

UNITED STATES DISTRICT COURT  
SOUTHERN DISTRICT OF NEW YORK

-----X  
AMERICAN LIBRARY ASSOCIATION; :  
FREEDOM TO READ FOUNDATION, INC.; :  
NEW YORK LIBRARY ASSOCIATION; :  
WESTCHESTER LIBRARY SYSTEM; :  
AMERICAN BOOKSELLERS FOUNDATION :  
FOR FREE EXPRESSION; ASSOCIATION :  
OF AMERICAN PUBLISHERS, INC.; :  
BIBLIOBYTES, INC.; MAGAZINE :  
PUBLISHERS OF AMERICA, INC.; :  
INTERACTIVE DIGITAL SOFTWARE :  
ASSOCIATION; PUBLIC ACCESS :  
NETWORKS CORPORATION; ECHO; :  
NEW YORK CITY NET; ART ON THE :  
NET; PEACEFIRE; and AMERICAN : Civil Action No. 97- 0222 (LAP)  
CIVIL LIBERTIES UNION, :  
:  
Plaintiffs, :  
:  
v. :  
:  
GEORGE PATAKI, in his official :  
capacity as Governor of the :  
State of New York; and :  
DENNIS VACCO, in his official :  
capacity as Attorney General of :  
the State of New York, :  
:  
Defendants. :  
-----X

**PLAINTIFFS' MEMORANDUM OF LAW  
IN SUPPORT OF THEIR MOTION FOR  
A PRELIMINARY INJUNCTION**

## TABLE OF CONTENTS

	PAGE
PRELIMINARY STATEMENT . . . . .	1
I. STATEMENT OF FACTS . . . . .	3
A. Plaintiffs and Their Speech . . . . .	3
B. The Challenged Statute . . . . .	6
C. The Internet . . . . .	8
1. The Nature of the Online Medium . . . . .	8
2. How Individuals Access the Internet . . . . .	10
3. Ways of Communicating and Exchanging Information on the Internet . . . . .	11
4. The Inability of Speakers to Prevent Their Speech from Reaching Minors . . . . .	16
5. The Availability of User-Based Filtering Programs . . . . .	17
II. ARGUMENT . . . . .	18
A. Plaintiffs Have a Substantial Likelihood of Success on the Merits . . . . .	19
1. The Act Effectively Bans Constitutionally Protected Speech, and Therefore Cannot Survive Strict Scrutiny . . . . .	20

2.	The Act's Defenses Fail to Save the Act . . . . .	23
a.	Credit Card and Age Verification Are Technologically Unavailable for the Vast Majority of Online Speakers, and Impose Unconstitutional Burdens on Other Speakers . . . . .	24
b.	There Is No Other Method That Enables an Online Speaker to Ascertain the Age of Her Audience . . . . .	28
c.	There Is No Way for Online Speakers to Label or Segregate Their Speech in a Way That Could Be Automatically Blocked From Minors . . . . .	28
d.	There Are No Other "Good Faith, Effective" Actions That Speakers Could Take to Restrict Access to Minors . . . . .	31
e.	There Is No Way for Online Speakers to Know the Characteristics or Purposes of Their Audience . . . . .	31
3.	The Act Is An Ineffective Method For Achieving the Government's Interest, and Less Restrictive, More Effective, Alternatives Are Available to Parents . . . . .	32
4.	The Act Is Substantially Overbroad . . . . .	35
a.	The Act's Failure to Define the Applicable Community Standard Renders It Overboard . . . . .	35

b.	The Act Is Overbroad Because It Criminalizes Speech That Is Constitutionally Protected for Older Minors . . . . .	36
5.	The Act Is Unconstitutionally Vague . . . . .	38
6.	The Act Violates the Commerce Clause of the United States Constitution . . . . .	42
a.	The Act Is Per Se Invalid Because It Regulates Commerce Entirely Outside of the State of New York . . . . .	42
b.	The Act Is Invalid Because the Burdens It Imposes Upon Interstate Commerce Exceed Any Local Benefit . . . . .	44
c.	The Act Violates the Commerce Clause Because It Subjects Interstate Use of the Internet to Inconsistent Regulations . . . . .	44
B.	Plaintiffs Will Suffer Irreparable Harm if Preliminary Relief Is Not Granted . . . . .	45
C.	There are Sufficiently Serious Questions to Make a Fair Ground for Litigation and the Balance of Hardships Weighs in the Plaintiffs' Favor . . . . .	47
CONCLUSION . . . . .		48

## TABLE OF AUTHORITIES

CASES	PAGE(S)
<u>ACLU v. Reno,</u> 929 F. Supp. 824 (E.D. Pa.), <u>prob. juris. noted.</u> 117 S. Ct. 554 (1996) .....	<u>passim</u>
<u>Able v. United States,</u> 44 F.3d 128 (2d Cir. 1995) .....	18
<u>Almonte v. Pierce,</u> 666 F. Supp. 517 (S.D.N.Y. 1987) .....	18
<u>American Booksellers Association, Inc. v. Virginia,</u> 882 F.2d 125 (4th Cir. 1989) .....	37
<u>American Booksellers v. Webb,</u> 919 F.2d 1493 (11th Cir. 1990) .....	21, 37
<u>Baldwin v. G.A.F. Seeling, Inc.,</u> 294 U.S. 511, 55 S. Ct. 497 (1935) .....	44
<u>Bantam Books Inc. v. Sullivan,</u> 372 U.S. 58, 83 S. Ct. 631 (1963) .....	29
<u>Board of Education v. Pico,</u> 457 U.S. 853, 102 S. Ct. 2799 (1982) .....	36
<u>Bolger v. Youngs Drug Products Corp.,</u> 463 U.S. 60, 103 S. Ct. 2875 (1983) .....	21, 33
<u>Broadrick v. Oklahoma,</u> 413 U.S. 601, 93 S. Ct. 2908 (1973) .....	22
<u>Brown-Forman Distillers Corp. v. New York State Liquor Authority,</u> 476 U.S. 578, 106 S. Ct. 2080 (1986) .....	42, 43
<u>Butler v. Michigan,</u> 352 U.S. 380, 77 S. Ct. 524 (1957) .....	21

<u>C. &amp; A. Carbone, Inc. v. Town of Clarkstown,</u> 770 F. Supp. 848 (S.D.N.Y. 1991) .....	46
<u>Carey v. Klutznick,</u> 637 F.2d 834 (2d Cir. 1980) .....	18
<u>Carey v. Population Services, International,</u> 431 U.S. 678, 97 S. Ct. 2010 (1977) .....	36
<u>Central Hudson Gas &amp; Electric Corp. v. Public Service Commission,</u> 447 U.S. 557, 100 S. Ct. 2343 (1980) .....	32
<u>City of Houston v. Hill,</u> 482 U.S. 451, 107 S. Ct. 2502 (1987) .....	22
<u>Commonwealth v. American Booksellers Association,</u> 236 Va. 168, 372 S.E.2d 618 (1988) .....	37
<u>Denver Area Education Telecommunications Consortium v. FCC,</u> 116 S. Ct. 2374 (1996) .....	21, 27, 33, 34
<u>Edgar v. MITE Corp.,</u> 457 U.S. 624, 102 S. Ct. 2629 (1982) .....	42, 44
<u>Elrod v. Burns,</u> 427 U.S. 347, 96 S. Ct. 2673 (1976) .....	30, 46
<u>Erznoznik v. City of Jacksonville,</u> 422 U.S. 205, 95 S. Ct. 2268 (1975) .....	26, 36
<u>Exxon Corp. v. Governor of Maryland,</u> 437 U.S. 117, 98 S. Ct. 2207, reh'g denied, 439 U.S. 884, 99 S. Ct. 232 (1978) .....	45
<u>Fabulous Associates, Inc. v. Pennsylvania Public Utility Commission,</u> 896 F.2d 780 (3d Cir. 1990) .....	22, 46
<u>Florida Star v. B.J.F.,</u> 491 U.S. 524, 109 S. Ct. 2603 (1989) .....	32
<u>Forsyth County, Georgia v. Nationalist Movement,</u> 505 U.S. 123, 112 S. Ct. 2395 (1992) .....	22

<u>Ginsberg v. New York,</u>	
390 U.S. 629, 88 S. Ct. 1274 (1968) . . . . .	20, 21, 38
<u>Grayned v. City of Rockford,</u>	
408 U.S. 104, 92 S. Ct. 2294 (1972) . . . . .	39
<u>Hamilton Watch Co. v. Benrus Watch Co.,</u>	
206 F.2d 738 (2d. Cir. 1953) . . . . .	47
<u>Healy v. Beer Institute,</u>	
491 U.S. 324, 109 S. Ct. 2491 (1989) . . . . .	20, 42, 44, 45
<u>Hughes v. Oklahoma,</u>	
441 U.S. 322, 99 S. Ct. 1727 (1979) . . . . .	42
<u>Hynes v. Mayor of Oradell,</u>	
425 U.S. 610, 96 S. Ct. 1755 (1977) . . . . .	38
<u>Interstate Circuit, Inc. v. City of Dallas,</u>	
390 U.S. 676, 88 S. Ct. 1298 (1968) . . . . .	29
<u>Kolender v. Lawson,</u>	
461 U.S. 352, 103 S. Ct. 1855 (1983) . . . . .	39
<u>Lamont v. Postmaster General,</u>	
381 U.S. 301, 85 S. Ct. 1493 (1965) . . . . .	27
<u>Lanzetta v. New Jersey,</u>	
306 U.S. 451, 59 S.Ct. 618 (1939) . . . . .	38
<u>McIntyre v. Ohio Elections Commission,</u>	
115 S. Ct. 1511 (1995) . . . . .	27
<u>Meyer v. Grant,</u>	
486 U.S. 414, 108 S. Ct. 1886 (1988) . . . . .	26
<u>Miller v. California,</u>	
413 U.S. 15, 93 S. Ct. 2607 (1973) . . . . .	20
<u>Paulsen v. County of Nassau,</u>	
925 F.2d 65 (2d Cir. 1991) . . . . .	18
<u>People v. P.J. Video, Inc.,</u>	
68 N.Y.2d 296, 501 N.E.2d 556, 508 N.Y.S.2d 907 (1986) . . . . .	35

<u>Pike v. Bruce Church, Inc.</u> , 397 U.S. 137, 90 S. Ct. 844 (1970) .....	20, 44
<u>R.A.V. v. St. Paul</u> , 505 U.S. 377, 112 S. Ct. 2538 (1992) .....	21
<u>Sable v. Communications v. FCC</u> , 492 U.S. 115, 109 S. Ct. 2829 (1989) .....	<u>passim</u>
<u>Shea v. Reno</u> , 930 F. Supp. 916 (S.D.N.Y.), <u>appeal docketed</u> , 65 U.S.L.W. 3323 (No. 96-595) .....	<u>passim</u>
<u>Simon &amp; Schuster, Inc. v. New York State Crime Victims Board</u> , 502 U.S. 115, 112 S. Ct. 501 (1991) .....	26
<u>Smith v. California</u> , 361 U.S. 147, 80 S. Ct. 215 (1959) .....	38
<u>Soundgarden v. Eikenberry</u> , 871 P.2d 1050 (Wash.), <u>cert. denied</u> , 115 S. Ct. 663 (1994) .....	29
<u>Southern Pacific Co. v. State of Arizona</u> , 325 U.S. 761, 65 S. Ct. 1515 (1945) .....	20, 44
<u>Sperry International Trade, Inc. v. Government of Israel</u> , 679 F.2d 8 (2d Cir. 1982) .....	45
<u>Streetwatch v. National R.R. Passenger Corp.</u> , 875 F. Supp. 1055 (S.D.N.Y. 1995) .....	18, 47
<u>Talley v. California</u> , 362 U.S. 60, 80 S. Ct. 536 (1960) .....	27
<u>Time Warner Cable v. City of New York</u> , 943 F. Supp. 1357 (S.D.N.Y. 1996) .....	46
<u>Tinker v. Des Moines Independent Committee School District</u> , 393 U.S. 503, 89 S. Ct. 733 (1969) .....	36
<u>Tucker Anthony Realty Corp. v. Schlesinger</u> , 888 F.2d 969 (2d Cir. 1989) .....	45



