No. 02-361

IN THE

Supreme Court of the United States

UNITED STATES OF AMERICA, *et al.*,
Appellants,

v.

AMERICAN LIBRARY ASSOCIATION, INC., *et al.*
Appellees.

On Appeal from the United States District Court for the Eastern District of Pennsylvania

BRIEF OF *AMICI CURIAE* ONLINE POLICY GROUP, INC. AND SETH FINKELSTEIN IN SUPPORT OF APPELLEES

DANIEL H. BROMBERG
(*Counsel of Record*)
CHARLES R.A. MORSE
JOSHUA A.T. FAIRFIELD
JONES DAY
51 Louisiana Ave., N.W.
Washington, D.C. 20001
(202) 879-3939

Counsel for Amici Curiae

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page

Cases

Statutes and Legislative Materials

TABLE OF AUTHORITIES
(continued)

Miscellaneous

TABLE OF AUTHORITIES
(continued)

Page

STATEMENT OF INTEREST[1]

The Online Policy Group, Inc. ("OPG") is a nonprofit organization dedicated to online policy research, outreach, and action. OPG is concerned with the privacy, safety, and civil liberties of Internet participants, as well as the uneven distribution of Internet resources along social, ethnic, racial, and economic lines. OPG works to end this "digital divide" by providing free Internet services to nonprofit organizations and individuals who are underrepresented, underserved, or facing unfair bias, discrimination, or defamation. Both of the funding programs at issue in this case, "E-rate" discounts under the Telecommunications Act of 1996, *see* 47 U.S.C. § 254, and direct grants under the Library Services and Technology Act, *see* 20 U.S.C. §§ 9133-34, 9141, are essential to ending the digital divide because they help public libraries make the Internet available to people with no other means of access. OPG is therefore critically concerned with whether public libraries will be able to continue providing these services without infringing upon the civil liberties of Internet participants.

Seth Finkelstein is a computer programmer and civil liberties advocate. Since 1995, he has dedicated thousands of hours to studying commercially developed Internet blocking software. These efforts have revealed many of the mechanisms employed by blocking software, which Mr. Finkelstein has described in articles and reports.[2] For his

---

[1] Counsel for all parties have consented to the filing of this brief, and *amici* have filed those consents with the Clerk of the Court. No counsel for a party in this case authored this brief in whole or in part, and no person or entity, other than the undersigned *amici* and their counsel, has made a monetary contribution to this brief's preparation and submission.

[2] *See, e.g.,* Seth Finkelstein, *BESS's Secret LOOPHOLE*, *at* http://sethf.com/anticensorware/bess/loophole.php; Seth Finkelstein, *BESS vs. The Google Search Engine (Cache, Groups, Images)*, *at*

efforts "in the fight against government mandated use" of such software, Mr. Finkelstein received the Electronic Frontier Foundation's Pioneer Award. Mr. Finkelstein is interested in ensuring that the Court understands how commercially developed blocking software operates and the dangers that it poses to free speech.

INTRODUCTION AND SUMMARY OF ARGUMENT

In the decision below, the panel held that libraries create a designated public forum when they provide Internet access to the public and that any content-based restrictions upon that access, such as CIPA's blocking provisions, are therefore subject to strict scrutiny. *See Am. Library Ass'n v. United States*, 201 F. Supp. 2d 401, 454-70 (E.D. Pa. 2002) ("*ALA*"). Although *amici* agree with this analysis, they believe that there is a more straightforward reason why CIPA's blocking provisions are subject to strict scrutiny.

The Children's Internet Protection Act ("CIPA"), Pub. L. No. 106-554, Div. B., Title XVII, 114 Stat. 2763A-335 (2000), requires libraries participating in certain federal funding programs to block Internet access to visual depictions that are obscene, child pornography, or (in some circumstances) harmful to minors through a particular method: the use of a "technology protection measure." *Id*. § 1712 (codified at 20 U.S.C. § 9134(f)(1)); *id*. § 1721 (codified at 47 U.S.C. § 254(h)(6)). Although the Act defines the term "technology protection measure," *id*.

---

http://sethf.com/anticensorware/bess/google.php; Seth Finkelstein & Lee Tien, *Blacklisting Bytes*, *at* http: //www.eff.org/Censorship/Censorware/20010306_eff_nrc_paper1.html; Seth Finkelstein, *The Pre-Slipped Slope—Censorware vs. the Wayback Machine Web Archive*, *at* http://sethf.com/anticensorware/general/slip.php; Seth Finkelstein, *Smartfilter's Greatest Evils*, *at* http://sethf.com/anticensorware/smartfilter/greatestevils.php.

