. Unlike Judge Preska, Judge Shoob did not limit Internet regulations to the federal sector.

E. People v. Lipsitz: Limitations to Commerce Clause Application?

Despite the *Pataki* disavowance of all state regulation of Internet content, a New York state court decision soon after *Pataki* contends some state Internet regulation passes constitutional muster. State consumer fraud statutes that merely "tangentially" imply a burden to interstate commerce should stand in the face of the Internet's geographically vague nature, said the court in *People v. Lipsitz*, a case decided three days after *Pataki*. The decision initially might beg distinction because it deals with an existing state law being applied to a new medium, rather than testing a law targeted directly at a particular medium. The extent of the impact potentially caused by the *Lipsitz* case is discussed below.

The defendant, Kevin Jay Lipsitz, was restrained from fraudulent activities he committed in association with his business of soliciting magazine subscriptions through bulk e-mail messages. Defendant, among other activities, used false e-mail addresses and false testimonials from fictitious members of listservs and newsgroups to attract sales from other members of those groups. After the interested parties sent their money to the defendant's service, they either received no magazines or a few sporadic issues. Determining that all of the defendant's activities occurred in New York, the state attorney general charged the defendant with violations of state consumer fraud laws.

Unlike the laws implicated in *Pataki* and *Miller*, the consumer fraud statute in question in *Lipsitz* specifically targets only residents of the state of New York. Consumer fraud laws affect people outside the state's boundaries on purpose but, the prosecution contended, only to include outsiders' fraud claims against a state resident. Judge Diane A. Lebedeff in the *Lipsitz* case

---

138 *Id.* at 1234.
139 *Id.*
140 *Lipsitz*, 663 N.Y.S.2d at 468.
141 *Id.* at 468, 475.
142 *Id.* at 471. *See also* N.Y. GEN. BUS. LAW §§ 349, 350 (McKinney 1984).
143 *Lipsitz*, 663 N.Y.S.2d at 470.
144 *Id.* at 470, 471.
145 *Id.* at 470.
146 *Id.* at 474.
148 *Lipsitz*, 663 N.Y.S.2d at 473.
termed the connection with interstate commerce "tangential." However, according to Judge Lebedeff, even if the law were more general, neither the Commerce Clause nor the Internet's complicated geographic problems would prevent the law's applicability at least in this particular situation.

For Internet consumer fraud claims, the Internet medium is essentially irrelevant, for the focus is primarily upon the location of the messenger and whether the messenger delivered what was purchased. In some cases, it might be necessary to analyze the location of certain other business operations, such as the site used or the place orders were received. Such refinements are unnecessary here for the entire enterprise was firmly based in New York State (emphasis added).

Concepts that might have invalidated state laws that have interstate effects should not stop New York's attorney general from enforcing a state law against a local seller who happened to sell his products on the Internet.

There is no compelling reason to find that local legal officials must take a "hands off" approach just because a crook or a con artist is technologically sophisticated enough to sell on the Internet. Invocation of 'the Internet' is not the equivalent to a cry of 'sanctuary' upon a criminal's entry into a medieval church.

Interestingly, the defendant in Lipsitz did not raise a Commerce Clause argument. The judge raised it. Perhaps because of that, readers have little on which to consider an argument that the burden on interstate commerce exceeds the benefits of the statute. Nor do we have knowledge of whether, as evidenced by the out-of-state complaints, Lipsitz subjected himself to inconsistent laws because of the access any Internet user could have to the messages he left in cyberspace, and because he targeted the world-wide Internet audience. An equally looming question is whether the sale occurred completely in cyberspace, or after an initial inquiry, the transaction happened in real space through a more locationally sound "snail-mail" system. Answers to such questions could determine whether the locational vagueness of the Internet

---

149 Id. at 475.

150 Id. In fact, Judge Lebedeff directly distinguishes the situation from the situation described in Pataki.

151 Id. at 474.

152 Id. at 475.

153 Lipsitz, 663 N.Y.S.2d at 475.

154 Id. at 474.

155 See supra note 10 and accompanying text.

156 "Snail mail" is the common Internet term for the postal system. Regarding activity completely in cyberspace, see supra note 81.
would strengthen or weaken a Commerce Clause argument against the New York statute.\textsuperscript{157}