<u>Turner Broadcasting System, Inc. v. FCC,</u>	
512 U.S. 622, 114 S. Ct. 2445 (1994)	21, 32, 33, 47
<u>Wabash St. L. &amp; P. Railway Co. v. Illinois,</u>	
118 U.S. 557, 7 S. Ct. 4 (1886)	45
<u>West Virginia State Board of Education v. Barnette,</u>	
319 U.S. 624, 63 S. Ct. 1178 (1943)	36

## **RULES AND STATUTES**

1996 N.Y. Laws 600	1
CDA § 223(e)(1)	41
CDA § 223(e)(5)(B)	24, 31
Commerce Clause of the United States Constitution	
U.S. Const., Art. I, § 8, cl.3	42
Ga. Code Ann. § 16-19-93.1 (1996)	45
N.Y.C.P.L.R. 4509 (McKinney 1996)	27
N.Y. Penal Law § 235.05	34
N.Y. Penal Law §§ 235.15 - 235.24	1
N.Y. Penal Law § 235.15(1)	7, 31
N.Y. Penal Law § 235.20(6)	6, 7
N.Y. Penal Law § 235.21	6, 34
N.Y. Penal Law § 235.21(1), (2)	28
N.Y. Penal Law § 235.21(3)	1, 6, 7
N.Y. Penal Law § 235.22	1
N.Y. Penal Law § 235.23(3)	7
N.Y. Penal Law § 235.23(3)(a)	28, 40

N.Y. Penal Law § 235.23(3)(b) . . . . .	31, 40
N.Y. Penal Law § 235.23(3)(c) . . . . .	24, 28
N.Y. Penal Law § 235.23(3)(d) . . . . .	28, 29, 31, 40
N.Y. Penal Law § 235.24(1) . . . . .	8, 41
N.Y. Penal Law § 235.24(2) . . . . .	8
N.Y. Penal Law § 263.05 . . . . .	34
N.Y. Penal Law § 263.15 . . . . .	34
Okla. Stat. tit. 21, § 1040.76 (1996) . . . . .	45

## OTHER

David R. Johnson & David Post, <u>Law and Borders - The Rise of Law in Cyberspace</u> , 48 Stan. L. Rev. 1367 (1996) . . . . .	35
New York State Senate Introducers Memorandum In Support, S. 210-E. p.1 (1996) . . . . .	34

## **PRELIMINARY STATEMENT**

Plaintiffs challenge New York Penal Law § 235.21(3) (the “Act”),<sup>1</sup> which imposes criminal penalties on the availability, display and dissemination of constitutionally protected speech on the Internet and other computer communications systems. The Internet has no parallel in the history of human communication. It provides millions of people around the globe with a low-cost method of conversing, publishing, and exchanging information on a vast array of subjects with a worldwide and virtually limitless audience. It also provides a foundation for new forms of community, based not on any accident of geographic proximity, but rather on bonds of common interest, belief and culture. Unless enjoined, the Act will greatly impair the tremendous speech-enhancing qualities of the Internet by reducing all of its content to a level deemed suitable for children.

Specifically, the Act makes it a felony to use the Internet to disseminate “indecent” material that is “harmful to minors.”<sup>2</sup> The Act was passed despite the recent, highly-publicized decisions by three-judge panels in this Court and in the United States District Court for the Eastern District of Pennsylvania that preliminarily enjoined enforcement of portions of the federal Communications Decency Act of 1996 (the “CDA”), which also imposed criminal penalties for communicating “indecent” speech to minors over the Internet. See Shea v. Reno, 930 F. Supp. 916 (S.D.N.Y.), appeal docketed, 65 U.S.L.W. 3323 (U.S. Oct. 15, 1996) (No. 96-595); ACLU v. Reno, 929 F. Supp. 824

---

<sup>1</sup> The challenged statute was enacted as Section 5 of the 1996 N.Y. Laws 600 and became effective on November 1, 1996. The Act, and other relevant provisions, are codified at N.Y. Penal Law §§ 235.15 - 235.24. Plaintiffs will use the statutory citations throughout this brief.

<sup>2</sup> Plaintiffs do not challenge other provisions in the Act that make it a crime to “importune[], invite[] or induce[] a minor to engage” in sexual conduct via the Internet. § 235.22.

(E.D. Pa.), prob. juris. noted, 117 S. Ct. 554 (1996).<sup>3</sup> After extensive evidentiary hearings on the nature of the Internet, including in-court online demonstrations, those courts unanimously held that the CDA violated the First Amendment rights of adults to communicate over the Internet. Crucial to their holdings were factual findings establishing that there is no way for the vast majority of online speakers to distinguish between adults and minors in their audience, thus requiring all speakers to reduce their speech to a level suitable for children or risk prosecution under the CDA. The Act is fatally unconstitutional for precisely the same reason -- it effectively bans adults from communicating constitutionally protected speech over the Internet.

The Act is also substantially overbroad because it criminalizes a wide range of speech that is constitutionally protected for older minors, and because it infringes on the rights of adults in communities outside of New York State. In addition, the Act is unconstitutionally vague. "Indecency" under the Act is defined as material that is "harmful to minors" according to "prevailing standards in the adult community."<sup>4</sup> Because content on the Internet is automatically available to a worldwide audience, speakers have no way to determine which "community" is relevant, and therefore no clear way to avoid prosecution under the Act.

In addition, the Act violates the Commerce Clause of the Constitution.

---

<sup>3</sup> The Supreme Court will hear oral argument in Reno v. ACLU on March 19, 1997.

<sup>4</sup> The definition of "indecentcy" under the CDA differs from the definition used in the Act. Two of the judges on the three-judge panel in ACLU v. Reno held that the CDA was unconstitutionally vague. ACLU, 929 F. Supp. at 856 (Sloviter, C.J.), 858 (Buckwalter, J.). The three-judge panel in Shea v. Reno held that the CDA was not vague. Shea, 930 F. Supp. at 936-39.

Because of the borderless nature of the online medium, the Act imposes restrictions on communications occurring wholly outside the State of New York, effects an impermissible burden on interstate commerce, and subjects online speakers to inconsistent state obligations.

Plaintiffs and other online speakers are currently protected from federal prosecution under the CDA. By passing the Act, the State of New York once again forced many of those same plaintiffs, and millions of other online speakers around the country, to cease engaging in constitutionally protected speech or risk criminal prosecution in New York. Thus, plaintiffs seek a preliminary injunction against enforcement of the Act because it violates the First, Fifth and Fourteenth Amendments and the Commerce Clause of the United States Constitution.

## **I. STATEMENT OF FACTS**

### **A. Plaintiffs and Their Speech**

Plaintiffs represent a spectrum of individuals and organizations who use the Internet to communicate, disseminate, display and access a broad range of speech.<sup>5</sup> Plaintiffs do not speak with a single voice or on a single issue, but all engage in speech that may be regarded as “indecent” under the Act, and that is constitutionally protected for adults and older minors.<sup>6</sup> Plaintiffs include speakers, content providers, readers, users, and Internet access providers; many of the plaintiffs assume all of these roles. Plaintiffs communicate online both within and outside of the State of New York, and plaintiffs’ speech is accessible within and outside of the State of New York.

---

<sup>5</sup> Hereinafter, “plaintiffs” will refer collectively to plaintiffs, their members, subscribers, readers and users.

<sup>6</sup> See discussion infra at pp. 20-22, 36-38.

More specifically, plaintiffs include the following:

- **American Library Association, Freedom to Read Foundation, Inc., New York Library Association, and Westchester Library System** are organizations devoted to protecting the interests of libraries. Libraries serve as both access and content providers on the Internet, providing their patrons with facilities to access the Internet; post their card catalogues, information about current events, and online versions of text or art from their library collections; and sponsor chat rooms.

- **American Booksellers Foundation For Free Expression ("ABFFE")** is a national association of general interest and specialized bookstores formed to protect free expression rights. ABFFE has many members that use the Internet and electronic communications to obtain from publishers information and excerpts, some of which contain passages that are sexually frank.

- **Association of American Publishers ("AAP")** is a national association of publishers of general books, textbooks, and educational materials. AAP has many members who actively use and provide content on the Internet, both creating and posting electronic products and using the Internet as a communication and promotional tool for their print publishing activities.

- **BiblioBytes** is a company 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. MPA has many members that publish magazines that, in

addition to being published in print form, are now or soon will be published in electronic formats available to the public on the Internet or through online service providers.

- **Interactive Digital Software Association (“IDSA”)** is a non-profit trade association of United States publishers of entertainment software. IDSA has many members that both sell their software in retail outlets and make their entertainment software available to the public on the Internet for demonstration ("demos"), purchase and play.

- **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 an Internet service provider that provides a "virtual salon" for Internet users in the New York area. ECHO and its subscribers provide content on the Internet through the posting of Web sites, including personal home pages, and through over 50 discussion groups oriented to subscriber interests.

- **New York City Net (“NYC Net”)** is an Internet service provider for 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 over 110 international artists in maintaining online studio or gallery rooms.

- **Peacefire** is an organization whose membership is primarily comprised of

minors. Peacefire was formed to protect the right of citizens under age 18 to use the Internet. Peacefire's members use the Internet to communicate and access a wide variety of information that is valuable and constitutionally protected for older minors but that might be deemed harmful to younger minors.

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

#### **B. The Challenged Statute<sup>7</sup>**

Plaintiffs challenge the Act, which amends New York Penal Law § 235.21 by adding a new subdivision 3. The Act makes it a crime for a person:

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 § 235.21(3) is a Class E felony punishable by one to four years in prison. The Act applies to both commercial and non-commercial dissemination of material, and thus specifically applies to libraries, educational institutions, and non-profit organizations.

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

that quality of any description or representation, in whatever form, of nudity, sexual

---

<sup>7</sup> A comparison between the language of the Act and the CDA is provided in Appendix A to this brief. As can be seen from this chart, the New York State Legislature borrowed heavily from the CDA when drafting the Act and copied a number of provisions verbatim.



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.

§ 235.20(6).

There are six affirmative defenses to criminal liability under § 235.21(3).

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 the second degree in violation of subdivision three of section 235.21 of this article, it is an affirmative defense that the persons to whom 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.

Section 235.23(3) provides the following four defenses to prosecution under

§ 235.21(3):

- (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 to circumvent any such screening or blocking.

Section 235.24 provides the following defense to § 235.21(3):

No person shall be held to have violated such provisions 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.

Exceptions to this defense for conspiracies and co-ownership situations and an employer liability defense are set out in subsections 235.24 (1)(a)-(b) and (2).

