IN THE UNITED STATES DISTRICT COURT

FOR THE EASTERN DISTRICT OF PENNSYLVANIA

AMERICAN LIBRARY ASSOCIATION, INC., et al.	:	CIVIL ACTION
v.	:	
UNITED STATES, et al.	:	NO. 01-1303
MULTNOMAH COUNTY PUBLIC LIBRARY, et al.	:	CIVIL ACTION
v.	:	
UNITED STATES OF AMERICA, et al.	:	NO. 01-1322

Before: BECKER, Chief Circuit Judge,
FULLAM and BARTLE, District Judges.

OPINION OF THE COURT

May 31, 2002

Becker, Chief Circuit Judge

I. Preliminary Statement

This case challenges an act of Congress that makes the use of filtering software by public libraries a condition of the receipt of federal funding. The Internet, as is well known, is a vast, interactive medium based on a decentralized network of computers around the world. Its most familiar feature is the World Wide Web (the "Web"), a network of computers known as servers that provide content to users. The Internet provides easy access to anyone who wishes to provide or distribute information to a worldwide audience; it is used by more than 143 million Americans. Indeed, much of the world's knowledge accumulated over centuries is available to Internet users almost instantly. Approximately 10% of the Americans who use the Internet access it at public libraries. And approximately 95% of all public libraries in the United States provide public access to the Internet.

While the beneficial effect of the Internet in expanding the amount of information available to its users is self-evident, its low entry barriers have also led to a perverse result – facilitation of the widespread dissemination of hardcore pornography within the easy reach not only of adults who have every right to access it (so long as it is not legally obscene or child pornography), but also of children and adolescents to whom it may be quite harmful. The volume of pornography on the Internet is huge, and the record before us demonstrates that public library patrons of all ages, many from ages 11 to 15, have regularly sought to access it in public library settings. There are more than 100,000 pornographic Web sites that can be accessed for free and without providing any registration information, and tens of thousands of Web sites contain child pornography.

Libraries have reacted to this situation by utilizing a number of means designed to insure that patrons avoid illegal (and unwanted) content while also enabling patrons to find the content they desire. Some libraries have trained patrons in how to use the Internet while avoiding illegal content, or have directed their patrons to "preferred" Web sites that librarians have reviewed. Other libraries have utilized such devices as recessing the computer monitors, installing privacy screens, and monitoring implemented by a "tap on the shoulder" of patrons perceived to be offending library policy. Still others, viewing the foregoing approaches as inadequate or uncomfortable (some librarians do not wish to confront patrons), have purchased commercially available software that blocks certain categories of material deemed by the library board as unsuitable for use in their facilities. Indeed, 7% of American public libraries use blocking software for adults. Although such programs are somewhat effective in blocking large quantities of pornography, they are blunt instruments that not only "underblock," i.e., fail to block access to substantial amounts of content that the library boards wish to exclude, but also, central to this litigation, "overblock," i.e., block access to large quantities of material that library boards do not wish to exclude and that is constitutionally protected.

Most of the libraries that use filtering software seek to block sexually explicit speech. While most libraries include in their physical collection copies of volumes such as *The Joy of Sex* and *The Joy of Gay Sex*, which contain quite explicit photographs and descriptions, filtering software blocks large quantities of other, comparable information about health and sexuality that adults and teenagers seek on the Web. One teenager

testified that the Internet access in a public library was the only venue in which she could obtain information important to her about her own sexuality. Another library patron witness described using the Internet to research breast cancer and reconstructive surgery for his mother who had breast surgery. Even though some filtering programs contain exceptions for health and education, the exceptions do not solve the problem of overblocking constitutionally protected material. Moreover, as we explain below, the filtering software on which the parties presented evidence in this case overblocks not only information relating to health and sexuality that might be mistaken for pornography or erotica, but also vast numbers of Web pages and sites that could not even arguably be construed as harmful or inappropriate for adults or minors.

The Congress, sharing the concerns of many library boards, enacted the Children's Internet Protection Act ("CIPA"), Pub. L. No. 106-554, which makes the use of filters by a public library a condition of its receipt of two kinds of subsidies that are important (or even critical) to the budgets of many public libraries – grants under the Library Services and Technology Act, 20 U.S.C. § 9101 *et seq.* ("LSTA"), and so-called "E-rate discounts" for Internet access and support under the Telecommunications Act, 47 U.S.C. § 254. LSTA grant funds are awarded, *inter alia*, in order to: (1) assist libraries in accessing information through electronic networks, and (2) provide targeted library and information services to persons having difficulty using a library and to underserved and rural communities, including children from families with incomes below the poverty line. E-rate discounts serve the similar purpose of extending Internet access to schools and libraries in low-

income communities. CIPA requires that libraries, in order to receive LSTA funds or E-rate discounts, certify that they are using a "technology protection measure" that prevents patrons from accessing "visual depictions" that are "obscene," "child pornography," or in the case of minors, "harmful to minors." 20 U.S.C. § 9134(f)(1)(A) (LSTA); 47 U.S.C. § 254(h)(6)(B) & (C) (E-rate).

The plaintiffs, a group of libraries, library associations, library patrons, and Web site publishers, brought this suit against the United States and others alleging that CIPA is facially unconstitutional because: (1) it induces public libraries to violate their patrons' First Amendment rights contrary to the requirements of *South Dakota v. Dole*, 483 U.S. 203 (1987); and (2) it requires libraries to relinquish their First Amendment rights as a condition on the receipt of federal funds and is therefore impermissible under the doctrine of unconstitutional conditions. In arguing that CIPA will induce public libraries to violate the First Amendment, the plaintiffs contend that given the limits of the filtering technology, CIPA's conditions effectively require libraries to impose content-based restrictions on their patrons' access to constitutionally protected speech. According to the plaintiffs, these content-based restrictions are subject to strict scrutiny under public forum doctrine, *see Rosenberger v. Rector & Visitors of Univ. of Va.*, 515 U.S. 819, 837 (1995), and are therefore permissible only if they are narrowly tailored to further a compelling state interest and no less restrictive alternatives would further that interest, *see Reno v. ACLU*,

521 U.S. 844, 874 (1997).[1] The government responds that CIPA will not induce public libraries to violate the First Amendment, since it is possible for at least some public libraries to constitutionally comply with CIPA's conditions. Even if some libraries' use of filters might violate the First Amendment, the government submits that CIPA can be facially invalidated only if it is impossible for any public library to comply with its conditions without violating the First Amendment.

Pursuant to CIPA, a three-judge Court was convened to try the issues. Pub. L. No. 106-554. Following an intensive period of discovery on an expedited schedule to allow public libraries to know whether they need to certify compliance with CIPA by July 1, 2002, to receive subsidies for the upcoming year, the Court conducted an eight-day trial at which we heard 20 witnesses, and received numerous depositions, stipulations and documents. The principal focus of the trial was on the capacity of currently available filtering software. The plaintiffs adduced substantial evidence not only that filtering programs bar access to a substantial amount of speech on the Internet that is clearly

---

[1] Plaintiffs advance three other alternative, independent grounds for holding CIPA facially invalid. First, they submit that even if CIPA will not induce public libraries to violate the First Amendment, CIPA nonetheless imposes an unconstitutional condition on public libraries by requiring them to relinquish their own First Amendment rights to provide unfiltered Internet access as a condition on their receipt of federal funds. *See infra* n.36. Second, plaintiffs contend that CIPA is facially invalid because it effects an impermissible prior restraint on speech by granting filtering companies and library staff unfettered discretion to suppress speech before it has been received by library patrons and before it has been subject to a judicial determination that it is unprotected under the First Amendment. *See Southeastern Promotions, Ltd. v. Conrad*, 420 U.S. 546, 558 (1975). Finally, plaintiffs submit that CIPA is unconstitutionally vague. *See City of Chicago v. Morales*, 527 U.S. 41 (1999).

constitutionally protected for adults and minors, but also that these programs are intrinsically unable to block only illegal Internet content while simultaneously allowing access to all protected speech.

As our extensive findings of fact reflect, the plaintiffs demonstrated that thousands of Web pages containing protected speech are wrongly blocked by the four leading filtering programs, and these pages represent only a fraction of Web pages wrongly blocked by the programs. The plaintiffs' evidence explained that the problems faced by the manufacturers and vendors of filtering software are legion. The Web is extremely dynamic, with an estimated 1.5 million new pages added every day and the contents of existing Web pages changing very rapidly. The category lists maintained by the blocking programs are considered to be proprietary information, and hence are unavailable to customers or the general public for review, so that public libraries that select categories when implementing filtering software do not really know what they are blocking.

There are many reasons why filtering software suffers from extensive over- and underblocking, which we will explain below in great detail. They center on the limitations on filtering companies' ability to: (1) accurately collect Web pages that potentially fall into a blocked category (e.g., pornography); (2) review and categorize Web pages that they have collected; and (3) engage in regular re-review of Web pages that they have previously reviewed. These failures spring from constraints on the technology of automated classification systems, and the limitations inherent in human review, including error, misjudgment, and scarce resources, which we describe in detail *infra* at 58-74. One failure

of critical importance is that the automated systems that filtering companies use to collect Web pages for classification are able to search only text, not images. This is crippling to filtering companies' ability to collect pages containing "visual depictions" that are obscene, child pornography, or harmful to minors, as CIPA requires. As will appear, we find that it is currently impossible, given the Internet's size, rate of growth, rate of change, and architecture, and given the state of the art of automated classification systems, to develop a filter that neither underblocks nor overblocks a substantial amount of speech.

The government, while acknowledging that the filtering software is imperfect, maintains that it is nonetheless quite effective, and that it successfully blocks the vast majority of the Web pages that meet filtering companies' category definitions (e.g., pornography). The government contends that no more is required. In its view, so long as the filtering software selected by the libraries screens out the bulk of the Web pages proscribed by CIPA, the libraries have made a reasonable choice which suffices, under the applicable legal principles, to pass constitutional muster in the context of a facial challenge. Central to the government's position is the analogy it advances between Internet filtering and the initial decision of a library to determine which materials to purchase for its print collection. Public libraries have finite budgets and must make choices as to whether to purchase, for example, books on gardening or books on golf. Such content-based decisions, even the plaintiffs concede, are subject to rational basis review and not a stricter form of First Amendment scrutiny. In the government's view, the fact that the Internet reverses the acquisition process and requires the libraries to, in effect, purchase

the entire Internet, some of which (e.g., hardcore pornography) it does not want, should not mean that it is chargeable with censorship when it filters out offending material.

The legal context in which this extensive factual record is set is complex, implicating a number of constitutional doctrines, including the constitutional limitations on Congress's spending clause power, the unconstitutional conditions doctrine, and subsidiary to these issues, the First Amendment doctrines of prior restraint, vagueness, and overbreadth. There are a number of potential entry points into the analysis, but the most logical is the spending clause jurisprudence in which the seminal case is *South Dakota v. Dole*, 483 U.S. 203 (1987). *Dole* outlines four categories of constraints on Congress's exercise of its power under the Spending Clause, but the only *Dole* condition disputed here is the fourth and last, i.e., whether CIPA requires libraries that receive LSTA funds or E-rate discounts to violate the constitutional rights of their patrons. As will appear, the question is not a simple one, and turns on the level of scrutiny applicable to a public library's content-based restrictions on patrons' Internet access. Whether such restrictions are subject to strict scrutiny, as plaintiffs contend, or only rational basis review, as the government contends, depends on public forum doctrine.

The government argues that, in providing Internet access, public libraries do not create a public forum, since public libraries may reserve the right to exclude certain speakers from availing themselves of the forum. Accordingly, the government contends that public libraries' restrictions on patrons' Internet access are subject only to rational basis review.

Plaintiffs respond that the government's ability to restrict speech on its own property, as in the case of restrictions on Internet access in public libraries, is not unlimited, and that the more widely the state facilitates the dissemination of private speech in a given forum, the more vulnerable the state's decision is to restrict access to speech in that forum. We agree with the plaintiffs that public libraries' content-based restrictions on their patrons' Internet access are subject to strict scrutiny. In providing even filtered Internet access, public libraries create a public forum open to any speaker around the world to communicate with library patrons via the Internet on a virtually unlimited number of topics. Where the state provides access to a "vast democratic forum[]," *Reno v. ACLU*, 521 U.S. 844, 868 (1997), open to any member of the public to speak on subjects "as diverse as human thought," *id.* at 870 (internal quotation marks and citation omitted), the state's decision selectively to exclude from the forum speech whose content the state disfavors is subject to strict scrutiny, as such exclusions risk distorting the marketplace of ideas that the state has facilitated. Application of strict scrutiny finds further support in the extent to which public libraries' provision of Internet access uniquely promotes First Amendment values in a manner analogous to traditional public fora such as streets, sidewalks, and parks, in which content-based restrictions are always subject to strict scrutiny.

Under strict scrutiny, a public library's use of filtering software is permissible only if it is narrowly tailored to further a compelling government interest and no less restrictive alternative would serve that interest. We acknowledge that use of filtering software furthers public libraries' legitimate interests in preventing patrons from accessing visual

depictions of obscenity, child pornography, or in the case of minors, material harmful to minors. Moreover, use of filters also helps prevent patrons from being unwillingly exposed to patently offensive, sexually explicit content on the Internet.

We are sympathetic to the position of the government, believing that it would be desirable if there were a means to ensure that public library patrons could share in the informational bonanza of the Internet while being insulated from materials that meet CIPA's definitions, that is, visual depictions that are obscene, child pornography, or in the case of minors, harmful to minors. Unfortunately this outcome, devoutly to be wished, is not available in this less than best of all possible worlds. No category definition used by the blocking programs is identical to the legal definitions of obscenity, child pornography, or material harmful to minors, and, at all events, filtering programs fail to block access to a substantial amount of content on the Internet that falls into the categories defined by CIPA. As will appear, we credit the testimony of plaintiffs' expert Dr. Geoffrey Nunberg that the blocking software is (at least for the foreseeable future) incapable of effectively blocking the majority of materials in the categories defined by CIPA without overblocking a substantial amount of materials. Nunberg's analysis was supported by extensive record evidence. As noted above, this inability to prevent both substantial amounts of underblocking and overblocking stems from several sources, including limitations on the technology that software filtering companies use to gather and review Web pages, limitations on resources for human review of Web pages, and the necessary error that results from human review processes.

Because the filtering software mandated by CIPA will block access to substantial amounts of constitutionally protected speech whose suppression serves no legitimate government interest, we are persuaded that a public library's use of software filters is not narrowly tailored to further any of these interests. Moreover, less restrictive alternatives exist that further the government's legitimate interest in preventing the dissemination of obscenity, child pornography, and material harmful to minors, and in preventing patrons from being unwillingly exposed to patently offensive, sexually explicit content. To prevent patrons from accessing visual depictions that are obscene and child pornography, public libraries may enforce Internet use policies that make clear to patrons that the library's Internet terminals may not be used to access illegal speech. Libraries may then impose penalties on patrons who violate these policies, ranging from a warning to notification of law enforcement, in the appropriate case. Less restrictive alternatives to filtering that further libraries' interest in preventing minors from exposure to visual depictions that are harmful to minors include requiring parental consent to or presence during unfiltered access, or restricting minors' unfiltered access to terminals within view of library staff. Finally, optional filtering, privacy screens, recessed monitors, and placement of unfiltered Internet terminals outside of sight-lines provide less restrictive alternatives for libraries to prevent patrons from being unwillingly exposed to sexually explicit content on the Internet.

In an effort to avoid the potentially fatal legal implications of the overblocking problem, the government falls back on the ability of the libraries, under CIPA's disabling provisions, *see* CIPA § 1712 (codified at 20 U.S.C. § 9134(f)(3)), CIPA §1721(b)

(codified at 47 U.S.C. § 254(h)(6)(D)), to unblock a site that is patently proper yet improperly blocked. The evidence reflects that libraries can and do unblock the filters when a patron so requests. But it also reflects that requiring library patrons to ask for a Web site to be unblocked will deter many patrons because they are embarrassed, or desire to protect their privacy or remain anonymous. Moreover, the unblocking may take days, and may be unavailable, especially in branch libraries, which are often less well staffed than main libraries. Accordingly, CIPA's disabling provisions do not cure the constitutional deficiencies in public libraries' use of Internet filters.

Under these circumstances we are constrained to conclude that the library plaintiffs must prevail in their contention that CIPA requires them to violate the First Amendment rights of their patrons, and accordingly is facially invalid, even under the standard urged on us by the government, which would permit us to facially invalidate CIPA only if it is impossible for a single public library to comply with CIPA's conditions without violating the First Amendment. In view of the limitations inherent in the filtering technology mandated by CIPA, any public library that adheres to CIPA's conditions will necessarily restrict patrons' access to a substantial amount of protected speech, in violation of the First Amendment. Given this conclusion, we need not reach plaintiffs' arguments that CIPA effects a prior restraint on speech and is unconstitutionally vague. Nor do we decide their cognate unconstitutional conditions theory, though for reasons explained *infra* at note 36, we discuss the issues raised by that claim at some length.

For these reasons, we will enter an Order declaring Sections 1712(a)(2) and

1721(b) of the Children's Internet Protection Act, codified at 20 U.S.C. § 9134(f) and 47 U.S.C. § 254(h)(6), respectively, to be facially invalid under the First Amendment and permanently enjoining the defendants from enforcing those provisions.**II.**

Findings of Fact

A. Statutory Framework

1. Nature and Operation of the E-rate and LSTA Programs

In the Telecommunications Act of 1996 ("1996 Act"), Congress directed the Federal Communications Commission ("FCC") to take the steps necessary to establish a system of support mechanisms to ensure the delivery of affordable telecommunications service to all Americans. This system, referred to as "universal service," is codified in section 254 of the Communications Act of 1934, as amended by the 1996 Act. *See* 47 U.S.C. § 254. Congress specified several groups as beneficiaries of the universal service support mechanism, including consumers in high-cost areas, low-income consumers, schools and libraries, and rural health care providers. *See* 47 U.S.C. § 254(h)(1). The extension of universal service to schools and libraries in section 254(h) is commonly referred to as the Schools and Libraries Program, or "E-rate" Program.

Under the E-rate Program, "[a]ll telecommunications carriers serving a geographic area shall, upon a bona fide request for any of its services that are within the definition of universal service . . ., provide such services to elementary schools, secondary schools, and libraries for educational purposes at rates less than the amounts charged for similar services to other parties." 47 U.S.C. § 254(h)(1)(B). Under FCC regulations, providers of

"interstate telecommunications" (with certain exceptions, *see* 47 C.F.R. § 54.706(d)), must contribute a portion of their revenue for disbursement among eligible carriers that are providing services to those groups or areas specified by Congress in section 254. To be eligible for the discounts, a library must: (1) be eligible for assistance from a State library administrative agency under the Library Services and Technology Act, *see infra*; (2) be funded as an independent entity, completely separate from any schools; and (3) not be operating as a for-profit business. *See* 47 C.F.R. § 54.501(c). Discounts on services for eligible libraries are set as a percentage of the pre-discount price, and range from 20% to 90%, depending on a library's level of economic disadvantage and its location in an urban or rural area. *See* 47 C.F.R. § 54.505. Currently, a library's level of economic disadvantage is based on the percentage of students eligible for the national school lunch program in the school district in which the library is located.

The Library Services and Technology Act ("LSTA"), Subchapter II of the Museum and Library Services Act, 20 U.S.C. § 9101 *et seq.*, was enacted by Congress in 1996 as part of the Omnibus Consolidated Appropriations Act of 1997, Pub. L. No. 104-208. The LSTA establishes three grant programs to achieve the goal of improving library services across the nation. Under the Grants to States Program, LSTA grant funds are awarded, *inter alia*, in order to assist libraries in accessing information through electronic networks and pay for the costs of acquiring or sharing computer systems and telecommunications technologies. *See* 20 U.S.C. § 9141(a). Through the Grants to States program, LSTA funds have been used to acquire and pay costs associated with Internet-accessible computers

located in libraries.

2. CIPA

The Children's Internet Protection Act ("CIPA") was enacted as part of the Consolidated Appropriations Act of 2001, which consolidated and enacted several appropriations bills, including the Miscellaneous Appropriations Act, of which CIPA was a part. *See* Pub. L. No. 106-554. CIPA addresses three distinct types of federal funding programs: (1) aid to elementary and secondary schools pursuant to Title III of the Elementary and Secondary Education Act of 1965, *see* CIPA § 1711 (amending Title 20 to add § 3601); (2) LSTA grants to states for support of libraries, *see* CIPA § 1712 (amending the Museum and Library Services Act, 20 U.S.C. § 9134); and (3) discounts under the E-rate program, *see* CIPA § 1721(a) & (b) (both amending the Communications Act of 1934, 47 U.S.C. § 254(h)). Only sections 1712 and 1721(b) of CIPA, which apply to libraries, are at issue in this case.

As explained in more detail below, CIPA requires libraries that participate in the LSTA and E-rate programs to certify that they are using software filters on their computers to protect against visual depictions that are obscene, child pornography, or in the case of minors, harmful to minors. CIPA permits library officials to disable the filters for patrons for bona fide research or other lawful purposes, but disabling is not permitted for minor patrons if the library receives E-rate discounts.

a. CIPA's Amendments to the E-rate Program

Section 1721(b) of CIPA imposes conditions on a library's participation in the E-

rate program. A library "having one or more computers with Internet access may not receive services at discount rates," CIPA § 1721(b) (codified at 47 U.S.C. § 254(h)(6)(A)(i)), unless the library certifies that it is "enforcing a policy of Internet safety that includes the operation of a technology protection measure with respect to any of its computers with Internet access that protects against access through such computers to visual depictions that are – (I) obscene; (II) child pornography; or (III) harmful to minors," and that it is "enforcing the operation of such technology protection measure during any use of such computers by minors." CIPA § 1721(b) (codified at 47 U.S.C. § 254(h)(6)(B)).[2] CIPA defines a "technology protection measure" as "a specific technology

---

[2] CIPA defines "[m]inor" as "any individual who has not attained the age of 17 years." CIPA § 1721(c) (codified at 47 U.S.C. § 254(h)(7)(D)). CIPA further provides that "[o]bscene" has the meaning given in 18 U.S.C. § 1460, and "child pornography" has the meaning given in 18 U.S.C. § 2256. CIPA § 1721(c) (codified at 47 U.S.C. § 254(h)(7)(E) & (F)). CIPA defines material that is "harmful to minors" as:

> any picture, image, graphic image file, or other visual depiction that – (i) taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion; (ii) depicts, describes, or represents, in a patently offensive way with respect to what is suitable for minors, an actual or simulated sexual act or sexual contact, actual or simulated normal or perverted sexual acts, or a lewd exhibition of the genitals; and (iii) taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors.

CIPA § 1721(c) (codified at 47 U.S.C. § 254(h)(7)(G)).

CIPA prohibits federal interference in local determinations regarding what Internet content is appropriate for minors:

> A determination regarding what matter is appropriate for minors shall be made by the school board, local educational agency, library or other authority responsible for making the determination. No agency or instrumentality of

that blocks or filters access to visual depictions that are obscene, . . . child pornography, . . . or harmful to minors." CIPA § 1703(b)(1) (codified at 47 U.S.C. § 254(h)(7)(I)).

To receive E-rate discounts, a library must also certify that filtering software is in operation during adult use of the Internet. More specifically, with respect to adults, a library must certify that it is "enforcing a policy of Internet safety that includes the operation of a technology protection measure with respect to any of its computers with Internet access that protects against access through such computers to visual depictions that are – (I) obscene; or (II) child pornography," and that it is "enforcing the operation of such technology protection measure during any use of such computers." CIPA § 1721(b) (codified at 47 U.S.C. § 254(h)(6)(C)). Interpreting the statutory terms "any use," the FCC has concluded that "CIPA makes no distinction between computers used only by staff and those accessible to the public." *In re Federal-State Joint Board on Universal Service: Children's Internet Protection Act*, CC Docket No. 96-45, Report and Order, FCC 01-120, ¶ 30 (Apr. 5, 2001).

With respect to libraries receiving E-rate discounts, CIPA further specifies that "[a]n administrator, supervisor, or other person authorized by the certifying authority . . . may disable the technology protection measure concerned, during use by an adult, to enable

---

> the United States Government may – (A) establish criteria for making such determination; (B) review the determination made by the certifying [entity] . . . ; or (C) consider the criteria employed by the certifying [entity] . . . in the administration of subsection (h)(1)(B).

CIPA § 1732 (codified at 47 U.S.C. § 254(l)(2)).

access for bona fide research or other lawful purpose." CIPA §1721(b) (codified at 47 U.S.C. § 254(h)(6)(D)).

b. CIPA's Amendments to the LSTA Program

Section 1712 of CIPA amends the Museum and Library Services Act (20 U.S.C. § 9134(f)) to provide that no funds made available under the Act "may be used to purchase computers used to access the Internet, or to pay for direct costs associated with accessing the Internet," unless such library "has in place" and is enforcing "a policy of Internet safety that includes the operation of a technology protection measure with respect to any of its computers with Internet access that protects against access through such computers to visual depictions" that are "obscene" or "child pornography," and, when the computers are in use by minors, also protects against access to visual depictions that are "harmful to minors." CIPA § 1712 (codified at 20 U.S.C. § 9134(f)(1)). Section 1712 contains definitions of "technology protection measure," "obscene," "child pornography," and "harmful to minors," that are substantially similar to those found in the provisions governing the E-rate program. CIPA § 1712 (codified at 20 U.S.C. § 9134(f)(7)); *see also supra* note 2.

As under the E-rate program, "an administrator, supervisor or other authority may disable a technology protection measure . . . to enable access for bona fide research or other lawful purposes." CIPA § 1712 (codified at 20 U.S.C. § 9134(f)(3)). Whereas CIPA's amendments to the E-rate program permit disabling for bona fide research or other lawful purposes only during adult use, the LSTA provision permits disabling for both adults

and minors.

B. Identity of the Plaintiffs

1. Library and Library Association Plaintiffs

Plaintiffs American Library Association, Alaska Library Association, California Library Association, Connecticut Library Association, Freedom to Read Foundation, Maine Library Association, New England Library Association, New York Library Association, and Wisconsin Library Association are non-profit organizations whose members include public libraries that receive either E-rate discounts or LSTA funds for the provision of Internet access. Because it is a prerequisite to associational standing, we note that the interests that these organizations seek to protect in this litigation are central to their *raison d'être*.

Plaintiffs Fort Vancouver Regional Library District, in southwest Washington state; Multnomah County Public Library, in Multnomah County, Oregon; Norfolk Public Library System, in Norfolk, Virginia; Santa Cruz Public Library Joint Powers Authority, in Santa Cruz, California; South Central Library System ("SCLS"), centered in Madison, Wisconsin; and the Westchester Library System, in Westchester County, New York, are public library systems with branch offices in their respective localities that provide Internet access to their patrons.

The Fort Vancouver Regional Library District, for over three years from 1999-2001, received $135,000 in LSTA grants and $19,500 in E-rate discounts for Internet access. The Multnomah County Public Library received $70,000 in E-rate discounts for Internet access this year, and has applied for $100,000 in E-rate discounts for the

upcoming year. The Norfolk Public Library System received $90,000 in E-rate discounts for Internet access this year, and has received a $200,000 LSTA grant to put computer labs in eight of its libraries. The Santa Cruz Public Library Joint Powers Authority received $20,560 in E-rate discounts for Internet access in 2001-02. The SCLS received between $3,000 and $5,000 this year in E-rate discounts for Internet access.

The Fort Vancouver Regional Library District Board is a public board whose members are appointed by elected county commissioners. The Multnomah County Library is a county department, whose board is appointed by the county chair and confirmed by the other commissioners. The SCLS is an aggregation of 51 independently governed statutory member public libraries, whose relationship to SCLS is defined by state law. The governing body of the SCLS is the Library Board of Trustees, which consists of 20 members nominated by county executives and ratified by county boards of supervisors.

2. Patron and Patron Association Plaintiffs

Plaintiffs Association of Community Organizations for Reform Now, Friends of the Philadelphia City Institute Library, and the Pennsylvania Alliance for Democracy are nonprofit organizations whose members include individuals who access the Internet at public libraries that receive E-rate discounts or LSTA funds for the provision of public Internet access. We note for the purpose of associational standing that the interests that these organizations seek to protect in this litigation are germane to their purposes.

Plaintiffs Emmalyn Rood, Mark Brown, Elizabeth Hrenda, C. Donald Weinberg, Sherron Dixon, by her father and next friend Gordon Dixon, James Geringer, Marnique

Tynesha Overby, by her next friend Carolyn C. Williams, William J. Rosenbaum, Carolyn C. Williams, and Quiana Williams, by her mother and next friend Sharon Bernard, are adults and minors who use the Internet at public libraries that, to the best of their knowledge, do not filter patrons' access to the Internet. Several of these plaintiffs do not have Internet access from home.

Emmalyn Rood is a sixteen-year-old who uses the Multnomah County Public Library. When she was 13, she used the Internet at the Multnomah County Public Library to research issues relating to her sexual identity. Ms. Rood did not use her home or school computer for this research, in part because she wished her searching to be private. Although the library offered patrons the option of using filtering software, Ms. Rood did not use that option because she had had previous experience with such programs blocking information that was valuable to her, including information relating to gay and lesbian issues.

Plaintiff Mark Brown used the Internet at the Philadelphia Free Library to research breast cancer and reconstructive surgery for his mother who had breast surgery. Mr. Brown's research at the library provided him and his mother with essential information about his mother's medical condition and potential treatments.