In addition, despite Judge Lebedeff's insistence that the law was of a local concern and "touch[es] upon no known federal policy which requires uniformity," the opinion cites the law's similarity to laws in other states and states the sections are based on section 5 of the Federal Trade Commission Act.\textsuperscript{158} With such evidence, instead of distinguishing the Lipsitz situation from Pataki, Judge Lebedeff's opinion actually implies that any state law regulating Internet content must have its basis in federal, uniform law, in line with what Judge Preska in Pataki recommends.\textsuperscript{159}

Lipsitz is perhaps the most recent argument for some type of state internet content regulation. Other recent arguments in favor of state regulation have surfaced on two fronts: the state's right under its police power and the federal government's lack of right under any affirmative Commerce Clause power.\textsuperscript{160}

As before mentioned, much of the states' content regulation centers on a child's access to pornographic material on the Internet. Historically, the power to "control the conduct of children" lies within a state's police power, much like its rights to deny minors the right to marry or to vote.\textsuperscript{161} Specifically, sexual morality falls within state concerns.\textsuperscript{162} Congress, on the other hand, has no substantive power over sexual morality, nor does it have a general police power.\textsuperscript{163}

Instead, Congress must find its regulation power in the Commerce Clause. As demonstrated in the 1995 case, United States v. Lopez, the federal government's commerce power has limits.\textsuperscript{164} The Court in Lopez struck down a federal statute that outlawed knowing possession of firearms in an area the violator knows or has reason to know is a school zone.\textsuperscript{165} "If under Lopez Congress lacks power under the Commerce Clause to protect children from the very serious problem of violence associated with guns in schools, it is hard to see why its interest in shielding them from private online speech should be con-

\textsuperscript{157}See supra notes 83-101 and accompanying text.


\textsuperscript{160}Amicus Curie Brief of Apollomedica Corp. and Bay Area Lawyers for Individual Freedom in Support of Affirmance, Reno v. ACLU, 117 S. Ct. 2329 (1997) (No. 1997 WL 74391) [hereinafter Apollomedica].

\textsuperscript{161}Apollomedica, 1997 WL 74391 at *10 (citing Ginsberg v. New York, 390 U.S. 629, 638-639 (1968)).

\textsuperscript{162}Id. at *6 (citing Roth v. United States, 354 U.S. 476, 502 (1957)).

\textsuperscript{163}Id.

\textsuperscript{164}514 U.S. 549 (1995).

\textsuperscript{165}Id.
considered 'compelling'."166 Such an argument does not account for states' recent problems with violating the federal government's dormant Commerce Clause arena, nor addresses any potential conflict with the Internet's geographical ignorance.

Of course, commentators Glenn Harlan Reynolds and Gregory A. Ichel suggest the federal government can always, in its authority, authorize a Commerce Clause violation to allow the states to regulate the internet.167 Recent events, however, show that rationale does not appear to be in the federal government's interest,168 as Congress and the Clinton administration attempt to regulate the Internet from a national perspective.

V. FEDERAL REGULATION: ZONING WITHOUT ZONES

Congress has already tried and failed once to regulate content on the Internet, with 1996's CDA.169 Nonetheless, several commentators,170 including two Supreme Court justices,171 see in the failed act's intent an indirect way to harness the Internet's content: to zone it.

The first attempt to zone the Internet would likely affect pornographic material.172 Zoning by content must pass the muster of particular rules set down by the Court. Internet sites' lack of fixed location, at first glance, makes

---

166Apollomedia, 1997 WL 74391 at *7.
168See infra notes 223-30 and accompanying text.
170Lawrence Lessig, who was recently asked to help the government in the recent Microsoft antitrust litigation, is perhaps the most prominent. See, e.g., The Constitution of Code: Limitations on Choice-Based Critiques of Cyberspace Regulation, 5 COMM. LAW. CONSPectus 181, 185 (1997).
172Indeed, the Philadelphia group that formed the CDA only wanted to target pornography. See Rebecca Dessoffy, Salvaging the Communications Decency Act in the Wake of ACLU v. Reno and Shea v. Reno, 45 CLEV. ST. L. REV. 271 (1997) (citing ACLU, 929 F. Supp. at 879).
application of those rules difficult.\textsuperscript{173} However, other facets of the medium, such as the small burden to access it, could justify location restrictions.\textsuperscript{174}

\textbf{A. ACLU v. Reno: Justice O'Connor's Prognosis for the CDA's "Zoning" Motive}

