UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

-x

BARBARA NITKE, THE NATIONAL COALITION FOR SEXUAL FREEDOM, and THE NATIONAL COALITION FOR SEXUAL FREEDOM FOUNDATION,

Index No. 01 Civ 1476 (RMB)

Plaintiffs,

-against-

JOHN ASHCROFT, ATTORNEY GENERAL OF THE UNITED STATES OF AMERICA, .nd THE UNITED STATES OF AMERICA

Defendants.

- - - - -x

BRIEF *AMICUS CURIAE* OF ELECTRONIC FRONTIER FOUNDATION IN SUPPORT OF PLAINTIFF

LEE TIEN
ELECTRONIC FRONTIER FOUNDATION
454 Shotwell Street
San Francisco, CA 94110
Tel. (415) 436-9333 x102
Fax (415) 436-9993

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

INTRODUCTION

The obscenity provisions of the Communications Decency Act ("CDA"), Section 502 of the Telecommunications Act of 1996, 47 U.S.C. § 223(a)(1)(B), are unconstitutionally overbroad because the threat of the CDA's criminal sanctions will chill substantial amounts of protected speech. In this supplemental amicus brief, however, amicus Electronic Frontier Foundation ("EFF") challenges the government's argument, advanced at trial, that the burdens that the CDA imposes on web site publishers like plaintiff Barbara Nitke are practically reasonable and legally "incidental."[2]

The threshold problem is that while our prevailing "community standards" jurisprudence of obscenity is based on geographically defined communities, the Internet is a geography-indifferent medium of expression. *Nitke v. Ashcroft*, 253 F.Supp.2d 587, 604 (S.D.N.Y. 2004) ("because Internet content providers cannot control the geographic distribution of their materials, Internet obscenity statutes restrict protected speech") (citing *Ashcroft v. Am. Civil Liberties Union*, 535 U.S. 564, 122 S.Ct. 700, 1714 (2002) (O'Connor, J., concurring)).

The Internet's indifference to geography means that an online content provider "has no way to distribute online materials to New York but not to Maine." *Ibid.* Online providers who must comply with an Internet obscenity statute "by tailoring their materials to Maine's community standards[] have no choice but to refrain from distributing *anywhere* those materials that are obscene in Maine but not in New York." *Ibid.* (emphasis in original).

The problem runs deeper, however; it is not merely that online publishers cannot restrict publication to particular geographical areas, but also that the Internet does not lend itself to the identification and location of those who receive and read online

---

[1] Amicus also remains convinced that the CDA poses vagueness issues and refers the Court to the vagueness arguments in our first amicus brief in this case.

[2] Amicus was unable to attend the trial and in this brief relies on a portion of the trial transcript for Oct. 28, 2004, provided by Mr. John Wirenius.

materials. Even more important, given this baseline of Internet anonymity, government action that would effectively require the identification and location of Internet users conflicts directly with clear lines of precedent and principle that protect and even celebrate the right to speak and read anonymously

Accordingly, amicus EFF urges this Court to reject the government's argument and hold that the government's suggested self-identification mechanisms do not pass muster under the First Amendment.

INTERESTS OF AMICUS

The Electronic Frontier Foundation ("EFF") is a non-profit civil liberties organization working to protect rights in the digital world. EFF actively encourages and challenges industry and government to support free expression and privacy in the information society. Founded in 1990, EFF is based in San Francisco. EFF has members all over the United States and maintains one of the most-linked-to Web sites in the world, <http://www.eff.org>.

I. ARGUMENT

In an attempt to salvage the CDA's obscenity provisions, the government has suggested that there are reasonable options for ascertaining the geographic location of web site visitors, and that these burdens are merely "incidental" from a First Amendment perspective. Mr. Chris McCulloh of Sinetimore testified that in his opinion, plaintiff and others similarly situated could "reasonably" comply with the CDA by asking each visitor to their sites to reveal their geographic location and check that location against some "master list" of "liberal" or "conservative" communities. To verify the visitor's representation as to his or her geographic location, the visitor should submit a form, print it out, sign it and mail it in. In this scheme, the postmark – which identifies geographic location – would constitute verification.