## C. The Internet<sup>8</sup>

### 1. The Nature of the Online Medium

The Internet is a decentralized, global communications medium that links people, institutions, corporations and governments around the world. ACLU, 929 F. Supp. at 831; Shea, 930 F. Supp. at 926. Offering a range of digital information including text, images, sound and video, the Internet is a giant computer network which interconnects

---

<sup>8</sup> The facts in this section are derived primarily from the extensive factual findings issued by the three-judge panels in ACLU v. Reno, 929 F. Supp. 824, and in Shea v. Reno, 930 F. Supp. 916. The majority of the factual findings about the history and basic technology of the medium were derived from stipulations agreed to by the Department of Justice. See ACLU, 929 F. Supp. at 830; Shea, 930 F. Supp. at 925. Plaintiffs will submit testimony at the hearing on the Motion for Preliminary Injunction that will establish that the basic facts about online communications are essentially unchanged since the trial courts in Shea and ACLU issued their factual findings.

innumerable smaller groups of linked computer networks and individual computers.<sup>9</sup> While estimates are difficult due to its constant and rapid growth, the Internet is currently believed to connect approximately 9.4 million host computers, 159 countries, and 40 million users. By some estimates, there will be as many as 200 million Internet users by the year 1999. ACLU, 929 F. Supp. at 831; Shea, 930 F. Supp. at 926.

The information made available on the Internet is “as diverse as human thought.” ACLU, 929 F. Supp. at 842, ¶ 74. Content ranges from academic writings, to art, to humor, to literature, to medical information, to music, to news, to sexually oriented material.<sup>10</sup> For example, one can view on the Internet the full text of the Bible, all of the works of Shakespeare, and numerous other classic works of literature. One can browse through paintings from museums around the world, view in close-up detail the ceiling of the Sistine Chapel, or see the latest photographs transmitted by the Jupiter space probe. Moreover, at any one time, the Internet serves as the communication medium for literally tens of thousands of global conversations, political debates, and social dialogues.

A revolutionary medium that is dramatically altering traditional views of communications and community, the Internet is distinguishable in important ways from traditional media. See ACLU, 929 F. Supp. at 843-44. For instance, “[no] single entity -- academic, corporate, governmental, or non-profit -- administers the Internet. . . . There is no centralized storage location, control point, or communications channel.” Id. at 832, ¶ 11;

---

<sup>9</sup> For a history of the Internet’s origins as a network that linked computers owned by the military, defense contractors, and universities, see ACLU, 929 F. Supp. at 831-32; Shea, 930 F. Supp. at 925-26.

<sup>10</sup> While some sexually explicit material is available on the Internet, it is not “the primary type of content on this new medium.” ACLU, 929 F. Supp. at 844, ¶ 83.

Shea, 930 F. Supp. at 926. In addition, the Internet is a truly global medium. At least 40% of the content of the Internet originates abroad, and all of the content on the Internet is equally available to all Internet users worldwide. ACLU, 929 F. Supp. at 848, ¶ 117.

The Internet also differs from traditional media in that it provides users with an unprecedented ability to interact with other users and with content. See ACLU, 929 F. Supp. at 843-44, ¶¶ 76-80; Shea, 930 F. Supp. at 927-28. Unlike radio or television, communications on the Internet do not “‘invade’ an individual’s home or appear on one’s computer screen unbidden.” ACLU, 929 F. Supp. at 844, ¶ 88. Rather, the receipt of information on the Internet “requires a series of affirmative steps more deliberate and directed than merely turning a dial.” Id. at 845, ¶ 89. Because the Internet presents extremely low entry barriers to publishers and distributors of information, it is an especially attractive method of communicating for non-profit and public interest groups. Id. at 843, ¶¶ 76, 80. Also, unlike radio, television, newspapers and books, the Internet “is not exclusively, or even primarily, a means of commercial communication.” Id. at 842, ¶ 75. In sum, the Internet is “a unique and wholly new medium of worldwide human communication.” Id. at 844, ¶ 81.

## **2. How Individuals Access the Internet**

Individuals have several easy means of gaining access to computer communication systems in general, and to the Internet in particular. First, many educational institutions, businesses, libraries, and individual communities maintain computer networks linked directly to the Internet and provide account numbers and passwords enabling users to gain access to the network. ACLU, 929 F. Supp. at 832, ¶ 13. For example, plaintiff

Westchester Library System provides online access to its patrons through 130 computers located at its member libraries. See Complaint ¶ 99. Second, Internet service providers ("ISPs"), which generally are commercial entities that charge a monthly fee, offer their subscribers modem access to computers or networks maintained by the ISP which are linked directly to the Internet. ACLU, 929 F. Supp. at 832-33, ¶¶ 18-19. For example, plaintiffs ECHO, NYC Net and Panix provide Internet access to subscribers in a particular geographic region and may also provide access to content within their own proprietary networks. Complaint ¶¶ 115-125. Third, there are a growing number of "cyberspace cafes," where customers, for a small hourly fee, can use computers provided by the cafe to access the Internet. ACLU, 929 F. Supp. at 833, ¶ 17. Finally, individuals and organizations can establish computer bulletin board systems ("BBSs"), which are usually stand-alone computer communication systems independent of the Internet that allow subscribers to dial directly from their computers into a BBS host computer. Id. at 833-34, ¶ 20.

### **3. Ways of Communicating and Exchanging Information on the Internet**

Most users of the Internet are provided with a username, password and electronic mail (or "e-mail") address that allow them to sign on to the Internet and to communicate with other users. Many usernames are pseudonyms or pen names known as "handles"; these "handles" provide users with a distinct online identity and help to preserve their anonymity. The username and e-mail address are the only indicators of the user's identity; that is, persons communicating with the user will know them only by their username and e-mail address (unless the user reveals other information about herself through her messages).

Once an individual signs on to the Internet, there are a wide variety of methods for communicating and exchanging information with other users. See generally ACLU, 929 F. Supp. at 834-38, ¶¶ 22-48; Shea, 930 F. Supp. at 927-30. The primary methods are:

E-Mail: The simplest and perhaps most widely used method of communication on the Internet is via e-mail. E-mail allows an online user to address and transmit an electronic message to one or more people, “comparable in principle to sending a first class letter.” ACLU, 929 F. Supp. at 834, ¶ 23.

Online Discussion Groups: In addition, there are a wide variety of online discussion forums that allow groups of users to discuss and debate subjects of interest. Thousands of discussion groups have been organized by individuals, institutions, and organizations on many different computer networks and cover virtually every topic imaginable -- creating a new, global version of the village green. The three most common methods for online discussion are mail exploders, USENET newsgroups, and chat rooms.

Mail Exploders: Mail exploders, also called 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. Subscribers can reply to the message by sending a response to the list. ACLU, 929 F. Supp. at 834, ¶ 24. Users of mailing lists typically can add or remove their names from the list automatically, with no direct human involvement. Id.; Shea, 930 F. Supp. at 927.

USENET Newsgroups: "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." ACLU, 929 F. Supp. at 834-35, ¶ 25. Users may read or send messages to newsgroups without a prior "subscription," and there is no way for a speaker who posts an article to a newsgroup to know who is reading her message. *Id.*; Shea, 930 F. Supp. at 927-28. There are currently USENET newsgroups on more than 15,000 different subjects, and over 100,000 new messages are posted to these groups each day. ACLU, 929 F. Supp. at 835, ¶ 26.

Chat Rooms: "Chat rooms" provide additional online discussion forums that allow users to engage in simultaneous conversations with one or many other users by typing messages and reading the messages typed by others participating in the chat, "analogous to a telephone party line, using a computer and keyboard rather than a telephone." ACLU, 929 F. Supp. at 835, ¶ 27; Shea, 930 F. Supp. at 928. There are thousands of different chat rooms available "in which collectively tens of thousands of users are engaging in conversations on a huge range of subjects." ACLU, 929 F. Supp. at 835, ¶ 27. For example, plaintiff ACLU hosts an unmoderated online chat about current civil liberties issues and live "auditorium" events, in which a featured speaker "talks" online about a particular issue and users can simultaneously respond with online questions.

The World Wide Web: Finally, one of the most well-known methods for communicating information online is the Web, which allows users to publish documents, also

called “Web pages,” that can then be accessed by any other user in the world.<sup>11</sup> See generally ACLU, 929 F. Supp. at 836-38, ¶¶ 33-48; Shea, 930 F. Supp. at 929-30. The Web 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 her own 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 now provide online editions of their publications and reports on the Web or operate independent Web sites. Many government agencies and courts also use the Web to disseminate information to the public. At the same time, many individual users and small community organizations have established individualized home pages on the Web that provide information of interest to others. Plaintiff Panix, for example, hosts Web pages for many organizations including an organization active in raising awareness about AIDS, as well as for individual Panix subscribers. Complaint ¶ 116.

Though 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 through protocols that allow the information to become part of a single body of knowledge accessible by all Web users. ACLU, 929 F. Supp. at 836, ¶ 34, 837 ¶ 42. To gain access to the information available on the Web, a person uses a “browser” -- software, such as Netscape Navigator, Mosaic, or Internet Explorer -- to

---

<sup>11</sup> There are also a range of other methods for publishing, storing, locating and retrieving information on the Internet. See ACLU, 929 F. Supp. at 835-36, ¶¶ 30-32; Shea, 930 F. Supp. at 928-29. Those methods have largely been replaced by the more advanced technology of the Web. ACLU, 929 F. Supp. at 836, ¶ 34.



display, print and download documents that are formatted in the standard Web formatting language. Shea, 930 F. Supp. at 929.

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. Second, if a user wants to conduct a generalized search, or wants a particular site but does not know the address, she can also use one of a number of “search engines,” which are available free of charge to help users navigate the Web. ACLU, 929 F. Supp. at 837, ¶ 44. The user simply types a word or string of words as a search request and the search engine provides a list of sites that match the search string. Id. For example, a user who types “civil liberties” in a search engine will bring up a list of Web sites that includes the site of the ACLU.

Finally, online users may browse or “surf” the Web by “linking” from one Web page to another. Almost all Web documents contain “links,” which are short sections of text or image that refer and link to another Web document. Id. at 836, ¶ 36. When selected by the user, the “linked” document is automatically displayed, wherever in the world it is actually stored. Id. For example, the American Library Association (“ALA”) home page contains several links. Some of these links are to other Web pages or documents within the ALA site, including documents entitled “Libraries Online,” “Library Promotional Events,” and the “ALA Bookstore.” Other links from the ALA home page provide links to sites maintained by other organizations or individuals and stored on other computers around the world. For example, the ALA Web site provides links to the American Association of

Law Libraries, the Art Libraries Society of North America, and the Medical Library Association. “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.” Id. at 836-37, ¶ 39.

4. **The Inability of Speakers to Prevent Their Speech from Reaching Minors**

For the vast majority of communications over the Internet, including all communications by e-mail, newsgroups, mail exploders, and chat rooms, it is not technologically possible for a speaker to determine the age of a user who is accessing such communications. See id. at 845, ¶ 90 (“There is no effective way to determine the identity or the age of a user who is accessing material through e-mail, mail exploders, newsgroups, or chat rooms.”); Shea, 930 F. Supp. at 941 (“[A]s the government concedes, for the vast majority of applications and services available on the Internet, a user has no way of communicating . . . with certainty that the content will not reach a person under eighteen . . .”). In addition, all of the speakers who publish on the Web through Web sites provided by the major commercial online services, such as America Online, Prodigy, and Compuserve, also lack any technological means to screen their users for age. ACLU, 929 F. Supp. at 845-46, ¶ 96. Thus, these categories of speakers must either make their information available to all users of the Internet, including users who may be minors, or not make it available at all.