3. Web Publisher Plaintiffs

Plaintiff Afraid to Ask, Inc., based in Saunderstown, Rhode Island, publishes a health education Web site, www.AfraidtoAsk.com. Dr. Jonathan Bertman, the president and medical director of Afraid to Ask, is a family practice physician in rural Rhode Island and a

clinical assistant professor of family medicine at Brown University. AfraidtoAsk.com's mission is to provide detailed information on sensitive health issues, often of a sexual nature, such as sexually transmitted diseases, male and female genitalia, and birth control, sought by people of all ages who would prefer to learn about sensitive health issues anonymously, i.e., they are "afraid to ask." As part of its educational mission, AfraidtoAsk.com often uses graphic images of sexual anatomy to convey information. Its primary audience is teens and young adults. Based on survey data collected on the site, half of the people visiting the site are under 24 years old and a quarter are under 18. AfraidtoAsk.com is blocked by several leading blocking products as containing sexually explicit content.

Plaintiff Alan Guttmacher Institute has a Web site that contains information about its activities and objectives, including its mission to protect the reproductive choices of women and men. Plaintiff Planned Parenthood Federation of America, Inc. ("Planned Parenthood") is a national voluntary organization in the field of reproductive health care. Planned Parenthood owns and operates several Web sites that provide a range of information about reproductive health, from contraception to prevention of sexually transmitted diseases, to finding an abortion provider, and to information about the drug Mifepristone. Plaintiff Safersex.org is a Web site that offers free educational information on how to practice safer sex.

Plaintiff Ethan Interactive, Inc., d/b/a Out In America, is an online content provider that owns and operates 64 free Web sites for gay, lesbian, bisexual and transgendered

persons worldwide. Plaintiff PlanetOut Corporation is an online content provider for gay, lesbian, bisexual and transgendered persons. Plaintiff the Naturist Action Committee ("NAC") is the nonprofit political arm of the Naturist Society, a private organization that promotes a way of life characterized by the practice of nudity. The NAC Web site provides information about Naturist Society activities and about state and local laws that may affect the rights of Naturists or their ability to practice Naturism, and includes nude photographs of its members.

Plaintiff Wayne L. Parker was the Libertarian candidate in the 2000 U.S. Congressional election for the Fifth District of Mississippi (and is running again in 2002). He publishes a Web site that communicates information about his campaign and that provides information about his political views and the Libertarian Party to the public. Plaintiff Jeffrey Pollock was the Republican candidate in the 2000 U.S. Congressional election for the Third District of Oregon. He operates a Web site that is now promoting his candidacy for Congress in 2002.[3]

---

[3] The government challenges the standing of several of the plaintiffs and the ripeness of their claims. These include all of the Web site publishers and all of the individual library patrons. Notwithstanding these objections, we are confident that the "case or controversy" requirement of Article III, § 2 of the Constitution is met by the existence of the plaintiff libraries that qualify for LSTA and E-rate funding and the library associations whose members qualify for such funding. These plaintiffs are faced with the impending choice of either certifying compliance with CIPA by July 1, 2002, or foregoing subsidies under the LSTA and E-rate programs, and therefore clearly have standing to challenge the constitutionality of the conditions to which they will be subject should they accept the subsidies. We also note that the presence of the Web site publishers and individual library patrons does not affect our legal analysis or disposition of the case.

C. The Internet

1. Background

As we noted at the outset, the Internet is a vast, interactive medium consisting of a decentralized network of computers around the world. The Internet presents low entry barriers to anyone who wishes to provide or distribute information. Unlike television, cable, radio, newspapers, magazines or books, the Internet provides an opportunity for those with access to it to communicate with a worldwide audience at little cost. At least 400 million people use the Internet worldwide, and approximately 143 million Americans were using the Internet as of September 2001. Nat'l Telecomm. & Info. Admin., *A Nation Online: How Americans Are Expanding Their Use of the Internet* (February 2002), *available at* http://www.ntia.doc.gov/ntiahome/dn/.

The World Wide Web is a part of the Internet that consists of a network of computers, called "Web servers," that host "pages" of content accessible via the Hypertext Transfer Protocol or "HTTP." Anyone with a computer connected to the Internet can search for and retrieve information stored on Web servers located around the world. Computer users typically access the Web by running a program called a "browser" on their computers. The browser displays, as individual pages on the computer screen, the various types of content found on the Web and lets the user follow the connections built into Web pages – called "hypertext links," "hyperlinks," or "links" – to additional content. Two popular browsers are Microsoft Internet Explorer and Netscape Navigator.

A "Web page" is one or more files a browser graphically assembles to make a

viewable whole when a user requests content over the Internet. A Web page may contain a variety of different elements, including text, images, buttons, form fields that the user can fill in, and links to other Web pages. A "Web site" is a term that can be used in several different ways. It may refer to all of the pages and resources available on a particular Web server. It may also refer to all the pages and resources associated with a particular organization, company or person, even if these are located on different servers, or in a subdirectory on a single server shared with other, unrelated sites. Typically, a Web site has as an intended point of entry, a "home page," which includes links to other pages on the same Web site or to pages on other sites. Online discussion groups and chat rooms relating to a variety of subjects are available through many Web sites.

Users may find content on the Web using engines that search for requested keywords. In response to a keyword request, a search engine will display a list of Web sites that may contain relevant content and provide links to those sites. Search engines and directories often return a limited number of sites in their search results (e.g., the Google search engine will return only 2,000 sites in response to a search, even if it has found, for example, 530,000 sites in its index that meet the search criteria).

A user may also access content on the Web by typing a URL (Uniform Resource Locator) into the address line of the browser. A URL is an address that points to some resource located on a Web server that is accessible over the Internet. This resource may be a Web site, a Web page, an image, a sound or video file, or other resource. A URL can be either a numeric Internet Protocol or "IP" address, or an alphanumeric "domain name"

address. Every Web server connected to the Internet is assigned an IP address. A typical IP address looks like "13.1.64.14." Typing the URL "http://13.1.64.14/" into a browser will bring the user to the Web server that corresponds to that address. For convenience, most Web servers have alphanumeric domain name addresses in addition to IP addresses. For example, typing in "http://www.paed.uscourts.gov" will bring the user to the same Web server as typing in "http://204.170.64.143."

Every time a user attempts to access material located on a Web server by entering a domain name address into a Web browser, a request is made to a Domain Name Server, which is a directory of domain names and IP addresses, to "resolve," or translate, the domain name address into an IP address. That IP address is then used to locate the Web server from which content is being requested. A Web site may be accessed by using either its domain name address or its IP address.

A domain name address typically consists of several parts. For example, the alphanumeric URL http://www.paed.uscourts.gov/documents/opinions can be broken down into three parts. The first part is the transfer protocol the computer will use in accessing the content (e.g., "http" for Hypertext Transfer Protocol); next is the name of the host server on which the information is stored (e.g., www.paed.uscourts.gov); and then the name of the particular file or directory on that server (e.g., /documents/opinions).

A single Web page may be associated with more than one URL. For example, the URLs http://www.newyorktimes.com and http://www.nytimes.com will both take the user to the *New York Times* home page. The topmost directory in a Web site is often referred to

as that Web site's root directory or root URL. For example, in http://www.paed.uscourts.gov/documents, the root URL is http://www.paed.uscourts.gov. There may be hundreds or thousands of pages under a single root URL, or there may be one or only a few.

There are a number of Web hosting companies that maintain Web sites for other businesses and individuals, which can lead to vast amounts of diverse content being located at the same IP address. Hosting services are offered either for a fee, or in some cases, for free, allowing any individual with Internet access to create a Web site. Some hosting services are provided through the process of "IP-based hosting," where each domain name is assigned a unique IP number. For example, www.baseball.com might map to the IP address "10.3.5.9" and www.XXX.com might map to the IP address "10.0.42.5." Other hosting services are provided through the process of "name-based hosting," where multiple domain name addresses are mapped to a single IP address. If the hosting company were using this method, both www.baseball.com and www.XXX.com could map to a single IP address, e.g., "10.3.5.9." As a result of the "name-based hosting" process, up to tens of thousands of pages with heterogeneous content may share a single IP address.

2. The Indexable Web, the "Deep Web"; Their Size and Rates of Growth and Change

The universe of content on the Web that could be indexed, in theory, by standard search engines is known as the "publicly indexable Web." The publicly indexable Web is limited to those pages that are accessible by following a link from another Web page that is recognized by a search engine. This limitation exists because online indexing techniques

used by popular search engines and directories such as Yahoo, Lycos and AltaVista, are based on "spidering" technology, which finds sites to index by following links from site to site in a continuous search for new content. If a Web page or site is not linked by others, then spidering will not discover that page or site.

Furthermore, many larger Web sites contain instructions, through software, that prevent spiders from investigating that site, and therefore the contents of such sites also cannot be indexed using spidering technology. Because of the vast size and decentralized structure of the Web, no search engine or directory indexes all of the content on the publicly indexable Web. We credit current estimates that no more than 50% of the content currently on the publicly indexable Web has been indexed by all search engines and directories combined. No currently available method or combination of methods for collecting URLs can collect the addresses of all URLs on the Web.

The portion of the Web that is not theoretically indexable through the use of "spidering" technology, because other Web pages do not link to it, is called the "Deep Web." Such sites or pages can still be made publicly accessible without being made publicly indexable by, for example, using individual or mass emailings (also known as "spam") to distribute the URL to potential readers or customers, or by using types of Web links that cannot be found by spiders but can be seen and used by readers. "Spamming" is a common method of distributing to potential customers links to sexually explicit content that is not indexable.

Because the Web is decentralized, it is impossible to say exactly how large it is. A

2000 study estimated a total of 7.1 million unique Web sites, which at the Web's historical rate of growth, would have increased to 11 million unique sites as of September 2001. Estimates of the total number of Web pages vary, but a figure of 2 billion is a reasonable estimate of the number of Web pages that can be reached, in theory, by standard search engines. We need not make a specific finding as to a figure, for by any measure the Web is extremely vast, and it is constantly growing. The indexable Web is growing at a rate of approximately 1.5 million pages per day. The size of the un-indexable Web, or the "Deep Web," while impossible to determine precisely, is estimated to be two to ten times that of the publicly indexable Web.

In addition to growing rapidly, Web pages and sites are constantly being removed, or changing their content. Web sites or pages can change content without changing their domain name addresses or IP addresses. Individual Web pages have an average life span of approximately 90 days.

3. The Amount of Sexually Explicit Material on the Web

There is a vast amount of sexually explicit material available via the Internet and the Web. Sexually explicit material on the Internet is easy to access using any public search engine, such as, for example, Google or AltaVista. Although much of the sexually explicit material available on the Web is posted on commercial sites that require viewers to pay in order to gain access to the site, a large number of sexually explicit sites may be accessed for free and without providing any registration information. Most importantly, some Web sites that contain sexually explicit content have innocuous domain names and therefore can

be reached accidentally. A commonly cited example is http://www.whitehouse.com. Other innocent-sounding URLs that retrieve graphic, sexually explicit depictions include http://www.boys.com, http://www.girls.com, http://www.coffeebeansupply.com, and http://www.BookstoreUSA.com. Moreover, commercial Web sites that contain sexually explicit material often use a technique of attaching pop-up windows to their sites, which open new windows advertising other sexually explicit sites without any prompting by the user. This technique makes it difficult for a user quickly to exit all of the pages containing sexually explicit material, whether he or she initially accessed such material intentionally or not.

The percentage of Web pages on the indexed Web containing sexually explicit content is relatively small. Recent estimates indicate that no more than 1-2% of the content on the Web is pornographic or sexually explicit. However, the absolute number of Web sites offering free sexually explicit material is extremely large, approximately 100,000 sites.

D. American Public Libraries

The more than 9,000 public libraries in the United States are typically funded (at least in large part) by state or local governments. They are frequently overseen by a board of directors that is either elected or is appointed by an elected official or a body of elected officials. We heard testimony from librarians and library board members working in eight public library systems in different communities across the country, some of whom are also plaintiffs in this case. They hailed from the following library systems: Fort Vancouver,

Washington; Fulton County, Indiana; Greenville, South Carolina; a regional consortium of libraries centered in Madison, Wisconsin; Multnomah County, Oregon; Norfolk, Virginia; Tacoma, Washington; and Westerville, Ohio. The parties also took depositions from several other librarians and library board members who did not testify during the trial, and submitted a number of other documents regarding individual libraries' policies.

1. The Mission of Public Libraries, and Their Reference and Collection Development Practices

American public libraries operate in a wide variety of communities, and it is not surprising that they do not all view their mission identically. Nor are their practices uniform. Nevertheless, they generally share a common mission – to provide patrons with a wide range of information and ideas.

Public libraries across the country have endorsed the American Library Association's ("ALA") "Library Bill of Rights" and/or "Freedom to Read Statement," including every library testifying on behalf of the defendants in this case. The "Library Bill of Rights," first adopted by the ALA in 1948, provides, among other things, that "[b]ooks and other library resources should be provided for the interest, information, and enlightenment of all people of the community the library serves." It also states that libraries "should provide materials and information presenting all points of view on current and historical issues" and that library materials "should not be proscribed or removed because of partisan or doctrinal disapproval."

The ALA's "Freedom to Read" statement, adopted in 1953 and most recently

updated in July 2000, states, among other things, that "[i]t is in the public interest for publishers and librarians to make available the widest diversity of views and expressions, including those that are unorthodox or unpopular with the majority." It also states that "[i]t is the responsibility of . . . librarians . . . to contest encroachments upon th[e] freedom [to read] by individuals or groups seeking to impose their own standards or tastes upon the community at large."

Public libraries provide information not only for educational purposes, but also for recreational, professional, and other purposes. For example, Ginnie Cooper, Director of the Multnomah County Library, testified that some of the library's most popular items include video tapes of the British Broadcasting Corporation's "Fawlty Towers" series, and also print and "books on tape" versions of science fiction, romance, and mystery novels. Many public libraries include sexually explicit materials in their print collection, such as *The Joy of Sex* and *The Joy of Gay Sex*. Very few public libraries, however, collect more graphic sexually explicit materials, such as XXX-rated videos, or *Hustler* magazine.[4]

The mission of public librarians is to provide their patrons with a wide array of information, and they surely do so. Reference librarians across America answer more than 7 million questions weekly. If a patron has a specialized need for information not available

---

[4] The OCLC database, a cooperative cataloging service established to facilitate interlibrary loan requests, includes 40 million catalog records from approximately 48,000 libraries of all types worldwide. Slightly more than 400 of the libraries in the OCLC database are listed as carrying *Playboy* in their collections, while only eight subscribe to *Hustler*.

in the public library, the professional librarian will use a reference interview to find out what information is needed to help the user, including the purpose for which an item will be used. Reference librarians are trained to assist patrons without judging the patron's purpose in seeking information, or the content of the information that the patron is seeking.

Many public libraries routinely provide patrons with access to materials not in their collections through the use of bibliographic access tools and interlibrary loan programs. Public libraries typically will assist patrons in obtaining access to all materials except those that are illegal, even if they do not collect those materials in their physical collection. In order to provide this access, a librarian may attempt to find material not included in the library's own collection in other libraries in the system, through interlibrary loan, or through a referral, perhaps to a government agency or a commercial bookstore. Interlibrary loan is expensive, however, and is therefore used infrequently.

Public librarians also apply professional standards to their collection development practices. Public libraries generally make material selection decisions and frame policies governing collection development at the local level. Collection development is a key subject in the curricula of Masters of Library Science programs and is defined by certain practices. In general, professional standards guide public librarians to build, develop and create collections that have certain characteristics, such as balance in its coverage and requisite and appropriate quality. To this end, the goal of library collections is not universal coverage, but rather to find those materials that would be of the greatest direct

benefit or interest to the community. In making selection decisions, librarians consider criteria including the content of the material, its accuracy, the title's niche in relation to the rest of the collection, the authority of the author, the publisher, the work's presentation, and how it compares with other material available in the same genre or on the same subject.

In pursuing the goal of achieving a balanced collection that serves the needs and interests of their patrons, librarians generally have a fair amount of autonomy, but may also be guided by a library's collection development policy. These collection development policies are often drawn up in conjunction with the libraries' governing boards and with representatives from the community, and may be the result of public hearings, discussions and other input.

Although many librarians use selection aids, such as review journals and bibliographies, as a guide to the quality of potential acquisitions, they do not generally delegate their selection decisions to parties outside of the public library or its governing body. One limited exception is the use of third-party vendors or approval plans to acquire print and video resources. In such arrangements, third-party vendors provide materials based on the library's description of its collection development criteria. The vendor sends materials to the library, and the library retains the materials that meet its collection development needs and returns the materials that do not. Even in this arrangement, however, the librarians still retain ultimate control over their collection development and review all of the materials that enter their library's collection.

2. The Internet in Public Libraries

The vast majority of public libraries offer Internet access to their patrons. According to a recent report by the U.S. National Commission on Libraries and Information Science, approximately 95% of all public libraries provide public access to the Internet. John C. Bertot & Charles R. McClure, *Public Libraries and the Internet 2000: Summary Findings and Data Tables*, Report to National Commission on Libraries and Information Science, at 3. The Internet vastly expands the amount of information available to patrons of public libraries. The widespread availability of Internet access in public libraries is due, in part, to the availability of public funding, including state and local funding and the federal funding programs regulated by CIPA.

Many libraries face a large amount of patron demand for their Internet services. At some libraries, patron demand for Internet access during a given day exceeds the supply of computer terminals with access to the Internet. These libraries use sign-in and time limit procedures and/or establish rules regarding the allowable uses of the terminals, in an effort to ration their computer resources. For example, some of the libraries whose librarians testified at trial prohibit the use of email and chat functions on their public Internet terminals.

Public libraries play an important role in providing Internet access to citizens who would not otherwise possess it. Of the 143 million Americans using the Internet, approximately 10%, or 14.3 million people, access the Internet at a public library. Internet access at public libraries is more often used by those with lower incomes than those with

higher incomes. About 20.3% of Internet users with household family income of less than $15,000 per year use public libraries for Internet access. Approximately 70% of libraries serving communities with poverty levels in excess of 40% receive E-rate discounts.

a. Internet Use Policies in Public Libraries

Approximately 95% of libraries with public Internet access have some form of "acceptable use" policy or "Internet use" policy governing patrons' use of the Internet. These policies set forth the conditions under which patrons are permitted to access and use the library's Internet resources. These policies vary widely. Some of the less restrictive policies, like those held by Multnomah County Library and Fort Vancouver Regional Library, do not prohibit adult patrons from viewing sexually explicit materials on the Web, as long as they do so at terminals with privacy screens or recessed monitors, which are designed to prevent other patrons from seeing the material that they are viewing, and as long as it does not violate state or federal law to do so. Other libraries prohibit their patrons from viewing all "sexually explicit" or "sexually graphic" materials.

Some libraries prohibit the viewing of materials that are not necessarily sexual, such as Web pages that are "harmful to minors," "offensive to the public," "objectionable," "racially offensive," or simply "inappropriate." Other libraries restrict access to Web sites that the library just does not want to provide, even though the sites are not necessarily offensive. For example, the Fulton County Public Library restricts access to the Web sites of dating services. Similarly, the Tacoma Public Library's policy does not allow patrons to use the library's Internet terminals for personal email, for online chat, or for playing

games.

In some cases, libraries instituted Internet use policies after having experienced specific problems, whereas in other cases, libraries developed detailed Internet use policies and regulatory measures (such as using filtering software) before ever offering public Internet access. Essentially four interests motivate libraries to institute Internet use policies and to apply the methods described above to regulate their patrons' use of the Internet.

First, libraries have sought to protect patrons (especially children) and staff members from accidentally viewing sexually explicit images, or other Web pages containing content deemed harmful, that other patrons are viewing on the Internet. For example, some librarians who testified described situations in which patrons left sexually explicit images minimized on an Internet terminal so that the next patron would see them when they began using it, or in which patrons printed sexually explicit images from a Web site and left them at a public printer.

Second, libraries have attempted to protect patrons from unwittingly or accidentally accessing Web pages that they do not wish to see while they are using the Internet. For example, the Memphis-Shelby County (Tennessee) Public Library's Internet use policy states that the library "employs filtering technology to reduce the possibility that customers may encounter objectionable content in the form of depictions of full nudity and sexual acts."

Third, libraries have sought to keep patrons (again, especially children) from

intentionally accessing sexually explicit materials or other materials that the library deems inappropriate. For example, a study of the Tacoma Public Library's Internet use logs for the year 2000 showed that users between the ages of 11 and 15 accounted for 41% of the filter blocks that occurred on library computers. The study, which we credit, concluded that children and young teens were actively seeking to access sexually explicit images in the library. The Greenville Library's Board of Directors was particularly concerned that patrons were accessing obscene materials in the public library in violation of South Carolina's obscenity statute.

Finally, some libraries have regulated patrons' Internet use to attempt to control patrons' inappropriate (or illegal) behavior that is thought to stem from viewing Web pages that contain sexually explicit materials or content that is otherwise deemed unacceptable.

We recognize the concerns that led several of the public libraries whose librarians and board members testified in this case to start using Internet filtering software. The testimony of the Chairman of the Board of the Greenville Public Library is illustrative. In December 1999, there was considerable local press coverage in Greenville concerning adult patrons who routinely used the library to surf the Web for pornography. In response to public outcry stemming from the newspaper report, the Board of Trustees held a special board meeting to obtain information and to communicate with the public concerning the library's provision of Internet access. At this meeting, the Board learned for the first time of complaints about children being exposed to pornography that was displayed on the library's Internet terminals.

In late January to early February of 2000, the library installed privacy screens and recessed terminals in an effort to restrict the display of sexually explicit Web sites at the library. In February, 2000, the Board informed the library staff that they were expected to be familiar with the South Carolina obscenity statute and to enforce the policy prohibition on access to obscene materials, child pornography, or other materials prohibited under applicable local, state, and federal laws. Staff were told that they were to enforce the policy by means of a "tap on the shoulder." Prior to adopting its current Internet Use Policy, the Board adopted an "Addendum to Current Internet Use Policy." Under the policy, the Board temporarily instituted a two-hour time limit per day for Internet use; reduced substantially the number of computers with Internet access in the library; reconfigured the location of the computers so that librarians had visual contact with all Internet-accessible terminals; and removed the privacy screens from terminals with Internet access.

Even after the Board implemented the privacy screens and later the "tap-on-the-shoulder" policy combined with placing terminals in view of librarians, the library experienced a high turnover rate among reference librarians who worked in view of Internet terminals. Finding that the policies that it had tried did not prevent the viewing of sexually explicit materials in the library, the Board at one point considered discontinuing Internet access in the library. The Board finally concluded that the methods that it had used to regulate Internet use were not sufficient to stem the behavioral problems that it thought were linked to the availability of pornographic materials in the library. As a result, it

implemented a mandatory filtering policy.

We note, however, that none of the libraries proffered by the defendants presented any systematic records or quantitative comparison of the amount of criminal or otherwise inappropriate behavior that occurred in their libraries before they began using Internet filtering software compared to the amount that happened after they installed the software. The plaintiffs' witnesses also testified that because public libraries are public places, incidents involving inappropriate behavior in libraries (sexual and otherwise) existed long before libraries provided access to the Internet.

b. Methods for Regulating Internet Use

The methods that public libraries use to regulate Internet use vary greatly. They can be organized into four categories: (1) channeling patrons' Internet use; (2) separating patrons so that they will not see what other patrons are viewing; (3) placing Internet terminals in public view and having librarians observe patrons to make sure that they are complying with the library's Internet use policy; and (4) using Internet filtering software.

The first category – channeling patrons' Internet use – frequently includes offering training to patrons on how to use the Internet, including how to access the information that they want and to avoid the materials that they do not want. Another technique that some public libraries use to direct their patrons to pages that the libraries have determined to be accurate and valuable is to establish links to "recommended Web sites" from the public library's home page (i.e., the page that appears when patrons begin a session at one of the library's public Internet terminals). Librarians select these recommended Web sites by

using criteria similar to those employed in traditional collection development. However, unless the library determines otherwise, selection of these specific sites does not preclude patrons from attempting to access other Internet Web sites.

Libraries may extend the "recommended Web sites" method further by limiting patrons' access to only those Web sites that are reviewed and selected by the library's staff. For example, in 1996, the Westerville, Ohio Library offered Internet access to children through a service called the "Library Channel." This service was intended to be a means by which the library could organize the Internet in some fashion for presentation to patrons. Through the Library Channel, the computers in the children's section of the library were restricted to 2,000 to 3,000 sites selected by librarians. After three years, Westerville stopped using the Library Channel system because it overly constrained the children's ability to access materials on the Internet, and because the library experienced several technical problems with the system.

Public libraries also use several different techniques to separate patrons during Internet sessions so that they will not see what other patrons are viewing. The simplest way to achieve this result is to position the library's public Internet terminals so that they are located away from traffic patterns in the library (and from other terminals), for example, by placing them so that they face a wall. This method is obviously constrained by libraries' space limitations and physical layout. Some libraries have also installed privacy screens on their public Internet terminals. These screens make a monitor appear blank unless the

viewer is looking at it head-on.[5] Although the Multnomah and Fort Vancouver Libraries submitted records showing that they have received few complaints regarding patrons' unwilling exposure to materials on the Internet, privacy screens do not always prevent library patrons or employees from inadvertently seeing the materials that another patron is viewing when passing directly behind a terminal. They also have the drawback of making it difficult for patrons to work together at a single terminal, or for librarians to assist patrons at terminals, because it is difficult for two people to stand side by side and view a screen at the same time. Some library patrons also find privacy screens to be a hindrance and have attempted to remove them in order to improve the brightness of the screen or to make the view better.

Another method that libraries use to prevent patrons from seeing what other patrons are viewing on their terminals is the installation of "recessed monitors." Recessed monitors are computer screens that sit below the level of a desk top and are viewed from above. Although recessed monitors, especially when combined with privacy screens, eliminate almost all of the possibility of a patron accidentally viewing the contents on another patron's screen, they suffer from the same drawbacks as privacy screens, that is, they make it difficult for patrons to work together or with a librarian at a single terminal.

---

[5] Fort Vancouver Regional Library, for example, combines the methods of strategically placing terminals in low traffic areas and using privacy screens. A section headed "Confidentiality and Privacy" on the library's home page states: "in order to protect the privacy of the user and the interests of other library patrons, the library will attempt to minimize unintentional viewing of the Internet. This will be done by use of privacy screens, and by judicious placement of the terminals and other appropriate means."

Some librarians also testified that recessed monitors are costly, but did not indicate how expensive they are compared to privacy screens or filtering software. A related technique that some public libraries use is to create a separate children's Internet viewing area, where no adults except those accompanying children in their care may use the Internet terminals. This serves the objective of keeping children from inadvertently viewing materials appropriate only for adults that adults may be viewing on nearby terminals.

A third set of techniques that public libraries have used to enforce their Internet use policies takes the opposite tack from the privacy screens/recessed monitors approach by placing all of the library's public Internet terminals in prominent and visible locations, such as near the library's reference desk. This approach allows librarians to enforce their library's Internet use policy by observing what patrons are viewing and employing the tap-on-the-shoulder policy. Under this approach, when patrons are viewing materials that are inconsistent with the library's policies, a library staff member approaches them and asks them to view something else, or may ask them to end their Internet session. A patron who does not comply with these requests, or who repeatedly views materials not permitted under the library's Internet use policy, may have his or her Internet or library privileges suspended or revoked. But many librarians are uncomfortable with approaching patrons who are viewing sexually explicit images, finding confrontation unpleasant. Hence some libraries are reluctant to apply the tap-on-the-shoulder policy.

The fourth category of methods that public libraries employ to enforce their Internet use policies, and the one that gives rise to this case, is the use of Internet filtering software.

According to the June 2000 *Survey of Internet Access Management in Public Libraries*, approximately 7% of libraries with public Internet access had mandated the use of blocking programs by adult patrons. Some public libraries provide patrons with the option of using a blocking program, allowing patrons to decide whether to engage the program when they or their children access the Internet. Other public libraries require their child patrons to use filtering software, but not their adult patrons.

Filtering software vendors sell their products on a subscription basis. The cost of a subscription varies with the number of computers on which the filtering software will be used. In 2001, the cost of the Cyber Patrol filtering software was $1,950 for 100 terminal licenses. The Greenville County Library System pays $2,500 per year for the N2H2 filtering software, and a subscription to the Websense filter costs Westerville Public Library approximately $1,200 per year.

No evidence was presented on the cost of privacy screens, recessed monitors, and the tap-on-the-shoulder policy, relative to the costs of filtering software. Nor did any of the libraries proffered by the government present any quantitative evidence on the relative effectiveness of use of privacy screens to prevent patrons from being unwillingly exposed to sexually explicit material, and the use of filters, discussed below. No evidence was presented, for example, comparing the number of patron complaints in those libraries that have tried both methods.

The librarians who testified at trial whose libraries use Internet filtering software all provide methods by which their patrons may ask the library to unblock specific Web sites

or pages. Of these, only the Tacoma Public Library allows patrons to request that a URL be unblocked without providing any identifying information; Tacoma allows patrons to request a URL by sending an email from the Internet terminal that the patron is using that does not contain a return email address for the user. David Biek, the head librarian at the Tacoma Library's main branch, testified at trial that the library keeps records that would enable it to know which patrons made unblocking requests, but does not use that information to connect users with their requests. Biek also testified that he periodically scans the library's Internet use logs to search for: (1) URLs that were erroneously blocked, so that he may unblock them; or (2) URLs that should have been blocked, but were not, in order to add them to a blocked category list. In the course of scanning the use logs, Biek has also found what looked like attempts to access child pornography. In two cases, he communicated his findings to law enforcement and turned over the logs in response to a subpoena.