Amicus respectfully submits that any such scheme is a mere makeweight offered to shore up the weaknesses of the government's position.

II. THE BURDENS ASSOCIATED WITH COMPELLED IDENTIFICATION ARE PRACTICALLY AND LEGALLY SIGNIFICANT

The Internet is a new and powerful medium of expression that covers a range of topics "as diverse as human thought." *Reno v. ACLU*, 521 U.S. 844, 852 (1997) (citation omitted); *id.* at 870 ("our cases provide no basis for qualifying the level of First Amendment scrutiny that should be applied to this medium.").

Accordingly, the Supreme Court has been reluctant to uphold content-based prohibitions on Internet speech. "Content-based prohibitions, enforced by severe criminal penalties, have the constant potential to be a repressive force in the lives and thoughts of a free people. To guard against that threat the Constitution demands that content-based restrictions on speech be presumed invalid, and that the Government bear the burden of showing their constitutionality." *Ashcroft v. ACLU*, 542 U.S. , 124 S.Ct. 2783, 2788 (2004) (upholding preliminary injunction against enforcement of Child Online Protection Act ("COPA"), 47 U.S.C. § 231, which seeks to restrict provision of "harmful-to-minors" (HTM) material) (citations omitted).

In reviewing content-based restrictions on speech, the courts must pay close attention to the existence of "plausible, less restrictive alternatives." *Id.* at 2792. "A statute that 'effectively suppresses a large amount of speech that adults have a constitutional right to receive and to address to one another . is unacceptable if less restrictive alternatives would be at least as effective in achieving the legitimate purpose that the statute was enacted to serve.'" *Ibid.* (quoting *Reno v. ACLU*, 521 U.S., at 874). "The purpose of the test is to ensure that speech is restricted no further than necessary to achieve the goal, for it is important to assure that legitimate speech is not chilled or punished." *Ibid.*

III. THE GOVERNMENT'S SCHEME IS UNDULY RESTRICTIVE

Like COPA, the CDA imposes "universal restrictions at the source." *See Ashcroft v. ACLU*, 124 S.Ct., at 2792. In an attempt to mitigate this bluntness, the government speculates that Internet publishers like plaintiff might be able to comply with the CDA

with schemes like visitor self-identification.

As a threshold matter, any such scheme would significantly burden Internet speech. Each visitor must not only reveal him or herself by name and address, but also wait for (by Mr. McCulloh's estimate) two to three weeks to be permitted access. Trial Transcript (Oct. 28, 2004), at 237 (agreeing that "the time from initial registration to your receipt of the hard copy verification was about two to three weeks"); *ibid.* (agreeing that "if the user chose not to submit the verification, then you simply deny them access to the material"); *id.* at 238. If the government can seriously suggest that a medium like the Internet, whose hallmark is speed, should be subject to access delays of two or three weeks — and that the automatic response when a person fails to submit location or other identifying information should be to deny access to speech then the First Amendment is being turned upside-down.

Equally important, content-based restrictions that require recipients to identify themselves affirmatively before being granted access to disfavored speech have been found to produce an impermissible chilling effect on those would-be recipients. *See, e.g.*, *Lamont v. Postmaster General*, 381 U.S. 301 (1965) (federal statute requiring Postmaster to halt delivery of communist propaganda unless affirmatively requested by addressee violated First Amendment); *Denver Area Educ. Telecomms. Consortium v. FCC*, 518 U.S. 727, 732-33 (1996) (invalidating federal law requiring cable operators to allow access to sexually explicit programming only to those subscribers who request access to the programming in advance and in writing).

As this Court is aware, the Third Circuit found that "COPA will likely deter many adults from accessing restricted content, because many Web users are simply unwilling to provide identification information in order to gain access to content, especially where the information they wish to access is sensitive or controversial." *ACLU v. Ashcroft*, 322

F.3d 240, 259 (3d Cir. 2003), *aff'd*, *Ashcroft v. ACLU*, 124 S.Ct. 2783 (2004).[3] The Third Circuit also noted that "[p]eople may fear to transmit their personal information, and may also fear that their personal, identifying information will be collected and stored in the records of various Web sites or providers of adult identification numbers." *Ibid.*; *id.* at 259 n. 21 (noting that statutory privacy protection "does not negate the likelihood that adults will be chilled in accessing speech protected for them; adults may reasonably fear that their information will be disclosed, this provision notwithstanding.").

