## B. Federal vs. State Power to Regulate the Internet

### AMERICAN LIBRARY ASSOCIATION v. PATAKI
969 F. Supp. 160 (S.D.N.Y. 1997)

**OPINION**

LORETTA A. PRESKA, United States District Judge:

The Internet may well be the premier technological innovation of the present age. Judges and legislators faced with adapting existing legal standards to the novel environment of cyberspace struggle with terms and concepts that the average American five-year-old tosses about with breezy familiarity. Not surprisingly, much of the legal analysis of Internet-related issues has focused on seeking a familiar analogy for the unfamiliar. Commentators reporting on the recent oral argument before the Supreme Court of the United States, which is considering a First Amendment challenge to the Communications Decency Act, noted that the Justices seemed bent on finding the appropriate analogy which would tie the Internet to some existing line of First Amendment jurisprudence: is the Internet more like a television? a radio? a newspaper? a 900-line? a village green? This case, too, depends on the appropriate analogy. I find, as described more fully below, 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.

**BACKGROUND**

The plaintiffs filed this action challenging New York Penal Law § 235.21(3) (the "Act" or the "New York Act"), seeking declaratory and injunctive relief. Plaintiffs contend that the Act is unconstitutional both because it unduly burdens free speech in violation of the First Amendment and because it unduly burdens interstate commerce in violation of the Commerce Clause. Plaintiffs moved for a preliminary injunction enjoining enforcement of the Act. For the reasons that follow, the motion for a preliminary injunction is granted.

I. Parties to the Action

Plaintiffs in the present action represent 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. Plaintiffs include:

. American Library Association, Freedom to Read Foundation, Inc., New York Library Association, and Westchester Library System are organizations representing libraries.

. American Booksellers Foundation For Free Expression ("ABFFE") is a national association of bookstores formed to protect free expression rights. ABFFE has many members who use the Internet to obtain from publishers information and excerpts, some of which may contain sexually explicit passages.

. Association of American Publishers ("AAP") is a national association of publishers of general books, textbooks, and educational materials.

. BiblioBytes is a private, profit-seeking enterprise that uses the World Wide Web (the "Web") to provide information about and to sell electronic books. BiblioBytes offers titles in a variety of genres, including romance, erotica, classics, adventure, and horror.

. Magazine Publishers of America ("MPA") is a national association of publishers of consumer magazines.

. Interactive Digital Software Association ("IDSA") is a non-profit trade association of United States publishers of entertainment software.

. Public Access Networks Corporation ("Panix") is an Internet service provider serving subscribers located in the New York area. Panix also hosts various organizational Web pages, assists its subscribers in creating individual Web pages, and hosts online discussion groups and chat rooms.

. ECHO is a for-profit Internet service provider. ECHO and its subscribers provide content on the Internet through posting of Web sites and over 50 discussion groups.

. New York City Net ("NYC Net") is a for-profit Internet service provider catering primarily to lesbians and gay men in the New York area. NYC Net provides access services and content specifically oriented to gay and lesbian interests, including a large number of online discussion groups and chat rooms.

. Art on the Net is a non-profit organization with an international artist site ("art.net") on the Web. Art on the Net assists artists from all over the world in maintaining online studios.

. Peacefire is an organization whose membership consists primarily of minors. It was formed to protect the rights of citizens under the age of 18 to use the Internet.

. American Civil Liberties Union ("ACLU") is a national civil rights organization. The ACLU maintains a Web site on which it posts civil liberties information and resources, including material about arts censorship, obscenity laws, discrimination against lesbians and gays, and reproductive choice. In addition, the ACLU hosts unmoderated online discussion groups that allow citizens to discuss and debate a variety of civil liberties issues.

Defendants in this case are the Governor and the Attorney General of New York.

II. The Challenged Statute

The Act in question amended N.Y. Penal Law § 235.21 by adding a new subdivision. The amendment makes it a crime for an individual:

> Knowing 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, [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 such communication with a person who is a minor.

Violation of the Act is a Class E felony, punishable by one to four years of incarceration. The Act applies to both commercial and non-commercial disseminations of material.

Section 235.20(6) defines "harmful to minors" as:

> that quality of any description or representation, in whatever form, of nudity, sexual conduct, sexual excitement, or sado-masochistic abuse, when it:
>
> (a) Considered as a whole, appeals to the prurient interest in sex of minors; and
>
> (b) Is patently offensive to prevailing standards in the adult community as a whole with respect to what is suitable material for minors; and
>
> (c) Considered as a whole, lacks serious literary, artistic, political and scientific value for minors.

N.Y. Penal Law § 235.20 (6).

The statute provides six defenses to liability. First, Section 235.15(1) provides the following affirmative defense to prosecution under § 235.21(3):

> In any prosecution for obscenity, or disseminating indecent material to minors in violation of subdivision three of section 235.21 of this article, it is an affirmative defense that the persons to whom the allegedly obscene or indecent material was disseminated, or the audience to an allegedly obscene performance, consisted of persons or institutions having scientific, educational, governmental or other similar justification for possessing, disseminating or viewing the same.

The statute further provides four regular defenses to prosecution:

> (a) The defendant made a reasonable effort to ascertain the true age of the minor and was unable to do so as a result of the actions taken by the minor; or
>
> (b) The defendant has taken, in good faith, reasonable, effective and appropriate actions under the circumstances to restrict or prevent access by minors to materials specified in such subdivision, which may involve any appropriate measures to restrict minors from access to such communications, including any method which is feasible under available technology; or
>
> (c) The defendant has restricted access to such materials by requiring use of a verified credit card, debit account, adult access code or adult personal identification number; or
>
> (d) The defendant has in good faith established a mechanism such that the labelling, segregation or other mechanism enables such material to be automatically blocked or screened by software or other capabilities reasonably available to responsible adults wishing to effect such blocking or screening and the defendant has not otherwise solicited minors not subject to such screening or blocking capabilities to access that material or circumvent any such screening or blocking.

N.Y. Penal Law § 235.23(3). And, finally, Section 235.24 provides that no individual shall be held liable:

> Solely for providing access or connection to or from a facility, system, or network not under that person's control, including transmission, downloading, intermediate storage, access software, or other related capabilities that are incidental to providing such access or connection that do not include the creation of the content of the communication.

N.Y. Penal Law § 235.24. Exceptions to this defense for conspirators or co-owners and an additional employer liability defense are set forth in Section 235.24(1)(a)-(b) and (2).

III. The Internet

The Internet is a decentralized, global communications medium linking people, institutions, corporations, and governments all across the world. ACLU v. Reno, 929 F. Supp. 824 (E.D. Pa.), prob. juris. noted, 117 S. Ct. 554 (1996), argued, March 19, 1997. The Internet has experienced extraordinary growth in recent years. In 1981, fewer than 300 computers were linked to the Internet; in 1989, the number stood at fewer than 90,000 computers. By 1993, over 1,000,000 computers were linked. Today, over 9,400,000 host computers worldwide, 60% of them located in the United States, are linked to the Internet. As many as 40 million people worldwide currently enjoy access to the Internet's resources, and that number is expected to grow to 200 million by the year 1999.

The Internet is a network of networks -- a decentralized, self-maintaining series of redundant links among computers and computer networks, capable of rapidly transmitting communications without direct human involvement or control. No organization or entity controls the Internet; in fact, the chaotic, random structure of the Internet precludes any exercise of such control.

The information available on the Internet is "as diverse as human thought." Every facet of art, literature, music, news, and debate is represented. There can be no question that the overwhelming variety of available information includes some sexually explicit materials.

Individuals obtain access to the Internet via a number of avenues. Students and faculty often obtain access via their educational institutions; similarly, some corporations provide their employees with access to the Internet. Individuals in some communities can access the Internet via a community network or a local library. Storefront "computer coffee shops" offer another option, serving up access to cyberspace accompanied by coffee and snacks for a small hourly fee. "Internet service providers" typically offer modem telephone access to a computer or computer network linked to the Internet. Many such providers are commercial entities offering Internet access for a monthly or hourly fee. Another common way for individuals to access the Internet is through one of the major national commercial "online services" such as America Online, Compuserve, the Microsoft Network, or Prodigy. Finally, local dial-in computer services, called "bulletin board systems" or "BBSs" provide Internet access.

The Internet permits a user to communicate pictures and text in several ways including:

(1) one-to-one messaging (such as "e-mail");

(2) one-to-many messaging (such as "listserv" or "mail exploder");

(3) distributed message databases (such as "USENET newsgroups");

(4) real time remote computer utilization (such as "Internet Relay Chat");

(5) real time remote computer utilization (such as "telnet"); and

(6) remote information retrieval (such as "ftp," "gopher," and the Web).

In addition to transmitting pictures and text, many of these communication methods can be used to transmit data, computer programs, sound, and moving video images.

Most users of the Internet are provided with a username, password and e-mail address that allow them to sign on to the Internet and communicate with other users. Many usernames are pseudonyms which provide users with a distinct online identity and preserve anonymity. The username and e-mail address are the only indicators of a user's identity; generally speaking, neither datum discloses a party's age or geographic location.