§ 1703, it offers no guidance on how such measures should distinguish between the low-value speech banned by CIPA and other speech on the Internet that is entitled to full First Amendment protection. Instead, CIPA simply defines a "technology protection measure" as a "specific technology that blocks or filters Internet access." *Id*. This blind faith in technology is badly—and dangerously—misplaced.

Because libraries lack the technological capability to block the Internet in any narrowly tailored fashion, CIPA's "technology protection measure" requirement effectively forces them to use commercial blocking software. Commercial blocking software is, however, ill-suited to the requirements of the First Amendment. First, the current market does not offer products designed to filter out only the low-value speech barred by CIPA. As a consequence, the blocking software currently available on the market purposefully blocks far broader categories that include protected speech. Second, companies that produce blocking software have little incentive to tailor their products narrowly. To the contrary, because underblocking, not overblocking, generates complaints, these companies have strong economic incentives to design their software to block in an overbroad fashion. Third, commercial blocking software companies can, and in some instances do, use criteria that systematically discriminate against certain viewpoints. As a consequence, CIPA's "technology protection measure" requirement forces libraries to regulate speech in manner that is systematically overbroad and that can involve viewpoint discrimination. Whether or not libraries create a designated public forum when they provide access to the Internet, the use of such an inherently suspect method of regulating speech should be subject to strict scrutiny.

ARGUMENT

CIPA'S "TECHNOLOGY PROTECTION MEASURE" REQUIREMENT SHOULD BE SUBJECT TO STRICT SCRUTINY BECAUSE IT REGULATES SPEECH IN A SUSPECT MANNER

A. CIPA Forces Libraries to Regulate Speech Through Commercial Blocking Software

To comply with CIPA, libraries that wish to provide their patrons with broad access to the Internet are forced, as a practical matter, to rely upon commercial blocking software. The Internet is massive. In 1997, it consisted of approximately 9.4 million host computers used by over 40 million people. *See Reno v. Am. Civil Liberties Union*, 521 U.S. 844, 850 (1997). As of September 2001, the number of people using the Internet had expanded tenfold to at least 400 million, including approximately 143 million in the United States alone. *See ALA*, 201 F. Supp. 2d at 416. Moreover, by that time, the rapidly expanding Internet had over 11 million unique "web" sites with more than two billion web pages reachable through ordinary search engines. *See id*. at 418-19. Libraries do not have the technological capacity or expertise to write software that can filter through such a vast store of information and determine which sites contain visual depictions that are obscene, child pornography, or harmful to minors. As a consequence, libraries that are not content to provide their patrons with access to only a small number of pre-screened sites are generally forced to rely upon commercially developed blocking software, also sometimes known as "censorware," to comply with CIPA's "technology protection measure" requirement.

Although the Government correctly points out that commercial blocking software permits users to "unblock" specific sites, Gov't Br. at 4, libraries in fact have little ability to customize blocking software. Blocking software

typically prohibits Internet users from accessing any domain name or Internet Protocol address that is contained on "control lists" compiled by the software's vendor. *See ALA*, 201 F. Supp. 2d at 428. Software companies do not, however, reveal how these control lists are compiled. To the contrary, the companies treat the heuristics and other methods they use as well as the lists of sites that those methods generate as proprietary information, which they do not reveal to libraries and other consumers. *See id*. at 430; *see also* 17 U.S.C. § 1201(a)(1)(A) (making it illegal to circumvent measures protecting software). Moreover, while users can unblock particular sites, *see ALA*, 201 F. Supp. 2d at 429, it is impossible for a user to personalize blocking software in any significant manner because the control lists compiled by blocking companies typically contain hundreds of thousands of sites, and the Internet is ever-expanding. *See Youth, Pornography, and the Internet* 286 (Dick Thornburgh & Herbert S. Lin eds., 2002) (noting that "detailed editorial control on a site-by-site basis for all sites in the vendor's database is not possible in practice"). Thus, libraries that purchase blocking software effectively cede to their software vendors the decision about which sites to block. *See* Lawrence Lessig, *What Things Regulate Speech: CDA 2.0 vs. Filtering*, 38 Jurimetrics J. 629, 657 (1998).

B. Commercial Blocking Software Regulates Speech in a Systematically Overbroad Fashion and Creates a Significant Danger of Viewpoint Discrimination.