Other speakers on the Web can, in theory, use special technology to interrogate users through a fill-in-the-blank form using technology known as “cgi script.” Id. at 845, ¶ 95. However, the mandatory use of this technology to request credit card

numbers or other age verification would pose insurmountable economic burdens on non-commercial and even many commercial speakers on the Web. Id. at 846, ¶¶ 97-102.

Similarly, the vast majority of speakers on the Internet lack any mechanism for labeling or segregating specific communications -- whether distributed by e-mail, newsgroups, mail exploders, chat rooms or Web sites -- in a way that would enable those communications to be automatically blocked or screened from minors. See id. at 847-48, ¶¶ 108-116; Shea, 930 F. Supp. at 932-33.

Finally, Internet speakers have no way to determine any other characteristics of their audience. Indeed, in online communications through newsgroups, mailing lists, chat rooms, and the Web, the speaker has no way to determine with certainty that any particular person has accessed her speech. ACLU, 929 F. Supp. at 844, ¶ 85 ("Once a provider posts content on the Internet, it is available to all other Internet users worldwide."). Thus, a speaker cannot determine the location of a recipient, or why the recipient has accessed her speech.

##### **5. The Availability of User-Based Filtering Programs**

Although there is no way for the vast majority of speakers to prevent minors from accessing their speech, there are a variety of options available to parents and other users who wish to restrict access to online communications that they might consider unsuitable for children. Id. at 838-42, ¶¶ 49-73; Shea, 930 F. Supp. at 931-34. First, there are a variety of user-based software products such as SurfWatch and CyberPatrol that allow users to block access to certain sexually explicit sites, to prevent children from giving personal information to strangers by e-mail or in chat rooms, and to keep a log of all online

activity that occurs on the home computer. ACLU, 929 F. Supp. at 839, ¶ 55, 841 ¶ 66; Shea, 930 F. Supp. at 932. “The market for this type of [user-based] software is growing, and there is increasing competition among software providers to provide products.” ACLU, 929 F. Supp. at 839, ¶ 54. Second, large commercial online services such as America Online provide features to prevent children from accessing chat rooms and to block access to certain newsgroups based on keywords, subject matter, or specific newsgroup. Id. at 842, ¶¶ 69, 71. They also offer screening software that automatically blocks messages containing certain words, and tracking and monitoring software to determine which resources a particular online user (e.g., a child) has accessed. Finally, these large online services offer children-only discussion groups that are closely monitored by adults. Id. at 842, ¶ 69.

## II. ARGUMENT

Plaintiffs more than satisfy the Second Circuit requirements for preliminary injunctive relief. In order for the Court to grant a preliminary injunction, the plaintiffs must demonstrate (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<sup>12</sup> and a balance of hardships tipping decidedly in the plaintiffs’ favor. Paulsen v. County of Nassau, 925 F.2d 65, 68 (2d Cir. 1991); Streetwatch v. National R.R. Passenger Corp., 875 F. Supp. 1055, 1058 (S.D.N.Y. 1995).

---

<sup>12</sup> The fair-ground-for-litigation standard is clearly applicable in this action because (i) the action alleges constitutional violations, Almonte v. Pierce, 666 F.Supp. 517, 526 (S.D.N.Y. 1987); (ii) the public interest in a robust flow of free speech served by enjoinder of enforcement of the Act counterbalances the public interest in protecting children arguably served by the Act, Carey v. Klutznick, 637 F.2d 834, 839 (2d Cir. 1980); and (iii) the New York legislature did not engage in any fact-finding regarding the public interest served by the Act before promulgating it. Able v. United States, 44 F.3d 128, 131 (2d Cir. 1995).

**A. Plaintiffs Have a Substantial Likelihood of Success on the Merits**

Plaintiffs are likely to succeed on their constitutional claims. First, because there is no way for the vast majority of online speakers to distinguish between adults and minors in their audience, the Act, like the recently enjoined CDA, violates the First Amendment because it effectively bans constitutionally protected speech among adults. See generally Shea, 930 F. Supp. 916; ACLU, 929 F. Supp. 824. The Act fails to survive the strict constitutional scrutiny required of content-based regulations of speech because, as a criminal ban on protected speech between adults, it is not a narrowly tailored way to achieve the government's asserted interest in protecting minors from "indecenty." Moreover, the statutory defenses fail to cure the constitutional defects of the Act because they are either technologically unavailable or economically prohibitive for most speakers on the Internet. In addition, the Act is a strikingly ineffective means of keeping inappropriate materials from minors because it will do nothing to prevent minors from accessing the large percentage of "indecent" material that is posted from sites in foreign countries. There are also a myriad of less restrictive alternatives, including user-based filtering programs, that enable parents to decide what their children will read and see.

Second, the Act is substantially overbroad because it criminalizes a wide range of speech that is constitutionally protected for older minors, see ACLU, 929 F. Supp. at 853 (Sloviter, C.J.), and because it infringes on the rights of adults in communities outside of New York. Id. at 877-78 (Dalzell, J.).

Third, the Act is unconstitutionally vague because it fails to define the relevant community for determining what is "indecent" on the global Internet, id. at 863 (Buckwalter,

J.), and because the defenses provide inadequate guidance to speakers about how to avoid prosecution. Id. at 856 (Sloviter, C.J.), 859 (Buckwalter, J.).

Finally, the Act violates the Commerce Clause because it regulates communications occurring wholly outside the State of New York, imposes an impermissible burden on interstate commerce, and subjects plaintiffs to inconsistent state obligations. See Healy v. Beer Institute, 491 U.S. 324, 332, 109 S. Ct. 2491, 2497 (1989); Pike v. Bruce Church, Inc., 397 U.S. 137, 142, 90 S. Ct. 844, 847 (1970); Southern Pac. Co. v. State of Arizona, 325 U.S. 761, 767, 65 S. Ct. 1515, 1519 (1945).

**1. The Act Effectively Bans Constitutionally Protected Speech, and Therefore Cannot Survive Strict Scrutiny**

Because the vast majority of Internet speakers cannot distinguish between minors and adults in their audience, they cannot comply with the Act unless they speak only in language suitable for children. Thus, the Act, like the recently enjoined CDA, effectively operates as a criminal ban on constitutionally protected speech among adults on the Internet. See Shea, 930 F. Supp. at 950; ACLU, 929 F. Supp. at 854, 879. The category of non-obscene speech criminalized by the Act (material that is “harmful to minors”)<sup>13</sup> arguably is narrower than the category criminalized by the CDA (material that is “patently offensive”). See Appendix A. But that distinction is irrelevant to the First Amendment claims in this case because the two statutes share the same fundamental constitutional defect -- they both effectively ban speech that is constitutionally protected between adults.

---

<sup>13</sup> The “harmful to minors” standard in the Act tracks the standard applied in Ginsberg v. New York, 390 U.S. 629, 88 S. Ct. 1274 (1968) (upholding variable obscenity test for commercial sale of material deemed “harmful to minors”), as modified by the Supreme Court’s most recent definition of obscenity in Miller v. California, 413 U.S. 15, 93 S. Ct. 2607 (1973).

Even under the guise of protecting children, the government may not justify the complete suppression of constitutionally protected speech because to do so would “burn up the house to roast the pig.” Butler v. Michigan, 352 U.S. 380, 383, 77 S. Ct. 524, 526 (1957); see also Denver Area Educ. Telecomms. Consortium v. FCC, 116 S. Ct. 2374, 2393 (1996) (the government may not “reduc[e] the adult population . . . to . . . only what is fit for children” (quoting Sable Communications v. FCC, 492 U.S. 115, 128, 109 S. Ct. 2829, 2837 (1989))). Similarly, in Sable, the Court struck down a total ban on the commercial sale of indecency over the telephone because it had the “effect of limiting the content of adult [communications] to that which is suitable for children.” Sable, 492 U.S. at 131, 109 S. Ct. at 2839. Indeed, because “[t]he level of discourse reaching a mailbox simply cannot be limited to that which would be suitable for a sandbox,” the Supreme Court has never upheld a criminal ban on non-obscene communications between adults. Bolger v. Youngs Drug Prods. Corp., 463 U.S. 60, 74, 103 S. Ct. 2875, 2884 (1983) (striking down a ban on mail advertisements for contraceptives).<sup>14</sup>

As a content-based regulation of protected speech, the Act is presumptively invalid. R.A.V. v. St. Paul, 505 U.S. 377, 391, 112 S. Ct. 2538, 2547 (1992). Subject only to “narrow and well-understood exceptions, [the First Amendment] does not countenance governmental control over the content of messages expressed by private individuals.” Turner Broad. Sys., Inc. v. FCC, 512 U.S. 622, 114 S. Ct. 2445, 2458-59

---

<sup>14</sup> Cf. Ginsberg, 390 U.S. at 634, 88 S. Ct. at 1277-78 (upholding restriction on the direct commercial sale to minors of material deemed “harmful to minors” because it “does not bar the appellant from stocking the magazines and selling them” to adults); American Booksellers v. Webb, 919 F.2d 1493, 1501 (11th Cir. 1990) (noting that Ginsberg did not address the “difficulties which arise when the government’s protection of minors burdens (even indirectly) adults’ access to material protected as to them”).

(1994). Content-based regulations of speech will be upheld only when they are justified by compelling governmental interests and “narrowly tailored” to effectuate those interests. See Shea, 930 F. Supp. at 939-40 (applying strict scrutiny to invalidate online indecency ban); ACLU, 929 F. Supp. at 851, 858, 866 (same); see also Sable, 492 U.S. at 126, 109 S. Ct. at 2836 (The government may effectuate even a compelling interest only “by narrowly drawn regulations designed to serve those interests without unnecessarily interfering with First Amendment freedoms”) (applying strict scrutiny to invalidate indecency ban on telephone communications); Fabulous Assocs., Inc. v. Pennsylvania Pub. Util. Comm’n, 896 F.2d 780, 788 (3d Cir. 1990) (striking down “harmful to minors” restrictions in telephone communications because they unconstitutionally burdened adult rights).

The Act is also unconstitutionally overbroad because its ban on adult communications “sweeps too broadly.” Forsyth County, Ga. v. Nationalist Movement, 505 U.S. 123, 130, 112 S. Ct. 2395, 2401 (1992); see also City of Houston v. Hill, 482 U.S. 451, 458, 107 S. Ct. 2502, 2508 (1987); Broadrick v. Oklahoma, 413 U.S. 601, 612-13, 93 S. Ct. 2908, 2916 (1973). Under the substantial overbreadth doctrine, a law must be struck down as facially invalid if it would “‘penalize a substantial amount of speech that is constitutionally protected’ . . . even if some applications would be ‘constitutionally unobjectionable.’” ACLU, 929 F. Supp. at 867 (Dalzell, J.) (quoting Forsyth County, 505 U.S. at 129-30, 112 S. Ct. at 2401); see also Shea, 930 F. Supp. at 950 (indecency regulation was overbroad because “the set of content providers whose speech could be constitutionally proscribed is in fact exceeded, perhaps even overshadowed, by the number of users whose speech is constitutionally protected”).



## 2. The Act's Defenses Fail to Save the Act

Standing alone, the Act clearly fails strict scrutiny and is unconstitutionally overbroad. See Shea, 930 F. Supp. at 941. The vast majority of speech on the Internet is disseminated in spaces that minors as well as adults can access. An Internet user simply “has no way of communicating or making available . . . content with certainty that the content will not reach a [minor].” Id. Thus, every time a speaker communicates “indecent” on the Internet, she risks prosecution under the Act for “initiating or engaging” in communications with a minor. As the Shea court reasoned in striking down the CDA:

Because content providers using most forms of Internet communication have no way of transmitting indecent content with certainty that it will not reach a minor, the only way for a content provider to comply with [the statute], standing alone, would be to refrain from transmitting any indecent content. Because adults would lack means of engaging in constitutionally protected indecent communications over the Internet without fear of criminal liability, the statute would unquestionably be unconstitutional.