E-mail is the simplest method of Internet communication. E-mail allows an online user to address and transmit an electronic message to one or more people. The ACLU court noted that e-mail is "comparable in principle to sending a first class letter." The analogy is not a perfect one, however, for two reasons. First, the sender directs his message to a logical rather than geographic address, and therefore need not know the location of his correspondent in real space. Second, most programs provide for a "reply" option which enables the recipient to respond to the sender's message simply by clicking on a button; the recipient will therefore not even need to type in the sender's e-mail address. A further distinction concerns the level of security that protects a communication. While first-class letters are sealed, e-mail communications are more easily intercepted. Concerns about the relatively easy accessibility of e-mail communications have led bar associations in some states to require that lawyers encrypt sensitive e-mail messages in order to protect client confidentiality.

The Internet also includes a variety of online discussion fora that allow groups of users to discuss and debate subjects of interest. The three most common means by which such discussion groups come together are through mail exploders, USENET newsgroups, and chat rooms.

Mail exploders, also known as "listservs," allow online users to subscribe to automated mailing lists that disseminate information on particular subjects. Subscribers send an e-mail message to the "list," and the mail exploder automatically and simultaneously sends the message to all of the other subscribers on the list. Users of mailing lists can add or delete their names from the list automatically, without any direct human involvement.

USENET newsgroups are a very popular set of discussion groups arranged according to subject matter and automatically disseminated "using ad hoc peer to peer connections between approximately 200,000 computers . . . around the world." Users may read or send messages to newsgroups without any prior subscription, and there is no way for a speaker who posts an article to a newsgroup to know who is reading the message. Currently, more than 15,000 different subjects are represented in USENET newsgroups, and over 100,000 new messages are posted to these groups every day.

Chat rooms allow online discussion in real time. Users are able to engage in simultaneous conversations with one or many "occupants" by typing in messages and reading the messages typed by others participating in the chat; the ACLU court analogized this Internet application to

a telephone party line.

Finally, perhaps the most well-known method of communicating information online is the Web; many laypeople erroneously believe that the Internet is co-extensive with the Web. The Web is really a publishing forum; it is comprised of millions of separate "Web sites" that display content provided by particular persons or organizations. Any Internet user anywhere in the world with the proper software can create a Web page, view Web pages posted by others, and then read text, look at images and video, and listen to sounds posted at these sites. Many large corporations, banks, brokerage houses, newspapers and magazines provide online editions of their reports and publications or operate independent Web sites. Government agencies and even courts use the Web to disseminate information to the public. At the same time, many individual users and small community organizations have established individual "home pages" on the Web that provide information to any interested person who "surfs by."

Although information on the Web is contained on innumerable Web sites located on individual computers around the world, each of these Web sites and computers is connected to the Internet by means of protocols that permit the information to become part of a single body of knowledge accessible by all Web visitors. To gain access to the resources of the Web, an individual employs a "browser." A browser is software that allows the user to display, print, and download documents that are formatted in the standard Web formatting language.

There are a number of different ways that Internet users can browse or search for content on the Web. First, every document on the Web has an address that allows users to find and retrieve it, and a user can simply type in the address and go directly to that site. Again, however, the address is a logical rather than geographic concept, and the user will not necessarily know where the site is located in real space. Additionally, a user who wants to conduct a generalized search or wants to reach a particular site but does not know the address, can use a "search engine," which is available free of charge to help users navigate the Web.

Finally, online users may "surf" the Web by "linking" from one Web page to another. Almost all Web documents contain "links," segments of text or images that refer to another Web document. When the user clicks on the link, the linked document is automatically displayed, wherever in the world it is stored. "These links from one computer to another, from one document to another across the Internet, are what unify the Web into a single body of knowledge, and what makes the Web unique."

Internet users have no way to determine the characteristics of their audience that are salient under the New York Act -- age and geographic location. In fact, in online communications through newsgroups, mailing lists, chat rooms, and the Web, the user has no way to determine with certainty that any particular person has accessed the user's speech. "Once a provider posts content on the Internet, it is available to all other Internet users worldwide." A speaker thus has no way of knowing the location of the recipient of his or her communication. As the poet said, "I shot an arrow into the air; it fell to the earth I know not where."

This highly simplified description of the Internet is not intended to minimize its marvels. The innovativeness of the technology does not preclude the application of traditional legal principles -- provided that those principles are adaptable to cyberspace. In the present case, as discussed more fully below, the Internet fits easily within the parameters of interests traditionally protected

by the Commerce Clause. The New York Act represents an unconstitutional intrusion into interstate commerce; plaintiffs are therefore entitled to the preliminary injunction that they seek.

**DISCUSSION**

I. Standard Applicable to a Preliminary Injunction

To demonstrate their entitlement to a preliminary injunction, plaintiffs must show (a) that they will suffer irreparable harm and (b) either (i) a likelihood of success on the merits or (ii) sufficiently serious questions going to the merits to make them a fair ground for litigation and a balance of hardships tipping decidedly in the plaintiffs' favor. In the present case, plaintiffs have amply demonstrated the likelihood of their successful prosecution of their claim that the Act violates the Commerce Clause because it seeks to regulate communications occurring wholly outside New York, imposes a burden on interstate commerce that is disproportionate to the local benefits it is likely to engender, and subjects plaintiffs, as well as other Internet users, to inconsistent state obligations.

Plaintiffs have also shown that they face irreparable injury in the absence of an injunction. Irreparable injury means "the kind of injury for which money cannot compensate," and which is "neither remote nor speculative, but actual and imminent." Deprivation of the rights guaranteed under the Commerce Clause constitutes irreparable injury.

II. Federalism and the Internet: The Commerce Clause

The borderless world of the Internet raises profound questions concerning the relationship among the several states and the relationship of the federal government to each state, questions that go to the heart of "our federalism." See Younger v. Harris, 401 U.S. 37, 44 (1971). The Act at issue in the present case is only one of many efforts by state legislators to control the chaotic environment of the Internet. For example, the Georgia legislature has enacted a recent law prohibiting Internet users from "falsely identifying" themselves online. Similar legislation is pending in California. Texas and Florida have concluded that law firm web pages (apparently including those of out of state firms) are subject to the rules of professional conduct applicable to attorney advertising. Further, states have adopted widely varying approaches in the application of general laws to communications taking place over the Internet. Minnesota has aggressively pursued out-of-state advertisers and service providers who reach Minnesotans via the Internet; Illinois has also been assertive in using existing laws to reach out-of-state actors whose connection to Illinois occurs only by virtue of an Internet communication.[1]

---

[1] Other jurisdictions internationally have also gotten into the act. In January, 1997, two associations dedicated to the preservation of France's linguistic purity filed suit against two private corporations and Georgia Tech Lorraine, a French university affiliated with the Georgia Institute of Technology, claiming that the defendants violated a French law that prohibits advertising in any language other than French by operating English-language sites on the World Wide Web. The French court dismissed the action as to Georgia Tech, but other efforts by foreign jurisdictions to regulate the Internet are likely to follow. In addition, Germany made headlines recently when its anti-pornography laws forced Compuserve to close access to over 200 Internet sites from anywhere in the world.

The unique nature of the Internet highlights the likelihood that a single actor might be subject to haphazard, uncoordinated, and even outright inconsistent regulation by states that the actor never intended to reach and possibly was unaware were being accessed. Typically, states' jurisdictional limits are related to geography; geography, however, is a virtually meaningless construct on the Internet. The menace of inconsistent state regulation invites analysis under the Commerce Clause of the Constitution, 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 and trade -- as a whole.

The Commerce Clause is more than an affirmative grant of power to Congress. As long ago as 1824, Justice Johnson in his concurring opinion in Gibbons v. Ogden recognized that the Commerce Clause has a negative sweep as well. In what commentators have come to term its negative or "dormant" aspect, the Commerce Clause restricts the individual states' interference with the flow of interstate commerce in two ways. The Clause prohibits discrimination aimed directly at interstate commerce, see, e.g., Philadelphia v. New Jersey, 437 U.S. 617 (1978), and bars state regulations that, although facially nondiscriminatory, unduly burden interstate commerce, see, e.g., Kassel v. Consolidated Freightways Corp. of Del., 450 U.S. 662 (1981). Moreover, courts have long held that state regulation of those aspects of commerce that by their unique nature demand cohesive national treatment is offensive to the Commerce Clause.

Thus, as will be discussed in more detail below, the New York Act is concerned with interstate commerce and contravenes the Commerce Clause for three reasons. First, the Act represents an unconstitutional projection of New York law into conduct that occurs wholly outside New York. Second, the Act is invalid because although protecting children from indecent material is a legitimate and indisputably worthy subject of state legislation, the burdens on interstate commerce resulting from the Act clearly exceed any local benefit derived from it. Finally, the Internet is one of those areas of commerce that must be marked off as a national preserve to protect users from inconsistent legislation that, taken to its most extreme, could paralyze development of the Internet altogether. Thus, the Commerce Clause ordains that only Congress can legislate in this area.

***A. The Act Concerns Interstate Commerce***

At oral argument, the defendants advanced the theory that the Act is aimed solely at intrastate conduct. This argument is unsupportable in light of the text of the statute itself, its legislative history, and the reality of Internet communications. The section in question contains no such limitation; it reads:

> A person is guilty of disseminating indecent material to minors in the second degree when:
>
> . . .
>
> (3) Knowing 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 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 such communication with a person who is a minor.