At all events, it takes time for librarians to make decisions about whether to honor patrons' requests to unblock Web pages. In the libraries proffered by the defendants, unblocking decisions sometimes take between 24 hours and a week. Moreover, none of these libraries allows unrestricted access to the Internet pending a determination of the validity of a Web site blocked by the blocking programs. A few of the defendants' proffered libraries represented that individual librarians would have the discretion to allow a patron to have full Internet access on a staff computer upon request, but none claimed that allowing such access was mandatory, and patron access is supervised in every instance. None of these libraries makes differential unblocking decisions based on the patrons' age.

Unblocking decisions are usually made identically for adults and minors. Unblocking decisions even for adults are usually based on suitability of the Web site for minors.

It is apparent that many patrons are reluctant or unwilling to ask librarians to unblock Web pages or sites that contain only materials that might be deemed personal or embarrassing, even if they are not sexually explicit or pornographic. We credit the testimony of Emmalyn Rood, discussed above, that she would have been unwilling as a young teen to ask a librarian to disable filtering software so that she could view materials concerning gay and lesbian issues. We also credit the testimony of Mark Brown, who stated that he would have been too embarrassed to ask a librarian to disable filtering software if it had impeded his ability to research treatments and cosmetic surgery options for his mother when she was diagnosed with breast cancer.

The pattern of patron requests to unblock specific URLs in the various libraries involved in this case also confirms our finding that patrons are largely unwilling to make unblocking requests unless they are permitted to do so anonymously. For example, the Fulton County Library receives only about 6 unblocking requests each year, the Greenville Public Library has received only 28 unblocking requests since August 21, 2000, and the Westerville, Ohio Library has received fewer than 10 unblocking requests since 1999. In light of the fact that a substantial amount of overblocking occurs in these very libraries, *see infra* Subsection II.E.4, we find that the lack of unblocking requests in these libraries does not reflect the effectiveness of the filters, but rather reflects patrons' reluctance to ask librarians to unblock sites.

E. Internet Filtering Technology

1. What Is Filtering Software, Who Makes It, and What Does It Do?

Commercially available products that can be configured to block or filter access to certain material on the Internet are among the "technology protection measures" that may be used to attempt to comply with CIPA. There are numerous filtering software products available commercially. Three network-based filtering products – SurfControl's Cyber Patrol, N2H2's Bess/i2100, and Secure Computing's SmartFilter – currently have the lion's share of the public library market. The parties in this case deposed representatives from these three companies. Websense, another network-based blocking product, is also currently used in the public library market, and was discussed at trial.

Filtering software may be installed either on an individual computer or on a computer network. Network-based filtering software products are designed for use on a network of computers and funnel requests for Internet content through a centralized network device. Of the various commercially available blocking products, network-based products are the ones generally marketed to institutions, such as public libraries, that provide Internet access through multiple terminals.

Filtering programs function in a fairly simple way. When an Internet user requests access to a certain Web site or page, either by entering a domain name or IP address into a Web browser, or by clicking on a link, the filtering software checks that domain name or IP address against a previously compiled "control list" that may contain up to hundreds of thousands of URLs. The three companies deposed in this case have control lists containing

between 200,000 and 600,000 URLs. These lists determine which URLs will be blocked.

Filtering software companies divide their control lists into multiple categories for which they have created unique definitions. SurfControl uses 40 such categories, N2H2 uses 35 categories (and seven "exception" categories), Websense uses 30 categories, and Secure Computing uses 30 categories. Filtering software customers choose which categories of URLs they wish to enable. A user "enables" a category in a filtering program by configuring the program to block all of the Web pages listed in that category.

The following is a list of the categories offered by each of these four filtering programs. SurfControl's Cyber Patrol offers the following categories: Adult/Sexually Explicit; Advertisements; Arts & Entertainment; Chat; Computing & Internet; Criminal Skills; Drugs, Alcohol & Tobacco; Education; Finance & Investment; Food & Drink; Gambling; Games; Glamour & Intimate Apparel; Government & Politics; Hacking; Hate Speech; Health & Medicine; Hobbies & Recreation; Hosting Sites; Job Search & Career Development; Kids' Sites; Lifestyle & Culture; Motor Vehicles; News; Personals & Dating; Photo Searches; Real Estate; Reference; Religion; Remote Proxies; Sex Education; Search Engines; Shopping; Sports; Streaming Media; Travel; Usenet News; Violence; Weapons; and Web-based Email.

N2H2 offers the following categories: Adults Only; Alcohol; Auction; Chat; Drugs; Electronic Commerce; Employment Search; Free Mail; Free Pages; Gambling; Games; Hate/Discrimination; Illegal; Jokes; Lingerie; Message/Bulletin Boards; Murder/Suicide; News; Nudity; Personal Information; Personals; Pornography; Profanity;

Recreation/Entertainment; School Cheating Information; Search Engines; Search Terms; Sex; Sports; Stocks; Swimsuits; Tasteless/Gross; Tobacco; Violence; and Weapons. The "Nudity" category purports to block only "non-pornographic" images. The "Sex" category is intended to block only those depictions of sexual activity that are not intended to arouse. The "Tasteless/Gross" category includes contents such as "tasteless humor" and "graphic medical or accident scene photos." Additionally, N2H2 offers seven "exception categories." These exception categories include Education, Filtered Search Engine, For Kids, History, Medical, Moderated, and Text/Spoken Only. When an exception category is enabled, access to any Web site or page via a URL associated with both a category and an exception, for example, both "Sex" and "Education," will be allowed, even if the customer has enabled the product to otherwise block the category "Sex." As of November 15, 2001, of those Web sites categorized by N2H2 as "Sex," 3.6% were also categorized as "Education," 2.9% as "Medical," and 1.6% as "History."

Websense offers the following categories: Abortion Advocacy; Advocacy Groups; Adult Material; Business & Economy; Drugs; Education; Entertainment; Gambling; Games; Government; Health; Illegal/Questionable; Information Technology; Internet Communication; Job Search; Militancy/Extremist; News & Media; Productivity Management; Bandwidth Management; Racism/Hate; Religion; Shopping; Society & Lifestyle; Special Events; Sports; Tasteless; Travel; Vehicles; Violence; and Weapons. The "Adult" category includes "full or partial nudity of individuals," as well as sites offering "light adult humor and literature" and "[s]exually explicit language." The

"Sexuality/Pornography" category includes, *inter alia*, "hard-core adult humor and literature" and "[s]exually explicit language." The "Tasteless" category includes "hard-to-stomach sites, including offensive, worthless or useless sites, grotesque or lurid depictions of bodily harm." The "Hacking" category blocks "sites providing information on or promoting illegal or questionable access to or use of communications equipment and/or software."

SmartFilter offers the following categories: Anonymizers/Translators; Art & Culture; Chat; Criminal Skills; Cults/Occult; Dating; Drugs; Entertainment; Extreme/Obscene/Violence; Gambling; Games; General News; Hate Speech; Humor; Investing; Job Search; Lifestyle; Mature; MP3 Sites; Nudity; On-line Sales; Personal Pages; Politics, Opinion & Religion; Portal Sites; Self-Help/Health; Sex; Sports; Travel; Usenet News; and Webmail.

Most importantly, no category definition used by filtering software companies is identical to CIPA's definitions of visual depictions that are obscene, child pornography, or harmful to minors. And category definitions and categorization decisions are made without reference to local community standards. Moreover, there is no judicial involvement in the creation of filtering software companies' category definitions and no judicial determination is made before these companies categorize a Web page or site.

Each filtering software company associates each URL in its control list with a "tag" or other identifier that indicates the company's evaluation of whether the content or features of the Web site or page accessed via that URL meets one or more of its category

definitions. If a user attempts to access a Web site or page that is blocked by the filter, the user is immediately presented with a screen that indicates that a block has occurred as a result of the operation of the filtering software. These "denial screens" appear only at the point that a user attempts to access a site or page in an enabled category.

All four of the filtering programs on which evidence was presented allow users to customize the category lists that exist on their own PCs or servers by adding or removing specific URLs. For example, if a public librarian charged with administering a library's Internet terminals comes across a Web site that he or she finds objectionable that is not blocked by the filtering program that his or her library is using, then the librarian may add that URL to a category list that exists only on the library's network, and it would thereafter be blocked under that category. Similarly, a customer may remove individual URLs from category lists. Importantly, however, no one but the filtering companies has access to the complete list of URLs in any category. The actual URLs or IP addresses of the Web sites or pages contained in filtering software vendors' category lists are considered to be proprietary information, and are unavailable for review by customers or the general public, including the proprietors of Web sites that are blocked by filtering software.[6]

Filtering software companies do not generally notify the proprietors of Web sites when they block their sites. The only way to discover which URLs are blocked and which

---

[6] Indeed, we granted leave for N2H2's counsel to intervene in order to object to testimony that would potentially reveal N2H2's trade secrets, which he did on several occasions.

are not blocked by any particular filtering company is by testing individual URLs with filtering software, or by entering URLs one by one into the "URL checker" that most filtering software companies provide on their Web sites. Filtering software companies will entertain requests for recategorization from proprietors of Web sites that discover their sites are blocked. Because new pages are constantly being added to the Web, filtering companies provide their customers with periodic updates of category lists. Once a particular Web page or site is categorized, however, filtering companies generally do not re-review the contents of that page or site unless they receive a request to do so, even though the content on individual Web pages and sites changes frequently.

2. The Methods that Filtering Companies Use to Compile Category Lists

While the way in which filtering programs operate is conceptually straightforward – by comparing a requested URL to a previously compiled list of URLs and blocking access to the content at that URL if it appears on the list – accurately compiling and categorizing URLs to form the category lists is a more complex process that is impossible to conduct with any high degree of accuracy. The specific methods that filtering software companies use to compile and categorize control lists are, like the lists themselves, proprietary information. We will therefore set forth only general information on the various types of methods that all filtering companies deposed in this case use, and the sources of error that are at once inherent in those methods and unavoidable given the current architecture of the Internet and the current state of the art in automated classification systems. We base our understanding of these methods largely on the detailed testimony and expert report of Dr.

Geoffrey Nunberg, which we credit. The plaintiffs offered, and the Court qualified, Nunberg as an expert witness on automated classification systems.[7]

When compiling and categorizing URLs for their category lists, filtering software companies go through two distinct phases. First, they must collect or "harvest" the relevant URLs from the vast number of sites that exist on the Web. Second, they must sort through the URLs they have collected to determine under which of the company's self-defined categories (if any), they should be classified. These tasks necessarily result in a tradeoff between overblocking (i.e., the blocking of content that does not meet the category definitions established by CIPA or by the filtering software companies), and underblocking (i.e., leaving off of a control list a URL that contains content that would meet the category definitions defined by CIPA or the filtering software companies).

a. The "Harvesting" Phase

Filtering software companies, given their limited resources, do not attempt to index or classify all of the billions of pages that exist on the Web. Instead, the set of pages that they attempt to examine and classify is restricted to a small portion of the Web. The companies use a variety of automated and manual methods to identify a universe of Web

---

[7] Geoffrey Nunberg (Ph.D., Linguistics, C.U.N.Y. 1977) is a researcher at the Center for the Study of Language and Information at Stanford University and a Consulting Full Professor of Linguistics at Stanford University. Until 2001, he was also a principal scientist at the Xerox Palo Alto Research Center. His research centers on automated classification systems, with a focus on classifying documents on the Web with respect to their linguistic properties. He has published his research in numerous professional journals, including peer-reviewed journals.

sites and pages to "harvest" for classification. These methods include: entering certain key words into search engines; following links from a variety of online directories (e.g., generalized directories like Yahoo or various specialized directories, such as those that provide links to sexually explicit content); reviewing lists of newly-registered domain names; buying or licensing lists of URLs from third parties; "mining" access logs maintained by their customers; and reviewing other submissions from customers and the public. The goal of each of these methods is to identify as many URLs as possible that are likely to contain content that falls within the filtering companies' category definitions.

The first method, entering certain keywords into commercial search engines, suffers from several limitations. First, the Web pages that may be "harvested" through this method are limited to those pages that search engines have already identified. However, as noted above, a substantial portion of the Web is not even theoretically indexable (because it is not linked to by any previously known page), and only approximately 50% of the pages that are theoretically indexable have actually been indexed by search engines. We are satisfied that the remainder of the indexable Web, and the vast "Deep Web," which cannot currently be indexed, includes materials that meet CIPA's categories of visual depictions that are obscene, child pornography, and harmful to minors. These portions of the Web cannot presently be harvested through the methods that filtering software companies use (except through reporting by customers or by observing users' log files), because they are not linked to other known pages. A user can, however, gain access to a Web site in the unindexed Web or the Deep Web if the Web site's proprietor or some other third party

informs the user of the site's URL. Some Web sites, for example, send out mass email advertisements containing the site's URL, the spamming process we have described above.

Second, the search engines that software companies use for harvesting are able to search text only, not images. This is of critical importance, because CIPA, by its own terms, covers only "visual depictions." 20 U.S.C. § 9134(f)(1)(A)(i); 47 U.S.C. § 254(h)(5)(B)(i). Image recognition technology is immature, ineffective, and unlikely to improve substantially in the near future. None of the filtering software companies deposed in this case employs image recognition technology when harvesting or categorizing URLs. Due to the reliance on automated text analysis and the absence of image recognition technology, a Web page with sexually explicit images and no text cannot be harvested using a search engine. This problem is complicated by the fact that Web site publishers may use image files rather than text to represent words, i.e., they may use a file that computers understand to be a picture, like a photograph of a printed word, rather than regular text, making automated review of their textual content impossible. For example, if the Playboy Web site displays its name using a logo rather than regular text, a search engine would not see or recognize the Playboy name in that logo.

In addition to collecting URLs through search engines and Web directories (particularly those specializing in sexually explicit sites or other categories relevant to one of the filtering companies' category definitions), and by mining user logs and collecting URLs submitted by users, the filtering companies expand their list of harvested URLs by using "spidering" software that can "crawl" the lists of pages produced by the previous four

methods, following their links downward to bring back the pages to which they link (and the pages to which those pages link, and so on, but usually down only a few levels). This spidering software uses the same type of technology that commercial Web search engines use.

While useful in expanding the number of relevant URLs, the ability to retrieve additional pages through this approach is limited by the architectural feature of the Web that page-to-page links tend to converge rather than diverge. That means that the more pages from which one spiders downward through links, the smaller the proportion of new sites one will uncover; if spidering the links of 1000 sites retrieved through a search engine or Web directory turns up 500 additional distinct adult sites, spidering an additional 1000 sites may turn up, for example, only 250 additional distinct sites, and the proportion of new sites uncovered will continue to diminish as more pages are spidered.

These limitations on the technology used to harvest a set of URLs for review will necessarily lead to substantial underblocking of material with respect to both the category definitions employed by filtering software companies and CIPA's definitions of visual depictions that are obscene, child pornography, or harmful to minors.

b. The "Winnowing" or Categorization Phase

Once the URLs have been harvested, some filtering software companies use automated key word analysis tools to evaluate the content and/or features of Web sites or pages accessed via a particular URL and to tentatively prioritize or categorize them. This process may be characterized as "winnowing" the harvested URLs. Automated systems

currently used by filtering software vendors to prioritize, and to categorize or tentatively categorize the content and/or features of a Web site or page accessed via a particular URL operate by means of (1) simple key word searching, and (2) the use of statistical algorithms that rely on the frequency and structure of various linguistic features in a Web page's text. The automated systems used to categorize pages do not include image recognition technology. All of the filtering companies deposed in the case also employ human review of some or all collected Web pages at some point during the process of categorizing Web pages. As with the harvesting process, each technique employed in the winnowing process is subject to limitations that can result in both overblocking and underblocking.

First, simple key-word-based filters are subject to the obvious limitation that no string of words can identify all sites that contain sexually explicit content, and most strings of words are likely to appear in Web sites that are not properly classified as containing sexually explicit content. As noted above, filtering software companies also use more sophisticated automated classification systems for the statistical classification of texts. These systems assign weights to words or other textual features and use algorithms to determine whether a text belongs to a certain category. These algorithms sometimes make reference to the position of a word within a text or its relative proximity to other words. The weights are usually determined by machine learning methods (often described as "artificial intelligence"). In this procedure, which resembles an automated form of trial and error, a system is given a "training set" consisting of documents preclassified into two or more groups, along with a set of features that might be potentially useful in classifying the

sets. The system then "learns" rules that assign weights to those features according to how well they work in classification, and assigns each new document to a category with a certain probability.

Notwithstanding their "artificial intelligence" description, automated text classification systems are unable to grasp many distinctions between types of content that would be obvious to a human. And of critical importance, no presently conceivable technology can make the judgments necessary to determine whether a visual depiction fits the legal definitions of obscenity, child pornography, or harmful to minors.

Finally, all the filtering software companies deposed in this case use some form of human review in their process of winnowing and categorizing Web pages, although one company admitted to categorizing some Web pages without any human review. SmartFilter states that "the final categorization of every Web site is done by a human reviewer." Another filtering company asserts that of the 10,000 to 30,000 Web pages that enter the "work queue" to be categorized each day, two to three percent of those are automatically categorized by their PornByRef system (which only applies to materials classified in the pornography category), and the remainder are categorized by human review. SurfControl also states that no URL is ever added to its database without human review.

Human review of Web pages has the advantage of allowing more nuanced, if not more accurate, interpretations than automated classification systems are capable of making, but suffers from its own sources of error. The filtering software companies involved here have limited staff, of between eight and a few dozen people, available for hand reviewing

Web pages. The reviewers that are employed by these companies base their categorization decisions on both the text and the visual depictions that appear on the sites or pages they are assigned to review. Human reviewers generally focus on English language Web sites, and are generally not required to be multi-lingual.

Given the speed at which human reviewers must work to keep up with even a fraction of the approximately 1.5 million pages added to the publicly indexable Web each day, human error is inevitable. Errors are likely to result from boredom or lack of attentiveness, overzealousness, or a desire to "err on the side of caution" by screening out material that might be offensive to some customers, even if it does not fit within any of the company's category definitions. None of the filtering companies trains its reviewers in the legal definitions concerning what is obscene, child pornography, or harmful to minors, and none instructs reviewers to take community standards into account when making categorization decisions.

Perhaps because of limitations on the number of human reviewers and because of the large number of new pages that are added to the Web every day, filtering companies also widely engage in the practice of categorizing entire Web sites at the "root URL," rather than engaging in a more fine-grained analysis of the individual pages within a Web site. For example, the filtering software companies deposed in this case all categorize the entire Playboy Web site as Adult, Sexually Explicit, or Pornography. They do not differentiate between pages within the site containing sexually explicit images or text, and for example, pages containing no sexually explicit content, such as the text of interviews of

celebrities or politicians. If the "root" or "top-level" URL of a Web site is given a category tag, then access to all content on that Web site will be blocked if the assigned category is enabled by a customer.

In some cases, whole Web sites are blocked because the filtering companies focus only on the content of the home page that is accessed by entering the root URL. Entire Web sites containing multiple Web pages are commonly categorized without human review of each individual page on that site. Web sites that may contain multiple Web pages and that require authentication or payment for access are commonly categorized based solely on a human reviewer's evaluation of the pages that may be viewed prior to reaching the authentication or payment page.

Because there may be hundreds or thousands of pages under a root URL, filtering companies make it their primary mission to categorize the root URL, and categorize subsidiary pages if the need arises or if there is time. This form of overblocking is called "inheritance," because lower-level pages inherit the categorization of the root URL without regard to their specific content. In some cases, "reverse inheritance" also occurs, i.e., parent sites inherit the classification of pages in a lower level of the site. This might happen when pages with sexual content appear in a Web site that is devoted primarily to non-sexual content. For example, N2H2's Bess filtering product classifies every page in the Salon.com Web site, which contains a wide range of news and cultural commentary, as "Sex, Profanity," based on the fact that the site includes a regular column that deals with sexual issues.

Blocking by both domain name and IP address is another practice in which filtering companies engage that is a function both of the architecture of the Web and of the exigencies of dealing with the rapidly expanding number of Web pages. The category lists maintained by filtering software companies can include URLs in either their human-readable domain name address form, their numeric IP address form, or both. Through "virtual hosting" services, hundreds of thousands of Web sites with distinct domain names may share a single numeric IP address. To the extent that filtering companies block the IP addresses of virtual hosting services, they will necessarily block a substantial amount of content without reviewing it, and will likely overblock a substantial amount of content.

Another technique that filtering companies use in order to deal with a structural feature of the Internet is blocking the root level URLs of so-called "loophole" Web sites. These are Web sites that provide access to a particular Web page, but display in the user's browser a URL that is different from the URL with which the particular page is usually associated. Because of this feature, they provide a "loophole" that can be used to get around filtering software, i.e., they display a URL that is different from the one that appears on the filtering company's control list. "Loophole" Web sites include caches of Web pages that have been removed from their original location, "anonymizer" sites, and translation sites.

Caches are archived copies that some search engines, such as Google, keep of the Web pages they index. The cached copy stored by Google will have a URL that is different from the original URL. Because Web sites often change rapidly, caches are the only way to

access pages that have been taken down, revised, or have changed their URLs for some reason. For example, a magazine might place its current stories under a given URL, and replace them monthly with new stories. If a user wanted to find an article published six months ago, he or she would be unable to access it if not for Google's cached version.

Some sites on the Web serve as a proxy or intermediary between a user and another Web page. When using a proxy server, a user does not access the page from its original URL, but rather from the URL of the proxy server. One type of proxy service is an "anonymizer." Users may access Web sites indirectly via an anonymizer when they do not want the Web site they are visiting to be able to determine the IP address from which they are accessing the site, or to leave "cookies" on their browser.[8] Some proxy servers can be used to attempt to translate Web page content from one language to another. Rather than directly accessing the original Web page in its original language, users can instead indirectly access the page via a proxy server offering translation features.

As noted above, filtering companies often block loophole sites, such as caches, anonymizers, and translation sites. The practice of blocking loophole sites necessarily results in a significant amount of overblocking, because the vast majority of the pages that are cached, for example, do not contain content that would match a filtering company's

---

[8] A "cookie" is "a small file or part of a file stored on a World Wide Web user's computer, created and subsequently read by a Web site server, and containing personal information (as a user identification code, customized preferences, or a record of pages visited)." *Merriam-Webster's Collegiate Dictionary*, *available at* http://www.m-w.com/dictionary.htm.

category definitions. Filters that do not block these loophole sites, however, may enable users to access any URL on the Web via the loophole site, thus resulting in substantial underblocking.

c. The Process for "Re-Reviewing" Web Pages After Their Initial Categorization

Most filtering software companies do not engage in subsequent reviews of categorized sites or pages on a scheduled basis. Priority is placed on reviewing and categorizing new sites and pages, rather than on re-reviewing already categorized sites and pages. Typically, a filtering software vendor's previous categorization of a Web site is not re-reviewed for accuracy when new pages are added to the Web site. To the extent the Web site was previously categorized as a whole, the new pages added to the site usually share the categorization assigned by the blocking product vendor. This necessarily results in both over- and underblocking, because, as noted above, the content of Web pages and Web sites changes relatively rapidly.

In addition to the content on Web sites or pages changing rapidly, Web sites themselves may disappear and be replaced by sites with entirely different content. If an IP address associated with a particular Web site is blocked under a particular category and the Web site goes out of existence, then the IP address likely would be reassigned to a different Web site, either by an Internet service provider or by a registration organization, such as the American Registry for Internet Numbers, *see* http://www.arin.net. In that case, the site that received the reassigned IP address would likely be miscategorized. Because filtering companies do not engage in systematic re-review of their category lists, such a

site would likely remain miscategorized unless someone submitted it to the filtering company for re-review, increasing the incidence of over- and underblocking.

This failure to re-review Web pages primarily increases a filtering company's rate of overblocking. However, if a filtering company does not re-review Web pages after it determines that they do not fall into any of its blocking categories, then that would result in underblocking (because, for example, a page might add sexually explicit content).

3. The Inherent Tradeoff Between Overblocking and Underblocking

There is an inherent tradeoff between any filter's rate of overblocking (which information scientists also call "precision") and its rate of underblocking (which is also referred to as "recall"). The rate of overblocking or precision is measured by the proportion of the things a classification system assigns to a certain category that are appropriately classified. The plaintiffs' expert, Dr. Nunberg, provided the hypothetical example of a classification system that is asked to pick out pictures of dogs from a database consisting of 1000 pictures of animals, of which 80 were actually dogs. If it returned 100 hits, of which 80 were in fact pictures of dogs, and the remaining 20 were pictures of cats, horses, and deer, we would say that the system identified dog pictures with a precision of 80%. This would be analogous to a filter that overblocked at a rate of 20%.

The recall measure involves determining what proportion of the actual members of a category the classification system has been able to identify. For example, if the hypothetical animal-picture database contained a total of 200 pictures of dogs, and the system identified 80 of them and failed to identify 120, it would have performed with a

recall of 40%. This would be analogous to a filter that underblocked 60% of the material in a category.

In automated classification systems, there is always a tradeoff between precision and recall. In the animal-picture example, the recall could be improved by using a looser set of criteria to identify the dog pictures in the set, such as any animal with four legs, and all the dogs would be identified, but cats and other animals would also be included, with a resulting loss of precision. The same tradeoff exists between rates of overblocking and underblocking in filtering systems that use automated classification systems. For example, an automated system that classifies any Web page that contains the word "sex" as sexually explicit will underblock much less, but overblock much more, than a system that classifies any Web page containing the phrase "free pictures of people having sex" as sexually explicit.

This tradeoff between overblocking and underblocking also applies not just to automated classification systems, but also to filters that use only human review. Given the approximately two billion pages that exist on the Web, the 1.5 million new pages that are added daily, and the rate at which content on existing pages changes, if a filtering company blocks only those Web pages that have been reviewed by humans, it will be impossible, as a practical matter, to avoid vast amounts of underblocking. Techniques used by human reviewers such as blocking at the IP address level, domain name level, or directory level reduce the rates of underblocking, but necessarily increase the rates of overblocking, as discussed above.

To use a simple example, it would be easy to design a filter intended to block sexually explicit speech that completely avoids overblocking. Such a filter would have only a single sexually explicit Web site on its control list, which could be re-reviewed daily to ensure that its content does not change. While there would be no overblocking problem with such a filter, such a filter would have a severe underblocking problem, as it would fail to block all the sexually explicit speech on the Web other than the one site on its control list. Similarly, it would also be easy to design a filter intended to block sexually explicit speech that completely avoids underblocking. Such a filter would operate by permitting users to view only a single Web site, e.g., the Sesame Street Web site. While there would be no underblocking problem with such a filter, it would have a severe overblocking problem, as it would block access to millions of non-sexually explicit sites on the Web other than the Sesame Street site.

While it is thus quite simple to design a filter that does not overblock, and equally simple to design a filter that does not underblock, it is currently impossible, given the Internet's size, rate of growth, rate of change, and architecture, and given the state of the art of automated classification systems, to develop a filter that neither underblocks nor overblocks a substantial amount of speech. The more effective a filter is at blocking Web sites in a given category, the more the filter will necessarily overblock. Any filter that is reasonably effective in preventing users from accessing sexually explicit content on the Web will necessarily block substantial amounts of non-sexually explicit speech.

4. Attempts to Quantify Filtering Programs' Rates of Over- and Underblocking

The government presented three studies, two from expert witnesses, and one from a librarian fact witness who conducted a study using Internet use logs from his own library, that attempt to quantify the over- and underblocking rates of five different filtering programs. The plaintiffs presented one expert witness who attempted to quantify the rates of over- and underblocking for various programs. Each of these attempts to quantify rates of over- and underblocking suffers from various methodological flaws.

The fundamental problem with calculating over- and underblocking rates is selecting a universe of Web sites or Web pages to serve as the set to be tested. The studies that the parties submitted in this case took two different approaches to this problem. Two of the studies, one prepared by the plaintiffs' expert witness Chris Hunter, a graduate student at the University of Pennsylvania, and the other prepared by the defendants' expert, Chris Lemmons of eTesting Laboratories, in Research Triangle Park, North Carolina, approached this problem by compiling two separate lists of Web sites, one of URLs that they deemed should be blocked according to the filters' criteria, and another of URLs that they deemed should not be blocked according to the filters' criteria. They compiled these lists by choosing Web sites from the results of certain key word searches.[9] The problem with this

---

[9] Hunter drew three different "samples" for his test. The first consisted of "50 randomly generated Web pages from the Webcrawler search engine." The "second sample of 50 Web pages was drawn from searches for the terms 'yahoo, warez, hotmail, sex, and MP3,' using the AltaVista.com search engine." And the "final sample of 100 Web sites was drawn from the sites of organizations who filed amicus briefs in support of the ACLU's challenges to the Community [sic] Decency Act (CDA) and COPA [the Children's Online Protection Act], and from Internet portals, political Web sites, feminist Web sites, hate speech sites, gambling sites, religious sites, gay pride/homosexual sites, alcohol, tobacco,

selection method is that it is neither random, nor does it necessarily approximate the universe of Web pages that library patrons visit.

The two other studies, one by David Biek, head librarian at the Tacoma Public Library's main branch, and one by Cory Finnell of Certus Consulting Group, of Seattle, Washington, chose actual logs of Web pages visited by library patrons during specific time periods as the universe of Web pages to analyze. This method, while surely not as accurate as a truly random sample of the indexed Web would be (assuming it would be possible to take such a sample), has the virtue of using the actual Web sites that library patrons visited during a specific period. Because library patrons selected the universe of Web sites that Biek and Finnell's studies analyzed, this removes the possibility of bias resulting from the study author's selection of the universe of sites to be reviewed. We find that the Lemmons and Hunter studies are of little probative value because of the methodology used to select

---

and drug sites, pornography sites, new sites, violent game sites, safe sex sites, and pro and anti-abortion sites listed on the popular Web directory, Yahoo.com."