On its face, the CDA prohibited Internet users from communicating in certain ways with minors.\textsuperscript{175} Specifically, users could not knowingly transmit "obscene or indecent communications by means of telecommunication device" to persons aged eighteen and under, nor use an "interactive computer service" to transmit "patently offensive communications" to minors.\textsuperscript{176}

According to the Court, the Act did not adequately define the content it prohibited.\textsuperscript{177} Although the Act did offer several defenses for users to avoid sanctions,\textsuperscript{178} the Court struck down the act because its "overbreadth and vagueness" restricted adult users' access to several forms of First Amendment protected speech, and because the government had less restrictive options that could foster the act's purpose.\textsuperscript{179} The Court's majority did leave open the possibility for future Internet regulatory legislation.\textsuperscript{180}

However, Justice Sandra Day O'Connor, in her concurring opinion,\textsuperscript{181} pointed out that while some of the provisions indeed restricted adults, none of the CDA's contested portions purported to keep indecent or patently offensive material on the Internet away from them.\textsuperscript{182} "Thus," she said, "the undeniable purpose of the CDA is to segregate indecent material on the Internet into certain areas that minors cannot access," or zoning.\textsuperscript{183}

Creation of "adult zones" on the Internet is perfectly valid and fits with Court precedent, O'Connor said.\textsuperscript{184} In addition, according to O'Connor, the Internet as a medium is almost as conducive to zoning as the physical world,\textsuperscript{185} as evidenced by the identity screens many Web sites construct as an entrance gate.

\begin{footnotesize}
\begin{itemize}
\item \textsuperscript{173}See infra notes 216-19 and accompanying text.
\item \textsuperscript{174}See infra notes 220-22 and accompanying text.
\item \textsuperscript{175}Reno, 117 S. Ct. at 2338.
\item \textsuperscript{176}47 U.S.C.A. § 223(a),(d) (West 1994, Supp. 1997).
\item \textsuperscript{177}Reno, 117 S. Ct. at 2344.
\item \textsuperscript{178}See 47 U.S.C.A. § 223(e)(5).
\item \textsuperscript{179}Reno, 117 S. Ct. at 2344-46, 2348.
\item \textsuperscript{180}Id. at 2339, n.30. See also It's Back to the Drawing Board After High Court Ruling in Reno, 14-3 COMPUTER L. STRATEGIST 3, 4 (1997).
\item \textsuperscript{181}Reno, 117 S. Ct. at 2351.
\item \textsuperscript{182}Id. at 2352.
\item \textsuperscript{183}Id.
\item \textsuperscript{184}Id. at 2351.
\item \textsuperscript{185}Id. at 2353. O'Connor called cyberspace "malleable," making it "more amenable to zoning laws." Id.
\end{itemize}
\end{footnotesize}
Commentators agree: "If zoning is a perfectly permissible activity in real space, what possible argument would there be that this zoning is impermissible in cyberspace?" 186

There are a few arguments. To pass constitutional muster, no zoning law may "unduly" restrict adult access to material or restrict minors from any material which they have a First Amendment right to access. 187 Several provisions of the CDA failed the test's first part when compared to certain possible Internet situations, according to O'Connor. She recommended invalidating those sections only. 188 For example, the rights of two adults, who should be able to communicate offensive material to each other, are infringed when in an Internet unit such as IRC, an unknown party entered and the adults could not determine the party's age. 189

The aforementioned factual hypothesis demonstrates a more general problem that O'Connor said she feared: that a zoning law constructed to mirror the physical world's zoning laws might not zone out minors, presumably because of the locational and identificational vaguities associated with the Internet medium. 190 The zoning law theory is further weakened, O'Connor said, because it must rely on technological advance for its backbone. 191 As of yet, the "gateway technology" O'Connor sees as necessary to Internet zoning regulation is not prevalent. 192 Site-based software that requires users to enter information about themselves, and self-screening software are both available to some extent, however. 193 But without "ubiquitous" gateway technology since the Internet presumably cannot be broken down into physical areas - the Internet remains "unzoned—and unzoneable." 194

B. The First Amendment's Time, Place, Manner Analysis Applied to Internet Technology

The Court has initially reviewed most zoning statutes that regulate speech—especially those that appear to restrict pornographic material—under