N.Y. Penal Law § 235.21(3) (McKinney's 1997). Section 235.20, which contains the definitions applicable to the challenged portion of the 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.

Further, the legislative history of the Act clearly evidences the legislators' understanding and intent that the Act would apply to communications between New Yorkers and parties outside the State. The New York State Senate Introducer's Memorandum in Support of the Act contains a paragraph under the subtitle, "Justification," which states:

> Law enforcement agencies around the nation are becoming increasingly alarmed at the growing use of computer networks and other communications by pedophiles. As one observer noted, "perverts are moving from the playground to the internet." Several cases have come to light wherein a pedophile has traveled clear across the country to have sexual relations with a minor initially contacted and engaged through various computer networks.

A letter from the Bill's sponsor to Governor Pataki characterized sexually-infused Internet communications between adults and minors as "long-distance, high-tech sexual abuse." Jeanine Pirro, the Westchester County District Attorney, wrote a letter to Governor Pataki that similarly reflects the expectations of the Act's proponents that it would apply to interstate communications. Ms. Pirro's letter states:

> This bill was proposed partly in response to a Westchester County case wherein an adult male resident of Seattle, Washington, [one Alan Paul Barlow,] communicated about sexually explicit matters by computer with a thirteen year old girl over several months.

Ms. Pirro's references to this incident, known as the Barlow case, are echoed throughout defendants' memorandum of law. Obviously, however, the Act would be completely ineffective in forestalling a pedophile like Barlow if it applied only to purely intrastate communications.

The conclusion that the Act must apply to interstate as well as intrastate communications receives perhaps its strongest support from the nature of the Internet itself. The Internet is wholly insensitive to geographic distinctions. In almost every case, users of the Internet neither know nor care about the physical location of the Internet resources they access. Internet protocols were designed to ignore rather than document geographic location; while computers on the network do have "addresses," they are logical addresses on the network rather than geographic addresses in real space. The majority of Internet addresses contain no geographic clues and, even where an Internet address provides such a clue, it may be misleading.

Moreover, no aspect of the Internet can feasibly be closed off to users from another state. An internet user who posts a Web page cannot prevent New Yorkers or Oklahomans or Iowans from accessing that page and will not even know from what state visitors to that site hail. Nor can a participant in a chat room prevent other participants from a particular state from joining the

conversation. Someone who uses a mail exploder is similarly unaware of the precise contours of the mailing list that will determine the recipients of his or her message, because users can add or remove their names from a mailing list automatically. Thus, a person could choose a list believed not to include any New Yorkers, but an after-added New Yorker would still receive the message.

E-mail, because it is a one-to-one messaging system, stands on a slightly different footing than the other aspects of the Internet. Even in the context of e-mail, however, a message from one New Yorker to another New Yorker may well pass through a number of states en route. The Internet is, as described above, a redundant series of linked computers. Thus, a message from an Internet user sitting at a computer in New York may travel via one or more other states before reaching a recipient who is also sitting at a terminal in New York.

The system is further complicated by two Internet practices: packet switching and caching. "Packet switching" protocols subdivide individual messages into smaller packets that are then sent independently to the destination, where they are automatically reassembled by the receiving computer. If computers along the route become overloaded, packets may be rerouted to computers with greater capacity. A single message may -- but does not always -- travel several different pathways before reaching the receiving computer. "Caching" is the Internet practice of storing partial or complete duplicates of materials from frequently accessed sites to avoid repeatedly requesting copies from the original server. The recipient has no means of distinguishing between the cached materials and the original. Thus, the user may be accessing materials at the original site, or he may be accessing copies of those materials cached on a different machine located anywhere in the world.

The New York Act, therefore, cannot effectively be limited to purely intrastate communications over the Internet because no such communications exist. No user could reliably restrict her communications only to New York recipients. Moreover, no user could avoid liability under the New York Act simply by directing his or her communications elsewhere, given that there is no feasible way to preclude New Yorkers from accessing a Web site, receiving a mail exploder message or a newsgroup posting, or participating in a chat room. Similarly, a user has no way to ensure that an e-mail does not pass through New York even if the ultimate recipient is not located there, or that a message never leaves New York even if both sender and recipient are located there.

This conclusion receives further support from the unchallenged testimony that plaintiffs introduced in the form of declarations. For example, Stacy Horn, the president of ECHO, an electronic cultural salon, testified that "conference participants do not know, and have no way to determine, the . . . geographic location of other participants." Lawrence J. Kaufman, the Vice President of the Magazine Publishers of America, Inc., noted that "On-line users anywhere in the world can access the content provided by MPA members on the Web and via e-mail. These members cannot effectively prevent their Web sites from being accessed by New York users."

The Act is therefore necessarily concerned with interstate communications. The next question that requires an answer as a threshold matter is whether the types of communication involved constitute "commerce" within the meaning of the Clause.

The definition of commerce in the Supreme Court's decisions has been notably broad. Most recently, in Camps Newfound Owatonna, Inc. v. Town of Harrison, Maine, 117 S. Ct. 1590

(1997), the Court rejected defendant's arguments that the Commerce Clause was inapplicable to a discriminatory real estate tax deduction, either because "campers are not 'articles of commerce'" or because the camp's "product is delivered and 'consumed' entirely within Maine."

In the present case, the parties have stipulated that:

> The Internet is not exclusively, or even primarily, a means of commercial communication. Many commercial entities maintain Web sites to inform potential consumers about their goods and services, or to solicit purchases, but many other Web sites exist solely for the dissemination of non-commercial information. The Internet is an especially attractive means for not-for-profit entities or public interest groups to reach their desired audiences.

The non-profit nature of certain entities that use the Internet or of certain transactions that take place over the Internet does not take the Internet outside the Commerce Clause. The Supreme Court has expressly held that the dormant commerce clause is applicable to activities undertaken without a profit motive.

In addition, many of those users who are communicating for private, noncommercial purposes are nonetheless participants in interstate commerce by virtue of their Internet consumption. Many users obtain access to the Internet by means of an on-line service provider which charges a fee for its services. "Internet service providers," also offer Internet access for a monthly or hourly fee. Patrons of storefront "computer coffee shops" similarly pay for their access to the Internet, in addition to partaking of food and beverages sold by the cafe.

The courts have long recognized that railroads, trucks, and highways are themselves "instruments of commerce," because they serve as conduits for the transport of products and services. The Internet is more than a means of communication; it also serves as a conduit for transporting digitized goods, including software, data, music, graphics, and videos which can be downloaded from the provider's site to the Internet user's computer.

The inescapable conclusion is that the Internet represents an instrument of interstate commerce, albeit an innovative one; the novelty of the technology should not obscure the fact that regulation of the Internet impels traditional Commerce Clause considerations. The New York Act is therefore closely concerned with interstate commerce, and scrutiny of the Act under the Commerce Clause is entirely appropriate. As discussed in the following sections, the Act cannot survive such scrutiny, because it places an undue burden on interstate traffic, whether that traffic be in goods, services, or ideas.

### *B. New York Has Overreached by Enacting a Law That Seeks To Regulate Conduct Occurring Outside its Borders*

The interdiction against direct interference with interstate commerce by state legislative overreaching is apparent in a number of the Supreme Court's decisions. In Baldwin v. G.A.F. Seelig, Inc., 294 U.S. 511, 521 (1935), for example, Justice Cardozo authored an opinion enjoining enforcement of a law that prohibited a dealer from selling within New York milk purchased from the producer in Vermont at less than the minimum price fixed for milk produced in New York. Justice Cardozo sternly admonished, "New York has no power to project its legislation into Vermont by regulating the price to be paid in that state for milk," finding that

"such a power, if exerted, [would] set a barrier to traffic between one state and another as effective as if customs duties, equal to the price differential, had been laid upon the thing transported."

The Court has more recently confirmed that the Commerce Clause precludes a state from enacting legislation that has the practical effect of exporting that state's domestic policies. In Edgar v. MITE, 457 U.S. 624 (1982), the Court examined the constitutionality of an Illinois anti-takeover statute. The Court found particularly egregious the fact that the Illinois law would apply to a transaction that would not affect a single Illinois shareholder if a corporation fit within the definition of a "target company." The Court concluded "the Illinois statute is a direct restraint on interstate commerce and has a sweeping extraterritorial effect," because the statute would prevent a tender offeror from communicating its offer to shareholders both within and outside Illinois. Acceptance of the offer by any of the shareholders would result in interstate transactions; the Illinois statute effectively stifled such transactions and thereby disrupted prospective interstate commerce. Under the Commerce Clause, the projection of these extraterritorial "practical effect[s]," regardless of the legislators' intentions, "'exceeded the inherent limits of the State's power.'"

In the present case, witnesses testified to the chill that they felt as a result of the enactment of the New York statute; these witnesses refrained from engaging in particular types of interstate commerce. In particular, I note the testimony of Rudolf Kinsky, an artist with a virtual studio on Art on the Net's Website. Mr. Kinsky testified that he removed several images from his virtual studio because he feared prosecution under the New York Act. As described above, no Web siteholder is able to close his site to New Yorkers. Thus, even if Mr. Kinsky were located in California and wanted to display his work to a prospective purchaser in Oregon, he could not employ his virtual studio to do so without risking prosecution under the New York law.