Finally, a visitor-identification scheme is likely to be more restrictive than a filtering regime. The same logic that plagued COPA in *Ashcroft v. ACLU* applies to the CDA here. Filters "are less restrictive than COPA" for several reasons: "[t]hey impose selective restrictions on speech at the receiving end, not universal restrictions at the source"; "[u]nder a filtering regime, adults without children may gain access to speech that they have a right to see without having to identify themselves or provide their credit card information"; "[e]ven adults with children may obtain access to the same speech on the same terms simply by turning off the filter on their home computers"; "[a]bove all, promoting the use of filters does not condemn as criminal any category of speech, and so the potential chilling effect is eliminated, or at least much diminished." *Id.* at 2792.

Accordingly, the CDA's obscenity provisions burden more speech than is necessary, and the proffered visitor-identification scheme would likely be more restrictive than a filtering regime.

---

[3] One government expert testified that the registration system used by other web sites like *The New York Times* could be a model for plaintiff. Trial Transcript (Oct. 28, 2004), at 236-237 (testimony of Mr. Chris McCulloh, Sinetimore); see Sinetimore Expert Report (Mr. Chris McCulloh), at 8. But such sites "are not analogous to Internet sites that provide speech that is protected for adults that might nonetheless be harmful to minors," because "adult readers would be deterred from obtaining if they were required to register or otherwise identify themselves." *ACLU v. Ashcroft*, 322 F.3d at 259 n. 20. The same reasoning applies where speech that is legally obscene in one community might not be legally obscene in another.

IV. ANY SUCH SCHEME WOULD UNCONSTITUTIONALLY INFRINGE THE RIGHT TO SPEAK AND READ ANONYMOUSLY

The Internet hosts millions of dialogues covering topics "as diverse as human thought." *Reno v. ACLU*, 521 U.S. at 852. Importantly, many of these dialogues occur anonymously or pseudonymously, whether through e-mail, message boards, or World Wide Web sites. The government's attempt to save the CDA by speculating as to the possibility of self-identification methods would create another First Amendment violation – violation of the right to anonymous speech and reading.

A. The First Amendment protects the right to speak and read anonymously

It is well established that the First Amendment protects the right to participate anonymously in expressive activity.[4] The First Amendment guarantee of freedom of speech thus includes the right to speak anonymously; freedom of assembly encompasses the right to associate without giving a name; and the freedom to receive includes the right to listen, watch, and read privately.

The First Amendment right to speak anonymously has a long historical pedigree. "[A]n author's decision to remain anonymous, like other decisions concerning omissions or additions to the content of a publication, is an aspect of the freedom of speech protected by the First Amendment." *McIntyre v. Ohio Elections Comm'n*, 514 U.S. 334, 342 (1995) ("anonymous pamphleteering is not a pernicious, fraudulent practice, but an honorable tradition of advocacy and dissent") (invalidating ID requirement for persons distributing campaign literature).

This right to anonymity is more than just one form of protected speech; it is part

---

[4] The analytical basis for the right to speak anonymously is simple. "[T]he fundamental rule of protection under the First Amendment" is "that a speaker has the autonomy to choose the content of his own message." *Hurley v. Irish-American Gay, Lesbian and Bisexual Group of Boston*, 515 U.S. 557, 573 (1995). "Since all speech inherently involves choices of what to say and what to leave unsaid, one important manifestation of the principle of free speech is that one who chooses to speak may also decide what not to say." *Ibid.* (internal quotation marks and citations omitted).

of "our national heritage and tradition." *Watchtower Bible & Tract Soc'y of New York, Inc. v. Village of Stratton*, 536 U.S. 150, 166 (2002) (invalidating ID requirement for persons engaged in door-to-door religious advocacy); *see also Buckley v. American Constitutional Law Found.*, 525 U.S. 182, 199-200 (1999) (invalidating ID requirement for persons circulating petitions for state ballot initiatives).