---

186 Lawrence Lessig, Reading the Constitution in Cyberspace, 45 EMORY L.J. 869, 894 (1997).
187 Reno, 117 S. Ct. at 2352.
188 Id. at 2355.
189 Id.
190 Id. at 2353. "[Before today] the Court did not question—and therefore necessarily assumed—that an adult zone, once created, would succeed in preserving adults' access while denying minors' access to the regulated speech. Before today, there was no reason to question this assumption . . ." Id.
191 Id. at 2354.
192 Reno, 117 S. Ct. at 2354.
194 Reno, 117 S. Ct. at 2354.
a "time, place and manner" ("TPM") First Amendment analysis. However, the majority in Reno cast aside suggestions to analyze the CDA as a time, place or manner regulation, deeming the Act a more invasive content-based "blanket" restriction instead:

According to the government, the CDA is constitutional because it constitutes a sort of "cyberzoning" on the Internet. But the CDA applies broadly to the entire universe of cyberspace. And the purpose of the CDA is to protect children from the primary effects of "indecent" and "patently offensive" speech, rather than any "secondary" effect of such speech. Thus the CDA is a content-based blanket restriction on speech, and, as such, cannot be properly analyzed as a form of time, place and manner regulation.

Content-based restrictions traditionally are deemed more of a burden on First Amendment rights and face a tougher "strict scrutiny" standard. Were the Court to apply the typical TPM analysis to any Internet zoning-type regulation, such a statute would be hard-pressed to pass muster under the lesser standard. Courts will view regulations under TPM standards only if it deems the statutes or laws as content neutral and as concerned with the secondary effects of the regulated medium or place. Once classified as a TPM regulation, a law passes constitutional muster if it is "narrowly tailored to serve a substantial governmental interest" and if it leaves "ample alternative channels for communication of the restricted expression."

Statutes are content neutral if their proponents can justify them "without reference to the content of the regulated speech." For example, the District of Columbia park service refused to allow all-night protests in certain parts of a park. The park agents justified the prohibition because the law prohibited all-night camping in that area, regardless of its expressive qualities, and provided other ample areas where the offenders could camp.

In some cases, the Court has expanded the definition of content neutral even more. For example, the Court in a recent adult movie theater zoning case determined that a city ordinance was content neutral—even though it plainly

196Reno, 117 S. Ct. at 2342.
197Id.
199U.S. Sound & Service, Inc. v. Township of Brick, 126 F.3d 555, 558 (3d Cir. 1997).
201Clark, 468 U.S. at 293.
202Id. at 292.
203Id. at 295.
treated adult theaters differently than other theaters—because its "predominate concerns" were secondary effects and not content.204

The Court has compiled over the years a laundry list of effects deemed secondary. They include preventing crime, protecting the city's retail track, maintaining property values, and generally protecting and preserving neighborhoods and commerce districts.205 In a 1970's case, also involving adult theaters, the court upheld a zoning regulation that outlawed the theaters within 1,000 feet of certain establishments,206 because the regulation was "unaffected by whatever social, political or philosophical message [the] film[s] may be intended to communicate.... What is at stake is nothing more than a limitation on the place where adult films may be exhibited."207 Though the ordinance forced viewers to travel to another part of town to see the films, such a restriction was incidental and minimal to expression.208

At first glance, Internet zoning would seem to analogize well to the park example in Clark v. Community for Creative Non-Violence. Restricting adult material to a certain series of domain names "neither attempts to ban ... generally nor to ban it everywhere" on the Internet.209 The Internet has "established areas for" pornographic material "and forbids it elsewhere."210

However, while federal legislators could theoretically zone the Internet in a number of ways, each way would potentially lack at least one characteristic of a TPM regulation. Although the CDA failed the content-neutral characteristic, recent technology offers more neutral avenues.

One potential scheme of Internet legislation involves incorporating a "tagging"211 technology—called The Platform for Internet Content Selection ("PICS")—into all Internet browser software. The legislation would require all Internet content providers either voluntarily to tag a "rating"212 to their site or to submit to a rating system. However, the legislation would allow search

205Id. at 48.
206Young, 427 U.S. at 50.
207Id. at 70, n.35. The situation would be quite different if the ordinance had the effect of suppressing, or greatly restricting, access to lawful speech.
208Id. at 71.
209Clark, 468 U.S. at 295.
210Id.
212See Weber, supra note 212. "The theory is that once PICS is in place throughout the Internet, a multiplicity of ratings systems would emerge. ... Parents and others could easily choose. ... [S]uch a tool will inevitably be used by public institutions and
engines to list any sites that had tags. The end result would be a system usable by parents to block certain content, recognizable by its tag, from view by their children. Because it in essence requires a tag on every Internet site, the regulation would have a neutral emphasis on content.