The "extraterritoriality" analysis of the Edgar opinion commanded only a plurality of the Court. Later majority holdings, however, expressly adopted the underlying principles on which Justice White relied in Edgar. See Healy v. The Beer Institute, 491 U.S. 324 (1989). In Healy, the Court derived three guiding principles from its prior cases. First, the Court emphasized that the "'Commerce Clause . . . precludes the application of a state statute to commerce that takes place wholly outside the State's borders, whether or not the commerce has effects within the state.'" Second, the Court instructed that "a statute that directly controls commerce occurring wholly outside the boundaries of a State exceeds the inherent limits of the enacting State's authority and is invalid regardless of whether the statute's extraterritorial reach was intended by the legislature. The critical inquiry is whether the practical effect of the regulation is to control conduct beyond the boundaries of the State." Finally, "the practical effect of the statute must be evaluated not only by considering the consequences of the statute itself, but also by considering how the challenged statute may interact with the legitimate regulatory regimes of other States and what effect would arise if not one, but many or every, State adopted similar legislation. Generally speaking, the Commerce Clause protects against inconsistent legislation arising from the projection of one state regulatory regime into the jurisdiction of another State."

The nature of the Internet makes it impossible to restrict the effects of the New York Act to conduct occurring within New York. An Internet user may not intend that a message be accessible to New Yorkers, but lacks the ability to prevent New Yorkers from visiting a

particular Website or viewing a particular newsgroup posting or receiving a particular mail exploder. Thus, conduct that may be legal in the state in which the user acts can subject the user to prosecution in New York and thus subordinate the user's home state's policy -- perhaps favoring freedom of expression over a more protective stance -- to New York's local concerns. New York has deliberately imposed its legislation on the Internet and, by doing so, projected its law into other states whose citizens use the Net. This encroachment upon the authority which the Constitution specifically confers upon the federal government and upon the sovereignty of New York's sister states is per se violative of the Commerce Clause.

***C. The Burdens the Act Imposes on Interstate Commerce Exceed Any Local Benefit***

Even if the Act were not a per se violation of the Commerce Clause by virtue of its extraterritorial effects, the Act would nonetheless be an invalid indirect regulation of interstate commerce, because the burdens it imposes on interstate commerce are excessive in relation to the local benefits it confers. The Supreme Court set forth the balancing test applicable to indirect regulations of interstate commerce in Pike v. Bruce Church, 397 U.S. 137, 142 (1970). Pike requires a two-fold inquiry. The first level of examination is directed at the legitimacy of the state's interest. The next, and more difficult, determination weighs the burden on interstate commerce in light of the local benefit derived from the statute.

In the present case, I accept that the protection of children against pedophilia is a quintessentially legitimate state objective. See New York v. Ferber, 458 U.S. 747, 756-57 (1982) ("It is evident beyond the need for elaboration that a State's interest in 'safeguarding the physical and psychological well-being of a minor' is 'compelling.'"); see also Sable v. Federal Communications Commission, 492 U.S. 115, 126 (1989) ("There is a compelling interest in protecting the physical and psychological well-being of minors. This interest extends to shielding minors from the influence of literature that is not obscene by adult standards."). Even with the fullest recognition that the protection of children from sexual exploitation is an indisputably valid state goal, however, the present statute cannot survive even the lesser scrutiny to which indirect regulations of interstate commerce are subject. The State cannot avoid the second stage of the inquiry simply by invoking the legitimate state interest underlying the Act.

The local benefits likely to result from the New York Act are not overwhelming. The Act can have no effect on communications originating outside the United States. As the three-judge panel that struck the federal analog of the New York Act, the Communications Decency Act, on First Amendment grounds concluded:

> [The Act] will almost certainly fail to accomplish the Government's interest in shielding children from pornography on the Internet. Nearly half of Internet communications originate outside the United States, and some percentage of that figure represents pornography. Pornography from, say, Amsterdam, will be no less appealing to a child on the Internet than pornography from New York City, and residents of Amsterdam have little incentive to comply with the [Act].

American Civil Liberties Union v. Reno, 929 F. Supp. 824, 882 (E.D. Pa. 1996). Further, in the present case, New York's prosecution of parties from out of state who have allegedly violated the Act, but whose only contact with New York occurs via the Internet, is beset with practical difficulties, even if New York is able to exercise criminal jurisdiction over such parties. The

prospect of New York bounty hunters dragging pedophiles from the other 49 states into New York is not consistent with traditional concepts of comity.

The Act is, of course, not the only law in New York's statute books designed to protect children against sexual exploitation. The State is able to protect children through vigorous enforcement of the existing laws criminalizing obscenity and child pornography. Moreover, plaintiffs do not challenge the sections of the statute that criminalize the sale of obscene materials to children, over the Internet or otherwise, and prohibit adults from luring children into sexual contact by communicating with them via the Internet. See N.Y. Penal Law § 235.21(1); N.Y. Penal Law § 235.22(2). The local benefit to be derived from the challenged section of the statute is therefore confined to that narrow class of cases that does not fit within the parameters of any other law. The efficacy of the statute is further limited, as discussed above, to those cases which New York is realistically able to prosecute.

Balanced against the limited local benefits resulting from the Act is an extreme burden on interstate commerce. The New York Act casts its net worldwide; moreover, the chilling effect that it produces is bound to exceed the actual cases that are prosecuted, as Internet users will steer clear of the Act by significant margin. At oral argument, the State asserted that only a small percentage of Internet communications are "harmful to minors" and would fall within the proscriptions of the statute; therefore, the State argued, the burden on interstate commerce is small. On the record before me, I conclude that the range of Internet communications potentially affected by the Act is far broader than the State suggests. In the past, various communities have found works including I Know Why the Caged Bird Sings by Maya Angelou, The Adventures of Huckleberry Finn by Mark Twain, and The Color Purple by Alice Walker to be indecent. Many libraries, museums and academic institutions post art on the Internet that some might conclude was "harmful to minors." Famous nude works by Botticelli, Manet, Matisse, Cezanne and others can be found on the Internet. Lesser known artists who post work over the Internet may face an even greater risk of prosecution, because the mantle of respectability that has descended on Manet is not associated with their as yet obscure names. Individuals who wish to communicate images that might fall within the Act's proscriptions must thus self-censor or risk prosecution, a Hobson's choice that imposes an unreasonable restriction on interstate commerce.

Moreover, as both three-judge panels that struck the federal statute have found, the costs associated with Internet users' attempts to comply with the terms of the defenses that the Act provides are excessive. Both courts that addressed the Communications Decency Act found that these costs of compliance, coupled with the threat of serious criminal sanctions for failure to comply, could drive some Internet users off the Internet altogether. While the defenses in the Act are not identical to those in the CDA, the cost analysis is equally applicable to both statutes.

The severe burden on interstate commerce resulting from the New York statute is not justifiable in light of the attenuated local benefits arising from it. The alternative analysis of the Act as an indirect regulation on interstate commerce therefore also mandates the issuance of the preliminary injunction sought by plaintiffs.

***D. The Act Unconstitutionally Subjects Interstate Use of the Internet to Inconsistent Regulations***

Finally, a third mode of Commerce Clause analysis further confirms that the plaintiffs are

likely to succeed on the merits of their claim. The courts have long recognized that certain types of commerce demand consistent treatment and are therefore susceptible to regulation only on a national level. The Internet represents one of those areas; effective regulation will require national, and more likely global, cooperation. Regulation by any single state can only result in chaos, because at least some states will likely enact laws subjecting Internet users to conflicting obligations. Without the limitations imposed by the Commerce Clause, these inconsistent regulatory schemes could paralyze the development of the Internet altogether.

In numerous cases, the Supreme Court has acknowledged the need for coordination in the regulation of certain areas of commerce. As long ago as 1886, the Supreme Court stated:

> Commerce with foreign countries and among the states, strictly considered, consists in intercourse and traffic, including in these terms navigation, and the transportation and transit of persons and property, as well as the purchase, sale, and exchange of commodities. For the regulation of commerce, as thus defined, there can be only one system of rules, applicable alike to the whole country; and the authority which can act for the whole country can alone adopt such a system. Action upon it by separate states is not, therefore, permissible.

Wabash, St. L. & P. Ry. Co. v. Illinois, 118 U.S. 557, 574-75 (1886). The Court in Wabash struck the Illinois statute at issue, which purported to establish interstate railway rates, stating "that this species of regulation is one which must be, if established at all, of a general and national character, and cannot be safely and wisely remitted to local rules and regulations, we think is clear from what has already been said."

Similarly, in Bibb v. Navajo Freight Lines, Inc., 359 U.S. 520 (1959), the Court examined an Illinois statute that required the use of contour mudguards on trucks in Illinois. The Court took note of the fact that straight or conventional mudguards were permissible in most other states and actually required in Arkansas. Recognizing the need for coordinated legislation, the Court stated that "the conflict between the Arkansas regulation and the Illinois regulation . . . suggests that this regulation of mudguards is not one of those matters 'admitting of diversity of treatment, according to the special requirements of local conditions.'" The Court struck the Illinois law as imposing an undue burden on interstate commerce, in part because Illinois was insisting upon "a design out of line with the requirements of almost all the other states."