The Supreme Court first documented the historical value of anonymity in *Talley v. California*, 362 U.S. 60 (1960):

> "Anonymous pamphlets, leaflets, brochures and even books have played an important role in the progress of mankind. Persecuted groups and sects from time to time throughout history have been able to criticize oppressive practices and laws either anonymously or not at all. . . . Even the Federalist Papers, written in favor of the adoption of our Constitution, were published under fictitious names. It is plain that anonymity has sometimes been assumed for the most constructive purposes."

Id. at 65

Protections for anonymous speech are vital to democratic discourse. Allowing dissenters to shield their identities frees them to express critical, minority views. "Anonymity is a shield from the tyranny of the majority. It thus exemplifies the purpose behind the Bill of Rights, and of the First Amendment in particular: to protect unpopular individuals from retaliation. at the hand of an intolerant society." *McIntyre*, 514 U.S. at 357 (citation omitted). Fears that their identity may be uncovered, and that they may be persecuted on account of their speech, may prevent minority speakers from speaking at all.

The constitutionally protected freedom of assembly depends upon the freedom to associate without being identified. *See NAACP v. Alabama*, 357 U.S. 449, 462 (1958) ("Inviolability of privacy in group association may in many circumstances be indispensable to preservation of freedom of association, particularly where a group espouses dissident beliefs."); *Gibson v. Fla. Legislative Investigation Comm.*, 372 U.S. 539, 558 (1963) (rejecting attempt of state legislative committee to require NAACP to produce membership records); *Shelton v. Tucker*, 364 U.S. 479, 490 (1960) (striking

down state statute requiring that teachers list all association memberships for the previous five years).

The right to receive speech anonymously is likewise protected. "It is now well established that the Constitution protects the right to receive information and ideas." *Stanley v. Georgia*, 394 U.S. 557, 564 (1969), *citing Martin v. City of Struthers*, 319 U.S. 141, 143 (1943) ("This freedom [of speech and press] necessarily protects the right to receive"); *Lamont*, 381 U.S. at 307-08 (Brennan, J., concurring).

Importantly, the most common argument for requiring speakers to disclose their identities is the supposed need to ensure accountability for speech-caused harms to others like defamation. *See, e.g., McIntyre*, 514 U.S. at 382-383 (Scalia, J., dissenting) (arguing that speaker identification requirements are desirable because they promote accountability for false and harmful statements). This concern simply does not apply for anonymous reading.

Fears of identification based on the speech one invites and receives can have chilling effects upon all parties to a correspondence. The Colorado Supreme Court recognized the importance of anonymous reading in a case involving bookstore purchase records. "The need to protect anonymity has particular applicability to book-buying activity," because "government inquiry and intrusion into the reading choices of bookstore customers will almost certainly chill their constitutionally protected rights." *Tattered Cover, Inc. v. City of Thornton*, 44 P.3d 1044, 1053 (Colo. Sup. Ct. 2002), quoting *United States v. Rumely*, 345 U.S. 41, 57 (1953) ("Once the government can demand of a publisher the names of the purchasers of the purchasers of his publications, the free press as we know it disappears.") (Douglas, J., concurring) (holding that statutory authority to investigate "lobbying activities" did not confer power to compel names of those who purchased political literature for subsequent distribution).

In the CDA context, these concerns are quite serious. Internet publishers operate the online equivalent of bookstores and libraries. Requiring visitors to plaintiff's website

to disclose their identities and locations not only discourages the timid but exposes the brave to identification by the government and intimidation or even prosecution.