However, the regulation and any potential zoning legislation—would likely fail to address effects other than primary effects, since few if any effects of the Internet have been proven to exist that do not relate to its content. Unlike adult theaters and bookstores, which reside in the physical world, the content of Internet sites and the people that access it have not been linked to a depreciation of the value of neighboring sites or a decrease in sales of a nearby commercial site. The explanation for such a failure is obviously the theme of this Note: Internet sites and communication have no fixed physical situs, from which to determine their effect on other fixed sites. And users nor commentators do not know nor, because of the Internet’s geographical ignorance, can they categorize all Internet sites in the various locations to track any secondary effects those sites might have on areas in the physical world.

Legislators have several arguments as to secondary effects. For example, Congress could introduce legislation, under the guise of the Renton case, to add a distinctive domain name level to the addresses of Internets sites that purvey indecent material. The purpose would be to eliminate the negative commercial effect the more innocuously named sites might have on the legitimate commercial sites they are grouped together with when a user searches by topic on an Internet search engine. Congress might also consider similar legislation regarding unauthorized links in the same context. The lack of a location basis for Internet sites would complicate the process.

At the same time, Internet sites’ lack of geographical boundaries might prove a saving grace. Even if Congressional legislation restricting pornographic content were to falter under TPM analysis and face strict scrutiny, it might still pass muster. To survive strict scrutiny, a regulation must serve a compelling state interest "in a manner which imposes least possible burden on expression." The Court has strongly considered the protection of minors

governments, if not here then abroad to restrict speech.” Id.

213 Id.

214 Id.

215 See U.S. Sound & Service, Inc., 126 F.3d. at 558.

216 Renton, 475 U.S. at 41.

217 See Shea, 930 F. Supp. at 930. Shea was upheld, without comment, by the U.S. Supreme Court the day after it announced the ACLU v. Reno decision.


219 U.S. Sound & Service, Inc., 126 F.3d at 558.
from material deemed harmful to them as a compelling state interest.\(^{220}\) In addition, the types of burdens recommended to be imposed on users and content providers are negligible—no more than a few clicks of a keyboard "mouse" and a minute of typing.\(^{221}\)

C. Government's Hands-Off Approach

Even presuming the federal government could constitutionally regulate the geographically vague Internet, as has been surmised in earlier sections of this Note, such presumption does not mean the government will do so. In fact, despite a flurry of possible legislation, President Clinton has announced that the government should and will take a hands-off approach to the Internet, leaving reforms to private industry.\(^{222}\) Industry monitoring of the Internet, while contingent upon antitrust obeyances, would push to the side problems caused by the Internet's ignorance of geography.

Since the CDA's virtual demise, Congress and the President have both attempted more Internet regulations. Some members of Congress have proposed a sequel to the CDA, with more specifically defined violations and parameters.\(^{223}\) Others have attempted to tie federal discounts for Internet installation at public schools and libraries to use of content-blocking software.\(^{224}\) In December, the President signed into law The No Electronic Theft Act ("NET" act), which expands copyright infringement liability on the Internet.\(^{225}\) In addition, in July 1997, the Clinton administration announced its intent to continue to enforce laws to protects minors on-line, as part of its "Strategy for a Family Friendly Internet."\(^{226}\)

However, in 1997 the President led a charge to pass legislation outlawing state Internet taxes.\(^{227}\) Even more, President Clinton publicly announced, in

\(^{220}\) Id. at 557.

\(^{221}\) Lawrence Lessig, Constitution and Code, 27 CUMB. L. REV. 1, 12 (1996-97). "This whole process took about a minute, and with this minute's investment, I was then armed with a code that would (I was promised) give me access to a wide range of web pages that similarly limit access. . . ." Id.


\(^{224}\) See S. 1619, 105th Cong.

\(^{225}\) See <http://www.aclu.org/issues/cyber/updates/ dec2497.html>.


\(^{227}\) See Cyberlex—Updated 8/97: Notable Legal Developments Reported in July 1997 Include the Following: (posted date unknown) (visited Jan. 3, 1998)
January 1998, a plan to "reduce the government's role as traffic cop for the Internet." The plan entails, among other initiatives, shifting many Net operating functions—especially the registering of domain names—to the private sector over a two-year period, and opening them to competition.