The abdication of decision-making responsibility to the creators of commercial blocking software required by CIPA poses great danger of unnecessary suppression of speech and viewpoint discrimination.

1. Commercial Blocking Software Purposefully Blocks Protected Speech

Commercial blocking software typically permits consumers to block several dozen categories of Internet

content. *See ALA*, 201 F. Supp. 2d at 429-30. There is, however, "no category definition used by filtering software companies [that] is identical to CIPA's definitions of visual depictions that are obscene, child pornography, or harmful to minors." *Id*. at 429. Indeed, commercial blocking software does not even offer categories limited to obscenity, child pornography, or visual depictions that are harmful to minors. The closest approximations are categories such as "Adult Material," "Adults Only," "Adult/Sexually Explicit," "Extreme/Obscene/Violence," "Pornography," "Sex," "Kids' Sites," "For Kids," "Illegal/Questionable," "Tasteless," and "Tasteless/Gross." *Id*. at 429-30.

This omission is not surprising. Commercial blocking software is not designed to comply with governmental obligations under the First Amendment. Like any commercial product, blocking software is designed to satisfy the market's primary customers, which in the case of blocking software are parents who want to protect their children from all sexually explicit material, businesses that want to keep their employees focused on work and maintain a hospitable atmosphere in the office, and religious groups that want to spare their members exposure to material that offends their values. For example, one blocking-software company provides services to several religious Internet service providers and web sites, such as Christianity.com, Christian.net, and Crosswalk.com. *See* Nancy Willard, *Filtering Software: The Religious Connection* (2002), *at* http://www.ntia.doc.gov/ntiahome/ntiageneral/cipacomments/pre/willard/FSRCreport.htm. Another company provides blocking services to 711.net/Global Internet Ministries, Christian Purity, and What Would Jesus View. *See id.* And a third company offers a product that the American Family Association has repackaged as the "American Family Filter" and described as "built on the Christian princip[le] of holiness." *Id.* (quoting http://www.afafilter.com/about.asp).

2. Commercial Blocking Software Is Inherently Overbroad

Blocking-software vendors have an economic incentive to err on the side of overblocking. When a consumer is improperly denied access to a web site by blocking software, he is unlikely to know that he has been denied access to anything of value and therefore is unlikely to become upset. By contrast, when a sexually graphic image appears on the screen of a consumer who has attempted to block such material, there is a good chance that the consumer will become incensed and complain to his blocking-software vendor. *Cf. Youth, Pornography, and the Internet, supra*, at 287 (noting that libraries "tend to receive many more complaints from parents and the community about sites that are not filtered (i.e., complaints about underblocking) than about sites that are filtered improperly (i.e., complaints about overblocking)"). As a consequence, companies offering blocking software have a natural "desire to 'err on the side of caution' by screening out material that might be offensive to some customers." *ALA*, 201 F. Supp. 2d at 433; *see also Youth, Pornography, and the Internet, supra*, at 287 (noting that blocking software companies "have many incentives to err on the side of overblocking and few to err on the side of underblocking"); Nancy Willard, *supra* ("Filtering companies generally perceive the risks of failing to block access to inappropriate material as more significant than the risks of blocking access to appropriate material.").[3]

---

[3] This tendency to err on the side of overblocking may explain why some software vendors block access to so-called "loophole" sites. Loophole sites include archives of Internet content such as the Internet Archive, a digital library of the Internet containing a historical collection of web pages, *see* http://www.archive.org, and the "caches" of web pages indexed by Google's popular search engine. Because web sites are constantly changing their content and being removed from their original Internet addresses, *see ALA*, 201 F. Supp. 2d at 419, such loophole sites are often the only source for older materials. But

In addition, as this Court has recognized before, institutions regularly engaged in suppressing speech tend to develop a bias in favor of suppression. When a "framework creates an agency or establishes an official charged particularly with reviewing speech," it "breed[s] an 'expertise' tending to favor censorship over speech." *City of Lakewood v. Plain Dealer Publ'g Co.*, 486 U.S. 750, 760 (1988); *see also Freedman v. Maryland*, 380 U.S. 51, 57-58 (1965) ("Because the censor's business is to censor, there inheres the danger that he may well be less responsive than a court—part of an independent branch of government—to the constitutionally protected interests in free expression."). For this reason as well, commercially developed blocking software has an inherent tendency to block more speech than necessary.