The Internet, like rail and highway traffic, requires a cohesive national scheme of regulation so that users are reasonably able to determine their obligations. Regulation on a local level, by contrast, will leave users lost in a welter of inconsistent laws, imposed by different states with different priorities. New York is not the only state to enact a law purporting to regulate the content of communications on the Internet. Already Oklahoma and Georgia have enacted laws designed to protect minors from indecent communications over the Internet; as might be expected, the states have selected different methods to accomplish their aims. Georgia has made it a crime to communicate anonymously over the Internet, while Oklahoma, like New York, has prohibited the online transmission of material deemed harmful to minors.

Moreover, the regulation of communications that may be "harmful to minors" taking place over the Internet poses particular difficulties. New York has defined "harmful to minors" as including:

> that quality of any description or representation, in whatever form, of nudity, sexual conduct, sexual excitement, or sado-masochistic abuse, when it:
>
> (a) Considered as a whole, appeals to the prurient interest in sex of minors; and
>
> (b) Is patently offensive to prevailing standards in the adult community as a whole with respect to what is suitable material for minors; and
>
> (c) Considered as a whole, lacks serious literary, artistic, political and scientific value for minors.

N.Y. Penal Law § 235.20(6). Courts have long recognized, however, that there is no single "prevailing community standard" in the United States. Thus, even were all 50 states to enact laws that were verbatim copies of the New York Act, Internet users would still be subject to discordant responsibilities. To use an example cited by the court in ACLU v. Reno, the Broadway play Angels in America, which concerns homosexuality and AIDS and features graphic language, was immensely popular in New York and in fact earned two Tony awards and a Pulitzer prize. In Charlotte, North Carolina, however, a production of the drama caused such a public outcry that the Mecklenberg County Commission voted to withhold all public funding from arts organizations whose works "expose the public to perverted forms of sexuality." The Supreme Court has always recognized that "our nation is simply too big and too diverse for this Court to reasonably expect that such standards [of what is patently offensive] could be articulated for all 50 states in a single formulation." Miller v. California, 413 U.S. 15, 30 (1973).

As discussed at length above, an Internet user cannot foreclose access to her work from certain states or send differing versions of her communication to different jurisdictions. In this sense, the Internet user is in a worse position than the truck driver or train engineer who can steer around Illinois, or change the mudguard at the state line; the Internet user has no ability to bypass any particular state. The user must thus comply with the regulation imposed by the state with the most stringent standard or forego Internet communication of the message that might or might not subject her to prosecution. For example, a teacher might invite discussion of Angels In America from a Usenet newsgroup dedicated to the literary interests of high school students. Quotations from the play might not subject her to prosecution in New York -- but could qualify as "harmful to minors" according to the community standards prevailing in Oklahoma. The teacher cannot tailor her message on a community-specific basis and thus must take her chances or avoid the discussion altogether.

Further development of the Internet requires that users be able to predict the results of their Internet use with some degree of assurance. Haphazard and uncoordinated state regulation can only frustrate the growth of cyberspace. The need for uniformity in this unique sphere of commerce requires that New York's law be stricken as a violation of the Commerce Clause.

III. The First Amendment and the Internet

Plaintiffs have also asserted their entitlement to a preliminary injunction on the grounds that the Act unconstitutionally burdens free speech. Plaintiffs' ability to demonstrate the Act's unconstitutionality under the Commerce Clause, however, provides fully adequate support for the issuance of a preliminary injunction. Moreover, the Supreme Court heard argument on a First

Amendment challenge to the federal statute, the CDA, on March 19, 1997. The New York Act was clearly modeled on the CDA. I believe any determination of plaintiffs' First Amendment challenge should therefore await the the Supreme Court's forthcoming opinion.

**CONCLUSION**

The protection of children from pedophilia is an entirely laudable goal of state legislation. The New York Act's attempts to effectuate that goal, however, fall afoul of the Commerce Clause for three reasons. First, the practical impact of the New York Act results in the extraterritorial application of New York law to transactions involving citizens of other states and is therefore per se violative of the Commerce Clause. Second, the benefits derived from the Act are inconsequential in relation to the severe burdens it imposes on interstate commerce. Finally, the unique nature of cyberspace necessitates uniform national treatment and bars the states from enacting inconsistent regulatory schemes. Because plaintiffs have demonstrated that they are likely to succeed on the merits of their claim and that they face irreparable injury in the absence of an injunction, the motion for a preliminary injunction is granted.

## THE STATE OF WASHINGTON v. HECKEL

24 P.3d 404 (Wash. 2001)

**OPINION**

En Banc. Owens, J. -- The State of Washington filed suit against Oregon resident Jason Heckel, alleging that his transmissions of e-mail to Washington residents violated Washington's commercial electronic mail act, chapter 19.190 RCW (the Act). On cross-motions for summary judgment, the trial court dismissed the State's suit against Heckel, concluding that the Act violated the dormant Commerce Clause of the United States Constitution. This court granted the State's request for direct review. We hold that the Act does not unduly burden interstate commerce. We reverse the trial court's dismissal of the State's suit.

FACTS

As early as February 1996, defendant Jason Heckel, an Oregon resident doing business as Natural Instincts, began sending unsolicited commercial e-mail (UCE), or "spam," over the Internet.[2] In 1997, Heckel developed a 46-page on-line booklet entitled "How to Profit from the Internet." The booklet described how to set up an on-line promotional business, acquire free e-

[2] "'Commercial electronic mail message' means an electronic mail message sent for the purpose of promoting real property, goods, or services for sale or lease." RCW 19.190.010(2). The term "spam" refers broadly to unsolicited bulk e-mail (or "'junk' e-mail"), which "can be either commercial (such as an advertisement) or noncommercial (such as a joke or chain letter)." Use of the term "spam" as Internet jargon for this seemingly ubiquitous junk e-mail arose out of a skit by the British comedy troupe Monty Python, in which a waitress can offer a patron no single menu item that does not include spam: "Well, there's spam, egg, sausage and spam. That's not got *much* spam in it."

mail accounts, and obtain software for sending bulk e-mail. From June 1998, Heckel marketed the booklet by sending between 100,000 and 1,000,000 UCE messages per week. To acquire the large volume of e-mail addresses, Heckel used the Extractor Pro software program, which harvests e-mail addresses from various on-line sources and enables a spammer to direct a bulk-mail message to those addresses by entering a simple command. The Extractor Pro program requires the spammer to enter a return e-mail address, a subject line, and the text of the message. The text of Heckel's UCE was a lengthy sales pitch that culminated in an order form that the recipient could download and print. The order form included the Salem, Oregon, mailing address for Natural Instincts. Charging $39.95 for the booklet, Heckel made 30 to 50 sales per month.

In June 1998, the Consumer Protection Division of the Washington State Attorney General's Office received complaints from Washington recipients of Heckel's UCE messages. The complaints alleged that Heckel's messages contained misleading subject lines and false transmission paths.[3] Responding to the June complaints, David Hill, an inspector from the Consumer Protection Division, sent Heckel a letter advising him of the existence of the Act. The Act provides that anyone sending a commercial e-mail message from a computer located in Washington or to an e-mail address held by a Washington resident may not use a third party's domain name without permission, misrepresent or disguise in any other way the message's point of origin or transmission path, or use a misleading subject line.[4] RCW 19.190.030 makes a

---

[3] Each e-mail message contains so-called "header" information in the "To," "From," and "Received" fields. When an e-mail message is transmitted from one e-mail address to another, the message generally passes through at least four computers: from the sender's computer, the message travels to the mail server computer of the sender's Internet Service Provider (ISP); that computer delivers the message to the mail server computer of the recipient's ISP, where it remains until the recipient retrieves it onto his or her own computer. Every computer on the Internet has a unique numerical address (an Internet Protocol or IP address), which is associated with a more readily recognizable domain name (such as "mysite.com"). As the e-mail message travels from sender to recipient, each computer transmitting the message attaches identifying data to the "Received" field in the header. The information serves as a kind of electronic postmark for the handling of the message. It is possible for a sender to alter (or "spoof") the header information by misidentifying either the computer from which the message originated or other computers along the transmission path.

[4] "(1) No person may initiate the transmission, conspire with another to initiate the transmission, or assist the transmission, of a commercial electronic mail message from a computer located in Washington or to an electronic mail address that the sender knows, or has reason to know, is held by a Washington resident that:

"(a) Uses a third party's internet domain name without permission of the third party, or otherwise misrepresents or obscures any information in identifying the point of origin or the transmission path of a commercial electronic mail message; or

"(b) Contains false or misleading information in the subject line.

"(2) For purposes of this section, a person knows that the intended recipient of a commercial

violation of the Act a per se violation of the Consumer Protection Act (CPA).

Responding to Hill's letter, Heckel telephoned Hill on or around June 25, 1998. According to Hill, he discussed with Heckel the provisions of the Act and the procedures bulk e-mailers can follow to identify e-mail addressees who are Washington residents. Nevertheless, the Attorney General's Office continued to receive consumer complaints alleging that Heckel's bulk e-mailings from Natural Instincts appeared to contain misleading subject lines, false or unusable return e-mail addresses, and false or misleading transmission paths.