B. Pseudonymity and anonymity are crucial aspects of the Internet

These long-standing rights to anonymity and privacy are critically important to a modem medium of expression, the Internet. The Supreme Court has recognized that the Internet offers a new and powerful democratic forum in which anyone can become a "pamphleteer" or "a town crier with a voice that resonates farther than it could from any soapbox." *Reno v. ACLU*, 521 U.S., at 870. Expansion of the Internet has created countless new opportunities for self-expression and discourse, ranging from the private diary to the multi-minion-reader broadcast. The medium hosts tens of millions of dialogues carried out via e-mail publications, Web publications, Usenet Newsgroup message boards, and more, as individuals and associations use the Internet to convey their opinions and ideas whenever they want and to whomever cares to read them.

Many of these millions of dialogues occur anonymously or pseudonymously. Most e-mail providers, including free Web-based services such as Yahoo! Mail and Hotmail, allow subscribers to create e-mail accounts using pseudonyms or to use pseudonymous e-mail addresses, such that subscribers can send messages or join newsletters without disclosing their real names. Subscribers who post to newsgroups hosted on Usenet servers, as well as other message board services such as Yahoo! Groups, are identified only by e-mail address, which again may be pseudonymous.

Similarly, hosts of online diaries and journals known as "Weblogs" or "blogs," such as LiveJournal.com and Blogger.com, allow subscribers to publish their blogs pseudonymously, and readers of these weblogs may join the discussion by posting anonymous comments. The widespread anonymity and pseudonymity on the Internet is crucial to its value as an expressive medium. *Doe v. 2TheMart.com*, 140 F.Supp.2d 1088, 1092 (W.D.Wash. 2001 ("The right to speak anonymously extends to speech via the Internet."); *Columbia Ins. Co. v. Seescandy.com*, 185 F.R.D. 573, 578 (N.D.Cal. 1999)

(there is a "legitimate and valuable right to participate in online forums anonymously and pseudonymously").

The *Reno* Court found that there is "no basis for qualifying the level of First Amendment scrutiny that should be applied to" the Internet. *Reno v. ACLU*, 521 U.S. at 870. It follows that there is no basis for qualifying the level of scrutiny that should be applied to restrictions on anonymous online speech. Laws that impair online privacy and anonymity of speech should face the full scrutiny required by the First Amendment offline. *See Doe v. Ashcroft*, F.Supp.2d , 2004 WL 2185571 (S.D.N.Y. Sept. 28, 2004) (holding unconstitutional "national security letters" seeking Internet users' identity information issued under 18 U.S.C. § 2709) ("Considering, as is undisputed here, the importance of the internet as a forum for speech and association, the Court rejects the invitation to permit the rights of internet anonymity and association to be placed at such grave risk.").

C. As a practical matter, any such scheme would be unworkable

Finally, any such scheme is likely to be unworkable and surely less effective than a filtering regime.[5] The Supreme Court's analysis of filters and COPA in *Ashcroft v. ACLU* is instructive. The Supreme Court found that "[f]ilters may well be more effective than COPA" for several reasons. *Ashcroft v. ACLU*, 124 S.Ct. at 2792.

First, while source restrictions like COPA and CDA will only affect access to content provided by domestic online providers, filters can apply to foreign as well as domestic content. *Ibid.* ("That alone makes it possible that filtering software might be more effective in serving Congress' goals."). The Supreme Court even noted that COPA's effectiveness "is likely to diminish even further if COPA is upheld," because online providers of HTM content "simply can move their operations overseas." *Ibid.*

Second, the Supreme Court approvingly cited the lower court's finding that

[5] Amicus emphasizes that it does not endorse filtering or blocking software, and only analyzes such technology in order to rebut the government's arguments in this case.

"verification systems may be subject to evasion and circumvention, for example by minors who have their own credit cards." *Ibid.* (citations omitted). Indeed, the Supreme Court noted that "a Government Commission appointed to consider the question" of COPA's effectiveness "unambiguously found that filters are more effective than age-verification requirements." *Id.*, at 2792-93.[6]

The analysis in *Ashcroft v. ACLU* applies strongly to the CDA's obscenity provisions, which are unlikely to be any more effective than COPA's HTM provisions with respect to foreign materials. For instance, the lower court had found that "40% of harmful-to-minors content comes from overseas." *Id.*, at 2792 (citing *ACLU v. Reno*, 31 F.Supp.2d 473, 484 (E.D. Pa. 1999)). While amicus cannot say that 40 percent of obscene content has a foreign source, there is no reason to believe that the percentage of foreign obscene content is not in the same range as the percentage of foreign HTM content.