Id. at 941-42 (citing Sable, 492 U.S. at 131, 109 S. Ct. at 2839).

The only hope for salvaging the constitutionality of the Act is through its defenses, which attempt to provide adult speakers with a “safe harbor” that would enable them “to engage in constitutionally protected communications without fear of criminal liability.” Shea, 930 F. Supp. at 944. But the defenses fail to narrow the Act’s unconstitutionality. See id. at 948; ACLU, 929 F. Supp. at 857.

First, the affirmative defenses do not protect an individual speaker from prosecution, as distinct from ultimate criminal liability. An online speaker may invoke the defenses only after a prosecutor has initiated criminal proceedings against her, and only as evidence that she might not have committed a criminal act. Shea, 930 F. Supp. at 944. Because the defenses “in no way shield[] a content provider from prosecution,” they are

unlikely to eliminate the severe chilling effect of the Act.<sup>15</sup> Id.

Second, as the discussion below will illustrate, the defenses are technologically unavailable to the vast majority of speakers on the Internet, and economically prohibitive for other speakers.

a. **Credit Card and Age Verification Are Technologically Unavailable for the Vast Majority of Online Speakers, and Impose Unconstitutional Burdens on Other Speakers**

Section 235.23(3)(c) provides a defense for a defendant who "has restricted access to such materials by requiring use of a verified credit card, debit account, adult access code or adult personal identification number." This defense is identical to a defense provided in § 223(e)(5)(B) of the CDA, and it suffers from the same infirmities. See Appendix A.

As the ACLU and Shea courts found after receiving extensive evidence, credit card or age verification is technologically impossible for all speakers using e-mail, mail exploders, chat rooms and newsgroups. There is likewise no technology available that would enable credit card or age verification by speakers on the Web who publish through America Online, CompuServe and Prodigy, who collectively have over 12 million subscribers. ACLU, 929 F. Supp. at 845-46, ¶ 96; Shea, 930 F. Supp. at 933. Thus, the millions of people communicating by e-mail and mail exploders, who daily send 100,000 messages to USENET newsgroups, carry on conversations in chat rooms, and provide content through the large commercial online services "would simply have to refrain from engaging in constitutionally protected speech." Shea, 930 F. Supp. at 944. As to this universe of

---

<sup>15</sup> At least one artist who displays his work on the Web site of plaintiff Art on the Net has already removed material that is constitutionally protected out of fear of prosecution.

speakers, who represent the overwhelming majority of speakers on the Internet, the Act clearly fails strict scrutiny, since it amounts to a flat ban on protected speech in violation of Butler and Sable. "For most speakers using most Internet applications," § 235.21(3)(c) "is no defense at all." Id. at 944; see also ACLU, 929 F. Supp. at 854 (Sloviter, C.J.) ("[N]o technology exists which allows those posting on the category of newsgroups, mail exploders or chat rooms to screen for age.").

While credit card verification is not technologically impossible for speakers on the Web who do not use the commercial online services (AOL, CompuServe, Prodigy), it is still practically unavailable for the vast number of these speakers on the Web -- including libraries (such as plaintiff Westchester Library System and the member libraries of plaintiffs ALA and NYLA), the ACLU, Art on the Net, Peacefire and individual Internet subscribers, users, and speakers -- who do not charge, and do not wish to charge, for their speech. Credit card companies will not verify credit cards in the absence of a commercial transaction. ACLU, 929 F. Supp. at 846, ¶ 98. To require noncommercial speakers to begin to charge for their speech in order to verify age would force most of the plaintiffs to close their Web sites. In ACLU, the court found that the high cost of credit card verification would require many noncommercial speakers to "shut down [their] site[s]." Id. at ¶ 100; see also id. at ¶¶ 97-102. Plaintiffs' only other option would be to steer clear of communicating potentially "indecent" information even to adults.

The credit card defense would pose an unconstitutional burden even on the narrow range of speakers on the Internet to whom it is not technologically or practically unavailable -- those communicating on the Web who do not use the commercial online

services and who charge for their speech. See Shea, 930 F. Supp. at 943 (finding that credit card verification or maintenance of a verification system would be “extremely costly” even for commercial entities); ACLU, 929 F. Supp. at 847, ¶ 105. Economic burdens on the exercise of protected speech are routinely struck down by the courts. Thus, in Erznoznik v. City of Jacksonville, 422 U.S. 205, 95 S. Ct. 2268 (1975), the Supreme Court found an unconstitutional deterrent effect on free speech where, to avoid prosecution, theater owners were required either to “restrict their movie offerings or [to] construct adequate protective fencing which may be extremely expensive or even physically impracticable.” Erznoznik, 422 U.S. at 217, 95 S. Ct. at 2277. In Simon & Schuster, Inc. v. New York State Crime Victims Bd., 502 U.S. 115, 112 S.Ct. 501 (1991), the Court stated that “[a] statute is presumptively inconsistent with the First Amendment if it imposes a financial burden on speakers because of the content of their speech,” because such a regulation “raises the specter that the government may effectively drive certain ideas or viewpoints from the marketplace.” Id. at 115, 112 S. Ct. at 508 (1991); see also Meyer v. Grant, 486 U.S. 414, 424, 108 S. Ct. 1886, 1893 (1988).

Credit card and age verification would also impose substantial additional burdens. The Supreme Court affirmed as recently as last Term that it is unconstitutional to require adults to “register” in order to gain access to constitutionally protected speech. In Denver Area, the Court struck down the statutory requirement that viewers provide written notice to cable operators if they want access to certain sexually oriented programs because the requirement “restrict[s] viewing by subscribers who fear for their reputations should the operator, advertently or inadvertently, disclose the list of those who wish to watch the . . .

channel.” Denver Area, 116 S. Ct. at 2391. To require speakers on the Web, under threat of criminal sanctions, to register their users by credit card or adult ID is at least as onerous a burden as the scheme found unconstitutional in Denver Area. See also Lamont v. Postmaster General, 381 U.S. 301, 307, 85 S. Ct. 1493, 1496 (1965) (finding unconstitutional a requirement that recipients of Communist literature notify the Post Office that they wish to receive it).

The requirement further infringes on plaintiffs’ First Amendment right to communicate anonymously. As the Supreme Court stated in McIntyre v. Ohio Elections Comm’n, anonymity “exemplifies the purpose behind the Bill of Rights, and of the First Amendment in particular: to protect unpopular individuals from retaliation -- and their ideas from suppression -- at the hand of an intolerant society.” 115 S. Ct. 1511, 1524 (1995) (striking down Ohio statute prohibiting anonymous distribution of campaign literature); see also Talley v. California, 362 U.S. 60, 64-65, 80 S. Ct. 536, 538-39 (1960) (declaring unconstitutional a California ordinance that prohibited the distribution of anonymous handbills). Plaintiff NYC Net believes that it is critical that it provide its resources to the gay and lesbian community, and particularly to gay and lesbian teenagers, on an anonymous basis; to require identification would deter many users from accessing NYC Net’s services, and curtail the effectiveness of this service. Complaint ¶ 124. Likewise, a fundamental goal of the NYLA is to provide anonymous access to all who desire to use the resources of its member libraries. Complaint ¶ 96; see also N.Y.C.P.L.R. 4509 (McKinney 1996) (prohibiting the disclosure of library records, including the names of persons requesting or using library materials.).

b. **There Is No Other Method That Enables an Online Speaker to Ascertain the Age of Her Audience**

Section 235.23(3)(a) provides a defense to a person who "made a reasonable effort to ascertain the true age of the minor and was unable to do so as a result of actions taken by the minor."<sup>16</sup> On the Internet, this defense provides no safe harbor to speakers because, as discussed above, there is no way for the vast majority of speakers to ascertain an Internet user's age. See supra pp. 16-17. Thus, § 235.23(3)(a) adds nothing to the credit card and age verification defense set forth in § 235.23(3)(c), and contains the same defects. As the Shea court noted,

If a content provider cannot discern who receives his messages, there is no way for him to obtain verification of recipients' ages. . . . [A] speaker posting a message to a newsgroup or to a list maintained by a mail exploder has no control over who will receive the message; a user who joins an IRC discussion channel cannot determine the identity of other participants, beyond viewing a list of names.

Shea, 930 F. Supp. at 942.

c. **There Is No Way for Online Speakers to Label or Segregate Their Speech in a Way That Could Be Automatically Blocked From Minors**

Section 235.23(3)(d) provides an affirmative defense for a person who "has in good faith established a mechanism such that the labeling, segregation or other mechanism enable 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 blocking or screening

---

<sup>16</sup> This defense existed in the prior statute which the Act amends, and which governed the commercial sale to minors of "indecentcy" of, among other things, pictures, drawings, motion pictures, books, pamphlets, and magazines. N.Y. Penal Law § 235.21(1), (2).

capabilities to access that material or to circumvent any such screening or blocking." As the Shea court found, a labeling and segregating defense to a criminal ban on protected speech fails to satisfy the Constitution "for several reasons."<sup>17</sup> Id. at 945; see also ACLU, 929 F. Supp. at 847-48, ¶¶ 108-116.

First, "[e]ven assuming that content providers are able to distinguish accurately between material subject to the [statute] and material not subject to the [statute],"<sup>18</sup> and even "assuming that . . . label[ing] . . . would not lead a significant number of content providers to refrain from transmitting such communications,"<sup>19</sup> labeling is "completely ineffective in preventing minors' access to [prohibited] material" on the Internet. Shea, 930 F. Supp. at 945.

There is currently no way for speakers in newsgroups, mailing lists and chat rooms to label their speech in a way that would enable the labeled material "to be automatically blocked," as required by § 235.23(3)(d). Id. at 946. Unlike the voluntary

---

<sup>17</sup> Although there was no explicit labeling defense in the CDA, the trial courts considered extensive evidence on the inability of online speakers to comply with the statute by labeling (or "tagging") their speech. See ACLU, 929 F. Supp. at 847-48, ¶¶ 108-116; Shea, 930 F. Supp. at 932-33. Mandatory labeling also amounts to an unconstitutional prior restraint because speakers would have to silence themselves entirely until the self-labeling process was complete. Bantam Books Inc. v. Sullivan, 372 U.S. 58, 70, 83 S. Ct. 631, 639 (1963) (prior restraint "bear[s] a heavy presumption against its constitutional validity"). Government attempts to impose government-mandated ratings have been struck down repeatedly by the courts. See Interstate Circuit, Inc. v. City of Dallas, 390 U.S. 676, 678-80, 88 S. Ct. 1298, 1300-01 (1968) (invalidating city ordinance that imposed penalties for showing movies deemed by classification board "not suitable for young persons"); Soundgarden v. Eikenberry, 871 P.2d 1050, 1065 (Wash.), cert. denied, 115 S. Ct. 663 (1994) (striking down law that required "erotic" music recordings to be labeled "adult only").

<sup>18</sup> See infra at pp. 38-42 for a discussion of the defense's inherent vagueness.