Lemmons testified that he compiled the list of sexually explicit sites that should have been blocked by entering the terms "free adult sex, anal sex, oral sex, fisting lesbians, gay sex, interracial sex, big tits, blow job, shaved pussy, and bondage" into the Google search engine and then "surfing" through links from pages generated by the list of sites that the search engine returned. Using this method, he compiled a list of 197 sites that he determined should be blocked according to the filtering programs' category definitions. Lemmons also attempted to compile a list of "sensitive" Web sites that, although they should not have been blocked according to the filtering programs' category definitions, might have been mistakenly blocked. In order to do this, he used the same method of entering terms into the Google search engine and surfing through the results. He used the following terms to compile this list: "breast feeding, bondages, fetishes, ebony, gay issues, women's health, lesbian, homosexual, vagina, vaginal dryness, pain, anal cancer, teen issues, safe sex, penis, pregnant, interracial, sex education, penis enlargement, breast enlargement, . . . and shave."

the sample universe of Web sites to be tested. We will therefore focus on the studies conducted by Finnell and Biek in trying to ascertain estimates of the rates of over- and underblocking that takes place when filters are used in public libraries.

The government hired expert witness Cory Finnell to study the Internet logs compiled by the public libraries systems in Tacoma, Washington; Westerville, Ohio; and Greenville, South Carolina. Each of these libraries uses filtering software that keeps a log of information about individual Web site requests made by library patrons. Finnell, whose consulting firm specializes in data analysis, has substantial experience evaluating Internet access logs generated on networked systems. He spent more than a year developing a reporting tool for N2H2, and, in the course of that work, acquired a familiarity with the design and operation of Internet filtering products.

The Tacoma library uses Cyber Patrol filtering software, and logs information only on sites that were blocked. Finnell worked from a list of all sites that were blocked in the Tacoma public library in the month of August 2001. The Westerville library uses the Websense filtering product, and logs information on both blocked sites and non-blocked sites. When the logs reach a certain size, they are overwritten by new usage logs. Because of this overwriting feature, logs were available to Finnell only for the relatively short period from October 1, 2001 to October 3, 2001. The Greenville library uses N2H2's filtering product and logs both blocked sites and sites that patrons accessed. The logs contain more than 500,000 records per day. Because of the volume of the records, Finnell restricted his analysis to the period from August 2, 2001 to August 15, 2001.

Finnell calculated an overblocking rate for each of the three libraries by examining the host Web site containing each of the blocked pages. He did not employ a sampling technique, but instead examined each blocked Web site. If the contents of a host Web site or the pages within the Web site were consistent with the filtering product's definition of the category under which the site was blocked, Finnell considered it to be an accurate block. Finnell and three others, two of whom were temporary employees, examined the Web sites to determine whether they were consistent with the filtering companies' category definitions. Their review was, of course, necessarily limited by: (1) the clarity of the filtering companies' category definitions; (2) Finnell's and his employees' interpretations of the definitions; and (3) human error. The study's reliability is also undercut by the fact that Finnell failed to archive the blocked Web pages as they existed either at the point that a patron in one of the three libraries was denied access or when Finnell and his team reviewed the pages. It is therefore impossible for anyone to check the accuracy and consistency of Finnell's review team, or to know whether the pages contained the same content when the block occurred as they did when Finnell's team reviewed them. This is a key flaw, because the results of the study depend on individual determinations as to overblocking and underblocking, in which Finnell and his team were required to compare what they saw on the Web pages that they reviewed with standard definitions provided by the filtering company.

Tacoma library's Cyber Patrol software blocked 836 unique Web sites during the month of August. Finnell determined that 783 of those blocks were accurate and that 53

were inaccurate.[10] The error rate for Cyber Patrol was therefore estimated to be 6.34%, and the true error rate was estimated with 95% confidence to lie within the range of 4.69% to 7.99%.[11] Finnell and his team reviewed 185 unique Web sites that were blocked by Westerville Library's Websense filter during the logged period and determined that 158 of them were accurate and that 27 of them were inaccurate. He therefore estimated the Websense filter's overblocking rate at 14.59% with a 95% confidence interval of 9.51% to 19.68%. Additionally, Finnell examined 1,674 unique Web sites that were blocked by the Greenville Library's N2H2 filter during the relevant period and determined that 1,520 were accurate and that 87 were inaccurate. This yields an estimated overblocking rate of 5.41% and a 95% confidence interval of 4.33% to 6.55%.

Finnell's methodology was materially flawed in that it understates the rate of overblocking for the following reasons. First, patrons from the three libraries knew that the filters were operating, and may have been deterred from attempting to access Web sites that they perceived to be "borderline" sites, i.e., those that may or may not have been

---

[10] If separate patrons attempted to reach the same Web site, or one or more patrons attempted to access more than one page on a single Web site, Finnell counted these attempts as a single block. For example, the total number of blocked requests for Web pages at Tacoma Library during the logged period was 2,812, but Finnell counted this as only 895 blocks of unique Web sites. Of the 895 unique blocked sites, Finnell was unable to access 59, yielding 836 unique blocked sites for his team to review.

[11] The confidence intervals that Finnell calculated represent the range of percentages within which we can be 95% confident that the actual rate of overblocking in that particular library falls. We note that these confidence intervals assume that the time period for which the study assessed the library's internet logs constitutes a random and representative sample.

appropriately filtered according to the filtering companies' category definitions. Second, in their cross-examination of Finnell, the plaintiffs offered screen shots of a number of Web sites that, according to Finnell, had been appropriately blocked, but that Finnell admitted contained only benign materials. Finnell's explanation was that the Web sites must have changed between the time when he conducted the study and the time of the trial, but because he did not archive the images as they existed when his team reviewed them for the study, there is no way to verify this. Third, because of the way in which Finnell counted blocked Web sites – i.e., if separate patrons attempted to reach the same Web site, or one or more patrons attempted to access more than one page on a single Web site, Finnell counted these attempts as a single block, *see supra* note 10 – his results necessarily understate the number of times that patrons were erroneously denied access to information.

At all events, there is no doubt that Finnell's estimated rates of overblocking, which are based on the filtering companies' own category definitions, significantly understate the rate of overblocking with respect to CIPA's category definitions for filtering for adults. The filters used in the Tacoma, Westerville, and Greenville libraries were configured to block, among other things, images of full nudity and sexually explicit materials. There is no dispute, however, that these categories are far broader than CIPA's categories of visual depictions that are obscene, or child pornography, the two categories of material that libraries subject to CIPA must certify that they filter during adults' use of the Internet.

Finnell's study also calculated underblocking rates with respect to the Westerville

and Greenville Libraries (both of which logged not only their blocked sites, but all sites visited by their patrons), by taking random samples of URLs from the list of sites that were not blocked. The study used a sample of 159 sites that were accessed by Westerville patrons and determined that only one of them should have been blocked under the software's category definitions, yielding an underblocking rate of 0.6%. Given the size of the sample, the 95% confidence interval is 0% to 1.86%. The study examined a sample of 254 Web sites accessed by patrons in Greenville and found that three of them should have been blocked under the filtering software's category definitions. This results in an estimated underblocking rate of 1.2% with a 95% confidence interval ranging from 0% to 2.51%.

We do not credit Finnell's estimates of the rates of underblocking in the Westerville and Greenville public libraries for several reasons. First, Finnell's estimates likely understate the actual rate of underblocking because patrons, who knew that filtering programs were operating in the Greenville and Westerville Libraries, may have refrained from attempting to access sites with sexually explicit materials, or other contents that they knew would probably meet a filtering program's blocked categories. Second, and most importantly, we think that the formula that Finnell used to calculate the rate of underblocking in these two libraries is not as meaningful as the formula that information scientists typically use to calculate a rate of recall, which we describe above in Subsection II.E.3. As Dr. Nunberg explained, the standard method that information scientists use to calculate a rate of recall is to sort a set of items into two groups, those that fall into a

particular category (e.g., those that should have been blocked by a filter) and those that do not. The rate of recall is then calculated by dividing the number of items that the system correctly identified as belonging to the category by the total number of items in the category.

In the example above, we discussed a database that contained 1000 photographs. Assume that 200 of these photographs were pictures of dogs. If, for example, a classification system designed to identify pictures of dogs identified 80 of the dog pictures and failed to identify 120, it would have performed with a recall rate of 40%. This would be analogous to a filter that underblocked at a rate of 60%. To calculate the recall rate of the filters in the Westerville and Greenville public libraries in accordance with the standard method described above, Finnell should have taken a sample of sites from the libraries' Internet use logs (including both sites that were blocked and sites that were not), and divided the number of sites in the sample that the filter incorrectly failed to block by the total number of sites in the sample that should have been blocked. What Finnell did instead was to take a sample of sites that were not blocked, and divide the total number of sites in this sample by the number of sites in the sample that should have been blocked. This made the denominator that Finnell used much larger than it would have been had he used the standard method for calculating recall, consequently making the underblocking rate that he calculated much lower than it would have been under the standard method.[12]

---

[12] To illustrate the two different methods, consider a random sample of 1010 web sites taken from a library's Internet use log, 10 of which fall within the category that a filter is

Moreover, despite the relatively low rates of underblocking that Finnell's study found, librarians from several of the libraries proffered by defendants that use blocking products, including Greenville, Tacoma, and Westerville, testified that there are instances of underblocking in their libraries. No quantitative evidence was presented comparing the effectiveness of filters and other alternative methods used by libraries to prevent patrons from accessing visual depictions that are obscene, child pornography, or in the case of minors, harmful to minors.

Biek undertook a similar study of the overblocking rates that result from the Tacoma Library's use of the Cyber Patrol software. He began with the 3,733 individual blocks that occurred in the Tacoma Library in October 2000 and drew from this data set a random sample of 786 URLs. He calculated two rates of overblocking, one with respect to the Tacoma Library's policy on Internet use – that the pictorial content of the site may not include "graphic materials depicting full nudity and sexual acts which are portrayed obviously and exclusively for sensational or pornographic purposes" – and the other with respect to Cyber Patrol's own category definitions. He estimated that Cyber Patrol

---

intended to block (e.g., pornography), and suppose that the filter incorrectly failed to block 2 of the 10 sites that it should have blocked and did not block any sites that should not have been blocked. The standard method of quantifying the rate of underblocking would divide the number of sites in the sample that the filter incorrectly failed to block by the number of sites in the sample that the filter should have blocked, yielding an underblocking rate in this example of 20%. Finnell's study, however, calculated the underblocking rate by dividing the number of sites that the filter incorrectly failed to block by the total number of sites in the sample that were not blocked (whether correctly or incorrectly) yielding an underblocking rate in this example of only .2%.

overblocked 4% of all Web pages in October 2000 with respect to the definitions of the Tacoma Library's Internet Policy and 2% of all pages with respect to Cyber Patrol's own category definitions.[13]

It is difficult to determine how reliable Biek's conclusions are, because he did not keep records of the raw data that he used in his study; nor did he archive images of the Web pages as they looked when he made the determination whether they were properly classified by the Cyber Patrol program. Without this information, it is impossible to verify his conclusions (or to undermine them). And Biek's study certainly understates Cyber Patrol's overblocking rate for some of the same reasons that Finnell's study likely understates the true rates of overblocking used in the libraries that he studied.

We also note that Finnell's study, which analyzed a set of Internet logs from the Tacoma Library during which the same filtering program was operating with the same set of blocking categories enabled, found a significantly higher rate of overblocking than the Biek study did. Biek found a rate of overblocking of approximately 2% while the Finnell study estimated a 6.34% rate of overblocking. At all events, the category definitions employed by CIPA, at least with respect to adult use – visual depictions that are obscene or child pornography – are narrower than the materials prohibited by the Tacoma Library policy, and therefore Biek's study understates the rate of overblocking with respect to CIPA's definitions for adults.

---

[13] According to Biek, the sample size that he used yielded a 95% confidence interval of plus or minus 3.11%.

In sum, we think that Finnell's study, while we do not credit its estimates of underblocking, is useful because it states lower bounds with respect to the rates of overblocking that occurred when the Cyber Patrol, Websense, and N2H2 filters were operating in public libraries. While these rates are substantial – between nearly 6% and 15% – we think, for the reasons stated above, that they greatly understate the actual rates of overblocking that occurs, and therefore cannot be considered as anything more than minimum estimates of the rates of overblocking that happens in all filtering programs.

5. Methods of Obtaining Examples of Erroneously Blocked Web Sites

The plaintiffs assembled a list of several thousand Web sites that they contend were, at the time of the study, likely to have been erroneously blocked by one or more of four major commercial filtering programs: SurfControl Cyber Patrol 6.0.1.47, N2H2 Internet Filtering 2.0, Secure Computing SmartFilter 3.0.0.01, and Websense Enterprise 4.3.0. They compiled this list using a two-step process. First, Benjamin Edelman, an expert witness who testified before us, compiled a list of more than 500,000 URLs and devised a program to feed them through all four filtering programs in order to compile a list of URLs that might have been erroneously blocked by one or more of the programs.[14] Second, Edelman forwarded subsets of the list that he compiled to librarians and professors of library science whom the plaintiffs had hired to review the blocked sites for suitability in

[14] Edelman is a Harvard University student and a systems administrator and multimedia specialist at the Berkman Center for Internet and Society at Harvard Law School. Despite Edelman's young age, he has been doing consulting work on Internet-related issues for nine years, since he was in junior high school.

the public library context.

Edelman assembled the list of URLs by compiling Web pages that were blocked by the following categories in the four programs: Cyber Patrol: Adult/Sexually Explicit; N2H2: Adults Only, Nudity, Pornography, and Sex, with "exceptions" engaged in the categories of Education, For Kids, History, Medical, Moderated, and Text/Spoken Only; SmartFilter: Sex, Nudity, Mature, and Extreme; Websense: Adult Content, Nudity, and Sex.

Edelman then assembled a database of Web sites for possible testing. He derived this list by automatically compiling URLs from the Yahoo index of Web sites, taking them from categories from the Yahoo index that differed significantly from the classifications that he had enabled in each of the blocking programs (taking, for example, Web sites from Yahoo's "Government" category). He then expanded this list by entering URLs taken from the Yahoo index into the Google search engine's "related" search function, which provides the user with a list of similar sites. Edelman also included and excluded specific Web sites at the request of the plaintiffs' counsel.

Taking the list of more than 500,000 URLs that he had compiled, Edelman used an automated system that he had developed to test whether particular URLs were blocked by each of the four filtering programs. This testing took place between February and October 2001. He recorded the specific dates on which particular sites were blocked by particular programs, and, using commercial archiving software, archived the contents of the home page of the blocked Web sites (and in some instances the pages linked to from the home

page) as it existed when it was blocked.[15] Through this process, Edelman, whose testimony we credit, compiled a list of 6,777 URLs that were blocked by one or more of the four programs. Because these sites were chosen from categories from the Yahoo directory that were unrelated to the filtering categories that were enabled during the test (i.e., "Government" vs. "Nudity"), he reasoned that they were likely erroneously blocked. As explained in the margin, Edelman repeated his testing and discovered that Cyber Patrol had unblocked most of the pages on the list of 6,777 after he had published the list on his Web site. His records indicate that an employee of SurfControl (the company that produces Cyber Patrol software) accessed his site and presumably checked out the URLs on the list, thus confirming Edelman's judgment that the majority of URLs on the list were erroneously blocked.[16]

Edelman forwarded the list of blocked sites to Dr. Joseph Janes, an Assistant

---

[15] The archiving process in some cases took up to 48 hours from when the page was blocked.

[16] In October 2001, Edelman published the results of his initial testing on his Web site. In February and March 2002 he repeated his testing of the 6,777 URLs originally found to be blocked by at least one of the blocking products, in order to determine whether and to what extent the blocking product vendors had corrected the mistakes that he publicized. Of those URLs blocked by N2H2 in the October 2001 testing, 55.10% remained blocked when tested by Edelman in March 2002. Of those URLs blocked by Websense in the October 2001 testing, 76.28% remained blocked when tested by Edelman in February 2002. Of those URLs blocked by SurfControl's Cyber Patrol product, only 7.16% remained blocked, i.e., Cyber Patrol had unblocked almost 93% of the Web pages originally blocked. Because the results posted to his Web site were accessed by an employee of SurfControl (as evidenced by Edelman's records of who was accessing his Web site), we infer that Cyber Patrol had determined that 93% of all 6,777 pages, or 6,302 Web pages, were originally wrongly blocked by the product.

Professor in the Information School of the University of Washington who also testified at trial as an expert witness. Janes reviewed the sites that Edelman compiled to determine whether they are consistent with library collection development, i.e., whether they are sites to which a reference librarian would, consistent with professional standards, direct a patron as a source of information.[17]

Edelman forwarded Janes a list of 6,775 Web sites, almost the entire list of blocked sites that he collected, from which Janes took a random sample of 859 using the SPSS statistical software package. Janes indicated that he chose a sample size of 859 because it would yield a 95% confidence interval of plus or minus 2.5%. Janes recruited a group of 16 reviewers, most of whom were current or former students at the University of

---

[17] Two other expert witnesses reviewed subsets of the list of Web pages that Edelman compiled. Dr. Michael T. Ryan, Director of the Rare Book and Manuscript Library and of the Center for Electronic Text and Image at the University of Pennsylvania, reviewed a list of 204 sites that Edelman forwarded to him in order to determine their appropriateness and usefulness in the library setting. Because the sites that Ryan reviewed were not selected randomly (i.e., they were chosen by plaintiffs' counsel), his study says little about the character of the set of 6,777 sites that Edelman compiled, or the total amount of overblocking by the four filtering programs that Edelman used.

Anne Lipow, a practicing librarian for more than 30 years and the director of a library consulting firm, also reviewed the same list of 204 URLs from the set that Edelman had collected for their appropriateness for a library's collection. She categorized sites in four different levels according to their appropriateness for a public library's collection. Again, because these URLs were not selected randomly, Lipow's study is not particularly relevant to the total set that Edelman compiled, or to the total amount of overblocking by the four filtering programs that Edelman used.

Although the methodology used to select the list of Web pages that was forwarded to Ryan and Lipow is problematic, Ryan's and Lipow's testimony established that many of the erroneously blocked sites that Edelman identified would be useful and appropriate sources of information for library patrons.

Washington's Information School, to help him identify which sites were appropriate for library use. We describe the process that he used in the margin.[18] Due to

---

[18] All of the reviewers that Janes recruited had some relevant experience in library reference services or library collection development. Janes divided the reviewers into two groups, a group of 11 less experienced reviewers, and a group of five more experienced reviewers. Janes assigned the less experienced group to do a first-round review with the purpose of identifying the most obviously overblocked sites. The more experienced group was to review the remaining sites (i.e., those that were not obviously overblocked) and to make final decisions regarding these sites.

In the first round, each person evaluated two sets of around 80 sites, and each group was evaluated by two different people. Each set of sites included the following instructions:

Look carefully at each of the Web sites on the list. Please make a notation of any site that appears to meet **any** of the following criteria:

> a. Contains information similar to that already found in libraries,
>
> **or**
>
> b. Contains information a librarian would want in the library if s/he had unlimited funds to purchase information and unlimited shelf space,
>
> **or**
>
> c. You would be willing to refer a patron (of any age) to the site if the patron appeared at a reference desk seeking information about the subject of the site. For this last criterion, we recognize that you might not refer a young child to a Calculus site just because it would not be useful to that child, but you should ignore that factor. Informational sites, such as a Calculus site, should be noted. A site that is purely erotica should not be noted.

Sites that received "Yes" votes from both reviewers were determined to be of sufficient interest in a library context and removed from further analysis. Sites receiving one or two "No" votes would go to the next round. In the first round, 243 sites received "Yes" votes from both reviewers, while 456 sites received one or more "No" votes or could not be found. These 456 sites were sent forward to the second round of judging.

The instructions for the second-round reviewers were the same as those given to the

the inability of a member of Janes's review team to complete the reviewing process, Janes had to cut 157 Web sites out of the sample, but because the Web sites were randomly assigned to reviewers, it is unlikely that these sites differed significantly from the rest of the sample. That left the sample size at 699, which widened the 95% confidence interval to plus or minus 2.8%.

Of the total 699 sites reviewed, Janes's team concluded that 165 of them, or 23.6% percent of the sample, were not of any value in the library context (i.e., no librarian would, consistent with professional standards, refer a patron to these sites as a source of information). They were unable to find 60 of the Web sites, or 8.6% of the sample. Therefore, they concluded that the remaining 474 Web sites, or 67.8% of the sample, were examples of overblocking with respect to materials that are appropriate sources of information in public libraries. Applying a 95% confidence interval of plus or minus 2.8%, the study concluded that we can be 95% confident that the actual percentage of sites in the list of 6,775 sites that are appropriate for use in public libraries is somewhere between 65.0% and 70.6%. In other words, we can be 95% certain that the actual number of sites out of the 6,775 that Edelman forwarded to Janes that are appropriate for use in public

---

first-round reviewers, except that in section c, the following sentence was added: "Sites that have a commercial purpose should be included here if they might be of use or interest to someone wishing to buy the product or service or doing research on commercial behavior on the Internet, much as most libraries include the Yellow Pages in their collections." The second round of review produced the following results: 60 sites could not be found (due to broken links, 404 "not found" errors, domain for sale messages, etc.), 231 sites were judged "Yes," and 165 judged "No."

libraries (under Janes's standard) is somewhere between 4,403 and 4,783.

The government raised some valid criticisms of Janes's methodology, attacking in particular the fact that, while sites that received two "yes" votes in the first round of voting were determined to be of sufficient interest in a library context to be removed from further analysis, sites receiving one or two "no" votes were sent to the next round. The government also correctly points out that results of Janes's study can be generalized only to the population of 6,775 sites that Edelman forwarded to Janes. Even taking these criticisms into account, and discounting Janes's numbers appropriately, we credit Janes's study as confirming that Edelman's set of 6,775 Web sites contains at least a few thousand URLs that were erroneously blocked by one or more of the four filtering programs that he used, whether judged against CIPA's definitions, the filters' own category criteria, or against the standard that the Janes study used. Edelman tested only 500,000 unique URLs out of the 4000 times that many, or two billion, that are estimated to exist in the indexable Web. Even assuming that Edelman chose the URLs that were most likely to be erroneously blocked by commercial filtering programs, we conclude that many times the number of pages that Edelman identified are erroneously blocked by one or more of the filtering programs that he tested.

Edelman's and Janes's studies provide numerous specific examples of Web pages that were erroneously blocked by one or more filtering programs. The Web pages that were erroneously blocked by one or more of the filtering programs do not fall into any neat patterns; they range widely in subject matter, and it is difficult to tell why they may have

been overblocked. The list that Edelman compiled, for example, contains Web pages relating to religion, politics and government, health, careers, education, travel, sports, and many other topics. In the next section, we provide examples from each of these categories.

6. Examples of Erroneously Blocked Web Sites

Several of the erroneously blocked Web sites had content relating to churches, religious orders, religious charities, and religious fellowship organizations. These included the following Web sites: the Knights of Columbus Council 4828, a Catholic men's group associated with St. Patrick's Church in Fallon, Nevada, http://msnhomepages.talkcity.com/SpiritSt/kofc4828, which was blocked by Cyber Patrol in the "Adult/Sexually Explicit" category; the Agape Church of Searcy, Arkansas, http://www.agapechurch.com, which was blocked by Websense as "Adult Content"; the home page of the Lesbian and Gay Havurah of the Long Beach, California Jewish Community Center, http://www.compupix.com/gay/havurah.htm, which was blocked by N2H2 as "Adults Only, Pornography," by Smartfilter as "Sex," and by Websense as "Sex"; Orphanage Emmanuel, a Christian orphanage in Honduras that houses 225 children, http://home8.inet.tele.dk/rfb_viva, which was blocked by Cyber Patrol in the "Adult/Sexually Explicit" category; Vision Art Online, which sells wooden wall hangings for the home that contain prayers, passages from the Bible, and images of the Star of David, http://www.visionartonline.com, which was blocked in Websense's "Sex" category; and the home page of Tenzin Palmo, a Buddhist nun, which contained a description of her project to build a Buddhist nunnery and international retreat center for women,

http://www.tenzinpalmo.com, which was categorized as "Nudity" by N2H2.

Several blocked sites also contained information about governmental entities or specific political candidates, or contained political commentary. These included: the Web site for Kelley Ross, a Libertarian candidate for the California State Assembly, http://www.friesian.com/ross/ca40, which N2H2 blocked as "Nudity"; the Web site for Bob Coughlin, a town selectman in Dedham, Massachusetts, http://www.bobcoughlin.org, which was blocked under N2H2's "Nudity" category; a list of Web sites containing information about government and politics in Adams County, Pennsylvania, http://www.geocities.com/adamscopa, which was blocked by Websense as "Sex"; the Web site for Wisconsin Right to Life, http://www.wrtl.org, which N2H2 blocked as "Nudity"; a Web site that promotes federalism in Uganda, http://federo.com, which N2H2 blocked as "Adults Only, Pornography"; "Fight the Death Penalty in the USA," a Danish Web site dedicated to criticizing the American system of capital punishment, http://www.fdp.dk, which N2H2 blocked as "Pornography"; and "Dumb Laws," a humor Web site that makes fun of outmoded laws, http://www.dumblaws.com, which N2H2 blocked under its "Sex" category.

Erroneously blocked Web sites relating to health issues included the following: a guide to allergies, http://www.x-sitez.com/allergy, which was categorized as "Adults Only, Pornography" by N2H2; a health question and answer site sponsored by Columbia University, http://www.goaskalice.com.columbia.edu, which was blocked as "Sex" by N2H2, and as "Mature" by Smartfilter; the Western Amputee Support Alliance Home Page,

http://www.usinter.net/wasa, which was blocked by N2H2 as "Pornography"; the Web site of the Willis-Knighton Cancer Center, a Shreveport, Louisiana cancer treatment facility, http://cancerftr.wkmc.com, which was blocked by Websense under the "Sex" category; and a site dealing with halitosis, http://www.dreamcastle.com/tungs, which was blocked by N2H2 as "Adults, Pornography," by Smartfilter as "Sex," by Cyber Patrol as "Adult/Sexually Explicit," and by Websense as "Adult Content."

The filtering programs also erroneously blocked several Web sites having to do with education and careers. The filtering programs blocked two sites that provide information on home schooling. "HomEduStation – the Internet Source for Home Education," http://www.perigee.net/~mcmullen/homedustation/, was categorized by Cyber Patrol as "Adult/Sexually Explicit." Smartfilter blocked "Apricot: A Web site made by and for home schoolers," http://apricotpie.com, as "Sex." The programs also miscategorized several career-related sites. "Social Work Search," http://www.socialworksearch.com/, is a directory for social workers that Cyber Patrol placed in its "Adult/Sexually Explicit" category. The "Gay and Lesbian Chamber of Southern Nevada," http://www.lambdalv.com, "a forum for the business community to develop relationships within the Las Vegas lesbian, gay, transsexual, and bisexual community" was blocked by N2H2 as "Adults Only, Pornography." A site for aspiring dentists, http://www.vvm.com/~bond/home.htm, was blocked by Cyber Patrol in its "Adult/Sexually Explicit" category.

The filtering programs erroneously blocked many travel Web sites, including: the Web site for the Allen Farmhouse Bed & Breakfast of Alleghany County, North Carolina,

http://planet-nc.com/Beth/index.html, which Websense blocked as "Adult Content"; Odysseus Gay Travel, a travel company serving gay men, http://www.odyusa.com, which N2H2 categorized as "Adults Only, Pornography"; Southern Alberta Fly Fishing Outfitters, http://albertaflyfish.com, which N2H2 blocked as "Pornography"; and "Nature and Culture Conscious Travel," a tour operator in Namibia, http://www.trans-namibia-tours.com, which was categorized as "Pornography" by N2H2.

The filtering programs also miscategorized a large number of sports Web sites. These included: a site devoted to Willie O'Ree, the first African-American player in the National Hockey League, http://www.missioncreep.com/mw/oree.html, which Websense blocked under its "Nudity" category; the home page of the Sydney University Australian Football Club, http://www.tek.com.au/suafc, which N2H2 blocked as "Adults Only, Pornography," Smartfilter blocked as "Sex," Cyber Patrol blocked as "Adult/Sexually Explicit" and Websense blocked as "Sex"; and a fan's page devoted to the Toronto Maple Leafs hockey team, http://www.torontomapleleafs.atmypage.com, which N2H2 blocked under the "Pornography" category.

7. Conclusion: The Effectiveness of Filtering Programs

Public libraries have adopted a variety of means of dealing with problems created by the provision of Internet access. The large amount of sexually explicit speech that is freely available on the Internet has, to varying degrees, led to patron complaints about such matters as unsought exposure to offensive material, incidents of staff and patron harassment by individuals viewing sexually explicit content on the Internet, and the use of

library computers to access illegal material, such as child pornography. In some libraries, youthful library patrons have persistently attempted to use the Internet to access hardcore pornography.

Those public libraries that have responded to these problems by using software filters have found such filters to provide a relatively effective means of preventing patrons from accessing sexually explicit material on the Internet. Nonetheless, out of the entire universe of speech on the Internet falling within the filtering products' category definitions, the filters will incorrectly fail to block a substantial amount of speech. Thus, software filters have not completely eliminated the problems that public libraries have sought to address by using the filters, as evidenced by frequent instances of underblocking. Nor is there any quantitative evidence of the relative effectiveness of filters and the alternatives to filters that are also intended to prevent patrons from accessing illegal content on the Internet.

Even more importantly (for this case), although software filters provide a relatively cheap and effective, albeit imperfect, means for public libraries to prevent patrons from accessing speech that falls within the filters' category definitions, we find that commercially available filtering programs erroneously block a huge amount of speech that is protected by the First Amendment. Any currently available filtering product that is reasonably effective in preventing users from accessing content within the filter's category definitions will necessarily block countless thousands of Web pages, the content of which does not match the filtering company's category definitions, much less the legal definitions

of obscenity, child pornography, or harmful to minors. Even Finnell, an expert witness for the defendants, found that between 6% and 15% of the blocked Web sites in the public libraries that he analyzed did not contain content that meets even the filtering products' own definitions of sexually explicit content, let alone CIPA's definitions.