Furthermore, none of the government's suggested improvements is likely to be workable. The CDA's credit card/age verification defenses were previously found to be infeasible for most noncommercial online publishers and of unproven effectiveness even for commercial publishers. *Reno v. ACLU*, 521 U.S. at 881; *see ACLU v. Ashcroft*, 322 F.3d 240, 244 (3d Cir. 2003), *aff'd*, *Ashcroft v. ACLU*, 124 S.Ct. 2783 (2004).

Mr. McCulloh's suggestion of a "location-verification" scheme fares no better than these rejected defenses. As noted above, Mr. McCulloh's expert report suggests that plaintiff Nitke could "implement a registration system akin to that of *The New York Times*," which would "require visitors to the site to fill out a form and complete a member agreement before being given access to certain parts of the site." McCulloh Declaration, at 8; see Trial Transcript (Oct. 28, 2004), at 236-240.

The problem with this scheme, of course, is that plaintiff would have no obvious

---

[6] A third reason for the superior effectiveness of blocking programs was that "they can be applied to all forms of Internet communication, including e-mail, not just communications available via the World Wide Web." *Ashcroft v. ACLU*, 124 S.Ct. at 2792.

way to verify any of the personal information submitted. Trial Transcript (Oct. 28, 2004), at 236 ("There would be no way to verify"). Such a scheme might be acceptable for a publisher who relies on such information for marketing purposes, but publishers like plaintiff would risk criminal prosecution if a visitor falsely represented his or her geographic location. The situations are not comparable.

Mr. McCulloh also suggested manual verification systems. One version would require users to "submit a hard copy of proof of identity, for example a photocopy of a driver's license." McCulloh Decl., at 9. "Ms. Nitke could implement something similar by having users print out and mail in a form." *Ibid.* Alternatively, plaintiff could defer her decision to permit access to controversial content until "the user has submitted information via the postal service"; the advantage of this scheme, according to Mr. McCulloh, is that "unlike the Internet, mail that travels through the postal service has a definitive point of origin." *Ibid.*

The flaws of such a manual verification scheme are obvious. First, a person who wanted to fake his true geographic location could simply mail his or her form from a different place. Such "evasion and circumvention" would seem as likely as minors' use of credit cards. Second, even absent circumvention there is no obvious way to ascertain the community standards associated with any particular place. Mr. McCulloh apparently suggested in his trial testimony that online content providers could check against some master list to determine whether a given community was "liberal" or "conservative." Amicus knows of no such authoritative "master list' of liberal and conservative communities. Given these problems, the probable effect of the CDA is to chill protected speech.

///

///

V. CONCLUSION

The CDA is unconstitutionally overbroad, and the government's speculative suggestions of visitor- and location-identification schemes will not cure that overbreadth; indeed, such identification schemes unconstitutionally abridge the right to read anonymously

Dated: November 9, 2004
San Francisco, California

Respectfully submitted,

Lee Tien (LT 3060)
Attorney for Amicus Curiae
Electronic Frontier Foundation
454 Shotwell Street
San Francisco, California 94110
(415) 436-9333 x 102

PROOF OF SERVICE BY MAIL

I, the undersigned, am over 18 years of age and not a party to this action. On the date indicated below, I served the foregoing Brief *Amicus Curiae* of Electronic Frontier Foundation in Support of Plaintiff on all parties to this action by mailing a true copy thereof to the following addresses:

David Kelly, Esq.
United States Attorney
Andrew W. Schilling
Assistant United States Attorney
100 Church Street, 19th Floor
New York, NY 10007

John F. Wirenius, Esq.
Office of General Counsel
N.Y. State United Teachers
52 Broadway, 9th Floor
New York, NY 10004

Dated: November 9, 2004
San Francisco, California

Barak Weinstein
Legal Assistant
Electronic Frontier Foundation
454 Shotwell Street
San Francisco, California 94110
(415) 436-9333