<sup>19</sup> As the ACLU court noted, the task of determining which material to tag indecent "would be extremely burdensome for organizations that provide large amounts of material." ACLU, 929 F. Supp. at 846, ¶110.

rating systems established by industries such as the Motion Picture Association, no uniform set of labels exists among Internet speakers. Similarly, there is no “label” which is universally recognized by user-based blocking programs for the Web. Id. at 945. Even if the technology were available, speaker-based labeling can never be effective without the cooperation of “third parties to block the material on which the tags are embedded” -- parties who are not subject to criminal prosecution under the Act. ACLU, 929 F. Supp. at 856 (Sloviter, C.J.); see also Shea, 930 F. Supp. at 946 (“[A] content provider would have to assume that third parties -- namely, the users -- install and reconfigure software, and would risk criminal liability if that dubious assumption proved incorrect.”). The ACLU court thus dismissed as speculative the suggestion that a “consensus among speakers” might soon emerge “to use the same tag to label ‘indecent’ material,” and that the industry might (at some future point) develop computer software “that recognizes tags and takes appropriate action when it notes tagged speech.” ACLU, 929 F. Supp. at 848, ¶¶ 113-114. As Chief Judge Sloviter wrote, “I can imagine few arguments less likely to persuade a court to uphold a criminal statute than one that depends on future technology.” Id. at 857; see also Shea, 930 F. Supp. at 948 (“We cannot uphold a statute against a First Amendment challenge in the uncertain expectation that future technology will remedy any constitutional infirmities.” (citing Elrod v. Burns, 427 U.S. 347, 373, 96 S. Ct. 2673, 2689 (1976))).

Similarly, virtually all online speakers lack any means to “segregate” their potentially indecent communications in a way that would “automatically block” them from reaching minors. See ACLU, 929 F. Supp. at 845, ¶ 92 (“The Government presented no evidence demonstrating the feasibility of its suggestion that [indecent material] could be



effectively segregated to ‘adult’ or ‘moderated’ areas of cyberspace.”); Shea, 930 F. Supp. at 946-47. Thus, § 235.23(3)(d) provides no available “safe harbor” from prosecution for adults communicating constitutionally protected material.

d. **There Are No Other “Good Faith, Effective” Actions That Speakers Could Take to Restrict Access to Minors**

Section 235.23(3)(b) provides a defense for one who “has taken, in good faith, reasonable, effective and appropriate actions under the circumstances to restrict or prevent access by minors to material 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.” This defense is identical to the defense provided in § 223(e)(5)(B) of the CDA, and it fails to provide any additional means for speakers to comply with the Act. See Appendix A. In Shea and ACLU, the government’s efforts to provide substance to the “good faith” defense focused on tagging and blocking schemes. Those efforts failed. See supra at pp. 29-31. For the reasons discussed above, online speakers have no “reasonable, effective and appropriate” actions available to prevent their speech from reaching minors. Thus, they must “choose between silence and the risk of prosecution.” ACLU, 929 F. Supp. at 849.

e. **There Is No Way for Online Speakers To Know the Characteristics or Purposes of Their Audience**

Section 235.15(1) provides an affirmative defense if “the persons to whom 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 similar justification for possessing, disseminating or viewing the same."<sup>20</sup>

But, just as Internet speakers have no way to verify the age of their audience, they have no way to determine any other characteristics about them. See discussion supra at p. 17. Thus, speakers cannot determine whether the recipient has any particular justification -- scientific, educational, governmental or otherwise -- for accessing their materials. ACLU, 929 F. Supp. at 845, ¶ 85 ("Once a provider posts content on the Internet, it is available to all other Internet users worldwide.").

3. **The Act Is An Ineffective Method For Achieving the Government's Interest, and Less Restrictive, More Effective, Alternatives Are Available to Parents**

The Act also fails the strict constitutional scrutiny required of content-based bans on speech because it is a strikingly ineffective method for addressing the government's asserted interest. Under strict (and even intermediate) scrutiny, a law "may not be sustained if it provides only ineffective or remote support for the government's purpose." Central Hudson Gas & Elec. Corp. v. Public Serv. Comm'n, 447 U.S. 557, 564, 100 S. Ct. 2343, 2350 (1980). The government bears the burden of showing that its scheme will in fact alleviate the alleged "harms in a direct and material way." Turner Broad., 114 S. Ct. at 2470. Here, the defendants cannot meet this burden. As Justice Scalia wrote in Florida Star v. B.J.F., 491 U.S. 524, 109 S. Ct. 2603 (1989), "a law cannot be regarded as . . . justifying a restriction upon truthful speech, when it leaves appreciable damage to [the government's] supposedly vital interest unprohibited." Id. at 541-42, 109 S. Ct. at 2613

---

<sup>20</sup> This defense existed in the prior statute which the Act amends. See supra p. 1 n.1

(Scalia, J., concurring).<sup>21</sup>

Because of the nature of the online medium, even a total ban will be ineffective at ridding online networks of “indecent” material. The Internet is a global medium, and material posted on a computer overseas is just as available as information posted next door. Thus, the Act will not prevent minors from gaining access to the large percentage of “indecent” material that originates abroad. See ACLU, 929 F. Supp. at 848, ¶ 117 (finding that “a large percentage, perhaps 40% or more, of content on the Internet originates abroad”); Shea, 930 F. Supp. at 931. As the ACLU trial court concluded based on undisputed facts in the record:

[T]he CDA 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 CDA.

ACLU, 929 F. Supp. at 882-83 (Dalzell, J.); see Shea, 930 F. Supp. at 941 (“the CDA will not reach a significant percentage of the sexually explicit material currently available”). In addition, adult-oriented content providers in the United States could circumvent the Act simply by moving their content to sites located outside of the country. ACLU, 929 F. Supp. at 883 n.22. Thus, the Act is unconstitutional because it clearly fails to alleviate the alleged “harms in a direct and material way.” Turner Broad., 114 S. Ct. at 2470.

---

<sup>21</sup> See also Denver Area, 116 S. Ct. at 2416 (“Partial service of a compelling interest is not narrow tailoring”) (Kennedy & Ginsburg, J.J., concurring in part and dissenting in part); Bolger v. Youngs Drug Prods. Corp., 463 U.S. 60, 73, 103 S. Ct. 2875, 2884 (1983) (restriction that “provides only the most limited incremental support for the interest asserted” cannot survive scrutiny under commercial speech standards).

Moreover, the Act is not the least restrictive means of achieving the government's asserted interest. See Sable, 492 U.S. at 126, 109 S. Ct. at 2837 ("It is not enough to show that the Government's ends are compelling; the means must be carefully tailored to achieve those ends."). The Legislature conducted no investigation and made no factual findings to establish that the Act is the least restrictive means of protecting minors from harmful speech. See New York State Senate Introducer's Memorandum In Support, S. 210-E, p.1 (1996). In Sable, the Supreme Court struck down a content-based statute banning "indecent" commercial telephone messages on the ground that "the congressional record contains no legislative findings that would justify us in concluding that there is no constitutionally acceptable less restrictive means, short of a total ban, to achieve the Government's interest in protecting minors." 492 U.S. at 29, 109 S. Ct. at 2838. Had the New York Legislature bothered to hold hearings on various ways to restrict minors' access to indecent communications, it would have learned of a variety of user-based filtering programs and other options that enable parents to limit the information their children receive online. See discussion supra at pp. 17-18; ACLU, 929 F. Supp. at 839-42, ¶¶ 49-73; Shea, 930 F. Supp. at 931-32. Unlike the Act, these options provide an effective way for users to prevent sexually oriented material originating from foreign sites from reaching minors. They are also notably less restrictive than the Act's effective total ban. See Denver Area, 116 S. Ct. at 2393 (informational requirements and user-based blocking are more narrowly tailored than speaker-based schemes as a means of limiting minors' access to indecent material).<sup>22</sup>

---

<sup>22</sup> The government can also address its interest by vigorously enforcing other criminal statutes. See, e.g., N.Y. Penal Law § 235.05 (promoting or possessing obscene material); id. § 235.21 (inviting or inducing a minor to engage in sexual contact by means of computer communication); id. § 263.05 (use of a child in a sexual performance); id. § 263.15

#### 4. The Act Is Substantially Overbroad

##### a. The Act's Failure to Define the Applicable Community Standard Renders It Overbroad

The act is also overbroad because it infringes on the rights of adults in communities outside of New York. The statute at issue defines "harmful to minors" according to "prevailing standards in the adult community," but fails to define the relevant community.<sup>23</sup> Even if the relevant community is intended to be the state-wide community of New York, see People v. P.J. Video, Inc., 68 N.Y.2d 296, 308-09, 501 N.E.2d 556, 564, 508 N.Y.S.2d 907, 915 (1986), the Act would ban speech across the entire Internet that may not be considered "indecent" in communities outside New York State.

As discussed above, there is no way for online speakers to restrict their messages to persons in a particular geographic area. See Shea, 930 F. Supp. at 937 ("[U]nlike a provider of obscene or indecent telephone communications or cable programming, who might be able to prevent a message from being transmitted to certain geographical areas, an Internet content provider has no way of identifying the receiving community."). Because all Internet communications can be received in New York, every Internet speaker in the United States must censor her message to meet the community standards of New York, even if the message would be constitutionally protected in her community. See David R. Johnson & David Post, Law and Borders - The Rise of Law in Cyberspace, 48 Stan. L. Rev. 1367, 1373-78 (1996). Thus, the "community standards" language of the Act prohibits speakers in communities outside of New York from engaging

---

(promoting sexual performance by a child).

<sup>23</sup> See infra at p. 39 discussing the vagueness of the Act's "community standards" provision.

in speech that is protected in their communities, and contributes to the Act's substantial overbreadth. See Shea, 930 F. Supp. at 938 (noting that the problem "appears to raise questions of overbreadth") (dictum).

b. **The Act Is Overbroad Because It Criminalizes Speech That Is Constitutionally Protected for Older Minors**

In addition to banning constitutionally protected speech among adults (see supra at pp. 20-22), the Act is unconstitutionally overbroad because it proscribes speech that may be "harmful" to younger minors but that unquestionably is constitutionally protected for older minors. The Supreme Court has ruled in many contexts that the First Amendment protects minors as well as adults, and that minors have the constitutional right to speak and to receive the information and ideas necessary for their intellectual development and their participation as citizens in a democracy,<sup>24</sup> including information about reproduction and sexuality. Carey v. Population Servs., Int'l, 431 U.S. 678, 693, 97 S. Ct. 2010, 2020 (1977). With only narrow exceptions, it is unconstitutional for the government to restrict minors' participation in the marketplace of ideas.

The Act impermissibly burdens minors' First Amendment rights in two ways. First, the Act could result in the outright exclusion of minors from many of the vast public spaces in the online medium that are currently accessible to both minors and adults. Even if there were some way for speakers in these spaces to determine the age of their audience (and currently there is not, supra at pp. 16-17), most speakers and content providers do not have

---

<sup>24</sup> See, e.g., Board of Educ. v. Pico, 457 U.S. 853, 864, 102 S. Ct. 2799, 2806 (1982); Erznoznik v. City of Jacksonville, 422 U.S. at 213-14, 95 S. Ct. at 2275; Tinker v. Des Moines Indep. Comm. School Dist., 393 U.S. 503, 89 S. Ct. 733 (1969); West Virginia State Bd. of Educ. v. Barnette, 319 U.S. 624, 63 S. Ct. 1178 (1943).

the resources to create two versions of their online communications -- one for adults, and one for minors. Thus, rather than shoulder the burden of creating two distinct versions of their material or message, many speakers would simply exclude all minors, regardless of their age, from all of their communications in order to comply with the Act. See Complaint ¶¶ 95, 110, 125.