On October 22, 1998, the State filed suit against Heckel, stating three causes of action. First, the State alleged that Heckel had violated RCW 19.190.020(1)(b) and, in turn, the CPA, by using false or misleading information in the subject line of his UCE messages. Heckel used one of two subject lines to introduce his solicitations: "Did I get the right e-mail address?" and "For your review--HANDS OFF!" In the State's view, the first subject line falsely suggested that an acquaintance of the recipient was trying to make contact, while the second subject line invited the misperception that the message contained classified information for the recipient's review.

As its second cause of action, the State alleged that Heckel had violated RCW 19.190.020(1)(a), and thus the CPA, by misrepresenting information defining the transmission paths of his UCE messages. Heckel routed his spam through at least a dozen different domain names without receiving permission to do so from the registered owners of those names.

Additionally, the State alleged that Heckel had violated the CPA by failing to provide a valid return e-mail address to which bulk-mail recipients could respond. When Heckel created his spam with the Extractor Pro software, he used at least a dozen different return e-mail addresses with the domain name "juno.com" (Heckel used the Juno accounts in part because they were free). None of the Juno e-mail accounts was readily identifiable as belonging to Heckel; the user names that he registered generally consisted of a name or a name plus a number (e.g., "marlin1374," "cindyt5667," "howardwesley13," "johnjacobson 1374," and "sjtowns"). During August and September 1998, Heckel's Juno addresses were canceled within two days of his sending out a bulk e-mail message on the account. According to Heckel, when Juno canceled one e-mail account, he would simply open a new one and send out another bulk mailing. Because Heckel's accounts were canceled so rapidly, recipients who attempted to reply were unsuccessful. The State thus contended that Heckel's practice of cycling through e-mail addresses ensured that those addresses were useless to the recipients of his messages. During the months that Heckel was sending out bulk e-mail solicitations on the Juno accounts, he maintained a personal e-mail account from which he sent no spam, but that e-mail address was not included in any of his spam messages. The State asserted that Heckel's use of such ephemeral e-mail addresses in his UCE amounted to a deceptive practice in violation of RCW 19.86.020.

ISSUE

Does the Act, which prohibits misrepresentation in the subject line or transmission path of

---

electronic mail message is a Washington resident if that information is available, upon request, from the registrant of the Internet domain name contained in the recipient's electronic mail address." RCW 19.190.020.

any commercial e-mail message sent to Washington residents or from a Washington computer, unconstitutionally burden interstate commerce?

ANALYSIS

*Heckel's Challenge under the Commerce Clause.* The Commerce Clause grants Congress the "power . . . to regulate commerce with foreign nations, and among the several states." Implicit in this affirmative grant is the negative or "dormant" Commerce Clause--the principle that the states impermissibly intrude on this federal power when they enact laws that unduly burden interstate commerce. Analysis of a state law under the dormant Commerce Clause generally follows a two-step process. We first determine whether the state law openly discriminates against interstate commerce in favor of intrastate economic interests. If the law is facially neutral, applying impartially to in-state and out-of-state businesses, the analysis moves to the second step, a balancing of the local benefits against the interstate burdens:

> Where the statute regulates evenhandedly 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, then the question becomes one of degree.

*Pike v. Bruce Church, Inc*., 397 U.S. 137, 142 (1970).

The Act is not facially discriminatory. The Act applies evenhandedly to in-state and out-of-state spammers: "*No person*" may transmit the proscribed commercial e-mail messages "from a computer located in Washington or to an electronic mail address that the sender knows, or has reason to know, is held by a Washington resident." Thus, just as the statute applied to Heckel, an Oregon resident, it is enforceable against a Washington business engaging in the same practices.

Because we conclude that the Act's local benefits surpass any alleged burden on interstate commerce, the statute likewise survives the *Pike* balancing test. The Act protects the interests of three groups--ISPs (Internet Sevice Provider), actual owners of forged domain names, and e-mail users. The problems that spam causes have been discussed in prior cases and legislative hearings. A federal district court described the harms a mass e-mailer caused ISP CompuServe:

> Handling the enormous volume of mass mailings that CompuServe receives places a tremendous burden on its equipment. Defendants' more recent practice of evading CompuServe's filters by disguising the origin of their messages commandeers even more computer resources because CompuServe's computers are forced to store undeliverable e-mail messages and labor in vain to return the messages to an address that does not exist. To the extent that defendants' multitudinous electronic mailings demand the disk space and drain the processing power of plaintiff's computer equipment, those resources are not available to serve CompuServe subscribers. Therefore, the value of that equipment to CompuServe is diminished even though it is not physically damaged by defendants' conduct.

*CompuServe Inc. v. Cyber Promotions, Inc*., 962 F. Supp. 1015, 1022 (S.D. Ohio 1997) (granting preliminary injunction against bulk e-mailer on theory of trespass to chattels). To handle the increased e-mail traffic attributable to deceptive spam, ISPs must invest in more computer

equipment. Operational costs likewise increase as ISPs hire more customer service representatives to field spam complaints and more system administrators to detect accounts being used to send spam.

Along with ISPs, the owners of impermissibly used domain names and e-mail addresses suffer economic harm. For example, the registered owner of "localhost.com" alleged that his computer system was shut down for three days by 7,000 responses to a bulk-mail message in which the spammer had forged the e-mail address "nobody@localhost.com" into his spam's header. *Seidl v. Greentree Mortgage Co*., 30 F. Supp. 2d 1292, 1297-98 (D. Colo. 1998).

Deceptive spam harms individual Internet users as well. When a spammer distorts the point of origin or transmission path of the message, e-mail recipients cannot promptly and effectively respond to the message (and thereby opt out of future mailings); their efforts to respond take time, cause frustration, and compound the problems that ISPs face in delivering and storing the bulk messages. And the use of false or misleading subject lines further hampers an individual's ability to use computer time most efficiently. When spammers use subject lines "such as 'Hi There!,' 'Information Request,' and 'Your Business Records,'" it becomes "virtually impossible" to distinguish spam from legitimate personal or business messages. Individuals who do not have flat-rate plans for Internet access but pay instead by the minute or hour are harmed more directly, but all Internet users (along with their ISPs) bear the cost of deceptive spam.

This cost-shifting--from deceptive spammers to businesses and e-mail users--has been likened to sending junk mail with postage due or making telemarketing calls to someone's pay-per-minute cellular phone. We thus recognize that the Act serves the "legitimate local purpose" of banning the cost-shifting inherent in the sending of deceptive spam.

Under the *Pike* balancing test, "if a legitimate local purpose is found, then the question becomes one of degree." In the present case, the trial court questioned whether the Act's requirement of truthfulness (in the subject lines and header information) would redress the costs associated with bulk e-mailings. As legal commentators have observed, however, "the truthfulness requirements make spamming unattractive to the many fraudulent spammers, thereby reducing the volume of spam." Jack L. Goldsmith & Alan O. Sykes, *The Internet and the Dormant Commerce Clause,* 110 Yale L.J. 785, 819 (2001). Calling "simply wrong" the trial court's view "that truthful identification in the subject header would do little to relieve the annoyance of spam," the commentators assert that "this identification alone would allow many people to delete the message without opening it (which takes time) and perhaps being offended by the content." The Act's truthfulness requirements thus appear to advance the Act's aim of protecting ISPs and consumers from the problems associated with commercial bulk e-mail.

To be weighed against the Act's local benefits, the only burden the Act places on spammers is the requirement of truthfulness, a requirement that does not burden commerce at all but actually "facilitates it by eliminating fraud and deception." Spammers must use an accurate, nonmisleading subject line, and they must not manipulate the transmission path to disguise the origin of their commercial messages. While spammers incur no costs in complying with the Act, they do incur costs for noncompliance, because they must take steps to introduce forged information into the header of their message. In finding the Act "unduly burdensome," the trial court apparently focused not on what spammers must do to comply with the Act but on what

they must do if they choose to use deceptive subject lines or to falsify elements in the transmission path. To initiate *deceptive* spam without violating the Act, a spammer must weed out Washington residents by contacting the registrant of the domain name contained in the recipient's e-mail address. This focus on the burden of noncompliance is contrary to the approach in the *Pike* balancing test, where the United States Supreme Court assessed the cost of compliance with a challenged statute. Indeed, the trial court could have appropriately considered the filtering requirement a burden only if Washington's statute had banned outright the sending of UCE messages to Washington residents. We therefore conclude that Heckel has failed to prove that "the burden imposed on . . . commerce [by the Act] is *clearly excessive* in relation to the putative local benefits."

Drawing on two "unsettled and poorly understood" aspects of the dormant Commerce Clause analysis, Heckel contended that the Act (1) created inconsistency among the states and (2) regulated conduct occurring wholly outside of Washington. The inconsistent-regulations test and the extraterritoriality analysis are appropriately regarded as facets of the *Pike* balancing test. The Act survives both inquiries. At present, 17 other states have passed legislation regulating electronic solicitations. The truthfulness requirements of the Act do not conflict with any of the requirements in the other states' statutes, and it is inconceivable that any state would ever pass a law requiring spammers to use misleading subject lines or transmission paths. Some states' statutes do include additional requirements; for example, some statutes require spammers to provide contact information (for opt-out purposes) or to introduce subject lines with such labels as "ADV" or "ADV-ADLT." But because such statutes "merely create additional, but not irreconcilable, obligations," they "are not considered to be 'inconsistent'" for purposes of the dormant Commerce Clause analysis. The inquiry under the dormant Commerce Clause is not whether the states have enacted different anti-spam statutes but whether those differences create compliance costs that are "clearly excessive in relation to the putative local benefits." *Pike*, 397 U.S. at 142. We do not believe that the differences between the Act and the anti-spam laws of other states impose extraordinary costs on businesses deploying spam.