This phenomenon occurs for a number of reasons explicated in the more detailed findings of fact *supra*. These include limitations on filtering companies' ability to: (1) harvest Web pages for review; (2) review and categorize the Web pages that they have harvested; and (3) engage in regular re-review of the Web pages that they have previously reviewed. The primary limitations on filtering companies' ability to harvest Web pages for review is that a substantial majority of pages on the Web are not indexable using the spidering technology that Web search engines use, and that together, search engines have indexed only around half of the Web pages that are theoretically indexable. The fast rate of growth in the number of Web pages also limits filtering companies' ability to harvest pages for review. These shortcomings necessarily result in significant underblocking.

Several limitations on filtering companies' ability to review and categorize the Web pages that they have harvested also contribute to over- and underblocking. First, automated review processes, even those based on "artificial intelligence," are unable with any consistency to distinguish accurately material that falls within a category definition from material that does not. Moreover, human review of URLs is hampered by filtering companies' limited staff sizes, and by human error or misjudgment. In order to deal with the vast size of the Web and its rapid rates of growth and change, filtering companies

engage in several practices that are necessary to reduce underblocking, but inevitably result in overblocking. These include: (1) blocking whole Web sites even when only a small minority of their pages contain material that would fit under one of the filtering company's categories (e.g., blocking the Salon.com site because it contains a sex column); (2) blocking by IP address (because a single IP address may contain many different Web sites and many thousands of pages of heterogenous content); and (3) blocking loophole sites such as translator sites and cache sites, which archive Web pages that have been removed from the Web by their original publisher.

Finally, filtering companies' failure to engage in regular re-review of Web pages that they have already categorized (or that they have determined do not fall into any category) results in a substantial amount of over- and underblocking. For example, Web publishers change the contents of Web pages frequently. The problem also arises when a Web site goes out of existence and its domain name or IP address is reassigned to a new Web site publisher. In that case, a filtering company's previous categorization of the IP address or domain name would likely be incorrect, potentially resulting in the over- or underblocking of many thousands of pages.

The inaccuracies that result from these limitations of filtering technology are quite substantial. At least tens of thousands of pages of the indexable Web are overblocked by each of the filtering programs evaluated by experts in this case, even when considered against the filtering companies' own category definitions. Many erroneously blocked pages contain content that is completely innocuous for both adults and minors, and that no

rational person could conclude matches the filtering companies' category definitions, such as "pornography" or "sex."

The number of overblocked sites is of course much higher with respect to the definitions of obscenity and child pornography that CIPA employs for adults, since the filtering products' category definitions, such as "sex" and "nudity," encompass vast amounts of Web pages that are neither child pornography nor obscene. Thus, the number of pages of constitutionally protected speech blocked by filtering products far exceeds the many thousands of pages that are overblocked by reference to the filtering products' category definitions.

No presently conceivable technology can make the judgments necessary to determine whether a visual depiction fits the legal definitions of obscenity, child pornography, or harmful to minors. Given the state of the art in filtering and image recognition technology, and the rapidly changing and expanding nature of the Web, we find that filtering products' shortcomings will not be solved through a technical solution in the foreseeable future.[19] In sum, filtering products are currently unable to block only visual

---

[19] Although it was not proffered as evidence in this trial, (and hence we do not rely on it to inform our findings), we note that *Youth, Pornography, and the Internet*, a congressionally commissioned study by the National Research Council, a division of the National Academies of Science, *see* Pub. L. 105-314, Title X, Sec. 901, comes to a conclusion similar to the one that we reach regarding the effectiveness of Internet filters. The commission concludes that:

> All filters–those of today and for the foreseeable future–suffer (and will suffer) from some degree of overblocking (blocking content that should be allowed through) and some degree of underblocking (passing content that

depictions that are obscene, child pornography, or harmful to minors (or, only content matching a filtering product's category definitions) while simultaneously allowing access to all protected speech (or, all content not matching the blocking product's category definitions). Any software filter that is reasonably effective in blocking access to Web pages that fall within its category definitions will necessarily erroneously block a substantial number of Web pages that do not fall within its category definitions.

III. Analytic Framework for the Opinion: The Centrality of *Dole* and the Role of the Facial Challenge

Both the plaintiffs and the government agree that, because this case involves a challenge to the constitutionality of the conditions that Congress has set on state actors' receipt of federal funds, the Supreme Court's decision in *South Dakota v. Dole*, 483 U.S. 203 (1987), supplies the proper threshold analytic framework. The constitutional source of Congress's spending power is Article I, § 8, cl. 1, which provides that "Congress shall have Power . . . to pay the Debts and provide for the common Defence and general Welfare of the United States." In *Dole*, the Court upheld the constitutionality of a federal statute requiring the withholding of federal highway funds from any state with a drinking age below

---

> should not be allowed through). While the extent of overblocking and underblocking will vary with the product (and may improve over time), underblocking and overblocking result from numerous sources, including the variability in the perspectives that humans bring to the task of judging content.

Youth, Pornography, and the Internet (Dick Thornburgh & Herbert S. Lin, eds., 2002), *available at* http://bob.nap.edu/html/youth_internet/.

21. *Id.* at 211-12. In sustaining the provision's constitutionality, *Dole* articulated four general constitutional limitations on Congress's exercise of the spending power.

First, "the exercise of the spending power must be in pursuit of 'the general welfare.'" *Id.* at 207. Second, any conditions that Congress sets on states' receipt of federal funds must be sufficiently clear to enable recipients "to exercise their choice knowingly, cognizant of the consequences of their participation." *Id.* (internal quotation marks and citation omitted). Third, the conditions on the receipt of federal funds must bear some relation to the purpose of the funding program. *Id.* And finally, "other constitutional provisions may provide an independent bar to the conditional grant of federal funds." *Id.* at 208. In particular, the spending power "may not be used to induce the States to engage in activities that would themselves be unconstitutional. Thus, for example, a grant of federal funds conditioned on invidiously discriminatory state action or the infliction of cruel and unusual punishment would be an illegitimate exercise of the Congress' broad spending power." *Id.* at 210.

Plaintiffs do not contend that CIPA runs afoul of the first three limitations. However, they do allege that CIPA is unconstitutional under the fourth prong of *Dole* because it will induce public libraries to violate the First Amendment.[20] Plaintiffs therefore submit that the First Amendment "provide[s] an independent bar to the conditional

[20] Because we find that the plaintiff public libraries are funded and controlled by state and local governments, they are state actors, subject to the constraints of the First Amendment, as incorporated by the Due Process Clause of the Fourteenth Amendment.

grant of federal funds" created by CIPA. *Id.* at 208. More specifically, they argue that by conditioning public libraries' receipt of federal funds on the use of software filters, CIPA will induce public libraries to violate the First Amendment rights of Internet content-providers to disseminate constitutionally protected speech to library patrons via the Internet, and the correlative First Amendment rights of public library patrons to receive constitutionally protected speech on the Internet.[21]

The government concedes that under the *Dole* framework, CIPA is facially invalid if its conditions will induce public libraries to violate the First Amendment. The government and the plaintiffs disagree, however, on the meaning of *Dole*'s "inducement" requirement in the context of a First Amendment facial challenge to the conditions that Congress places on state actors' receipt of federal funds. The government contends that because plaintiffs are bringing a facial challenge, they must show that under no circumstances is it possible for a public library to comply with CIPA's conditions without violating the First Amendment. The plaintiffs respond that even if it is possible for some public libraries to comply with CIPA without violating the First Amendment, CIPA is facially invalid if it "will result in the impermissible suppression of a substantial amount of protected speech."

---

[21] The Supreme Court has recognized that the First Amendment encompasses not only the right to speak, but also the right to receive information. *See Reno v. ACLU*, 521 U.S. 844, 874 (1997) (invalidating a statute because it "effectively suppresses a large amount of speech that adults have a constitutional right to receive and to address to one another"); *Stanley v. Georgia*, 394 U.S. 557, 564 (1969) ("[The] right to receive information and ideas, regardless of their social worth . . . is fundamental to our free society."); *see also Bd. of Educ. v. Pico*, 457 U.S. 853, 867-68 (1982) (plurality opinion) ("[T]he right to receive ideas follows ineluctably from the *sender*'s First Amendment right to send them.").

Because it was clear in *Dole* that the states could comply with the challenged conditions that Congress attached to the receipt of federal funds without violating the Constitution, the *Dole* Court did not have occasion to explain fully what it means for Congress to use the spending power to "induce [recipients] to engage in activities that would themselves be unconstitutional." *Dole*, 483 U.S. at 210; *see id.* at 211 ("Were South Dakota to succumb to the blandishments offered by Congress and raise its drinking age to 21, the State's action in so doing would not violate the constitutional rights of anyone."). Although the proposition that Congress may not pay state actors to violate citizens' First Amendment rights is unexceptionable when stated in the abstract, it is unclear what exactly a litigant must establish to facially invalidate an exercise of Congress's spending power on this ground.

In general, it is well-established that a court may sustain a facial challenge to a statute only if the plaintiff demonstrates that the statute admits of no constitutional application. *See United States v. Salerno*, 481 U.S. 739, 745 (1987) ("A facial challenge to a legislative Act is, of course, the most difficult challenge to mount successfully, since the challenger must establish that no set of circumstances exists under which the Act would be valid."); *see also Bowen v. Kendrick*, 487 U.S. 589, 612 (1988) ("It has not been the Court's practice, in considering facial challenges to statutes of this kind, to strike them down in anticipation that particular applications may result in unconstitutional use of funds.") (internal quotation marks and citation omitted).

First Amendment overbreadth doctrine creates a limited exception to this rule by

permitting facial invalidation of a statute that burdens a substantial amount of protected speech, even if the statute may be constitutionally applied in particular circumstances. "The Constitution gives significant protection from overbroad laws that chill speech within the First Amendment's vast and privileged sphere. Under this principle, [a law] is unconstitutional on its face if it prohibits a substantial amount of protected expression." *Ashcroft v. Free Speech Coalition*, 122 S. Ct. 1389, 1399 (2002); *see also Broadrick v. Oklahoma*, 413 U.S. 601, 612 (1973). This more liberal test of a statute's facial validity under the First Amendment stems from the recognition that where a statute's reach contemplates a number of both constitutional and unconstitutional applications, the law's sanctions may deter individuals from challenging the law's validity by engaging in constitutionally protected speech that may nonetheless be proscribed by the law. Without an overbreadth doctrine, "the contours of regulation would have to be hammered out case by case – and tested only by those hardy enough to risk criminal prosecution to determine the proper scope of regulation." *Dombrowski v. Pfister*, 380 U.S. 479, 487 (1965); *see also Brockett v. Spokane Arcades, Inc.*, 472 U.S. 491, 503 (1985) ("[A]n individual whose own speech or expressive conduct may validly be prohibited or sanctioned is permitted to challenge a statute on its face because it also threatens others not before the court – those who desire to engage in legally protected expression but who may refrain from doing so rather than risk prosecution or undertake to have the law declared partially invalid.").

Plaintiffs argue that the overbreadth doctrine is applicable here, since CIPA "threatens to chill free speech – because it will censor a substantial amount of protected

speech, because it is vague, and because the law creates a prior restraint . . . ." Unlike the statutes typically challenged as facially overbroad, however, CIPA does not impose criminal penalties on those who violate its conditions. *Cf. Freedom of Speech Coalition*, 122 S. Ct. at 1398 ("With these severe penalties in force, few legitimate movie producers or book publishers, or few other speakers in any capacity, would risk distributing images in or near the uncertain reach of this law."). Thus, the rationale for permitting facial challenges to laws that may be constitutionally applied in some instances is less compelling in cases such as this, which involve challenges to Congress's exercise of the spending power, than in challenges to criminal statutes.

Nonetheless, "even minor punishments can chill protected speech," *id.*, and absent the ability to challenge CIPA on its face, public libraries that depend on federal funds may decide to comply with CIPA's terms, thereby denying patrons access to substantial amounts of constitutionally protected speech, rather than refusing to comply with CIPA's terms and consequently losing the benefits of federal funds. *See* 47 C.F.R. § 54.520(e)(1) ("A school or library that knowingly fails to ensure the use of computers in accordance with the certifications required by this section, must reimburse any funds and discounts received under the federal universal support service support mechanism for schools and libraries for the period in which there was noncompliance."). Even in cases where the only penalty for failure to comply with a statute is the withholding of federal funds, the Court has sustained facial challenges to Congress's exercise of the spending power. *See, e.g.*, *Legal Servs. Corp. v. Velazquez*, 531 U.S. 533 (2001) (declaring unconstitutional on its face a federal

statute restricting the ability of legal services providers who receive federal funds to engage in activity protected by the First Amendment).

The Court's unconstitutional conditions cases, such as *Velazquez*, are not strictly controlling, since they do not require a showing that recipients who comply with the conditions attached to federal funding will, as state actors, violate others' constitutional rights, as is the case under the fourth prong of *Dole*. However, they are highly instructive.

The Supreme Court's pronouncements in the unconstitutional conditions cases on what is necessary for a plaintiff to mount a successful First Amendment facial challenge to an exercise of Congress's spending power have not produced a seamless web. For example, in *Rust v. Sullivan*, 500 U.S. 173 (1991), the Court rejected a First Amendment facial challenge to federal regulations prohibiting federally funded healthcare clinics from providing counseling concerning the use of abortion as a method of family planning, explaining that:

> Petitioners are challenging the *facial* validity of the regulations. Thus, we are concerned only with the question whether, on their face, the regulations are both authorized by the Act and can be construed in such a manner that they can be applied to a set of individuals without infringing upon constitutionally protected rights. Petitioners face a heavy burden in seeking to have the regulations invalidated as facially unconstitutional. . . . The fact that the regulations might operate unconstitutionally under some conceivable set of circumstances is insufficient to render them wholly invalid.

Id. at 183 (internal quotation marks, alterations, and citation omitted). In contrast, *NEA v. Finley*, 524 U.S. 569 (1998), which also involved a facial First Amendment challenge to an exercise of Congress's spending power, articulated a somewhat more liberal test of facial

validity than *Rust*, explaining that "[t]o prevail, respondents must demonstrate a substantial risk that application of the provision will lead to the suppression of speech." *Id.* at 580.

Against this background, it is unclear to us whether, to succeed in facially invalidating CIPA on the grounds that it will "induce the States to engage in activities that would themselves be unconstitutional," *Dole*, 483 U.S. at 210, plaintiffs must show that it is impossible for public libraries to comply with CIPA's conditions without violating the First Amendment, or rather simply that CIPA will effectively restrict library patrons' access to substantial amounts of constitutionally protected speech, therefore causing many libraries to violate the First Amendment. However, we need not resolve this issue. Rather, we may assume without deciding, for purposes of this case, that a facial challenge to CIPA requires plaintiffs to show that any public library that complies with CIPA's conditions will necessarily violate the First Amendment and, as explained in detail below, we believe that CIPA's constitutionality fails even under this more restrictive test of facial validity urged on us by the government. Because of the inherent limitations in filtering technology, public libraries can never comply with CIPA without blocking access to a substantial amount of speech that is both constitutionally protected and fails to meet even the filtering companies' own blocking criteria. We turn first to the governing legal principles to be applied to the facts in order to determine whether the First Amendment permits a library to use the filtering technology mandated by CIPA.

IV. Level of Scrutiny Applicable to Content-based Restrictions on Internet Access in Public Libraries

In analyzing the constitutionality of a public library's use of Internet filtering software, we must first identify the appropriate level of scrutiny to apply to this restriction on patrons' access to speech. While plaintiffs argue that a public library's use of such filters is subject to strict scrutiny, the government maintains that the applicable standard is rational basis review. If strict scrutiny applies, the government must show that the challenged restriction on speech is narrowly tailored to promote a compelling government interest and that no less restrictive alternative would further that interest. *United States v. Playboy Entm't Group, Inc.*, 529 U.S. 803, 813 (2000). In contrast, under rational basis review, the challenged restriction need only be reasonable; the government interest that the restriction serves need not be compelling; the restriction need not be narrowly tailored to serve that interest; and the restriction "need not be the most reasonable or the only reasonable limitation." *Cornelius v. NAACP Legal Def. & Educ. Fund*, 473 U.S. 788, 808 (1985).

Software filters, by definition, block access to speech on the basis of its content, and content-based restrictions on speech are generally subject to strict scrutiny. *See Playboy*, 529 U.S. at 813 ("[A] content-based speech restriction . . . can stand only if it satisfies strict scrutiny."). Strict scrutiny does not necessarily apply to content-based restrictions on speech, however, where the restrictions apply only to speech on government property, such as public libraries. "[I]t is . . . well settled that the government need not permit all forms of speech on property that it owns and controls." *Int'l Soc'y for Krishna Consciousness, Inc. v. Lee*, 505 U.S. 672, 678 (1992). We perforce turn to a discussion of

public forum doctrine.

A. Overview of Public Forum Doctrine

The government's power to restrict speech on its own property is not unlimited. Rather, under public forum doctrine, the extent to which the First Amendment permits the government to restrict speech on its own property depends on the character of the forum that the government has created. *See Cornelius v. NAACP Legal Def. & Educ. Fund, Inc.*, 473 U.S. 788 (1985). Thus, the First Amendment affords greater deference to restrictions on speech in those areas considered less amenable to free expression, such as military bases, *see Greer v. Spock*, 424 U.S. 828 (1976), jail grounds, *see Adderley v. Florida*, 385 U.S. 39 (1966), or public airport terminals, *see Int'l Soc'y for Krishna Consciousness, Inc. v. Lee*, 505 U.S. 672 (1992), than to restrictions on speech in state universities, *see Rosenberger v. Rector & Visitors of Univ. of Va.*, 515 U.S. 819 (1995), or streets, sidewalks and public parks, *see Frisby v. Schultz*, 487 U.S. 474 (1988); *Hague v. CIO*, 307 U.S. 496 (1939).

The Supreme Court has identified three types of fora for purposes of identifying the level of First Amendment scrutiny applicable to content-based restrictions on speech on government property: traditional public fora, designated public fora, and nonpublic fora. Traditional public fora include sidewalks, squares, and public parks:

> [S]treets and parks . . . have immemorially been held in trust for the use of the public and, time out of mind, have been used for purposes of assembly, communicating thoughts between citizens, and discussing public questions. Such use of the streets and public places has, from ancient times, been a part of the privileges, immunities, rights, and liberties of citizens.

Hague, 307 U.S. at 515. "In these quintessential public forums, . . . [f]or the State to enforce a content-based exclusion it must show that its regulation is necessary to serve a compelling state interest and that it is narrowly drawn to achieve that end." *Perry Educ. Ass'n v. Perry Local Educs. Ass'n*, 460 U.S. 37, 45 (1983); *see also Int'l Soc'y for Krishna Consciousness*, 505 U.S. at 678 ("[R]egulation of speech on government property that has traditionally been available for public expression is subject to the highest scrutiny."); *Frisby*, 487 U.S. at 480 ("[W]e have repeatedly referred to public streets as the archetype of a traditional public forum.").

A second category of fora, known as designated (or limited) public fora, "consists of public property which the State has opened for use by the public as a place for expressive activity." *Perry*, 460 U.S. at 46. Whereas any content-based restriction on the use of traditional public fora is subject to strict scrutiny, the state is generally permitted, as long as it does not discriminate on the basis of viewpoint, to limit a designated public forum to certain speakers or the discussion of certain subjects. *See Perry*, 460 U.S. at 45 n.7. Once it has defined the limits of a designated public forum, however, "[r]egulation of such property is subject to the same limitations as that governing a traditional public forum." *Int'l Soc'y for Krishna Consciousness*, 505 U.S. at 678. Examples of designated fora include university meeting facilities, *see Widmar v. Vincent*, 454 U.S. 263 (1981), school board meetings, *see City of Madison Joint School Dist. v. Wisc. Employment Relations Comm'n*, 429 U.S. 167 (1976), and municipal theaters, *see Southeastern Promotions, Ltd. v. Conrad*, 420 U.S. 546 (1975).

The third category, nonpublic fora, consists of all remaining public property. "Limitations on expressive activity conducted on this last category of property must survive only a much more limited review. The challenged regulation need only be reasonable, as long as the regulation is not an effort to suppress the speaker's activity due to disagreement with the speaker's view." *Int'l Soc'y for Krishna Consciousness*, 505 U.S. at 679.

B. Contours of the Relevant Forum: the Library's Collection as a Whole or the Provision of Internet Access?

To apply public forum doctrine to this case, we must first determine whether the appropriate forum for analysis is the library's collection as a whole, which includes both print and electronic resources, or the library's provision of Internet access. Where a plaintiff seeks limited access, for expressive purposes, to governmentally controlled property, the Supreme Court has held that the relevant forum is defined not by the physical limits of the government property at issue, but rather by the specific access that the plaintiff seeks:

> Although . . . as an initial matter a speaker must seek access to public property or to private property dedicated to public use to evoke First Amendment concerns, forum analysis is not completed merely by identifying the government property at issue. Rather, in defining the forum we have focused on the access sought by the speaker. When speakers seek general access to public property, the forum encompasses that property. In cases in which limited access is sought, our cases have taken a more tailored approach to ascertaining the perimeters of a forum within the confines of the government property.

Cornelius v. NAACP Legal Def. & Educ. Fund, Inc., 473 U.S. 788, 801 (1985).

Thus, in *Cornelius*, where the plaintiffs were legal defense and political advocacy

groups seeking to participate in the Combined Federal Campaign charity drive, the Court held that the relevant forum, for First Amendment purposes, was not the entire federal workplace, but rather the charity drive itself. *Id.* at 801. Similarly, in *Perry Education Association v. Perry Local Educators' Association*, 460 U.S. 37 (1983), which addressed a union's right to access a public school's internal mail system and teachers' mailboxes, the Court identified the relevant forum as the school's mail system, not the public school as a whole. In *Widmar v. Vincent*, 454 U.S. 263 (1981), in which a student group challenged a state university's restrictions on use of its meeting facilities, the Court identified the relevant forum as the meeting facilities to which the plaintiffs sought access, not the state university generally. And in *Christ's Bride Ministries, Inc. v. SEPTA*, 148 F.3d 242 (3d Cir. 1998), involving a First Amendment challenge to the removal of advertisements from subway and commuter rail stations, the Third Circuit noted that the forum at issue was not the rail and subway stations as a whole, but rather the advertising space within the stations. *Id.* at 248. Although these cases dealt with the problem of identifying the relevant forum where *speakers* are claiming a right of access, we believe that the same approach applies to identifying the relevant forum where the parties seeking access are listeners or readers.

In this case, the patron plaintiffs are not asserting a First Amendment right to compel public libraries to acquire certain books or magazines for their print collections. Nor are the Web site plaintiffs claiming a First Amendment right to compel public libraries to carry print materials that they publish. Rather, the right at issue in this case is the specific right of library patrons to access information on the Internet, and the specific right

of Web publishers to provide library patrons with information via the Internet. Thus, the relevant forum for analysis is not the library's entire collection, which includes both print and electronic media, such as the Internet, but rather the specific forum created when the library provides its patrons with Internet access.

Although a public library's provision of Internet access does not resemble the conventional notion of a forum as a well-defined physical space, the same First Amendment standards apply. *See Rosenberger v. Rector & Visitors of Univ. of Va.*, 515 U.S. 819, 830 (1995) (holding that a state university's student activities fund "is a forum more in a metaphysical than a spatial or geographic sense, but the same principles are applicable"); *see also Cornelius*, 473 U.S. at 801 (identifying the Combined Federal Campaign charity drive as the relevant unit of analysis for application of public forum doctrine).

C. Content-based Restrictions in Designated Public Fora

Unlike nonpublic fora such as airport terminals, *see Int'l Soc'y for Krishna Consciousness, Inc. v. Lee*, 505 U.S. 672 (1992), military bases, *see Greer v. Spock*, 424 U.S. 828 (1976), jail grounds, *see Adderley v. Florida*, 385 U.S. 39 (1966), the federal workplace, *see Cornelius v. NAACP Legal Def. & Educ. Fund*, 473 U.S. 788, 805 (1985), and public transit vehicles, *see Lehman v. City of Shaker Heights*, 418 U.S. 298 (1974), the purpose of a public library in general, and the provision of Internet access within a public library in particular, is "for use by the public . . . for expressive activity," *Perry Educ. Ass'n v. Perry Local Educs. Ass'n*, 460 U.S. 37, 45 (1983), namely, the dissemination and receipt by the public of a wide range of information. We are satisfied

that when the government provides Internet access in a public library, it has created a designated public forum. *See Mainstream Loudoun v. Bd. of Trustees of the Loudoun County Library*, 24 F. Supp. 2d 552, 563 (E.D. Va. 1998); *cf. Kreimer v. Bureau of Police*, 958 F.2d 1242, 1259 (3d Cir. 1992) (holding that a public library is a limited public forum).

Relying on those cases that have recognized that government has leeway, under the First Amendment, to limit use of a designated public forum to narrowly specified purposes, and that content-based restrictions on speech that are consistent with those purposes are subject only to rational basis review, the government argues for application of rational basis review to public libraries' decisions about which content to make available to their patrons via the Internet. *See Rosenberger*, 515 U.S. 819, 829 (1995) ("The necessities of confining a forum to the limited and legitimate purposes for which it was created may justify the State in reserving it for certain groups or for the discussion of certain topics."); *Perry*, 460 U.S. at 46 n.7 (1983) ("A public forum may be created for a limited purpose such as use by certain groups . . . or for the discussion of certain subjects.").

In particular, the government forcefully argues that a public library's decision to limit the content of its digital offerings on the Internet should be subject to no stricter scrutiny than its decisions about what content to make available to its patrons through the library's print collection. According to the government, just as a public library may choose to acquire books about gardening but not golf, without having to show that this content-based restriction on patrons' access to speech is narrowly tailored to further a compelling

state interest, so may a public library make content-based decisions about which speech to make available on the Internet, without having to show that such a restriction satisfies strict scrutiny.

Plaintiffs respond that the government's ability to restrict the content of speech in a designated public forum by restricting the purpose of the designated public forum that it creates is not unlimited. *Cf. Legal Servs. Corp. v. Velazquez*, 531 U.S. 533, 547 (2001) ("Congress cannot recast a condition on funding as a mere definition of its program in every case, lest the First Amendment be reduced to a simple semantic exercise."). As Justice Kennedy has explained:

> If Government has a freer hand to draw content-based distinctions in limiting a forum than in excluding someone from it, the First Amendment would be a dead letter in designated public forums; every exclusion could be recast as a limitation. . . . The power to limit or redefine forums for a specific legitimate purpose does not allow the government to exclude certain speech or speakers from them for any reason at all.

Denver Area Telecomm. Consortium, Inc. v. FCC, 518 U.S. 727, 801 (1996) (Kennedy, J., concurring in the judgment).

Although we agree with plaintiffs that the First Amendment imposes some limits on the state's ability to adopt content-based restrictions in defining the purpose of a public forum, precisely what those limits are is unclear, and presents a difficult problem in First Amendment jurisprudence. The Supreme Court's "cases have not yet determined . . . that government's decision to dedicate a public forum to one type of content or another is necessarily subject to the highest level of scrutiny. Must a local government, for example,

show a compelling state interest if it builds a band shell in the park and dedicates it solely to classical music (but not to jazz)? The answer is not obvious." *Denver*, 518 U.S. at 750 (plurality opinion); *see also Southeastern Promotions, Ltd. v. Conrad*, 420 U.S. 546, 572-73 (1975) (Rehnquist, J., dissenting) ("May an opera house limit its productions to operas, or must it also show rock musicals? May a municipal theater devote an entire season to Shakespeare, or is it required to book any potential producer on a first come, first served basis?").

We believe, however, that certain principles emerge from the Supreme Court's jurisprudence on this question. In particular, and perhaps somewhat counterintuitively, the more narrow the range of speech that the government chooses to subsidize (whether directly, through government grants or other funding, or indirectly, through the creation of a public forum) the more deference the First Amendment accords the government in drawing content-based distinctions.

At one extreme lies the government's decision to fund a particular message that the government seeks to disseminate. In this context, content-based restrictions on the speech that government chooses to subsidize are clearly subject to at most rational basis review, and even viewpoint discrimination is permissible. For example, "[w]hen Congress established a National Endowment for Democracy to encourage other countries to adopt democratic principles, 22 U.S.C. § 4411(b), it was not constitutionally required to fund a program to encourage competing lines of political philosophy such as communism and fascism." *Rust v. Sullivan*, 500 U.S. 173, 194 (1991); *see also Velazquez*, 531 U.S. at

541 ("[V]iewpoint-based funding decisions can be sustained in instances in which the government is itself the speaker, or in instances, like *Rust*, in which the government used private speakers to transmit information pertaining to its own program.") (internal quotation marks and citation omitted).

Although not strictly controlling, the Supreme Court's unconstitutional conditions cases, such as *Rust* and *Velazquez*, are instructive for purposes of analyzing content-based restrictions on the use of public fora. This is because the limitations that government places on the use of a public forum can be conceptualized as conditions that the government attaches to the receipt of a benefit that it offers, namely, the use of government property. Public forum cases thus resemble those unconstitutional conditions cases involving First Amendment challenges to the conditions that the state places on the receipt of a government benefit. *See Velazquez*, 531 U.S. at 544 ("As this suit involves a subsidy, limited forum cases . . . may not be controlling in the strict sense, yet they do provide some instruction.").