Second, the statute impermissibly burdens the right of older minors to obtain ideas and information about sexuality, reproduction, and the human body -- subjects which are of special interest to maturing adolescents. Because the Act makes no distinction between material that is “harmful” to younger minors and material that is “harmful” to older minors, the Act would make it a crime to provide, for example, explicit safer sex information to teenagers. Recognizing this problem, some states have upheld statutes regulating the dissemination of material deemed “harmful to minors” only after construing them to prohibit only that material that would lack serious value for older minors. Webb, 919 F.2d at 1504-05 (concluding that “if any reasonable minor, including a seventeen-year-old, would find serious value, the material was not ‘harmful to minors’” for purposes of the statute); American Booksellers Ass’n. Inc. v. Virginia, 882 F.2d 125 (4th Cir. 1989) (concluding that “‘if a work is found to have a serious literary, artistic, political or scientific value for a legitimate minority of normal, older adolescents, then it cannot be said to lack such value for the entire class of juveniles’” (quoting Commonwealth v. American Booksellers Ass’n., 236 Va. 168, 372 S.E.2d 618, 624 (1988))). Without further definition of the “harmful to minors” standard, the Act would effectively ban speech which is constitutionally protected for older minors as well as adults, thereby reducing the content on

the Internet to that which is appropriate for a young child.

## 5. The Act Is Unconstitutionally Vague

Like the CDA, the Act “attempts . . . to regulate protected speech through criminal sanctions, thus implicating not only the First but also the Fifth Amendment of our Constitution.” ACLU, 929 F. Supp. at 859 (Buckwalter, J.). As the Supreme Court has stated, criminal statutes should be scrutinized with extreme care for clarity because “[n]o one may be required at peril of life, liberty or property to speculate as to the meaning of penal statutes,” and this is particularly true of laws “having a potentially inhibiting effect on speech.” Hynes v. Mayor of Oradell, 425 U.S. 610, 620, 96 S. Ct. 1755, 1760 (1977) (quoting Lanzetta v. New Jersey, 306 U.S. 451, 453, 59 S. Ct. 618, 619 (1939), and Smith v. California, 361 U.S. 147, 151, 80 S. Ct. 215, 217 (1959)).

Plaintiffs do not claim that the definition of “harmful to minors” is vague as applied to other media. See Ginsberg, 390 U.S. 629, 98 S. Ct. 1274. Rather, plaintiffs challenge the application of the standard to the unique characteristics of the Internet.<sup>25</sup> See ACLU, 929 F. Supp. at 865 n.9 (Buckwalter, J.) (“[T]he unique nature of the online medium cannot be overemphasized in discussing and determining the vagueness issue”). The Act requires millions of ordinary citizens communicating through newsgroups, chat rooms, and mail exploders -- in conversations that are often as fleeting as chats on a street corner -- to determine whether their speech is criminal. Without any further guidance, there is no

---

<sup>25</sup> The trial courts that considered the constitutionality of the CDA disagreed about whether the CDA’s “indecentcy” standard, which differs from the “harmful to minors” standard in the New York Act, was unconstitutionally vague. Compare ACLU, 929 F. Supp. at 856 (Sloviter, C.J.), 859-65 (Buckwalter, J.) with Shea, 930 F. Supp. at 939. That issue, among others in the case, is currently on appeal before the Supreme Court. ACLU, 117 S. Ct. 554 (1996).



doubt that the Act will force many of these online speakers to “‘steer far wider of the unlawful zone’ . . . than if the boundaries of the forbidden areas were clearly marked.’” Grayned v. City of Rockford, 408 U.S. 104, 109, 92 S. Ct. 2294, 2299 (1972) (citations omitted).

Specifically, the Act fails to define the relevant community that will set the standard for what is “indecent” on the global Internet. Is it the state-wide adult community of New York, or the community of adults participating in the online medium? If it is the state-wide community of New York, how can an individual speaker in Hawaii posting a message to a newsgroup available worldwide predict what New York prosecutors and juries might deem “indecent”? See ACLU, 929 F. Supp. at 862-63 (Buckwalter, J.) (holding that the CDA is unconstitutionally vague because it failed to define the relevant “community standard” for determining “indecenty”). Similarly, the phrase “considered as a whole,” in the serious value prong of the Act’s definition of “harmful to minors,” is hopelessly vague when applied to online communications. For example, how should a speaker on the Web define the relevant “work as a whole” when trying to determine the potential “indecenty” of a Web site comprised of thousands of linked documents, images, and texts, simultaneously presented through the ad hoc linking feature of the Web? See id. at 871 n.11 (Dalzell, J.). The Act provides no clear answers to these questions which, if answered incorrectly, could send the speaker to jail.

Several of the Act’s defenses are also unconstitutionally vague because they fail to provide sufficient clarity so that “ordinary people can understand what conduct is prohibited.” Kolender v. Lawson, 461 U.S. 352, 357, 103 S. Ct. 1855, 1858 (1983).

Section 235.23(3)(a), for instance, purports to provide a defense to the Act if an individual makes a “reasonable effort to ascertain the true age of the minor and was unable to do so as a result of actions taken by the minor.” In the context of the Internet, where there is no face-to-face interaction between speakers and listeners, and where speakers have no way to determine the age or any other characteristics of the persons who access their speech, speakers simply do not know what “reasonable efforts” they could take to avoid prosecution. Similarly, the Act provides no guidance whatsoever regarding what might or might not constitute “good faith, reasonable, effective, and appropriate actions under the circumstances to restrict or prevent access by minors” under § 235.23(3)(b). As the Shea court suggested, “the fact that [this defense] nowhere identifies any specific steps that a content provider can take to enter its ‘safe harbor’ renders [it] unconstitutionally vague, because individuals lack sufficient notice as to how to shield themselves from criminal liability under the statute.” Shea, 930 F. Supp. at 944 n.18.<sup>26</sup>

Section 235.23(3)(d) -- the “labeling and segregating” defense -- is equally vague. It requires speakers to label or segregate their speech in a manner that would cause the material to be “automatically blocked or screened by software or other capabilities reasonably available to responsible adults wishing to effect such blocking or screening.” But the defense fails to tell speakers what label to use, and there is no consensus or set of standards among Internet speakers for labeling; likewise, there are no labels recognized by user-based blocking software. Id. at 945-46; see discussion supra at pp. 29-30. In addition,

---

<sup>26</sup> The Shea court declined to rule on this issue because it found the CDA to be unconstitutional on other grounds. Id.

the defense fails to clarify what a speaker must prove to establish that labeled material has been automatically blocked, and it is unclear how a speaker could even know the material had been blocked since blocking depends entirely on the actions of third parties. Shea, 930 F. Supp. at 946; ACLU, 929 F. Supp. at 856; see discussion supra at p. 30. Thus, the labeling and segregating defense provides absolutely no guidance to speakers that would enable them to avoid prosecution.

Finally, § 235.24(1) also is unconstitutionally vague. It provides the following defense:<sup>27</sup>

No person shall be held to have violated such provisions 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.

Plaintiffs ECHO, Panix, NYC Net, Westchester Library System and member libraries of ALA and NYLA all provide Internet access services. Complaint ¶¶ 93, 98, 99, 115, 118, 121. Although much of the content on their systems is not created by them, they can theoretically exercise “control” over the communications of their subscribers and patrons for which they are conduits (though exercising actual control over such material would be prohibitively expensive and an extreme intrusion on the privacy of their users). It is entirely unclear whether this degree of control renders them ineligible for the access provider defense. In addition, these plaintiffs and others sponsor online discussion forums and create chat rooms on particular subjects of interest to their users and subscribers. Complaint ¶¶ 93,

---

<sup>27</sup> This defense was taken verbatim from § 223(e)(1) of the CDA. See Appendix A.

116, 118, 121, 138. Because they create and exercise control over these discussion forums, it is entirely unclear under the Act whether they could be prosecuted for content posted by others in such forums.

**6. The Act Violates the Commerce Clause of the United States Constitution**

Finally, the Act violates the Commerce Clause of the United States Constitution (U.S. Const., Art. I, § 8, cl.3). Because of the borderless nature of the online medium, the Act imposes restrictions on communications occurring wholly outside the State of New York, effects an impermissible burden on interstate commerce, and subjects online speakers to inconsistent state obligations.

**a. The Act Is Per Se Invalid Because It Regulates Commerce Entirely Outside of the State of New York**

A state statute which “has the ‘practical effect’ of regulating commerce occurring wholly outside that State’s borders is invalid under the Commerce Clause.”<sup>28</sup> Healy, 491 U.S. at 336, 109 S. Ct. at 2499 (reaffirming that the “‘Commerce Clause . . . precludes the application of a state statute to commerce that takes place wholly outside of the State’s borders’” (quoting Edgar v. MITE Corp., 457 U.S. 624, 642-43, 102 S. Ct. 2629, 2640-41 (1982))); Brown-Forman Distillers Corp. v. New York State Liquor Auth., 476 U.S. 578, 582, 106 S. Ct. 2080, 2086 (1986) (New York liquor-price affirmation statute directly regulated out-of-state transactions in violation of the Commerce Clause). Because of the nature of the online medium, the Act’s criminal ban on protected speech extends to a

---

<sup>28</sup> The Supreme Court has long recognized that the Commerce Clause encompasses an implicit or “dormant” limitation on the authority of the states to enact legislation affecting interstate commerce. Healy, 491 U.S. at 326 n.1, 109 S. Ct. at 2494 n.1; Hughes v. Oklahoma, 441 U.S. 322, 326 & n.2, 99 S. Ct. 1727, 1731 & n.2 (1979).

wide range of online communications that occur entirely outside of the State of New York, and is thus a per se violation of the Commerce Clause.

The Act restricts virtually all online communications that take place around the world in newsgroups, mail exploders, and chat rooms on the Internet, because public messages posted to these forums from anywhere in the world can be accessed by users in New York. If, for example, a member of plaintiff ACLU in California posts a potentially “indecent” message to an Internet discussion group, that message may be accessed and read by a reader in New York. The posting of the message in California, therefore, may subject the California author to prosecution in New York under the Act. Moreover, online technology provides no means for the speaker to determine whether anyone from New York will actually read her message. Thus, to avoid the risk of prosecution, the author of the message must refrain from “indecentcy” when she posts to the discussion group -- regardless of whether anyone in New York actually reads any of her messages.

Similarly, the Act restricts the ability of any online user to publish a Web page on the Web, regardless of whether the site is located in New York. There is no way for a Web publisher to prevent Internet users in New York from accessing her site. Thus, any Web publisher anywhere in the world -- including all of the nonresident Web publishers who are plaintiffs in this case -- must refrain from “indecentcy” or risk prosecution under the Act in New York, regardless of whether anyone in New York ever accesses her Web page.