Nor does the Act violate the extraterritoriality principle in the dormant Commerce Clause analysis. Here, there is no "sweeping extraterritorial effect" that would outweigh the local benefits of the Act. Heckel offers the hypothetical of a Washington resident who downloads and reads the deceptive spam while in Portland or Denver. He contends that the dormant Commerce Clause is offended because the Act would regulate the recipient's conduct while out of state. However, the Act does not burden interstate commerce by regulating when or where recipients may open the proscribed UCE messages. Rather, the Act addresses the conduct of spammers in targeting Washington consumers. Moreover, the hypothetical mistakenly presumes that the Act must be construed to apply to Washington residents when they are out of state, a construction that creates a jurisdictional question not at issue in this case.

In sum, we reject the trial court's conclusion that the Act violates the dormant Commerce Clause. Although the trial court found particularly persuasive *American Libraries Association v. Pataki*, 969 F. Supp. 160 (S.D.N.Y. 1997), that decision--the first to apply the dormant Commerce Clause to a state law on Internet use--is distinguishable in a key respect. At issue in *American Libraries* was a New York statute that made it a crime to use a computer to distribute harmful, sexually explicit content to minors. The statute applied not just to initiation of e-mail

messages but to all Internet activity, including the creation of websites. Thus, under the New York statute, a website creator in California could inadvertently violate the law simply because the site could be viewed in New York. Concerned with the statute's "chilling effect," the court observed that, if an artist "were located in California and wanted to display his work to a prospective purchaser in Oregon, he could not employ his virtual [Internet] studio to do so without risking prosecution under the New York law." In contrast to the New York statute, which could reach all content posted on the Internet and therefore subject individuals to liability based on unintended access, the Act reaches only those deceptive UCE messages directed to a Washington resident or initiated from a computer located in Washington; in other words, the Act does not impose liability for messages that are merely routed through Washington or that are read by a Washington resident who was not the actual addressee.

CONCLUSION

We find that the local benefits of the Act outweigh any conceivable burdens the Act places on those sending commercial e-mail messages. Consequently, we hold that the Act does not violate the dormant Commerce Clause of the United States Constitution. We reverse the trial court and remand the matter for trial.

**Note:** In 2003, a federal law was enacted to regulate unsolicited commercial email. The federal statute known as the "Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003" or "CAN-SPAM Act" took effect on January 1, 2004. 15 U.S.C.A. § 7701 et seq. (2004). The CAN-SPAM Act preempts existing state anti-spam laws "except to the extent that any such statute, regulation, or rule prohibits falsity or deception in any portion of a commercial electronic mail message or information attached thereto." *Id.* at § 7707(b)(1). Because state laws regulating spam, like the Washington law at issue in *Heckel*, generally prohibit falsity or deception, rather than regulate spam in other ways, courts considering the impact of the federal law on state anti-spam laws have found that state laws fall within the "except" clause of the federal law and are, therefore, not pre-empted by the federal law. E.g., MaryCLE, LLC v. First Choice Holdings, Inc., 890 A.2d 818 (Md. Special App. Ct. 2006).

## NATIONAL FEDERATION OF THE BLIND v. TARGET CORPORATION

452 F. Supp. 2d 946 (N.D. Cal. 2006)

MARILYN HALL PATEL, United States District Judge.

Plaintiffs National Federation of the Blind, National Federation of the Blind of California, Bruce Sexton, and all those similarly situated, filed this action against Target Corporation ("Target"). Plaintiffs claim that Target.com is inaccessible to the blind, and thereby violates federal and state laws prohibiting discrimination against the disabled.

. . .

Commerce Clause

Defendant argues that even if plaintiffs state a claim under the Unruh and Disabled Persons Acts, applying these statutes to regulate Target.com violates the dormant commerce clause.

Defendant advances two reasons that such regulation would violate the commerce clause. First, state regulation of Target.com would regulate conduct occurring wholly outside of California. Second, state regulation of Target.com would regulate an area of commerce that is reserved exclusively for Congress.

1. Extraterritorial Regulation

Courts in several circuits have invalidated state laws regulating the internet on the grounds that *any* regulation of the internet regulates conduct occurring outside the borders of the state. See, e.g., American Booksellers Found. v. Dean, 342 F.3d 96 (2d Cir. 2003) (striking down a Vermont law outlawing the knowing distribution of material harmful to a minor because residents of other states who post to the web would be subject to prosecution in Vermont); Psinet, Inc. v. Chapman, 362 F.3d 227 (4th Cir. 2004) (invalidating a Virginia law that criminalized the dissemination of material harmful to minors over the internet on the grounds that any regulation of the internet necessarily regulates conduct occuring entirely out-of-state); ACLU v. Johnson, 194 F.3d 1149 (10th Cir. 1999) (concluding that a New Mexico law criminalizing the dissemination by computer of material harmful to a minor violated the commerce clause because state regulation of the internet necessarily controls transactions outside the state); Center for Democracy and Tech. v. Pappert, 337 F. Supp. 2d 606 (E.D. Pa. 2004) (holding that a law requiring Internet Service Providers to remove or disable access to child pornography applied the policies of Pennsylvania to internet transactions in other states).

The cases cited above relied extensively on the analysis of the Southern District of New York in American Libraries Association v. Pataki, 969 F. Supp. 160 (S.D.N.Y. 1997). At issue in that case was the constitutionality of a New York law criminalizing the intentional use of a computer to transmit sexually explicit material to a minor. The court held that the law violated the dormant commerce clause on three separate grounds: the statute regulated conduct occuring wholly outside of New York; the burdens of the law on interstate commerce outweighed the benefits; and regulation of the internet is reserved exclusively for Congress. According to the Pataki court, all on-line communication is inter-state; purely intra-state communication is impossible. State regulation of the internet, then, necessarily subjects people in other states to New York law. A California resident posting to the web, for intended viewing by a resident of Oregon, would risk prosecution under New York law, because New Yorkers could access the website.

By contrast, several state and federal courts have held that states may regulate the internet without violating the commerce clause. For example, courts have upheld state anti-spam statutes by distinguishing the regulation of e-mail from the regulation of internet postings; e-mail messages can be targeted at recipients in particular geographical areas, whereas a posting to the internet is accessible to any internet user, regardless of location. See Ferguson v. Friendfinders, Inc., 115 Cal. Rptr. 2d 258 (Cal. Ct. App. 2002) (holding that a state law regulating unsolicited e-mail applied only to California residents receiving email through equipment located in California and thus did not regulate conduct outside California); MaryCLE, LLC v. First Choice Internet, Inc., 890 A.2d 818 (Md. Ct. Spec. App. 2006) (upholding a law prohibiting the transmission of email containing false information to a Maryland email address, on the grounds that the regulation applied only to transactions that used a computer in Maryland or were sent to an address in Maryland); Washington v. Heckel, 24 P.3d 404 (Wash. 2001) (upholding a law

prohibiting the dissemination of false or misleading information from a computer in Washington or to an email address in Washington, on the grounds that the statute did not regulate conduct outside the state).

Other courts have upheld state laws regulating the internet by reasoning that the statute was intended to apply only to local conduct, or that the state would enforce the law only against conduct occurring within the state. See, e.g., Ford Motor Co. v. Texas Dept. Of Transp., 264 F.3d 493 (5th Cir. 2001) (upholding a Texas law that made it illegal for Ford to sell used vehicles via a website); People v. Hsu, 99 Cal. Rptr. 2d 184 (Cal. Ct. App. 2000) (rejecting a commerce clause challenge to a California law criminalizing use of the internet to knowingly distribute to a minor matter harmful to a minor on the grounds that the legislature intended to criminalize only conduct occurring within California); People v. Lipsitz, 663 N.Y.S.2d 468 (N.Y. App. Div. 1997) (rejecting a commerce clause challenge to application of consumer protection laws to an on-line business, on the grounds that the law was intended to regulate only local conduct);

Defendant distinguishes the cases relied upon by plaintiffs -- Ford, Hsu, and Friendfinders -- on three grounds. First, defendant contends that the laws at issue in these cases did not directly regulate the internet since they did not involve the programming of a website. This argument is factually correct but legally meaningless. Since programming of a website has no heightened constitutional protection (or even statutory protection), there is no basis for drawing any legal conclusion from this fact. All of these decisions impacted conduct that would occur on or through the internet.

Second, defendant asserts that none of these laws controlled conduct beyond the borders of the states. It is true that the statute challenged in Friendfinders did not control conduct outside California because the law regulated e-mail sent to residents of California via equipment located in California. Similarly, the Texas statute at issue in Ford did not control conduct outside of the state. If enforced, the statute would simply prohibit Ford from selling vehicles to Texas consumers and shipping them to Texas dealers; Ford's website and sales in other states would be unaffected.