Even when the government does not fund the dissemination of a particular government message, the First Amendment generally permits government, subject to the constraints of viewpoint neutrality, to create public institutions such as art museums and state universities, dedicated to facilitating the dissemination of private speech that the government believes to have particular merit. Thus, in *NEA v. Finley*, 524 U.S. 569 (1998), the Court upheld the use of content-based restrictions in a federal program awarding grants to artists on the basis of, *inter alia*, artistic excellence. "The very assumption of the NEA

is that grants will be awarded according to the artistic worth of competing applications, and absolute neutrality is simply inconceivable." *Id.* at 585 (internal quotation marks and citation omitted).

Similarly, as Justice Stevens explained in his concurring opinion in *Widmar v. Vincent*, 454 U.S. 263 (1981), the First Amendment does not necessarily subject to strict scrutiny a state university's use of content-based means of allocating scarce resources, including limited public fora such as its meeting facilities:

> Because every university's resources are limited, an educational institution must routinely make decisions concerning the use of the time and space that is available for extracurricular activities. In my judgment, it is both necessary and appropriate for those decisions to evaluate the content of a proposed student activity. I should think it obvious, for example, that if two groups of 25 students requested the use of a room at a particular time – one to view Mickey Mouse cartoons and the other to rehearse an amateur performance of Hamlet – the First Amendment would not require that the room be reserved for the group that submitted its application first. Nor do I see why a university should have to establish a "compelling state interest" to defend its decision to permit one group to use the facility and not the other.

Id. at 278 (Stevens, J., concurring in the judgment).[22]

---

[22] Indeed, if the First Amendment subjected to strict scrutiny the government's decision to dedicate a forum to speech whose content the government judges to be particularly valuable, many of our public institutions of culture would cease to exist in their current form:

> From here on out, the National Gallery in Washington, D.C., for example, would be required to display the art of all would-be artists on a first-come-first-served basis and would not be able to exercise any content control over its collection through evaluations of quality. Such a conclusion, of course, strikes us as absurd, but that is only because we feel that the government should be free to establish public cultural institutions guided by standards such as "quality."

The more broadly the government facilitates private speech, however, the less deference the First Amendment accords to the government's content-based restrictions on the speech that it facilitates. Thus, where the government creates a designated public forum to facilitate private speech representing a diverse range of viewpoints, the government's decision selectively to single out particular viewpoints for exclusion is subject to strict scrutiny. *Compare Rosenberger*, 515 U.S. at 834 (applying heightened First Amendment scrutiny to viewpoint-based restrictions on the use of a limited public forum where the government "does not itself speak or subsidize transmittal of a message it favors but instead expends funds to encourage a diversity of views from private speakers"), *with Finley*, 524 U.S. at 586 ("In the context of arts funding, in contrast to many other subsidies, the Government does not indiscriminately encourage a diversity of views from private speakers.") (internal quotation marks and citation omitted).

Similarly, although the government may create a designated public forum limited to speech on a particular topic, if the government opens the forum to members of the general

---

> . . .
> While the First Amendment articulates a deep fear of government intervention in the marketplace of ideas (because of the risk of distortion), it also seems prepared to permit state-sponsored and -supported cultural institutions that exercise considerable control over which art to fund, which pictures to hang, and which courses to teach. That these choices necessarily involve judgments about favored and disfavored content – judgments clearly prohibited in the realm of censorship – is indisputable.

Lee C. Bollinger, *Public Institutions of Culture and the First Amendment: The New Frontier*, 63 U. Cin. L. Rev. 1103, 1110-15 (1995).

public to speak on that topic while selectively singling out for exclusion particular speakers on the basis of the content of their speech, that restriction is subject to strict scrutiny. For instance, in *City of Madison Joint School District No. 8 v. Wisconsin Employment Relations Commission*, 429 U.S. 167 (1976), the Court held that where a school board opens its meetings for public participation, it may not, consistent with the First Amendment, prohibit teachers other than union representatives from speaking on the subject of pending collective-bargaining negotiations. *See id.* at 175 (noting that the state "has opened a forum for direct citizen involvement"); *see also Ark. Educ. Television Comm'n v. Forbes*, 523 U.S. 666, 680 (1998) (distinguishing, for purposes of determining the appropriate level of First Amendment scrutiny, a televised debate in which a public broadcasting station exercises editorial discretion in selecting participating candidates from a debate that has "an open-microphone format").

Finally, content-based restrictions on speech in a designated public forum are most clearly subject to strict scrutiny when the government opens a forum for virtually unrestricted use by the general public for speech on a virtually unrestricted range of topics, while selectively excluding particular speech whose content it disfavors. Thus, in *Conrad*, the Court held that a local government violated the First Amendment when it denied a group seeking to perform the rock musical "Hair" access to a general-purpose municipal theater open for the public at large to use for performances. *See also Denver*, 518 U.S. at 802 (Kennedy, J., concurring in the judgment) (suggesting that strict scrutiny would not apply to a local government's decision to "build[] a band shell in the park and dedicate[] it solely to

classical music (but not jazz)," but would apply to "the Government's creation of a band shell in which all types of music might be performed except for rap music").

Similarly, in *FCC v. League of Women Voters of Cal.*, 468 U.S. 364 (1984), the Court subjected to heightened scrutiny a federal program that funded a wide range of public broadcasting stations that disseminated speech on a wide range of subjects, where the federal program singled out for exclusion speech whose content amounted to editorializing. As the Court later explained:

> In *FCC v. League of Women Voters of Cal.*, 468 U.S. 364 (1984) the Court was instructed by its understanding of the dynamics of the broadcast industry in holding that prohibitions against editorializing by public radio networks were an impermissible restriction, even though the Government enacted the restriction to control the use of public funds. The First Amendment forbade the Government from using the forum in an unconventional way to suppress speech inherent in the nature of the medium.

Velazquez, 531 U.S. at 543.

In sum, the more widely the state opens a forum for members of the public to speak on a variety of subjects and viewpoints, the more vulnerable is the state's decision selectively to exclude certain speech on the basis of its disfavored content, as such exclusions distort the marketplace of ideas that the state has created in establishing the forum. *Cf. Velazquez*, 531 U.S. at 544 ("Restricting LSC attorneys in advising their clients and in presenting arguments and analyses to the courts distorts the legal system by altering the traditional role of the attorneys in much the same way broadcast systems or student publication networks were changed in the limited forum cases . . . .").

Thus, we believe that where the state designates a forum for expressive activity and

opens the forum for speech by the public at large on a wide range of topics, strict scrutiny applies to restrictions that single out for exclusion from the forum particular speech whose content is disfavored. "Laws designed or intended to suppress or restrict the expression of *specific* speakers contradict basic First Amendment principles." *United States v. Playboy Entm't Group, Inc.*, 529 U.S. 803, 812 (2000); *see also Denver*, 518 U.S. at 782 (Kennedy, J., concurring in the judgment) (noting the flaw in a law that "singles out one sort of speech for vulnerability to private censorship in a context where content-based discrimination is not otherwise permitted"). *Compare Forbes*, 523 U.S. at 679 (holding that the state does not create a public forum when it "allows selective *access* for individual speakers rather than general access for a class of speakers") (emphasis added), *with Police Dep't of the City of Chicago v. Mosley*, 408 U.S. 92, 96 (1972) ("Selective *exclusions* from a public forum may not be based on content alone, and may not be justified by reference to content alone.") (emphasis added).

We note further that to the extent that the government creates a public forum expressly designed to facilitate the dissemination of private speech, opens the forum to any member of the public to speak on any virtually any topic, and then selectively targets certain speech for exclusion based on its content, the government is singling out speech in a manner that resembles the discriminatory taxes on the press that the Supreme Court subjected to heightened First Amendment scrutiny in *Arkansas Writers' Project, Inc. v. Ragland*, 481 U.S. 221 (1987), and *Minneapolis Star & Tribune Co. v. Minnesota*

Commissioner of Revenue, 460 U.S. 575 (1983), which we explain in the margin.[23]

D. Reasons for Applying Strict Scrutiny

1. Selective Exclusion From a "Vast Democratic Forum"

Applying these principles to public libraries, we agree with the government that generally the First Amendment subjects libraries' content-based decisions about which print materials to acquire for their collections to only rational review. In making these decisions, public libraries are generally free to adopt collection development criteria that reflect not simply patrons' demand for certain material, but also the library's evaluation of the material's quality. *See* Bernard W. Bell, *Filth, Filtering, and the First Amendment: Ruminations on Public Libraries' Use of Internet Filtering Software*, 53 Fed. Comm. L.J. 191, 225 (2001) ("Librarians should have the discretion to decide that the library is committed to intellectual inquiry, not to the satisfaction of the full range of human desires."). Thus, a public library's decision to use the last $100 of its budget to purchase

---

[23] In both of these cases, the taxation scheme at issue effectively subsidized a vast range of publications, and singled out for penalty only a handful of speakers. *See Arkansas Writers' Project*, 460 U.S. at 228-29 (noting that "selective taxation of the press – . . . [by] targeting individual members of the press – poses a particular danger of abuse by the State" and explaining that "this case involves a more disturbing use of selective taxation than *Minneapolis Star*, because the basis on which Arkansas differentiates between magazines is particularly repugnant to First Amendment principles: a magazine's tax status depends entirely on its *content*"); *Minneapolis Star*, 460 U.S. at 591 ("Minnesota's ink and paper tax violates the First Amendment not only because it singles out the press, but also because it targets a small group of newspapers."); *see also Turner Broad. Sys., Inc. v. FCC*, 512 U.S. 622, 660 (1994) ("The taxes invalidated in *Minneapolis Star* and *Arkansas Writers' Project* . . . targeted a small number of speakers, and thus threatened to distort the market for ideas.") (internal quotation marks and citation omitted).

the complete works of Shakespeare even though more of its patrons would prefer the library to use the same amount to purchase the complete works of John Grisham, is not, in our view, subject to strict scrutiny. *Cf. NEA v. Finley*, 524 U.S. 569 (1998) (subjecting only to rational basis review the government's decision to award NEA grants on the basis of, *inter alia*, artistic excellence).

Nonetheless, we disagree with the government's argument that public libraries' use of Internet filters is no different, for First Amendment purposes, from the editorial discretion that they exercise when they choose to acquire certain books on the basis of librarians' evaluation of their quality. The central difference, in our view, is that by providing patrons with even filtered Internet access, the library permits patrons to receive speech on a virtually unlimited number of topics, from a virtually unlimited number of speakers, without attempting to restrict patrons' access to speech that the library, in the exercise of its professional judgment, determines to be particularly valuable. *Cf. Rosenberger v. Rector & Visitors of Univ. of Va.*, 515 U.S. 819, 834 (1995) (applying strict scrutiny to viewpoint-based restrictions where the state "does not itself speak or subsidize transmittal of a message it favors but instead expends funds to encourage a diversity of views from private speakers"). *See generally supra* Section IV.C.

In those cases upholding the government's exercise of editorial discretion in selecting certain speech for subsidization or inclusion in a state-created forum, the state actor exercising the editorial discretion has at least reviewed the content of the speech that the forum facilitates. Thus, in *Finley* the NEA examined the content of those works of art

that it chose to subsidize, and in *Arkansas Educational Television Commission v. Forbes*, 523 U.S. 666 (1998), the public broadcaster specifically reviewed and approved each speaker permitted to participate in the debate. *See id.* at 673 ("In the case of television broadcasting, . . . broad rights of access for outside speakers would be antithetical, as a general rule, to the discretion that stations and their editorial staff must exercise to fulfill their journalistic purpose and statutory obligations."); *Finley*, 524 U.S. at 586 ("The NEA's mandate is to make esthetic judgments, and the inherently content-based 'excellence' threshold for NEA support sets it apart from the subsidy at issue in *Rosenberger* – which was available to all student organizations that were 'related to the educational purpose of the University . . . .'") (quoting *Rosenberger*, 515 U.S. at 824); *see also Cornelius v. NAACP Legal Def. & Educ. Fund*, 473 U.S. 788, 804 (1985) ("The Government's consistent policy has been to limit participation in the [Combined Federal Campaign] to 'appropriate' voluntary agencies and to require agencies seeking admission to obtain permission from federal and local Campaign officials. . . . [T]here is no evidence suggesting that the granting of the requisite permission is merely ministerial."). The essence of editorial discretion requires the exercise of professional judgment in examining the content that the government singles out as speech of particular value.

This exercise of editorial discretion is evident in a library's decision to acquire certain books for its collection. As the government's experts in library science testified, in selecting a book for a library's collection, librarians evaluate the book's quality by reference to a variety of criteria such as its accuracy, the title's niche in relation to the rest

of the collection, the authority of the author, the publisher, the work's presentation, and how it compares with other material available in the same genre or on the same subject. Thus, the content of every book that a library acquires has been reviewed by the library's collection development staff or someone to whom they have delegated the task, and has been judged to meet the criteria that form the basis for the library's collection development policy. Although some public libraries use "approval plans" to delegate the collection development to third-party vendors which provide the library with recommended materials that the library is then free to retain or return to the vendor, the same principle nonetheless attains.

In contrast, in providing patrons with even filtered Internet access, a public library invites patrons to access speech whose content has never been reviewed and recommended as particularly valuable by either a librarian or a third party to whom the library has delegated collection development decisions. Although several of the government's librarian witnesses who testified at trial purport to apply the same standards that govern the library's acquisition of print materials to the library's provision of Internet access to patrons, when public libraries provide their patrons with Internet access, they intentionally open their doors to vast amounts of speech that clearly lacks sufficient quality to ever be considered for the library's print collection. Unless a library allows access to only those sites that have been preselected as having particular value, a method that, as noted above, was tried and rejected by the Westerville Ohio Public Library, *see supra* at 46-47, even a library that uses software filters has opened its Internet collection "for indiscriminate use

by the general public." *Perry Educ. Ass'n v. Perry Local Educs. Ass'n*, 460 U.S. 37, 47 (1983). "[M]ost Internet forums – including chat rooms, newsgroups, mail exploders, and the Web – are open to all comers." *Reno v. ACLU*, 521 U.S. 844, 880 (1997).

The fundamental difference between a library's print collection and its provision of Internet access is illustrated by comparing the extent to which the library opens its print collection to members of the public to speak on a given topic and the extent to which it opens its Internet terminals to members of the public to speak on a given topic. When a public library chooses to carry books on a selected topic, e.g. chemistry, it does not open its print collection to any member of the public who wishes to write about chemistry. Rather, out of the myriad of books that have ever been written on chemistry, each book on chemistry that the library carries has been reviewed and selected because the person reviewing the book, in the exercise of his or her professional judgment, has deemed its content to be particularly valuable. In contrast, when a public library provides Internet access, even filtered Internet access, it has created a forum open to any member of the public who writes about chemistry on the Internet, regardless of how unscientific the author's methods or of how patently false the author's conclusions are, regardless of the author's reputation or grammar, and regardless of the reviews of the scientific community.

Notwithstanding protestations in CIPA's legislative history to the contrary,[24]

---

[24] [P]atrons at a library do not have the right to make editorial decisions regarding the availability of certain material. It is the exclusive authority of the library to make affirmative decisions regarding what books, magazines, or other material is placed on library shelves, or otherwise made available to

members of the general public do define the content that public libraries make available to their patrons through the Internet. Any member of the public with Internet access could, through the free Web hosting services available on the Internet, tonight jot down a few musings on any subject under the sun, and tomorrow those musings would become part of public libraries' online offerings and be available to any library patron who seeks them out.

In providing its patrons with Internet access, a public library creates a forum for the facilitation of speech, almost none of which either the library's collection development staff or even the filtering companies have ever reviewed. Although filtering companies review a portion of the Web in classifying particular sites, the portion of the Web that the filtering companies actually review is quite small in relation to the Web as a whole. The filtering companies' harvesting process, described in our findings of fact, is intended to identify only a small fraction of Web sites for the filtering companies to review. Put simply, the state cannot be said to be exercising editorial discretion permitted under the First Amendment when it indiscriminately facilitates private speech whose content it makes no effort to examine. *Cf*. Bell, *supra*, at 226 ("[C]ourts should take a much more jaundiced view of library policies that block Internet access to a very limited array of subjects than they take of library policies that reserve Internet terminals for very limited use.").

> patrons. Libraries impose many restrictions on the use of their systems which demonstrate that the content of the library's offerings are not determined by the general public.

S. Rep. No. 106-141, at 8-9 (1999).

While the First Amendment permits the government to exercise editorial discretion in singling out particularly favored speech for subsidization or inclusion in a state-created forum, we believe that where the state provides access to a "vast democratic forum[]," *Reno*, 521 U.S. at 868, open to any member of the public to speak on subjects "as diverse as human thought," *id.* at 870, and then selectively excludes from the forum certain speech on the basis of its content, such exclusions are subject to strict scrutiny. These exclusions risk fundamentally distorting the unique marketplace of ideas that public libraries create when they open their collections, via the Internet, to the speech of millions of individuals around the world on a virtually limitless number of subjects.[25]

---

[25] In distinguishing restrictions on public libraries' print collections from restrictions on the provision of Internet access, we do not rely on the rationale adopted in *Mainstream Loudoun v. Board of Trustees of the Loudoun County Library*, 2 F. Supp. 2d 783 (E.D. Va. 1998). The *Loudoun* Court reasoned that a library's decision to block certain Web sites fundamentally differs from its decision to carry certain books but not others, in that unlike the money and shelf space consumed by the library's provision of print materials, "no appreciable expenditure of library time or resources is required to make a particular Internet publication available" once the library has acquired Internet access. *Id.* at 793-94.

We disagree. Nearly every librarian who testified at trial stated that patrons' demand for Internet access exceeds the library's supply of Internet terminals. Under such circumstances, every time library patrons visit a Web site, they deny other patrons waiting to use the terminal access to other Web sites. Just as the scarcity of a library's budget and shelf space constrains a library's ability to provide its patrons with unrestricted access to print materials, the scarcity of time at Internet terminals constrains libraries' ability to provide patrons with unrestricted Internet access:

> The same budget concerns constraining the number of books that libraries can offer also limits the number of terminals, Internet accounts, and speed of access links that can be purchased, and thus the number of Web pages that patrons can view. This is clear to anyone who has been denied access to a Website because no terminal was unoccupied.

A public library's content-based restrictions on patrons' Internet access thus resemble the content-based restrictions on speech subsidized by the government, whether through direct funding or through the creation of a designated public forum, that the Supreme Court has subjected to strict scrutiny, as discussed above in Section IV.C. Although the government may subsidize a particular message representing the government's viewpoint without having to satisfy strict scrutiny, *see Rust v. Sullivan*, 500 U.S. 173 (1991), strict scrutiny applies to restrictions that selectively exclude particular viewpoints from a public forum designed to facilitate a wide range of viewpoints, *see Rosenberger v. Rector & Visitors of Univ. of Va.*, 515 U.S. 819 (1995). Similarly, although the state's exercise of editorial discretion in selecting particular speakers for participation in a state-sponsored forum is subject to rational basis review, *see Ark. Educ. Television Comm'n v. Forbes*, 523 U.S. 666 (1998), selective exclusions of particular speakers from a forum otherwise open to any member of the public to speak are subject to strict scrutiny, *see City of Madison Joint School Dist. No. 8 v. Wis. Employment Relations Comm'n*, 429 U.S. 167 (1976).

And while the government may, subject only to rational basis review, make content-based decisions in selecting works of artistic excellence to subsidize, *see NEA v. Finley*, 524 U.S. 569 (1998), the Supreme Court has applied heightened scrutiny where the

---

Mark S. Nadel, *The First Amendment's Limitations on the Use of Internet Filtering in Public and School Libraries: What Content Can Libraries Exclude?*, 78 Tex. L. Rev. 1117, 1128 (2000).

government opens a general-purpose municipal theater for use by the public, but selectively excludes disfavored content, *see Southeastern Promotions, Ltd. v. Conrad*, 420 U.S. 546 (1975), where the government facilitates the speech of public broadcasters on a virtually limitless number of topics, but prohibits editorializing, *see FCC v. League of Women Voters of Cal.*, 468 U.S. 364 (1984), and where the government funds a wide range of legal services but restricts funding recipients from challenging welfare laws, *see Legal Servs. Corp. v. Velazquez*, 531 U.S. 533 (2001). Similarly, where a public library opens a forum to an unlimited number of speakers around the world to speak on an unlimited number of topics, strict scrutiny applies to the library's selective exclusions of particular speech whose content the library disfavors.

2. Analogy to Traditional Public Fora

Application of strict scrutiny to public libraries' use of software filters, in our view, finds further support in the extent to which public libraries' provision of Internet access promotes First Amendment values in an analogous manner to traditional public fora, such as sidewalks and parks, in which content-based restrictions on speech are always subject to strict scrutiny. The public library, by its very nature, is "designed for freewheeling inquiry." *Bd. of Education v. Pico*, 457 U.S. 853, 915 (1982) (Rehnquist, J., dissenting). As such, the library is a "mighty resource in the free marketplace of ideas," *Minarcini v. Strongsville City Sch. Dist.*, 541 F.2d 577, 582 (6th Cir. 1976), and represents a "quintessential locus of the receipt of information." *Kreimer v. Bureau of Police for Morristown*, 958 F.2d 1242, 1255 (3d Cir. 1992); *see also Sund v. City of Wichita Falls*,

121 F. Supp. 2d 530, 547 (N.D. Tex. 2000) ("The right to receive information is vigorously enforced in the context of a public library . . . ."); *cf. Int'l Soc'y for Krishna Consciousness, Inc. v. Lee*, 505 U.S. 672, 681 (1992) ("[A] traditional public forum is property that has as 'a principal purpose . . . the free exchange of ideas.'") (quoting *Cornelius v. NAACP Legal Def. & Educ. Fund*, 473 U.S. 788, 800 (1985)).

We acknowledge that the provision of Internet access in a public library does not enjoy the historical pedigree of streets, sidewalks, and parks as a vehicle of free expression. Nonetheless, we believe that it shares many of the characteristics of these traditional public fora that uniquely promote First Amendment values and accordingly warrant application of strict scrutiny to any content-based restriction on speech in these fora. Regulation of speech in streets, sidewalks, and parks is subject to the highest scrutiny not simply by virtue of history and tradition, but also because the speech-facilitating character of sidewalks and parks makes them distinctly deserving of First Amendment protection. Many of these same speech-promoting features of the traditional public forum appear in public libraries' provision of Internet access.

First, public libraries, like sidewalks and parks, are generally open to any member of the public who wishes to receive the speech that these fora facilitate, subject only to narrow limitations. *See Kreimer*, 958 F.2d at 1260 (noting that a public library does not retain unfettered discretion "to choose whom it will permit to enter the Library," but upholding the library's right to exclude patrons who harass patrons or whose offensive personal hygiene precludes the library's use by other patrons). Moreover, like traditional

public fora, public libraries are funded by taxpayers and therefore do not charge members of the public each time they use the forum. The only direct cost to library patrons who wish to receive information, whether via the Internet or the library's print collection, is the time spent reading.

By providing Internet access to millions of Americans to whom such access would otherwise be unavailable, public libraries play a critical role in bridging the digital divide separating those with access to new information technologies from those that lack access. *See generally* National Telecommunications and Information Administration, U.S. Department of Commerce, *Falling Through the Net: Defining the Digital Divide* (1999), *available at* http://www.ntia.doc.gov/ntiahome/fttn99/contents.html. *Cf. Velazquez*, 531 U.S. at 546 (invalidating a content-based restriction on the speech of federally funded legal services corporations and noting that given the financial hardship of legal services corporations' clients, "[t]he restriction on speech is even more problematic because in cases where the attorney withdraws from a representation, the client is unlikely to find other counsel"). Public libraries that provide Internet access greatly expand the educational opportunities for millions of Americans who, as explained in the margin, would otherwise be deprived of the benefits of this new medium.[26]

---

[26] We have found that approximately 14.3 million Americans access the Internet at a public library, and Internet access at public libraries is more often used by those with lower incomes than those with higher incomes. We found that about 20.3% of Internet users with household family income of less than $15,000 per year use public libraries for Internet access, and approximately 70% of libraries serving communities with poverty levels in excess of 40% receive E-rate discounts. The widespread availability of Internet access in

Just as important as the openness of a forum to listeners is its openness to speakers. Parks and sidewalks are paradigmatic loci of First Amendment values in large part because they permit speakers to communicate with a wide audience at low cost. One can address members of the public in a park for little more than the cost of a soapbox, and one can distribute handbills on the sidewalk for little more than the cost of a pen, paper, and some photocopies. *See Martin v. City of Struthers*, 319 U.S. 141, 146 (1943) ("Door to door distribution of circulars is essential to the poorly financed causes of little people."); Laurence H. Tribe, *American Constitutional Law* § 12-24 at 987 (2d ed. 1988) ("The 'public forum' doctrine holds that restrictions on speech should be subject to higher scrutiny when, all other things being equal, that speech occurs in areas playing a vital role in communication – such as in those places historically associated with first amendment activities, such as streets, sidewalks, and parks – especially because of how indispensable communication in these places is to people who lack access to more elaborate (and more costly) channels."); Daniel A. Farber, *Free Speech without Romance: Public Choice and the First Amendment*, 105 Harv. L. Rev. 554, 574 n.86 (1991) (noting that traditional public fora "are often the only place where less affluent groups and individuals can effectively express their message"); Harry Kalven, Jr., *The Concept of the Public Forum:* Cox v. Louisiana, 1965 Sup. Ct. Rev. 1, 30 ("[T]he parade, the picket, the leaflet, the sound truck, have been the media of communication exploited by those with little access to the

---

public libraries is due, in part, to the availability of public funding, including state and local funding and the federal funding programs regulated by CIPA.

more genteel means of communication.").

Similarly, given the existence of message boards and free Web hosting services, a speaker can, via the Internet, address the public, including patrons of public libraries, for little more than the cost of Internet access. As the Supreme Court explained in *Reno v. ACLU*, 521 U.S. 844 (1997), "the Internet can hardly be considered a 'scarce' expressive commodity. It provides relatively unlimited, low-cost capacity for communication of all kinds." *Id.* at 870. Although the cost of a home computer and Internet access considerably exceeds the cost of a soapbox or a few hundred photocopies, speakers wishing to avail themselves of the Internet may gain free access in schools, workplaces, or the public library. As Professor Lessig has explained:

> The "press" in 1791 was not the *New York Times* or the *Wall Street Journal*. It did not comprise large organizations of private interests, with millions of readers associated with each organization. Rather, the press then was much like the Internet today. The cost of a printing press was low, the readership was slight, and anyone (within reason) could become a publisher – and in fact an extraordinary number did. When the Constitution speaks of the rights of the "press," the architecture it has in mind is the architecture of the Internet.

Lawrence Lessig, *Code* 183 (1999).

While public libraries' provision of Internet access shares many of the speech-promoting qualities of traditional public fora, it also facilitates speech in ways that traditional public fora cannot.[27] In particular, whereas the architecture of real space limits

---

[27] We acknowledge that traditional public fora have characteristics that promote First Amendment values in ways that the provision of Internet access in public libraries does not. For example, a significant virtue of traditional public fora is their facilitation of face-to-face communication. "In a face-to-face encounter there is a greater opportunity for the

the audience of a pamphleteer or soapbox orator to people within the speaker's immediate vicinity, the Internet renders the geography of speaker and listener irrelevant:

> Through the use of chat rooms, any person with a phone line can become a town crier with a voice that resonates farther than it could from any soapbox. Through the use of Web pages, mail exploders, and newsgroups, the same individual can become a pamphleteer.

Reno, 521 U.S. at 870 . By providing patrons with Internet access, public libraries in effect open their doors to an unlimited number of potential speakers around the world, inviting the speech of any member of the public who wishes to communicate with library patrons via the Internet.

Due to the low costs for speakers and the irrelevance of geography, the volume of speech available to library patrons on the Internet is enormous and far exceeds the volume of speech available to audiences in traditional public fora. *See id.* at 868 (referring to "the vast democratic forums of the Internet"). Indeed, as noted in our findings of fact, the Web is estimated to contain over one billion pages, and is said to be growing at a rate of over 1.5 million pages per day. *See id.* at 885 (noting "[t]he dramatic expansion of this new

---

exchange of ideas and the propagation of views . . . ." *Cornelius*, 473 U.S. at 798. Face-to-face exchanges also permit speakers to confront listeners who would otherwise not actively seek out the information that the speaker has to offer. In contrast, the Internet operates largely by providing individuals with only that information that they actively seek out. Although the Internet does not permit face-to-face communication in the same way that traditional public fora do, the Internet, as a medium of expression, is significantly more interactive than the broadcast media and the press. "[T]he Web makes it possible to establish two-way linkages with potential sympathizers. Unlike the unidirectional nature of most mass media, websites, bulletin boards, chatrooms, and email are potentially interactive." Seth F. Kreimer, *Technologies of Protest: Insurgent Social Movements and the First Amendment in the Era of the Internet*, 150 U. Pa. L. Rev. 119, 130 (2001).

marketplace of ideas"). This staggering volume of content on the Internet "is as diverse as human thought," *id.* at 870, and "is thus comparable, from the reader's viewpoint, to . . . a vast library including millions of readily available and indexed publications," *id.* at 853. As a result of the Internet's unique speech-facilitating qualities, "it is hard to find an aspiring social movement, new or old, of left, right, or center, without a website, a bulletin board, and an email list." Kreimer, *supra* n.27, at 125. "[T]he growth of the Internet has been and continues to be phenomenal." *Reno*, 521 U.S. at 885.

This extraordinary growth of the Internet illustrates the extent to which the Internet promotes First Amendment values in the same way that the historical use of traditional public fora for speaking, handbilling, and protesting testifies to their effectiveness as vehicles for free speech. *Cf. Martin*, 319 U.S. at 145 ("The widespread use of this method of communication [door-to-door distribution of leaflets] by many groups espousing various causes attests its major importance."); *Schneider v. State*, 308 U.S. 147, 164 (1939) ("[P]amphlets have proved most effective instruments in the dissemination of opinion.").