VI. SELF-REGULATION: A THIRD VIABLE OPTION?

In several of his writings, commentator Lawrence Lessig predicts that to successfully regulate the Internet, the government will shift to a different regulatory technique: regulating indirectly. Perhaps the government already has.

Over the past few years, it has appeared as if private Internet industry, free from the problems of legislators who must deal with the physical limitations of the law, has begun to zone and regulate itself and create its own geography. Many Internet sites that house risque content have built "computer graphical interfaces" or "cgi's" around their sites. Providers use cgi's so that users must, before entering, provide either a password obtained directly from the content provider or a password obtained from an independent organization that checks user information. An independent group of Internet industry leaders recently recommended a further "cyber-


228See U.S. releases, supra, note 223.

229Id. Although access to the Internet and many operations are effectively controlled by private interests already, the government has maintained a management and bankrolling function in areas of cyberspace invisible to the average surfer of the World Wide Web. The Defense Department, for example, has financed the Internet Assigned Numbers Authority, which allocates blocks of numerical addresses used by Internet service providers and is run by an institute at the University of Southern California. That's one of the responsibilities the government wants to give up. Id.

230Lessig, supra note 187, at 910. See also Weber, supra note 212.

231Lessig, supra note 187, at 888. "Quite without government mandate and indeed without anything like a centralized process of decision, cyberspace is already becoming something quite different. . . . It is moving, that is, from a relatively unzoned place to a universe that is extraordinarily well-zoned." Id.

232Id. at 887.

233Id.
spacial" boundary: forcing all sites that contain indecent content to have the top domain designation ".xxx." 234

In December 1997, the on-line industry agreed with federal police organizations to report instances of pornography, and adopted voluntary guidelines to help keep social security numbers and other sensitive personal information "out of publicly accessed databases," 235 in effect creating its own police force. Microsoft and Netscape, two of the biggest giants in Internet software, agreed to gradually include parental control software that recognizes "tagging" into all of their Web browser products. 236

However, the independence of the industry efforts is questionable. It is disputed as to whether content providers would have built cgi's without the threat of CDA penalties, 237 and as to the influence the government might have over the industry's decisions. 238

VII. CONCLUSION

It appears as if, by a legal process of elimination, self-regulation is the most attractive and immediate means to regulate the Internet. Internet sites' lack of a firm physical situs could cause any state regulation to balloon into an extraterritorial regulation. 239 One result is predictable: chilled speech. Federal regulations, which still look promising in the form of zoning, face an uphill battle. Congressional legislators would have to prove the existence of secondary effects on the Internet, or face strict scrutiny, a battle they could win. 240

The intent of this Note is not to determine a solution for legislators attempting to regulate the Internet, because as of yet, the information is too sparse to formulate one. Instead, this Note attempts to flesh out the problems legislators on all levels have faced or will face when they attempt regulation.

True self-regulation has its own problems. Working without precedent, without even a firm handle on what analogy to use for the Internet, self-regulators could face the task of creating and implementing an entirely

---

234 See http://www.cyberlaw.com/cylx0997.html (listing notable Internet developments for September 1997). "The Generic Top-Level Domain Policy Oversight Committee, an influential body consisting of 150 technology companies from around the world, has proposed that the suffix .xxx be used in Internet addresses for adult-oriented Websites." Id.

235 See Weber, supra note 212.

236 See A 'Family Friendly' Internet, supra note 227.

237 See Dessoffy, supra note 167. See also Reno, 929 F. Supp. at 827.


239 See supra notes 101-03, 111-13, 127 and accompanying text.

240 See supra notes 217-19 and accompanying text.
new rule system. That is, if they decide to veer from the federal government’s recommendations.241

More immediately, the advent of PICS technology—the Internet industry’s most controversial step toward regulation—might be a step backward.242 Whereas the CDA regulated only pornographic sites and content, PICS “creates an infrastructure for regulating every conceivable form of content and to an indefinite degree.”243

Self-regulators admit they face an uncertain path toward creating an efficient, yet law-abiding framework for the Internet.244 Unlike the other legislative levels, though, their problems are lessened by their lack of need to address the sometimes unknown destinations and origins of Internet information.

CHRISTOPHER S.W. BLAKE


243Id.

244See Self-Regulation, supra note 242.