Because the Act regulates communications occurring wholly outside the State of New York, it is a per se violation of the Commerce Clause, and should be “struck down . . . without further inquiry.” Brown-Forman, 476 U.S. at 579, 106 S. Ct. at 2084; see also

Healy, 491 U.S. at 336, 109 S. Ct. at 2499; Edgar, 457 U.S. at 643, 102 S. Ct. at 2641; Baldwin v. G.A.F. Seeling, Inc., 294 U.S. 511, 521, 55 S. Ct. 497, 500 (1935).

b. **The Act Is Invalid Because the Burdens It Imposes Upon Interstate Commerce Exceed Any Local Benefit**

Even if it is not a per se violation of the Commerce Clause, the Act still is an invalid state regulation because the burdens it imposes upon interstate commerce clearly exceed any local benefits. Pike, 397 U.S. at 142, 90 S. Ct. at 847 (fruit-packing statute invalid because the burden it imposed on interstate commerce was “clearly excessive in relation to the putative local benefits”); Edgar, 457 U.S. at 643-44, 109 S. Ct. at 2641 (state interests in protecting shareholders and regulating state corporations were insufficient to outweigh burdens imposed by allowing state official to block tender offers). As set forth above, the Act regulates a wide range of entirely out-of-state communications which New York has no legitimate interest in regulating. New York’s interest in protecting resident minors from information that New Yorkers deem “indecent” cannot justify the significant burden on the online communications of speakers in forty-nine states, and worldwide.

c. **The Act Violates the Commerce Clause Because It Subjects Interstate Use of the Internet to Inconsistent Regulations**

The Act is also precluded by the Commerce Clause because the lack of national uniformity created by conflicting state regulations of the Internet will impede the flow of interstate communications on the Internet. Southern Pac., 325 U.S. at 767, 65 S. Ct. at 1519 (finding that Arizona regulation of train length impeded the flow of interstate commerce). Several state legislatures have either enacted or considered proposals regulating

the content of online communications.<sup>29</sup> Internet users who post to Web sites, discussion groups and chat rooms simply have no way to send different versions of their speech to different regions in order to comply with standards under often conflicting state statutes. The practical effect of the combination of fifty conflicting state laws regulating content on the Internet would be to “create just the kind of competing and interlocking local economic regulation that the Commerce Clause was meant to preclude.” Healy, 491 U.S. at 337, 109 S. Ct. at 2500. Arguably, therefore, the dormant Commerce Clause precludes the entire field of online communications from state regulation because “the lack of national uniformity would impede the flow of interstate goods.” Exxon Corp. v. Governor of Md., 437 U.S. 117, 128, 98 S. Ct. 2207, 2215 (retail market for gas did not preclude state regulation), reh’g denied, 439 U.S. 884, 99 S. Ct. 232 (1978); see Wabash St. L. & P. Ry. Co. v. Illinois, 118 U.S. 557, 7 S. Ct. 4 (1886) (railroad rates exempt from state regulation).

**B. Plaintiffs Will Suffer Irreparable Harm if Preliminary Relief Is Not Granted**

Plaintiffs have no adequate remedy at law for deprivation of their constitutional rights under the First, Fifth and Fourteenth Amendments and the Commerce Clause. Irreparable injury means “the kind of injury for which money cannot compensate,” Sperry Int’l Trade, Inc. v. Government of Israel, 679 F.2d 8, 12 (2d Cir. 1982), and which is “neither remote nor speculative, but actual and imminent.” Tucker Anthony Realty Corp. v. Schlesinger, 888 F.2d 969, 975 (2d Cir. 1989).

As the Supreme Court has stated, “the loss of First Amendment freedoms, for

---

<sup>29</sup> See, e.g., Ga. Code Ann. § 16-19-93.1 (1996) (making it a crime to communicate anonymously on the Internet); Okla. Stat. tit. 21, § 1040.76 (1996) (prohibiting online transmission of material deemed “harmful to minors”).

even minimal periods of time, unquestionably constitutes irreparable injury.” Elrod, 427 U.S. at 373; see also ACLU, 929 F. Supp. at 851 (“Subjecting speakers to criminal penalties for speech that is constitutionally protected in itself raises the specter of irreparable harm”); Shea, 930 F. Supp. at 935.

Plaintiffs who choose not to self-censor will face the risk of criminal prosecution if the Act is not preliminarily enjoined. See Complaint ¶¶ 89-90. The Act’s passage has already led members of plaintiff Art on the Net to remove potentially “indecent” artwork from their Web sites for fear of criminal prosecution. Thus, the Act has already caused irreparable harm by creating a chilling effect on free expression in violation of the First Amendment. See Time Warner Cable v. Citv of New York, 943 F. Supp. 1357, 1399 (S.D.N.Y. 1996) (city’s action had direct chilling effect on plaintiff’s First Amendment rights, causing irreparable injury); Fabulous, 896 F.2d at 785-87 (finding that statutory requirement of access codes for sexually suggestive telephone messages created chilling effect on protected speech).

Likewise, deprivation of plaintiffs’ constitutional rights under the Commerce Clause constitutes irreparable injury. C. & A. Carbone, Inc. v. Town of Clarkstown, 770 F. Supp. 848, 854 (S.D.N.Y. 1991) (local waste disposal law caused irreparable injury of plaintiffs’ rights under the Commerce Clause). Many of the plaintiffs conduct a substantial amount, if not all, of their communications over the Internet. See Complaint ¶¶ 107, 126, 131. Plaintiffs will be prohibited from exercising their right to engage in interstate use of the Internet if the Act is not enjoined.



C. There are Sufficiently Serious Questions to Make a Fair Ground for Litigation and the Balance of Hardships Weighs in the Plaintiffs' Favor

Plaintiffs have also clearly established that there are sufficiently serious questions going to the merits of this case to make a fair ground for litigation, and that the balance of hardships tips decidedly in their favor. See Hamilton Watch Co. v. Benrus Watch Co., 206 F.2d 738, 740 (2d. Cir. 1953); see also Streetwatch, 875 F.Supp at 1065 (stating that the fair-ground-for-litigation standard “is less rigorous than the likelihood of success test”). Because the Act threatens the First Amendment rights of millions of speakers on the Internet, the questions in this case could not be more serious. If the Act is not enjoined, plaintiffs will be forced to choose between censoring their own protected expression -- which unquestionably has value for adults and older minors -- or placing themselves at the risk of prosecution. By contrast, defendants could suffer no injury from an injunction barring enforcement of this unconstitutional law. Defendants will still be able to prosecute individuals under existing obscenity, solicitation, harassment and sexual assault laws. See discussion supra at p. 34 n.22. Thus, the balance of hardships tips decidedly in the plaintiffs' favor.

Finally, for all the reasons set forth above, the entry of a preliminary injunction would promote, not disserve, the public interest. As the ACLU court observed, “[n]o string of citations is necessary to find that the public interest weighs in favor of having access to a free flow of constitutionally protected speech.” ACLU, 929 F. Supp. at 851 (Sloviter, C.J.); see also Turner Broad., 114 S. Ct. at 2458.

### CONCLUSION

Plaintiffs respectfully request that the Court grant them preliminary injunctive relief, for any or all of the reasons set forth above.

Dated: New York, New York  
March 3, 1997

Respectfully submitted,

By: 

Michael K. Hertz (MH-5587)  
LATHAM & WATKINS  
885 Third Avenue  
Suite 1000  
New York, New York 10022  
(212) 906-1200

Christopher A. Hansen (CH-6776)  
Ann Beeson  
AMERICAN CIVIL LIBERTIES UNION  
132 West Forty-Third Street  
New York, New York 10036  
(212) 944-9800

Arthur N. Eisenberg (AE-2012)  
NEW YORK CIVIL LIBERTIES UNION  
132 West Forty-Third Street  
New York, New York 10036  
(212) 944-9800

Michael A. Bamberger (MB-9577)  
SONNENSCHN NATH & ROSENTHAL  
1221 Avenue of the Americas  
New York, New York 10020  
(212) 768-6700  
Attorneys for Plaintiffs

## Appendix A

## Comparison of the Communications Decency Act of 1996 and New York Penal Law § 235.15 -235.24

<u>Subject</u>	<u>Federal Section</u>	<u>Text</u>	<u>NY Section</u>	<u>Text</u>
Title		"Communications Decency Act of 1996"		"Disseminating Indecent Materials to Minors"
Description of Offense	223(1)(d)(1)	Punishes whoever knowingly "(A) uses an interactive computer service to send to a specific person or persons under 18 years of age, or (B) uses any interactive computer service to display in a manner available to a person under 18 years of age, any comment, request, suggestion, proposal, image, or other communication that, in context, depicts or describes, in terms patently offensive as measured by contemporary community standards, sexual or excretory activities or organs, regardless of whether the user of such service placed the call or initiated the communication."	235.21(3)  235.20(6)	Punishes whoever "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."  "'Harmful to minors' means 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."

Good faith Defense	223(e)(5)(A)	Provides defense if person “has taken, in good faith, reasonable, effective, and appropriate actions under the circumstances to restrict or prevent access by minors to a communication specified in such subsections, which may involve any appropriate measures to restrict minors from such communications, including any method which is feasible under available technology.”	235.23(3) (b)	Provides defense if person “has taken, in good faith, reasonable, effective and appropriate actions under the circumstances to restrict or prevent access by minors to <u>material</u> specified in such <u>subdivision</u> , which may involve any appropriate measures to restrict minors from access to such communications, including any method which is feasible under available technology.”  [Underlining indicates changes from federal version]
Credit card Defense	223(e)(5)(B)	Provides defense if person “has restricted access to such communication by requiring use of a verified credit card, debit account, adult access code, or adult personal identification number.”	235.23(3) (c)	Provides defense if person “has restricted access to such <u>materials</u> by requiring use of a verified credit card, debit account, adult access code, or adult personal identification number.”  [Underlining indicates changes from federal version]
Service Provider Defense	223(e)(1)	Provides that person is not 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 does not include the creation of the content of the communication.”	235.24(1)	Provides that person is not 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 <u>do</u> not include the creation of the content of the <u>communication</u> .”  [Underlining indicates changes from federal version]

Exception to Service Provider Defense	223(e)(2)	Provides that above defense “shall not be applicable to a person who is a conspirator with an entity actively involved in the creation or knowing distribution of communications that violate” this section “or who knowingly advertises the availability of such communications.”	235.24(1) (a)	Identical
Exception to Service Provider Defense	223(e)(3)	Provides that above defense “shall not be applicable to a person who provides access or connection to a facility, system, or network engaged in the violation of this section that is owned or controlled by such person.”	235.24(1) (b)	Identical
Employer Defense	223(e)(4)	“No employer shall be held liable under this section for the actions of an employee or agent unless the employee’s or agent’s conduct is within the scope of his or her employment or agency and the employer (A) having knowledge of such conduct, authorizes or ratifies such conduct, or (B) recklessly disregards such conduct.”	235.24(2)	“No employer shall be held liable under <u>such provisions</u> for the actions of an employee or agent unless the employee’s or agent’s conduct is within the scope of his __ employment or agency and the employer __ having knowledge of such conduct, authorizes or ratifies such conduct, or __ recklessly disregards such conduct.”  [Underlining indicates changes from federal version]
Effort to Ascertain Age Defense			235.23(3) (a)	Provides defense person “made a reasonable effort to ascertain the true age of the minor and was unable to do so as a result of actions taken by the minor.”

Blocking Defense			235.23(3)(d)	Provides defense if person "has in good faith established a mechanism such that the labeling, segregation or other mechanism enable 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 blocking or screening capabilities to access that material or to circumvent any such screening or blocking."
Justified Purpose Defense			235.15(1)	Provides defense if persons "to whom 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."
Definition of Access Software	223(h)(3)	"The term 'access software' means software (including client or server software) or enabling tools that do not create or provide the content of the communication but that allow a user to do any one or more of the following: (A) filter, screen, allow or disallow content; (B) pick, choose, analyze, or digest content; or (C) transmit, receive, display, forward, cache, search, subset, organize, reorganize, or translate content."	235.20(7)	Identical

CERTIFICATE OF SERVICE

I hereby certify that on March 3, 1997, I caused to be served by hand upon Jeanne LaHiff, counsel for defendants in this action, a true copy of Plaintiffs' Memorandum of Law in Support of their Motion for a Preliminary Injunction at the Attorney General's Office, New York State Department of Law - Litigation Dept., 120 Broadway, New York, New York 10271.



---

Christopher Harris