The provision of Internet access in public libraries, in addition to sharing the speech-enhancing qualities of fora such as streets, sidewalks, and parks, also supplies many of the speech-enhancing properties of the postal service, which is open to the public at large as both speakers and recipients of information, and provides a relatively low-cost means of disseminating information to a geographically dispersed audience. *See Lamont v. Postmaster Gen.*, 381 U.S. 301 (1965) (invalidating a content-based prior restraint on the use of the mails); *see also Blount v. Rizzi*, 400 U.S. 410 (1971) (same). Indeed, the

Supreme Court's description of the postal system in *Lamont* seems equally apt as a description of the Internet today: "the postal system . . . is now the main artery through which the business, social, and personal affairs of the people are conducted . . . ." 381 U.S. at 305 n.3.

In short, public libraries, by providing their patrons with access to the Internet, have created a public forum that provides any member of the public free access to information from millions of speakers around the world. The unique speech-enhancing character of Internet use in public libraries derives from the openness of the public library to any member of the public seeking to receive information, and the openness of the Internet to any member of the public who wishes to speak. In particular, speakers on the Internet enjoy low barriers to entry and the ability to reach a mass audience, unhindered by the constraints of geography.[28] Moreover, just as the development of new media "presents unique problems, which inform our assessment of the interests at stake, and which may justify restrictions that would be unacceptable in other contexts," *United States v. Playboy Entm't Group, Inc.*, 529 U.S. 803, 813 (2000), the development of new media, such as the

---

[28] We acknowledge that the Internet's architecture is a human creation, and is therefore subject to change. The foregoing analysis of the unique speech-enhancing qualities of the Internet is limited to the Internet as currently constructed. Indeed, the characteristics of the Internet that we believe render it uniquely suited to promote First Amendment values may change as the Internet's architecture evolves. *See* Lawrence Lessig, *Reading the Constitution in Cyberspace*, 45 Emory L.J. 869, 888 (1996) ("Cyberspace has no permanent nature, save the nature of a place of unlimited plasticity. We don't *find* cyberspace, we build it."); *see also* Lawrence Lessig, *The Death of Cyberspace*, 57 Wash. & Lee L. Rev. 337 (2000).

Internet, also presents unique possibilities for promoting First Amendment values, which also inform our assessment of the interests at stake, and which we believe, in the context of the provision of Internet access in public libraries, justify the application of heightened scrutiny to content-based restrictions that might be subject to only rational review in other contexts, such as the development of the library's print collection. *Cf. id.* at 818 ("Technology expands the capacity to choose; and it denies the potential of this revolution if we assume the Government is best positioned to make these choices for us.").

A faithful translation of First Amendment values from the context of traditional public fora such as sidewalks and parks to the distinctly non-traditional public forum of Internet access in public libraries requires, in our view, that content-based restrictions on Internet access in public libraries be subject to the same exacting standards of First Amendment scrutiny as content-based restrictions on speech in traditional public fora such as sidewalks, town squares, and parks:

> The architecture of the Internet, as it is right now, is perhaps the most important model of free speech since the founding. . . . Two hundred years after the framers ratified the Constitution, the Net has taught us what the First Amendment means. . . . The model for speech that the framers embraced was the model of the Internet – distributed, noncentralized, fully free and diverse.

Lessig, *Code*, at 167, 185. Indeed, "[m]inds are not changed in streets and parks as they once were. To an increasing degree, the more significant interchanges of ideas and shaping of public consciousness occur in mass and electronic media." *Denver Area Educ. Telecomms. Consortium, Inc. v. FCC*, 518 U.S. 727, 802-03 (1996) (Kennedy, J., concurring in the judgment).

In providing patrons with even filtered Internet access, a public library is not exercising editorial discretion in selecting only speech of particular quality for inclusion in its collection, as it may do when it decides to acquire print materials. By providing its patrons with Internet access, public libraries create a forum in which any member of the public may receive speech from anyone around the world who wishes to disseminate information over the Internet. Within this "vast democratic forum[]," *Reno*, 521 U.S. at 868, which facilitates speech that is "as diverse as human thought," *id.* at 870, software filters single out for exclusion particular speech on the basis of its disfavored content. We hold that these content-based restrictions on patrons' access to speech are subject to strict scrutiny.

V. Application of Strict Scrutiny

Having concluded that strict scrutiny applies to public libraries' content-based restrictions on patrons' access to speech on the Internet, we must next determine whether a public library's use of Internet software filters can survive strict scrutiny. To survive strict scrutiny, a restriction on speech "must be narrowly tailored to promote a compelling Government interest. If a less restrictive alternative would serve the Government's purpose, the legislature must use that alternative." *United States v. Playboy Entm't Group, Inc.*, 529 U.S. 803, 813 (2000) (citation omitted); *see also Fabulous Assocs., Inc. v. Pa. Pub. Util. Comm'n*, 896 F.2d 780, 787 (3d Cir. 1990) (holding that a content-based burden on speech is permissible "only if [the government] shows that the restriction serves a compelling interest and that there are no less restrictive alternatives").

The application of strict scrutiny to a public library's use of filtering products thus requires three distinct inquiries. First, we must identify those compelling government interests that the use of filtering software promotes. It is then necessary to analyze whether the use of software filters is narrowly tailored to further those interests. Finally, we must determine whether less restrictive alternatives exist that would promote the state interest.

A. State Interests

We begin by identifying those legitimate state interests that a public library's use of software filters promotes.

1. Preventing the Dissemination of Obscenity, Child Pornography, and Material Harmful to Minors

On its face, CIPA is clearly intended to prevent public libraries' Internet terminals from being used to disseminate to library patrons visual depictions that are obscene, child pornography, or in the case of minors, harmful to minors. *See* CIPA § 1712 (codified at 20 U.S.C. § 9134(f)(1)(A) & (B)), § 1721(b) (codified at 47 U.S.C. § 254(h)(6)(B) & (C)) (requiring any library that receives E-rate discounts to certify that it is enforcing "a policy of Internet safety that includes the operation of a technology protection measure with respect to any of its computers with Internet access that protects against access through such computers to visual depictions" that are "obscene" or "child pornography," and, when the computers are in use by minors, also protects against access to visual depictions that are "harmful to minors").

The government's interest in preventing the dissemination of obscenity, child pornography, or, in the case of minors, material harmful to minors, is well-established. Speech that is obscene, under the legal definition of obscenity set forth in the margin, is unprotected under the First Amendment, and accordingly the state has a compelling interest in preventing its distribution.[29] *See Miller v. California*, 413 U.S. 15, 18 (1973) ("This Court has recognized that the States have a legitimate interest in prohibiting dissemination or exhibition of obscene material."); *Stanley v. Georgia*, 394 U.S. 557, 563 (1969) ("[T]he First and Fourteenth Amendments recognize a valid governmental interest in dealing with the problem of obscenity."); *Roth v. United States*, 354 U.S. 476, 485 (1957) ("We hold that obscenity is not within the area of constitutionally protected speech of press.").

The First Amendment also permits the state to prohibit the distribution to minors of material that, while not obscene with respect to adults, is obscene with respect to minors. *See Ginsberg v. New York*, 390 U.S. 629, 637 (1968) (holding that it is constitutionally permissible "to accord minors under 17 a more restricted right than that assured to adults to judge and determine for themselves what sex material they may read or see"). Proscribing the distribution of such material to minors is constitutionally justified by the government's well-recognized interest in safeguarding minors' well-being. *See Reno v. ACLU*, 521 U.S. 844, 869-70 (1997) ("[T]here is a compelling interest in protecting the

---

[29] For First Amendment purposes, obscenity is "limited to works which, taken as a whole, appeal to the prurient interest in sex, which portray sexual conduct in a patently offensive way, and which, taken as a whole, do not have serious literary, artistic, political, or scientific value." *Miller v. California*, 413 U.S. 15, 24 (1973).

physical and psychological well-being of minors which extend[s] to shielding them from indecent messages that are not obscene by adult standards . . . .") (internal quotation marks and citation omitted); *New York v. Ferber*, 458 U.S. 747, 756-57 (1982) ("It is evident beyond the need for elaboration that a State's interest in safeguarding the physical and psychological well-being of a minor is compelling.") (internal quotation marks and citation omitted); *Ginsberg*, 390 U.S. at 640 ("The State . . . has an independent interest in the well-being of its youth.").

The government's compelling interest in protecting the well-being of its youth justifies laws that criminalize not only the distribution to minors of material that is harmful to minors, but also the possession and distribution of child pornography. *See Osborne v. Ohio*, 495 U.S. 103, 111 (1990) (holding that a state "may constitutionally proscribe the possession and viewing of child pornography"); *Ferber*, 458 U.S. at 757, 763 (noting that "[t]he prevention of sexual exploitation and abuse of children constitutes a government objective of surpassing importance," and holding that "child pornography [is] a category of material outside the protection of the First Amendment").

Thus, a public library's use of software filters survives strict scrutiny if it is narrowly tailored to further the state's well-recognized interest in preventing the dissemination of obscenity and child pornography, and in preventing minors from being exposed to material harmful to their well-being.

2. Protecting the Unwilling Viewer

Several of the libraries that use filters assert that filters serve the libraries' interest

in preventing patrons from being unwillingly exposed to sexually explicit speech that the patrons find offensive. Nearly every library proffered by either the government or the plaintiffs received complaints, in varying degrees of frequency, from library patrons who saw other patrons accessing sexually explicit material on the library's Internet terminals.

In general, First Amendment jurisprudence is reluctant to recognize a legitimate state interest in protecting the unwilling viewer from speech that is constitutionally protected. "Where the designed benefit of a content-based speech restriction is to shield the sensibilities of listeners, the general rule is that the right of expression prevails, even where no less restrictive alternative exists. We are expected to protect our own sensibilities simply by averting our eyes." *Playboy*, 529 U.S. at 813 (2000) (internal quotation marks and citation omitted); *see also Erznoznik v. City of Jacksonville*, 422 U.S. 205, 209 (1975) ("[W]hen the government, acting as censor, undertakes selectively to shield the public from some kinds of speech on the ground that they are more offensive than others, the First Amendment strictly limits its power.").

For example, in *Cohen v. California*, 403 U.S. 15 (1971), the Supreme Court reversed defendant's conviction for wearing, in a municipal courthouse, a jacket bearing the inscription "Fuck the Draft." The Court noted that "much has been made of the claim that Cohen's distasteful mode of expression was thrust upon unwilling or unsuspecting viewers, and that the State might therefore legitimately act as it did in order to protect the sensitive from otherwise unavoidable exposure to appellant's crude form of protest." *Id.* at 21. This justification for suppressing speech failed, however, because it "would effectively

empower a majority to silence dissidents simply as a matter of personal predilections." *Id.* The Court concluded that "[t]hose in the Los Angeles courthouse could effectively avoid further bombardment of their sensibilities simply by averting their eyes." *Id.*

Similarly, in *Erznoznik*, the Court invalidated on its face a municipal ordinance prohibiting drive-in movie theaters from showing films containing nudity if they were visible from a public street or place. The city's "primary argument [was] that it may protect its citizens against unwilling exposure to materials that may be offensive." 422 U.S. at 208. The Court soundly rejected this interest in shielding the unwilling viewer:

> The plain, if at times disquieting, truth is that in our pluralistic society, constantly proliferating new and ingenious forms of expression, we are inescapably captive audiences for many purposes. Much that we encounter offends our esthetic, if not our political and moral, sensibilities. Nevertheless, the Constitution does not permit government to decide which types of otherwise protected speech are sufficiently offensive to require protection for the unwilling listener or viewer. Rather, absent . . . narrow circumstances . . . the burden normally falls upon the viewer to avoid further bombardment of his sensibilities simply by averting his eyes.

422 U.S. at 210-11 (internal quotation marks and citation omitted).

The state's interest in protecting unwilling viewers from exposure to patently offensive material is accounted for, to some degree, by obscenity doctrine, which originated in part to permit the state to shield the unwilling viewer. "The *Miller* standard, like its predecessors, was an accommodation between the State's interests in protecting the sensibilities of unwilling recipients from exposure to pornographic material and the dangers of censorship inherent in unabashedly content-based laws." *Ferber*, 458 U.S. at 756 (internal quotation marks and citation omitted); *see also Miller*, 413 U.S. at 18-19

("This Court has recognized that the States have a legitimate interest in prohibiting dissemination or exhibition of obscene material when the mode of dissemination carries with it a significant danger of offending the sensibilities of unwilling recipients or of exposure to juveniles.") (citation omitted). To the extent that speech has serious literary, artistic, political, or scientific value, and therefore is not obscene under the *Miller* test of obscenity, the state's interest in shielding unwilling viewers from such speech is tenuous.

Nonetheless, the Court has recognized that in certain limited circumstances, the state has a legitimate interest in protecting the public from unwilling exposure to speech that is not obscene. This interest has justified restrictions on speech "when the speaker intrudes on the privacy of the home, or the degree of captivity makes it impractical for the unwilling viewer or auditor to avoid exposure." *Erznoznik*, 422 U.S. at 209 (citations omitted). Thus, in *FCC v. Pacifica Foundation*, 438 U.S. 726 (1978), the Court relied on the state's interest in shielding viewers' sensibilities to uphold a prohibition against profanity in radio broadcasts:

> Patently offensive, indecent material presented over the airwaves confronts the citizen, not only in public, but also in the privacy of the home, where the individual's right to be left alone plainly outweighs the First Amendment rights of an intruder. Because the broadcast audience is constantly tuning in and out, prior warnings cannot completely protect the listener or viewer from unexpected program content.

Id. at 748 (citation omitted); *accord Frisby v. Schultz*, 487 U.S. 474, 485 (1988) ("Although in many locations, we expect individuals simply to avoid speech they do not want to hear, the home is different."); *see also Lehman v. City of Shaker Heights*, 418

U.S. 298, 302 (1974) (plurality opinion) (upholding a content-based restriction on the sale of advertising space in public transit vehicles and noting that "[t]he streetcar audience is a captive audience").

Although neither the Supreme Court nor the Third Circuit has recognized a compelling state interest in shielding the sensibilities of unwilling viewers, beyond laws intended to preserve the privacy of individuals' homes or to protect captive audiences, we do not read the case law as categorically foreclosing recognition, in the public library setting, of the state's interest in protecting unwilling viewers. *See Pacifica*, 438 U.S. at 749 n.27 ("Outside the home, the balance between the offensive speaker and the unwilling audience may *sometimes* tip in favor of the speaker, requiring the offended listener to turn away.") (emphasis added). Under certain circumstances, therefore a public library might have a compelling interest in protecting library patrons and staff from unwilling exposure to sexually explicit speech that, although not obscene, is patently offensive.

3. Preventing Unlawful or Inappropriate Conduct

Several of the librarians proffered by the government testified that unfiltered Internet access had led to occurrences of criminal or otherwise inappropriate conduct by library patrons, such as public masturbation, and harassment of library staff and patrons, sometimes rising to the level of physical assault. As in the case with patron complaints, however, the government adduced no quantitative data comparing the frequency of criminal or otherwise inappropriate patron conduct before the library's use of filters and after the library's use of filters. The sporadic anecdotal accounts of the government's library

witnesses were countered by anecdotal accounts by the plaintiffs' library witnesses, that incidents of offensive patron behavior in public libraries have long predated the advent of Internet access.

Aside from a public library's interest in preventing patrons from using the library's Internet terminals to receive obscenity or child pornography, which constitutes criminal conduct, we are constrained to reject any compelling state interest in regulating patrons' conduct as a justification for content-based restrictions on patrons' Internet access. "[T]he Court's First Amendment cases draw vital distinctions between words and deeds, between ideas and conduct." *Ashcroft*, 122 S. Ct. at 1403. First Amendment jurisprudence makes clear that speech may not be restricted on the ground that restricting speech will reduce crime or other undesirable behavior that the speech is thought to cause, subject to only a narrow exception for speech that "is directed to inciting or producing imminent lawless action and is likely to incite or produce such action." *Brandenburg v. Ohio*, 395 U.S. 444, 447 (1969) (per curiam). "The mere tendency of speech to encourage unlawful acts is insufficient reason for banning it." *Ashcroft*, 122 S. Ct. at 1403.

Outside of the narrow "incitement" exception, the appropriate method of deterring unlawful or otherwise undesirable behavior is not to suppress the speech that induces such behavior, but to attach sanctions to the behavior itself. "Among free men, the deterrents ordinarily to be applied to prevent crime are education and punishment for violations of the law, not abridgement of the rights of free speech." *Kingsley Int'l Pictures Corp. v. Regents of the Univ. of the State of New York*, 360 U.S. 684, 689 (1959) (quoting

Whitney v. Cal., 274 U.S. 357, 378 (1927) (Brandeis, J., concurring)); *see also Bartnicki v. Vopper*, 532 U.S. 514, 529 (2001) ("The normal method of deterring unlawful conduct is to impose an appropriate punishment on the person who engages in it.").

4. Summary

In sum, we reject a public library's interest in preventing unlawful or otherwise inappropriate patron conduct as a basis for restricting patrons' access to speech on the Internet. The proper method for a library to deter unlawful or inappropriate patron conduct, such as harassment or assault of other patrons, is to impose sanctions on such conduct, such as either removing the patron from the library, revoking the patron's library privileges, or, in the appropriate case, calling the police. We believe, however, that the state interests in preventing the dissemination of obscenity, child pornography, or in the case of minors, material harmful to minors, and in protecting library patrons from being unwillingly exposed to offensive, sexually explicit material, could all justify, for First Amendment purposes, a public library's use of Internet filters, provided that use of such filters is narrowly tailored to further those interests, and that no less restrictive means of promoting those interests exist. Accordingly, we turn to the narrow tailoring question.

B. Narrow Tailoring

Having identified the relevant state interests that could justify content-based restrictions on public libraries' provision of Internet access, we must determine whether a public library's use of software filters is narrowly tailored to further those interests. "It is not enough to show that the Government's ends are compelling; the means must be

carefully tailored to achieve those ends." *Sable Communications of Cal., Inc. v. FCC*, 492 U.S. 115, 126 (1989). "[M]anifest imprecision of [a] ban . . . reveals that its proscription is not sufficiently tailored to the harms it seeks to prevent to justify . . . substantial interference with . . . speech." *FCC v. League of Women Voters of Cal.*, 468 U.S. 364, 392 (1984).

The commercially available filters on which evidence was presented at trial all block many thousands of Web pages that are clearly not harmful to minors, and many thousands more pages that, while possibly harmful to minors, are neither obscene nor child pornography. *See supra*, Subsection II.E.7. Even the defendants' own expert, after analyzing filtering products' performance in public libraries, concluded that of the blocked Web pages to which library patrons sought access, between 6% and 15% contained no content that meets even the filtering products' own definitions of sexually explicit content, let alone the legal definitions of obscenity or child pornography, which none of the filtering companies that were studied use as the basis for their blocking decisions. Moreover, in light of the flaws in these studies, discussed in detail in our findings of fact above, these percentages significantly underestimate the amount of speech that filters erroneously block, and at best provide a rough lower bound on the filters' rates of overblocking. Given the substantial amount of constitutionally protected speech blocked by the filters studied, we conclude that use of such filters is not narrowly tailored with respect to the government's interest in preventing the dissemination of obscenity, child pornography, and material harmful to minors.

To be sure, the quantitative estimates of the rates of overblocking apply only to those four commercially available filters analyzed by plaintiffs' and defendants' expert witnesses. Nonetheless, given the inherent limitations in the current state of the art of automated classification systems, and the limits of human review in relation to the size, rate of growth, and rate of change of the Web, there is a tradeoff between underblocking and overblocking that is inherent in *any* filtering technology, as our findings of fact have demonstrated. We credit the testimony of plaintiffs' expert witness, Dr. Geoffrey Nunberg, that no software exists that can automatically distinguish visual depictions that are obscene, child pornography, or harmful to minors, from those that are not. Nor can software, through keyword analysis or more sophisticated techniques, consistently distinguish web pages that contain such content from web pages that do not.

In light of the absence of any automated method of classifying Web pages, filtering companies are left with the Sisyphean task of using human review to identify, from among the approximately two billion web pages that exist, the 1.5 million new pages that are created daily, and the many thousands of pages whose content changes from day to day, those particular web pages to be blocked. To cope with the Web's extraordinary size, rate of growth, and rate of change, filtering companies that rely solely on human review to block access to material falling within their category definitions must use a variety of techniques that will necessarily introduce substantial amounts of overblocking. These techniques include blocking every page of a Web site that contains only some content falling within the filtering companies' category definitions, blocking every Web site that shares an IP-

address with a Web site whose content falls within the category definitions, blocking "loophole sites," such as anonymizers, cache sites, and translation sites, and allocating staff resources to reviewing content of uncategorized pages rather than re-reviewing pages, domain names, or IP-addresses that have been already categorized to determine whether their content has changed. While a filtering company could choose not to use these techniques, due to the overblocking errors they introduce, if a filtering company does not use such techniques, its filter will be ineffective at blocking access to speech that falls within its category definitions.

Thus, while it would be easy to design, for example, a filter that blocks only ten Web sites, all of which are either obscene, child pornography, or harmful to minors, and therefore completely avoids overblocking, such a filter clearly would not comply with CIPA, since it would fail to offer any meaningful protection against the hundreds of thousands of Web sites containing speech in these categories. As detailed in our findings of fact, any filter that blocks enough speech to protect against access to visual depictions that are obscene, child pornography, and harmful to minors, will necessarily overblock substantial amounts of speech that does not fall within these categories.

This finding is supported by the government's failure to produce evidence of any filtering technology that avoids overblocking a substantial amount of protected speech. Where, as here, strict scrutiny applies to a content-based restriction on speech, the burden rests with the government to show that the restriction is narrowly tailored to serve a compelling government interest. *See Playboy*, 529 U.S. at 816 ("When the Government

restricts speech, the Government bears the burden of proving the constitutionality of its actions."); *see also R.A.V. v. City of St. Paul*, 505 U.S. 377, 382 (1992) ("Content-based regulations are presumptively invalid."). Thus, it is the government's burden, in this case, to show the existence of a filtering technology that both blocks enough speech to qualify as a technology protection measure, for purposes of CIPA, and avoids overblocking a substantial amount of constitutionally protected speech.

Here, the government has failed to meet its burden. Indeed, as discussed in our findings of fact, every technology protection measure used by the government's library witnesses or analyzed by the government's expert witnesses blocks access to a substantial amount of speech that is constitutionally protected with respect to both adults and minors. In light of the credited testimony of Dr. Nunberg, and the inherent tradeoff between overblocking and underblocking, together with the government's failure to offer evidence of any technology protection measure that avoids overblocking, we conclude that any technology protection measure that blocks a sufficient amount of speech to comply with CIPA's requirement that it "protect[] against access through such computers to visual depictions that are – (I) obscene; (II) child pornography; or (III) harmful to minors" will necessarily block substantial amounts of speech that does not fall within these categories. CIPA § 1712 (codified at 20 U.S.C. § 9134(f)(1)(A)). Hence, any public library's use of a software filter required by CIPA will fail to be narrowly tailored to the government's compelling interest in preventing the dissemination, through Internet terminals in public libraries, of visual depictions that are obscene, child pornography, or harmful to minors.

Where, as here, strict scrutiny applies, the government may not justify restrictions on constitutionally *protected* speech on the ground that such restrictions are necessary in order for the government effectively to suppress the dissemination of constitutionally *unprotected* speech, such as obscenity and child pornography. "The argument . . . that protected speech may be banned as a means to ban unprotected speech . . . . turns the First Amendment upside down. The Government may not suppress lawful speech as the means to suppress unlawful speech." *Ashcroft*, 122 S. Ct. at 1404. This rule reflects the judgment that "[t]he possible harm to society in permitting some unprotected speech to go unpunished is outweighed by the possibility that protected speech of others may be muted . . . ." *Broadrick v. Oklahoma*, 413 U.S. at 612.

Thus, in *Ashcroft*, the Supreme Court rejected the government's argument that a statute criminalizing the distribution of constitutionally protected "virtual" child pornography, produced through computer imaging technology without the use of real children, was necessary to further the state's interest in prosecuting the dissemination of constitutionally unprotected child pornography produced using real children, since "the possibility of producing images by using computer imaging makes it very difficult for [the government] to prosecute those who produce pornography using real children." *Ashcroft*, 122 S. Ct. at 1404; *see also Stanley*, 394 U.S. at 567-58 (holding that individuals have a First Amendment right to possess obscene material, even though the existence of this right makes it more difficult for the states to further their legitimate interest in prosecuting the distribution of obscenity). By the same token, even if the use of filters is effective in

preventing patrons from receiving constitutionally unprotected speech, the government's interest in preventing the dissemination of such speech cannot justify the use of the technology protection measures mandated by CIPA, which necessarily block substantial amounts of constitutionally protected speech.

CIPA thus resembles the Communications Decency Act, which the Supreme Court facially invalidated in *Reno v. ACLU*, 521 U.S. 844 (1997). Although on its face, the CDA simply restricted the distribution to minors of speech that was constitutionally unprotected with respect to minors, as a practical matter, given Web sites' difficulties in identifying the ages of Internet users, the CDA effectively prohibited the distribution to adults of material that was constitutionally protected with respect to adults.[30] Similarly, although on its face, CIPA, like the CDA, requires the suppression of only constitutionally unprotected speech, it is impossible as a practical matter, given the state of the art of filtering technology, for a public library to comply with CIPA without also blocking significant amounts of

---

[30] The Supreme Court in *Reno* explained:

> The District Court found that at the time of trial existing technology did not include any effective method for a sender to prevent minors from obtaining access to its communications on the Internet without also denying access to adults. The Court found no effective way to determine the age of a user who is accessing material through e-mail, mail exploders, newsgroups, or chat rooms. As a practical matter, the Court also found that it would be prohibitively expensive for noncommercial – as well as some commercial – speakers who have Web sites to verify that their users are adults. These limitations must inevitably curtail a significant amount of adult communication on the Internet.

Reno, 521 U.S. at 876-77 (citation omitted).

constitutionally protected speech. We therefore hold that a library's use of a technology protection measure required by CIPA is not narrowly tailored to the government's legitimate interest in preventing the dissemination of visual depictions that are obscene, child pornography, or in the case of minors, harmful to minors.

For the same reason that a public library's use of software filters is not narrowly tailored to further the library's interest in preventing its computers from being used to disseminate visual depictions that are obscene, child pornography, and harmful to minors, a public library's use of software filters is not narrowly tailored to further the library's interest in protecting patrons from being unwillingly exposed to offensive, sexually explicit material. As discussed in our findings of fact, the filters required by CIPA block substantial numbers of Web sites that even the most puritanical public library patron would not find offensive, such as http://federo.com, a Web site that promotes federalism in Uganda, which N2H2 blocked as "Adults Only, Pornography," and http://www.vvm.com/~bond/home.htm, a site for aspiring dentists, which was blocked by Cyberpatrol as "Adult/Sexually Explicit." We list many more such examples in our findings of fact, *see supra*, and find that such erroneously blocked sites number in at least the thousands.

Although we have found large amounts of overblocking, even if only a small percentage of sites blocked are erroneously blocked, either with respect to the state's interest in preventing adults from viewing material that is obscene or child pornography and in preventing minors from viewing material that is harmful to minors, or with respect to the

state's interest in preventing library patrons generally from being unwillingly exposed to offensive, sexually explicit material, this imprecision is fatal under the First Amendment. *Cf. Reno*, 521 U.S. at 874 ("[T]he CDA lacks the precision that the First Amendment requires when a statute regulates the content of speech."); *League of Women Voters*, 468 U.S. at 398 ("[E]ven if some of the hazards at which [the challenged provision] was aimed are sufficiently substantial, the restriction is not crafted with sufficient precision to remedy those dangers that may exist to justify the significant abridgement of speech worked by the provision's broad ban . . . .").

While the First Amendment does not demand perfection when the government restricts speech in order to advance a compelling interest, the substantial amounts of erroneous blocking inherent in the technology protection measures mandated by CIPA are more than simply *de minimis* instances of human error. "The line between speech unconditionally guaranteed and speech which may legitimately be regulated, suppressed, or punished is finely drawn. Error in marking that line exacts an extraordinary cost." *Playboy*, 529 U.S. at 817 (internal quotation marks and citation omitted). Indeed, "precision of regulation must be the touchstone in an area so closely touching our most precious freedoms." *Keyishian v. Bd. of Regents of the Univ. of the State of N.Y.*, 385 U.S. 589, 603 (1967) (internal quotation marks and citation omitted); *see also Bantam Books, Inc. v. Sullivan*, 372 U.S. 58, 66 (1963) ("The separation of legitimate from illegitimate speech calls for sensitive tools.") (internal quotation marks and citation omitted). Where the government draws content-based restrictions on speech in order to

advance a compelling government interest, the First Amendment demands the precision of a scalpel, not a sledgehammer. We believe that a public library's use of the technology protection measures mandated by CIPA is not narrowly tailored to further the governmental interests at stake.

Although the strength of different libraries' interests in blocking certain forms of speech may vary from library to library, depending on the frequency and severity of problems experienced by each particular library, we conclude, based on our findings of fact, that any public library's use of a filtering product mandated by CIPA will necessarily fail to be narrowly tailored to address the library's legitimate interests. Because it is impossible for a public library to comply with CIPA without blocking substantial amounts of speech whose suppression serves no legitimate state interest, we therefore hold that CIPA is facially invalid, even under the more stringent standard of facial invalidity urged on us by the government, which would require upholding CIPA if it is possible for just a single library to comply with CIPA's conditions without violating the First Amendment. *See supra* Part III.