3. Commercial Blocking Software May Facilitate Viewpoint Discrimination

There is also reason to fear that commercially developed blocking software will systematically discriminate against certain viewpoints. Although the heuristics employed by blocking software are generally unknown, *amici* are aware of one product that used the presence of words such as "lesbian," "gay," and "homosexual" in identifying sites dealing with sexuality. That product assigned points to particular words or phrases based on the inherent offensiveness of the word and its context. It treated the words "lesbian" and "homosexual" as inherently offensive, and for each appearance of those words a web page received

---

loophole sites assign new Uniform Resource Locators ("URLs") to the content they contain, and therefore represent a potential way around a blocking product's list of prohibited sites. *See ALA*, 201 F. Supp. 2d at 434-35. To combat this problem, some vendors simply block access to the loophole sites, thereby suppressing a massive amount of unobjectionable and constitutionally protected content.

five points; sites accumulating 50 points were normally blocked. Words like "lesbian" and "homosexual," however, are likely to appear dozens of times in sites that discuss social and political issues of concern to the lesbian and gay communities, but have little to do with sexuality, much less obscenity and pornography. Thus, under the heuristics employed by this company, core political speech could be blocked by a category that a library might use to comply with CIPA.

Moreover, there is evidence that other blocking software routinely denies access to gay and lesbian sites that contain core political speech. To take an example, N2H2, seller of a popular blocking product called Bess, has blocked a number of sites having to do with gay and lesbian issues under the category "Sex." These include sites dedicated to the problem of harassment of gays (http://www.inform.umd.edu / EdRes / Topic / Diversity / Specific/ Sexual_Orientation / Reading/News/harassment); gay relationships (http://content. gay.com/channels/relationships); and the "Queer as Folk" television show (http: //www.sho.com/queer). By discriminating in this manner against certain viewpoints, the secret criteria used in blocking software "may result in hidden censorship." H.R. Rep. No. 105-775, at 19-20 (1998).

Nor is the risk of viewpoint discrimination confined to the software companies. There is also a danger that libraries could use the "technology protection measure" requirement as cover for viewpoint discrimination. Because CIPA does not place any limits on what type of blocking software a library may use, a librarian who was somehow aware of a systematic bias in a given blocking product could select software that discriminates against certain viewpoints based upon his or her own private agenda. Moreover, because the blocking software companies do not disclose the criteria that they use, the public would have little way of learning what had been done. Thus, commercial blocking software creates

the danger of purposeful as well as unwitting viewpoint discrimination by libraries.

C. As a Suspect Method of Regulating Speech, CIPA's "Technology Protection Measure" Requirement Should Be Subject to Strict Scrutiny

This Court has long recognized that certain methods of regulating speech pose a special danger to free speech and should therefore be subject to special scrutiny. Congress's attempt in CIPA to regulate speech by effectively forcing libraries to use technology produced by the market poses a similar danger and should therefore be subject to strict scrutiny.

Few propositions are more deeply ingrained in constitutional law than the proposition that one particularly dangerous method of regulating speech—prior restraint—is subject to special scrutiny. *See, e.g.*, *Neb. Press Ass'n v. Stuart*, 427 U.S. 539, 561 (1976) ("[I]t is . . . clear that the barriers to prior restraint remain high unless we are to abandon what the Court has said for nearly a quarter of our national existence and implied throughout all of it."); *Near v. Minnesota*, 283 U.S. 697, 713-18 (1931) (describing the "deep-seated conviction that such restraints" are generally unconstitutional). As this Court has explained, a state is "not free to adopt whatever procedures it pleases for dealing with obscenity" because "[t]he administration of a censorship system . . . presents peculiar dangers to constitutionally protected speech." *Freedman*, 380 U.S. at 57 (quotation omitted). *See generally* Thomas I. Emerson, *The Doctrine of Prior Restraint*, 20 Law & Contemp. Probs. 648 (1955). It is therefore well settled that "[a]ny system of prior restraints of expression comes to this Court bearing a heavy presumption against its constitutional validity." *Bantam Books, Inc. v. Sullivan*, 372 U.S. 58, 70 (1963).