Defendant's third argument is that the practical effect of regulating Target.com is to regulate conduct outside California *because of the nature of the internet*. Since Target.com is a single website viewed by customers nationwide, a modification mandated by California necessarily regulates the transactions of customers in other states who use Target.com. However, Plaintiffs respond that it is technologically and economically feasible to establish a separate website directing Target.com visitors to a California-specific site in compliance with state laws and avoiding a commerce clause violation. Defendant maintains that even if it could design a separate website for only California customers, this would still violate the commerce clause.

However, in Healy v. Beer Institute, 491 U.S. 324 (1989)(plurality opinion), the Supreme Court held that:

> . . . a statute that directly controls commerce occurring wholly outside the boundaries of a State exceeds the inherent limits of the enacting State's authority and is invalid regardless of whether the statute's extraterritorial reach was intended by the legislature. The critical inquiry is whether the practical effect of the regulation is

to control conduct beyond the boundaries of the State.

Healy, 491 U.S. at 336. Thus, to determine what the "practical" effects of the regulation are, courts should inquire into the actual effects of state legislation rather than the effects intended by the legislature. The Connecticut beer-pricing statute at issue in Healy stated that nothing in the statute prevented out-of-state shippers from changing their prices outside Connecticut. Yet the statute made it illegal for these shippers to sell beer in Connecticut at a higher price than that in a bordering state during the time period covered by the Connecticut posted price. Thus, despite the legislature's stated intentions, the statute had the effect of controlling prices outside Connecticut; the statute limited the prices a shipper could charge outside of Connecticut once the shipper had posted a price for Connecticut beer.

Defendant's argument -- that if this court applies the Unruh Act and the Disabled Persons Acts to Target.com, the practical effect will be to force it to modify its website for all customers nationwide -- is not sustainable. This assumes that Target would decline to design a separate California site, and instead simply modify its Target.com site for consumers nationwide. Healy lends no support to defendant's argument, since Healy does not address whether a statute violates the commerce clause when a defendant can comply with a statute in such a way as to avoid extraterritorial application. The commerce clause is not necessarily implicated since Target could choose to make a California-specific website.

Indeed, even if Target chooses to change its entire website in order to comply with California law, this does not mean that California is regulating out-of-state conduct. Courts have held that when a defendant chooses to manufacture one product for a nationwide market, rather than target its products to comply with state laws, defendant's choice does not implicate the commerce clause. See, e.g., Lorillard Tobacco Co. v. Reilly, 84 F. Supp. 2d 180, 199-200 (D. Mass. 2000) (holding that a Massachusetts labeling law for cigars did not violate the commerce clause even though cigar companies preferred to label their packages the same way nationwide for the purpose of efficiency); Ferguson, 94 Cal. App. 4th at 1265 (rejecting the argument that since e-mail advertisements are sent in an automated fashion, it is impractical to sort e-mails by location, and holding that a company's decision to conform all of its e-mail to California law did not implicate the commerce clause).

Moreover, it is noteworthy that various commentators have observed that the case which many courts have followed in invalidating state regulation of the internet, Pataki, rests on an incorrect technical understanding of the internet. See, e.g., Jack L, Goldsmith & Alan O. Sykes, *The Internet and the Dormant Commerce Clause*, 110 Yale L.J. 785, 882 (2001) (noting that contrary to the assumption of many courts, including the Pataki court, internet content providers can identify the geographic location of their users and target content based on the location of the users). Pataki asserts that someone who puts content on the internet has "no way to determine the characteristics of their audience . . . [such as] age and geographical location." This is simply incorrect. It is common practice for websites for entities operating in multiple countries to have a single site that directs customers to different versions based upon language. Websites can determine the location of a user from information they provide, such as a credit card number, or from the internet service provider an individual uses. It may, or may not, be prohibitively expensive for a website to tailor its content based on the location of its users, but it is certainly technically feasible.

Given the foregoing, the court finds that it is inappropriate at the motion to dismiss stage to assert a commerce clause violation based on the mere fact that Target, at the remedy stage, may ultimately choose to make its nationwide website accessible to the blind. The Supreme Court has noted that the relevant inquiry is the "practical effect" of the law. At this juncture, it would be premature for the court to determine what the practical effect of imposing California's accessibility requirements upon Target.com will be.

2. Exclusive Province of Congress

Defendant argues that under the dormant commerce clause California cannot regulate Target.com because the internet requires uniform, national regulations.

The commerce clause prevents a state from regulating "those phases of the national commerce which, because of the need of national uniformity, demand that their regulation, if any, be prescribed by a single authority." Southern Pac. Co. v. Arizona, 325 U.S. 761, 767 (1945). In 1912, Arizona passed a law prohibiting railroad trains from having more than fourteen passenger or seventy freight cars. Most other states did not regulate the number of cars in a train, although some states had length limits that differed from Arizona's limit. The practical effect of the Arizona law was to force railroad companies to break up and reconfigure their trains prior to entering, and after leaving, Arizona. The Supreme Court found that the Arizona law imposed a "serious burden" on interstate railroad traffic, costing Southern Pacific over one million dollars per year and forcing significant delays in service while the trains were broken up and reconfigured. The law did not significantly improve safety, and may have actually increased accidents by increasing the number of trains. Given the law's uncertain effect on safety, and the evidence of cost increases and service delays, the state interest in safety was outweighed by the national interest in "economical and efficient railway transportation service." The Court struck down the law as violating the commerce clause.

By contrast, in Exxon Corp v. Governor of Maryland, the Supreme Court upheld a Maryland law prohibiting a producer or refiner of petroleum from operating a retail gas station. 437 U.S. 117 (1978). The Supreme Court determined that the law did not seriously burden the flow of interstate commerce, because even if certain firms withdrew from the Maryland market, they would be replaced by others. The commerce clause does not protect the market structure, or the market share of firms. Moreover, the existence of a national market in gasoline did not preempt the states from regulating retail gasoline sales. Exxon did not face conflicting state regulations of its national enterprise, but rather feared that all states would follow Maryland; several states had enacted or proposed similar legislation requiring producers to divest their retail holdings.

Similarly, in Allied Artists Pictures Corp. v. Rhodes, a district court upheld an Ohio statute against a commerce clause challenge. 496 F. Supp. 408 (S.D. Ohio 1980). Ohio passed a law prohibiting "blind bidding" -- licensing a movie to a theatre before the theatre owner is able to view the picture. The law also altered other practices in the licensing of movies in Ohio. Following Exxon, the court rejected the argument that states cannot regulate movie licensing merely because the market for movies is national in scope. Other states which regulated the distribution and licensing of films had laws similar to the Ohio statute. The court found the situation analogous to Exxon, in that the companies did not face conflicting state regulations but rather feared that all states would adopt similar regulations banning blind bidding.

Regulations issued by the Attorney General of Massachusetts concerning advertising and warning labels for cigars were challenged in Lorillard Tobacco Co. v. Reilly, 84 F. Supp. 2d 180 (D. Mass. 2000). Cigar companies were required to place warning labels on their products for the first time. The court rejected the argument that Massachusetts could not require warning labels on cigars because the market for cigars is national in scope. Warning stickers could be placed on only those products sold in Massachusetts. If, as a result of the Massachusetts regulations, the cigar companies found it more efficient to put the same warning on all cigars, that did not implicate the commerce clause.

However, the court invalidated the application of the advertising regulations to national media, such as magazines, on the grounds that the burdens on interstate commerce would outweigh the state's interest in promoting public health. The regulations would otherwise require a company which placed an advertisement in a national market to comply with the Massachusetts regulations in the event that the edition wound up in Massachusetts. If a magazine runs a "Massachusetts edition," however, it must comply with the regulations.

Applying the forgoing commerce clause analysis to the internet, several courts have held that only Congress can regulate the internet, since the internet requires uniform, national regulations. The most extensive analysis is provided by Pataki. The court analogized the internet to the interstate railroad and highway systems, implying that just as a single train or car travels through interstate systems, so internet communication travels across states. Different state regulations would subject internet users to chaotic, conflicting mandates. A user would have to comply with the most stringent state standard or forgo use of the internet altogether. The court offered the example of different state standards for material harmful to minors posted on the internet. An individual posting information on-line could not restrict access to users from other states, so a user would be subject to prosecution in all states; each state might have a different definition of what material is considered "harmful to minors."

However, a state's ability to extend benefits or protections to its citizens through its laws is not necessarily precluded by the failure of Congress to act. Indeed, Congress' inaction can be viewed as an encouragement to state legislatures to fill the gaps left in the statute. Thus, the lack of congressional action explicitly addressing accessibility requirements for private websites should not be construed to bar the extension of the protections of California statutes to these websites. Such a construal would mean that in an age when commerce is increasingly conducted on and through the internet, a legal vacuum would be created whereby strategic actors could avoid prosecution and violate state laws with impunity. Indeed, some courts have found that the internet should not be exempt from state regulation. See, e.g., Ford, 264 F.3d at 505 (rejecting the idea that state laws of general applicability cannot apply to the internet, on the grounds that internet activity would otherwise be immune from state regulation); Lipsitz, 663 N.Y.S.2d at 475 (holding that states should be able to regulate conduct on the internet).

**Note:** Despite setting out her Commerce Clause analysis, Judge Patel found it unnecessary to rule on the Commerce Clause issue.