For example, licensing provisions that require prior approval of speech have long been recognized as "prior

restraint[s] on speech" and are therefore subject to careful scrutiny, particularly where specific standards are lacking to guide the official doing the licensing. *Forsyth County v. Nationalist Movement*, 505 U.S. 123, 130-31 (1992); *see also City of Lakewood*, 486 U.S. at 763 (noting that the danger of "content and viewpoint censorship . . . is at its zenith when the determination of who may speak and who may not is left to the unbridled discretion of a government official"). This Court has also considered other forms of regulation permitting public officials to review speech prior to its distribution to the public to be forms of censorship that should be treated as prior restraints and subjected to special scrutiny. *See, e.g.*, *United States v. Thirty-Seven Photographs*, 402 U.S. 363, 367-75 (1971) (treating seizure of allegedly obscene photographs as a prior restraint); *Blount v. Rizzi*, 400 U.S. 410, 416-17 (1971) (postal regulations allowing the Postmaster General to halt use of mails for obscene material). Moreover, in so doing, the Court has looked to the real-world effects of regulatory schemes to determine whether they act, as a practical matter, as prior restraints. *See Bantam Books*, 372 U.S. at 59-61, 70 (finding that obscenity-review commission "in fact . . . subject[ed] the distribution of publications to a system of prior administrative restraints"); *Near*, 283 U.S. at 712 (finding that abatement of newspapers publishing obscene or scandalous material as nuisances "operates . . . to put the publisher under an effective censorship).

CIPA's requirement that libraries wishing to make broad Internet access available to their patrons employ a commercially developed "technology protection measure" poses at least as great a risk of "freewheeling censorship," *Southeastern Promotions, Ltd. v. Conrad*, 420 U.S. 546, 559 (1975), as previously recognized prior restraints. Like pre-publication censorship, blocking software reviews speech for its propriety, and like the local officials granted licensing authority in *City of Lakewood* and *Forsyth County*, the developers of blocking software enjoy unfettered discretion

to select speech for suppression. Indeed, commercial blocking software is even more troubling because it effectively delegates censorship decisions to private individuals, who, unlike mayors, police officers, censor boards, and other public officials entrusted with issuing licenses, have no obligation to uphold the Constitution or narrowly tailor their censorship to comply with the First Amendment. To the contrary, as demonstrated above, blocking-software vendors may have powerful economic incentives to err on the side of suppressing more speech rather than less. *See supra* p. 7; *see also* Bernard W. Bell, *Filth, Filtering, and the First Amendment: Ruminations on Public Libraries' Use of Internet Filtering Software*, 53 Fed. Comm. L.J. 191, 236 (2001) ("The kinds of political constraints that cabin public officials' actions do not similarly constrain actions by private entities."). The efforts of private software developers therefore deserve none of the deference traditionally due the efforts of the legislature or other public officials. *Cf. Reno*, 521 U.S. at 876 (stressing "that *Congress* has designed its statute to accomplish its purpose 'without imposing an unnecessarily great restriction on speech'" (emphasis added) (quoting *Denver Area Telecommunications Consortium, Inc. v. FCC*, 518 U.S. 727, 741 (1996))). Moreover, unlike licensing schemes that provide for judicial review of decisions to block speech, *see, e.g.*, *Freedman*, 380 U.S. at 59-60, the use of blocking software proceeds without any "judicial determination." *ALA*, 201 F. Supp. 2d at 429. Thus, if any technique for regulating speech deserves judicial suspicion, it is CIPA's "technology protection measure."

The Government argues that strict scrutiny would be "incompatible with the discretion that public libraries must have to fulfill their traditional missions." Gov't Brief at 11. A library does not, however, exercise its traditional discretion to select the library's offerings when it adopts a "technology protection measure." *See* Frederick Schauer, *The Supreme Court 1997 Term—Comment: Principles,*

Institutions, and the First Amendment, 112 Harv. L. Rev. 84, 115 (1998). Indeed, because librarians normally have little way of knowing how commercially developed blocking software works, *see supra* p. 5, they do not exercise any meaningful discretion in implementing CIPA's mandate. Instead, those librarians who wish to give their patrons broad Internet access while still complying with CIPA are forced to purchase blocking software from commercial vendors, who exercise discretion unfettered by the professional standards of librarians or their commitment to free speech. Thus, far from showing that a lax standard of review is appropriate, the Government's focus on the "traditional missions" of librarians underscores the need for searching review of CIPA's "technology protection measure" requirement.

CONCLUSION

Whether or not this Court finds that libraries create a public forum by offering public access to the Internet, CIPA's "technology protection measure" should be subject to strict scrutiny.

Respectfully submitted,

DANIEL H. BROMBERG
(*Counsel of Record*)
CHARLES R.A. MORSE
JOSHUA A.T. FAIRFIELD
JONES DAY
51 Louisiana Avenue, N.W.
Washington, DC 20001
(202) 879-3939

Counsel for Amici Curiae

February 2003