C. Less Restrictive Alternatives

The constitutional infirmity of a public library's use of software filters is evidenced not only by the absence of narrow tailoring, but also by the existence of less restrictive alternatives that further the government's legitimate interests. *See Playboy*, 529 U.S. at 813 ("If a less restrictive alternative would serve the Government's purpose, the legislature must use that alternative."); *Sable*, 492 U.S. at 126 ("The Government may . . . regulate the

content of constitutionally protected speech in order to promote a compelling interest if it chooses the least restrictive means to further the articulated interest.").

As is the case with the narrow tailoring requirement, the government bears the burden of proof in showing the ineffectiveness of less restrictive alternatives. "When a plausible, less restrictive alternative is offered to a content-based speech restriction, it is the Government's obligation to prove that the alternative will be ineffective to achieve its goals." *Playboy*, 529 U.S. at 816; *see also Reno*, 521 U.S. at 879 ("The breadth of this content-based restriction of speech imposes an especially heavy burden on the Government to explain why a less restrictive provision would not be as effective . . . ."); *Fabulous Assocs., Inc. v. Pa. Pub. Util. Comm'n*, 896 F.2d 780, 787 (3d Cir. 1990) ("We focus . . . on the more difficult question whether the Commonwealth has borne its heavy burden of demonstrating that the compelling state interest could not be served by restrictions that are less intrusive on protected forms of expression.") (internal quotation marks and citation omitted).

We find that there are plausible, less restrictive alternatives to the use of software filters that would serve the government's interest in preventing the dissemination of obscenity and child pornography to library patrons. In particular, public libraries can adopt Internet use policies that make clear to patrons that the library's Internet terminals may not be used to access illegal content. Libraries can ensure that their patrons are aware of such policies by posting them in prominent places in the library, requiring patrons to sign forms agreeing to comply with the policy before the library issues library cards to patrons, and by

presenting patrons, when they log on to one of the library's Internet terminals, with a screen that requires the user to agree to comply with the library's policy before allowing the user access to the Internet.

Libraries can detect violations of their Internet use policies either through direct observation or through review of the library's Internet use logs. In some cases, library staff or patrons may directly observe a patron accessing obscenity and child pornography. Libraries' Internet use logs, however, also provide libraries with a means of detecting violations of their Internet use policies. These logs, which can be kept regardless whether a library uses filtering software, record the URL of every Web page accessed by patrons. Although ordinarily the logs do not link particular URLs with particular patrons, it is possible, using access logs, to identify the patron who viewed the Web page corresponding to a particular URL, if library staff discover in the access logs the URL of a Web page containing obscenity or child pornography. For example, David Biek, Director of Tacoma Public Library's main branch, testified that in the course of scanning Internet use logs he has found what looked like attempts to access child pornography, notwithstanding the fact that Tacoma uses Websense filtering software. In two cases, he communicated his findings to law enforcement and turned over the logs to law enforcement in response to a subpoena.[31]

---

[31] To the extent that filtering software is effective in identifying URLs of Web pages containing obscenity or child pornography, libraries may use filtering software as a tool for identifying URLs in their Internet use logs that fall within these categories, without requiring patrons to use filtering software. As the study of Benjamin Edelman, an expert

Once a violation of a library's Internet use policy is detected through the methods described above, a library may either issue the patron a warning, revoke the patron's Internet privileges, or notify law enforcement, if the library believes that the patron violated either state obscenity laws or child pornography laws. Although these methods of detecting use of library computers to access illegal content are not perfect, and a library, out of respect for patrons' privacy, may choose not to adopt such policies, the government has failed to show that such methods are substantially less effective at preventing patrons from accessing obscenity and child pornography than software filters. As detailed in our findings of fact, the underblocking that results from the size, rate of change, and rate of growth of the Internet significantly impairs the software filters from preventing patrons from accessing obscenity and child pornography. Unless software filters are themselves perfectly effective at preventing patrons from accessing obscenity and child pornography, "[i]t is no response that [a less restrictive alternative] . . . may not go perfectly every time." *Playboy*, 529 U.S. at 824; *cf. Denver Area Educ. Telecomm. Consortium, Inc. v. FCC*, 518 U.S. 727, 759 (1996) ("No provision . . . short of an absolute ban, can offer certain

---

witness for the plaintiffs, demonstrates, it is possible to develop software that automatically tests a list of URLs, such as the list of URLs in a public library's Internet use logs, to determine whether any of those URLs would be blocked by a particular software filter as falling within a particular category. Alternatively, library staff can review the Internet use logs by hand, skimming the list of URLs for those that are likely to correspond to Web pages containing obscenity or child pornography, as is the practice of Tacoma's David Biek, who testified as a government witness. Under either method, public libraries can assure patrons of their privacy by tracing a given URL to a particular patron only after determining that the URL corresponds to a Web site whose content is illegal.

protection against assault by a determined child.").

The government has not offered any data comparing the frequency with which obscenity and child pornography is accessed at libraries that enforce their Internet use policies through software filters with the frequency with which obscenity and child pornography is accessed at public libraries that enforce their Internet use policies through methods other than software filters. Although the government's library witnesses offered anecdotal accounts of a reduction in the use of library computers to access sexually explicit speech when filtering software was mandated, these anecdotal accounts are not a substitute for more robust analyses comparing the use of library computers to access child pornography and material that meets the legal definition of obscenity in libraries that use blocking software and in libraries that use alternative methods. *Cf*. *Playboy*, 529 U.S. at 822 ("[T]he Government must present more than anecdote and supposition.").

We acknowledge that some library staff will be uncomfortable using the "tap-on-the-shoulder" method of enforcing the library's policy against using Internet terminals to access obscenity and child pornography. The Greenville County Library, for example, experienced high turnover among library staff when staff were required to enforce the library's Internet use policy through the tap-on-the-shoulder technique. Given filters' inevitable underblocking, however, even a library that uses filtering will have to resort to a tap-on-the-shoulder method of enforcement, where library staff observes a patron openly violating the library's Internet use policy, by, for example, accessing material that is obviously child pornography but that the filtering software failed to block. Moreover, a

library employee's degree of comfort in using the tap-on-the-shoulder method will vary from employee to employee, and there is no evidence that it is impossible or prohibitively costly for public libraries to hire at least some employees who are comfortable enforcing the library's Internet use policy.

We also acknowledge that use of a tap on the shoulder delegates to librarians substantial discretion to determine which Web sites a patron may view. Nonetheless, we do not believe that this putative "prior restraint" problem can be avoided through the use of software filters, for they effectively delegate to the filtering company the same unfettered discretion to determine which Web sites a patron may view. Moreover, as noted above, violations of a public library's Internet use policy may be detected not only by direct observation, but also by reviewing the library's Internet use logs after the fact, which alleviates the need for library staff to directly confront patrons while they are viewing obscenity or child pornography.

Similar less restrictive alternatives exist for preventing minors from accessing material harmful to minors. First, libraries may use the tap-on-the-shoulder method when minors are observed using the Internet to access material that is harmful to minors. Requiring minors to use specific terminals, for example in a children's room, that are in direct view of library staff will increase the likelihood that library staff will detect minors' use of the Internet to access material harmful to minors. Alternatively, public libraries could require minors to use blocking software only if they are unaccompanied by a parent,

or only if their parent consents in advance to their child's unfiltered use of the Internet.[32] "A court should not assume that a plausible, less restrictive alternative would be ineffective; and a court should not presume parents, given full information, will fail to act." *Playboy*, 529 U.S. at 824.

In contrast to the "harmful to minors" statute upheld in *Ginsberg v. New York*, 390 U.S. 629 (1968), which permitted parents to determine whether to provide their children with access to material otherwise prohibited by the statute, CIPA, like the Communications Decency Act, which the Court invalidated in *Reno*, contains no exception for parental consent:

> [W]e noted in *Ginsberg* that "the prohibition against sales to minors does not bar parents who so desire from purchasing the magazines for their children." Under the CDA, by contrast, neither the parents' consent – nor even their participation – in the communication would avoid the application of the statute.

Reno, 521 U.S. at 865 (citation omitted); *see also Ginsberg*, 390 U.S. at 639 ("It is cardinal with us that the custody, care, and nurture of the child reside first in the parents, whose primary function and freedom include preparation for obligations the state can neither supply nor hinder." (quoting *Prince v. Massachusetts*, 321 U.S. 158, 166 (1944))).

The Court in *Playboy* acknowledged that although a regime of permitting parents

---

[32] We need not decide whether these less restrictive alternatives would themselves be constitutional. *See Fabulous Assocs., Inc. v. Pa. Pub. Util. Comm'n*, 896 F.2d 780, 787 n.6 (3d Cir. 1990) ("We intimate no opinion on the constitutionality of [a less restrictive alternative to the challenged law] . . ., inasmuch as we consider merely [its] comparative restrictiveness . . . .").

voluntarily to block cable channels containing sexually explicit programming might not be a completely effective alternative to the challenged law, which effectively required cable operators to transmit sexually explicit programming only during particular hours, the challenged law itself was not completely effective in serving the government's interest:

> There can be little doubt, of course, that under a voluntary blocking regime, even with adequate notice, some children will be exposed to signal bleed; and we need not discount the possibility that a graphic image could have a negative impact on a young child. It must be remembered, however, that children will be exposed to signal bleed under time channeling as well. . . . The record is silent as to the comparative effectiveness of the two alternatives.

Playboy, 529 U.S. at 826. Similarly, in this case, the government has offered no evidence comparing the effectiveness of blocking software and alternative methods used by public libraries to protect children from material harmful to minors.

Finally, there are other less restrictive alternatives to filtering software that further public libraries' interest in preventing patrons from unwillingly being exposed to patently offensive, sexually explicit content on the Internet. To the extent that public libraries are concerned with protecting patrons from accidentally encountering such material while using the Internet, public libraries can provide patrons with guidance in finding the material they want and avoiding unwanted material. Some public libraries also offer patrons the option of using filtering software, if they so desire. *Cf. Rowan v. Post Office Dept.*, 397 U.S. 728 (1970) (upholding a federal statute permitting individuals to instruct the Postmaster General not to deliver advertisements that are "erotically arousing or sexually provocative").

With respect to protecting library patrons from sexually explicit content viewed by other patrons, public libraries have used a variety of less restrictive methods. One alternative is simply to segregate filtered from unfiltered terminals, and to place unfiltered terminals outside of patrons' sight-lines and areas of heavy traffic. Even the less restrictive alternative of allowing unfiltered access on only a single terminal, well out of the line of sight of other patrons, however, is not permitted under CIPA, which requires the use of a technology protection measure on every computer in the library. *See* CIPA § 1721(b)(6)(C) (codified at 47 U.S.C. § 254(h)(6)(C)), CIPA § 1712 (codified at 20 U.S.C. § 9134(f)(1)(A)) (requiring a public library receiving E-rate discounts or LSTA grants to certify that it "has in place a policy of Internet safety that includes the operation of a technology protection measure with respect to *any* of its computers with Internet access . . . ." (emphasis added)); *In re Federal-State Joint Board on Universal Service: Children's Internet Protection Act*, CC Docket No. 96-45, Report and Order, FCC 01-120, ¶ 30 (Apr. 5, 2001) ("CIPA makes no distinction between computers used only by staff and those accessible to the public.").

Alternatively, libraries can use privacy screens or recessed monitors to prevent patrons from unwillingly being exposed to material viewed by other patrons. We acknowledge that privacy screens and recessed monitors suffer from imperfections as alternatives to filtering. Both impose costs on the library, particularly recessed monitors, which, according to the government's library witnesses, are expensive. Moreover, some libraries have experienced problems with patrons attempting to remove the privacy screens.

Privacy screens and recessed monitors also make it difficult for more than one person to work at the same terminal.

These problems, however, are not insurmountable. While there is no doubt that privacy screens and recessed terminals impose additional costs on libraries, the government has failed to show that the cost of privacy screens or recessed terminals is substantially greater than the cost of filtering software and the resources needed to maintain such software. Nor has the government shown that the cost of these alternatives is so high as to make their use prohibitive. With respect to the problem of patrons removing privacy screens, we find, based on the successful use of privacy screens by the Fort Vancouver Regional Library and the Multnomah County Public Library, that it is possible for public libraries to prevent patrons from removing the screens. Although privacy screens may make it difficult for patrons to work at the same terminal side by side with other patrons or with library staff, a library could provide filtered access at terminals that lack privacy screens, when patrons wish to use a terminal with others. Alternatively, a library can reserve terminals outside of patrons' sight lines for groups of patrons who wish unfiltered access.

We therefore conclude that the government has failed to show that the less restrictive alternatives discussed above are ineffective at furthering the government's interest either in preventing patrons from using library computers to access visual depictions that are obscene, child pornography, or in the case of minors, harmful to minors, or in preventing library patrons from being unwillingly exposed to patently offensive,

sexually explicit speech.

D. Do CIPA's Disabling Provisions Cure the Defect?

The Government argues that even if the use of software filters mandated by CIPA blocks a substantial amount of speech whose suppression serves no legitimate state interest, and therefore fails strict scrutiny's narrow tailoring requirement, CIPA's disabling provisions cure any lack of narrow tailoring inherent in filtering technology. The disabling provision applicable to libraries receiving LSTA grants states that "[a]n administrator, supervisor, or other authority may disable a technology protection measure . . . to enable access for bona fide research or other lawful purposes." CIPA § 1712(a)(2) (codified at 20 U.S.C. § 9134(f)(3)). CIPA's disabling provision with respect to libraries receiving E-rate discounts similarly states that "[a]n administrator, supervisor, or other person authorized by the certifying authority . . . may disable the technology protection measure concerned, during use by an adult, to enable access for bona fide research or other lawful purpose." CIPA § 1721(b) (codified at 47 U.S.C. § 254(h)(6)(D)).

To determine whether the disabling provisions cure CIPA's lack of narrow tailoring, we must first determine, as a matter of statutory construction, under what circumstances the disabling provisions permit libraries to disable the software filters.[33] It is unclear to us

[33] Whereas the disabling provision applicable to libraries that receive LSTA grants permits disabling for both adults and minors, the disabling provision applicable to libraries that receive E-rate discounts permits disabling only during adult use. Thus, the disabling provision applicable to libraries receiving E-rate discounts cannot cure the constitutional infirmity of CIPA's requirement that libraries receiving E-rate discounts use software filters when their Internet terminals are in use by minors.

whether CIPA's disabling provisions permit libraries to disable the filters any time a patron wishes to access speech that is neither obscenity, child pornography, or in the case of a minor patron, material that is harmful to minors. Whether CIPA permits disabling in such instances depends on the meaning of the provisions' reference to "bona fide research or other lawful purpose." On the one hand, the language "to enable access for bona fide research or other lawful purpose" could be interpreted to mean "to enable access to all constitutionally protected material." As a textual matter, this reading of the disabling provisions is plausible. If a patron seeks access to speech that is constitutionally protected, then it is reasonable to conclude that the patron has a "lawful purpose," since the dissemination and receipt of constitutionally protected speech cannot be made unlawful.

Moreover, since a narrower construction of the disabling provision creates more constitutional problems than a construction of the disabling provisions that permits access to all constitutionally protected speech, the broader interpretation is preferable. "[I]f an otherwise acceptable construction of a statute would raise serious constitutional problems, and where an alternative interpretation of the statute is fairly possible, we are obligated to construe the statute to avoid such problems." *INS v. St. Cyr*, 121 S. Ct. 2271, 2279 (2001) (internal quotation marks and citations omitted). On the other hand, interpreting CIPA's disabling provisions to permit disabling for access to all constitutionally protected speech presents several problems. First, if "other lawful purpose" means "for the purpose of accessing constitutionally protected speech," then this reading renders superfluous CIPA's reference to "bona fide research," which clearly contemplates some purpose beyond simply

accessing constitutionally protected speech. In general, "courts should disfavor interpretations of statutes that render language superfluous." *Conn. Nat'l Bank v. Germain*, 503 U.S. 249, 253 (1992).

Furthermore, Congress is clearly capable of explicitly specifying categories of constitutionally unprotected speech, as it did when it drafted CIPA to require funding recipients to use technology protection measures that protect against visual depictions that are "obscene," "child pornography," or, in the case of minors, "harmful to minors." CIPA § 1712(a) (codified at 20 U.S.C. § 9134(f)(1)(A)(i)(I)-(III)); CIPA § 1721(b) (codified at 47 U.S.C. § 254(h)(6)(B)(i)(I)-(III)). If Congress intended CIPA's disabling provisions simply to permit libraries to disable the filters to allow access to speech falling outside of these categories, Congress could have drafted the disabling provisions with greater precision, expressly permitting libraries to disable the filters "to enable access for any material that is not obscene, child pornography, or in the case of minors, harmful to minors," rather than "to enable access for bona fide research or other lawful purposes," which is the language that Congress actually chose.

At bottom, however, we need not definitively construe CIPA's disabling provisions, since it suffices in this case to assume without deciding that the disabling provisions permit libraries to allow a patron access to any speech that is constitutionally protected with respect to that patron. Although this interpretation raises fewer constitutional problems than a narrower interpretation, this interpretation of the disabling provisions nonetheless fails to cure CIPA's lack of narrow tailoring. Even if the disabling provisions permit public

libraries to allow patrons to access speech that is constitutionally protected yet erroneously blocked by the software filters, the requirement that library patrons ask a state actor's permission to access disfavored content violates the First Amendment.

The Supreme Court has made clear that content-based restrictions that require recipients to identify themselves before being granted access to disfavored speech are subject to no less scrutiny than outright bans on access to such speech. In *Lamont v. Postmaster General*, 381 U.S. 301 (1965), for example, the Court held that a federal statute requiring the Postmaster General to halt delivery of communist propaganda unless the addressee affirmatively requested the material violated the First Amendment:

> We rest on the narrow ground that the addressee in order to receive his mail must request in writing that it be delivered. This amounts in our judgment to an unconstitutional abridgment of the addressee's First Amendment rights. The addressee carries an affirmative obligation which we do not think the Government may impose on him. This requirement is almost certain to have a deterrent effect, especially as respects those who have sensitive positions.

Id. at 307.

Similarly, in *Denver Area Educational Telecommunications Consortium, Inc. v. FCC*, 518 U.S. 727 (1996), the Court held unconstitutional a federal law requiring cable operators to allow access to patently offensive, sexually explicit programming only to those subscribers who requested access to the programming in advance and in writing. *Id.* at 732-33. As in *Lamont*, the Court in *Denver* reasoned that this content-based restriction on recipients' access to speech would have an impermissible chilling effect: "[T]he written notice requirement will . . . restrict viewing by subscribers who fear for their reputations

should the operator, advertently or inadvertently, disclose the list of those who wish to watch the 'patently offensive' channel." *Id.* at 754; *see also Fabulous Assocs., Inc. v. Pa. Pub. Util. Comm'n*, 896 F.2d 780, 785 (3d Cir. 1990) (considering the constitutionality of a state law requiring telephone users who wish to listen to sexually explicit telephone messages to apply for an access code to receive such messages, and invalidating the law on the ground that "[a]n identification requirement exerts an inhibitory effect").

We believe that CIPA's disabling provisions suffer from the same flaws as the restrictions on speech in *Lamont*, *Denver*, and *Fabulous Associates*. By requiring library patrons affirmatively to request permission to access certain speech singled out on the basis of its content, CIPA will deter patrons from requesting that a library disable filters to allow the patron to access speech that is constitutionally protected, yet sensitive in nature. As we explain above, we find that library patrons will be reluctant and hence unlikely to ask permission to access, for example, erroneously blocked Web sites containing information about sexually transmitted diseases, sexual identity, certain medical conditions, and a variety of other topics. As discussed in our findings of fact, software filters block access to a wide range of constitutionally protected speech, including Web sites containing information that individuals are likely to wish to access anonymously.

That library patrons will be deterred from asking permission to access Web sites containing certain kinds of content is evident as a matter of common sense as well as amply borne out by the trial record. Plaintiff Emmalyn Rood, who used the Internet at a public library to research information relating to her sexual identity, testified that she would have

been unwilling as a young teen to ask a librarian to disable filtering software so that she could view materials concerning gay and lesbian issues.[34] Similarly, plaintiff Mark Brown stated that he would have been too embarrassed to ask a librarian to disable filtering software if it had impeded his ability to research surgery options for his mother when she was treated for breast cancer.[35] As explained in our findings of fact, *see supra* at Subsection II.D.2.b, the reluctance of patrons to request permission to access Web sites that were erroneously blocked is further established by the low number of patron unblocking requests, relative to the number of erroneously blocked Web sites, in those public libraries that use software filters and permit patrons to request access to incorrectly blocked Web sites. *Cf. Fabulous Assocs.*, 896 F.2d at 786 ("On the record before us, there is more than enough evidence to support the district court's finding that access codes will chill the exercise of some users' right to hear protected communications.").

To be sure, the government demonstrated that it is possible for libraries to permit patrons to request anonymously that a particular Web site be unblocked. In particular, the

---

[34] Software filters sometimes incorrectly block access to, *inter alia*, Web sites dealing with issues relating to sexual identity. For example, the "Gay and Lesbian Chamber of Southern Nevada," http://www.lambdalv.com, "a forum for the business community to develop relationships within the Las Vegas lesbian, gay transsexual, and bisexual community" was blocked by N2H2 as "Adults Only, Pornography." The home page of the Lesbian and Gay Havurah of the Long Beach, California Jewish Community Center, http://www.compupix.com/gay/havurah.htm, was blocked by N2H2 as "Adults Only, Pornography," by Smartfilter as "Sex," and by Websense as "Sex."

[35] Among the types of Web sites that filters erroneously block are Web sites dealing with health issues, such as the Web site of the Willis-Knighton Cancer Center, a Shreveport, Louisiana cancer treatment facility, http://cancerftr.wkmc.com, which was blocked by Websense under the "Sex" category.

Tacoma Public Library has configured its computers to present patrons with the option, each time the software filter blocks their access to a Web page, of sending an anonymous email to library staff requesting that the page be unblocked. Moreover, a library staff member periodically scans logs of URLs blocked by the filters, in an effort to identify erroneously blocked sites, which the library will subsequently unblock. Although a public library's ability to permit anonymous unblocking requests addresses the deterrent effect of requiring patrons to identify themselves before gaining access to a particular Web site, we believe that it fails adequately to address the overblocking problem.

In particular, even allowing anonymous requests for unblocking burdens patrons' access to speech, since such requests cannot immediately be acted on. Although the Tacoma Public Library, for example, attempts to review requests for unblocking within 24 hours, requests sometimes are not reviewed for several days. And delays are inevitable in libraries with branches that lack the staff necessary immediately to review patron unblocking requests. Because many Internet users "surf" the Web, visiting hundreds of Web sites in a single session and spending only a short period of time viewing many of the sites, the requirement that a patron take the time to affirmatively request access to a blocked Web site and then wait several days until the site is unblocked will, as a practical matter, impose a significant burden on library patrons' use of the Internet. Indeed, a patron's time spent requesting access to an erroneously blocked Web site and checking to determine whether access was eventually granted is likely to exceed the amount of time the patron would have actually spent viewing the site, had the site not been erroneously

blocked. This delay is especially burdensome in view of many libraries' practice of limiting their patrons to a half hour or an hour of Internet use per day, given the scarcity of terminal time in relation to patron demand.

The burden of requiring library patrons to ask permission to view Web sites whose content is disfavored resembles the burden that the Supreme Court found unacceptable in *Denver*, which invalidated a federal law requiring cable systems operators to block subscribers' access to channels containing sexually explicit programming, unless subscribers requested unblocking in advance. The Court reasoned that "[t]hese restrictions will prevent programmers from broadcasting to viewers who select programs day by day (or, through 'surfing,' minute by minute) . . . ." *Denver*, 518 U.S. at 754. Similarly, in *Fabulous Associates*, the Third Circuit explained that a law preventing adults from listening to sexually explicit phone messages unless they applied in advance for access to such messages would burden adults' receipt of constitutionally protected speech, given consumers' tendency to purchase such speech on impulse. *See Fabulous Assocs.*, 896 F.2d at 785 (noting that officers of two companies that sell access to sexually explicit recorded phone messages "testified that it is usually 'impulse callers' who utilize these types of services, and that people will not call if they must apply for an access code").

In sum, in many cases, as we have noted above, library patrons who have been wrongly denied access to a Web site will decline to ask the library to disable the filters so that the patron can access the Web site. Moreover, even if patrons requested unblocking every time a site is erroneously blocked, and even if library staff granted every such

request, a public library's use of blocking software would still impermissibly burden patrons' access to speech based on its content. The First Amendment jurisprudence of the Supreme Court and the Third Circuit makes clear that laws imposing content-based burdens on access to speech are no less offensive to the First Amendment than laws imposing content-based prohibitions on speech:

> It is of no moment that the statute does not impose a complete prohibition. The distinction between laws burdening and laws banning speech is but a matter of degree. The Government's content-based burdens must satisfy the same rigorous scrutiny as its content-based bans. . . . When the purpose and design of a statute is to regulate speech by reason of its content, special consideration or latitude is not afforded to the Government merely because the law can somehow be described as a burden rather than outright suppression.

United States v. Playboy Entm't Group, Inc., 529 U.S. 803, 812, 826 (2000) (invalidating a federal law requiring cable television operators to limit the transmission of sexually explicit programming to the hours between 10:00 p.m. and 6:00 a.m.); *see also Fabulous Assocs.*, 896 F.2d at 785 ("[H]ere . . . there is no outright prohibition of indecent communication. However, the First Amendment protects against government inhibition as well as prohibition.") (internal quotation marks and citation omitted).

Even if CIPA's disabling provisions could be perfectly implemented by library staff every time patrons request access to an erroneously blocked Web site, we hold that the content-based burden that the library's use of software filters places on patrons' access to speech suffers from the same constitutional deficiencies as a complete ban on patrons' access to speech that was erroneously blocked by filters, since patrons will often be

deterred from asking the library to unblock a site and patron requests cannot be immediately reviewed. We therefore hold that CIPA's disabling provisions fail to cure CIPA's lack of narrow tailoring.

VI. Conclusion; Severability

Based upon the foregoing discussion, we hold that a public library's content-based restriction on patrons' access to speech on the Internet is subject to strict scrutiny. Every item in a library's print collection has been selected because library staff, or a party to whom staff delegates the decision, deems the content to be particularly valuable. In contrast, the Internet, as a forum, is open to any member of the public to speak, and hence, even when a library provides filtered Internet access, it creates a public forum in which the vast majority of the speech has been reviewed by neither librarians nor filtering companies. Under public forum doctrine, where the state creates such a forum open to any member of the public to speak on an unlimited number of subjects, the state's decision selectively to exclude certain speech on the basis of its content, is subject to strict scrutiny, since such exclusions risk distorting the marketplace of ideas that the state has created.

Application of strict scrutiny to public libraries' content-based restrictions on their patrons' access to the Internet finds further support in the analogy to traditional public fora, such as sidewalks, parks, and squares, in which content-based restrictions on speech are always subject to strict scrutiny. Like these traditional public fora, Internet access in public libraries uniquely promotes First Amendment values, by offering low barriers to entry to speakers and listeners. The content of speech on the Internet is as diverse as

human thought, and the extent to which the Internet promotes First Amendment values is evident from the sheer breadth of speech that this new medium enables.

To survive strict scrutiny, a public library's use of filtering software must be narrowly tailored to further a compelling state interest, and there must be no less restrictive alternative that could effectively further that interest. We find that, given the crudeness of filtering technology, any technology protection measure mandated by CIPA will necessarily block access to a substantial amount of speech whose suppression serves no legitimate government interest. This lack of narrow tailoring cannot be cured by CIPA's disabling provisions, because patrons will often be deterred from asking the library's permission to access an erroneously blocked Web page, and anonymous requests for unblocking cannot be acted on without delaying the patron's access to the blocked Web page, thereby impermissibly burdening access to speech on the basis of its content.

Moreover, less restrictive alternatives exist to further a public library's legitimate interests in preventing its computers from being used to access obscenity, child pornography, or in the case of minors, material harmful to minors, and in preventing patrons from being unwillingly exposed to patently offensive, sexually explicit speech. Libraries may use a variety of means to monitor their patrons' use of the Internet and impose sanctions on patrons who violate the library's Internet use policy. To protect minors from material harmful to minors, libraries could grant minors unfiltered access only if accompanied by a parent, or upon parental consent, or could require minors to use unfiltered terminals in view of library staff. To prevent patrons from being unwillingly

exposed to offensive, sexually explicit content, libraries can offer patrons the option of using blocking software, can place unfiltered terminals outside of patrons' sight lines, and can use privacy screens and recessed monitors. While none of these less restrictive alternatives are perfect, the government has failed to show that they are significantly less effective than filtering software, which itself fails to block access to large amounts of speech that fall within the categories sought to be blocked.

In view of the severe limitations of filtering technology and the existence of these less restrictive alternatives, we conclude that it is not possible for a public library to comply with CIPA without blocking a very substantial amount of constitutionally protected speech, in violation of the First Amendment. Because this conclusion derives from the inherent limits of the filtering technology mandated by CIPA, it holds for any library that complies with CIPA's conditions. Hence, even under the stricter standard of facial invalidity proposed by the government, which would require us to uphold CIPA if only a single library can comply with CIPA's conditions without violating the First Amendment, we conclude that CIPA is facially invalid, since it will induce public libraries, as state actors, to violate the First Amendment. Because we hold that CIPA is invalid on these grounds, we need not reach the plaintiffs' alternative theories that CIPA is invalid as a prior restraint on speech and is unconstitutionally vague. Nor need we decide whether CIPA is invalid because it requires public libraries, as a condition on the receipt of federal funds, to relinquish their own First Amendment rights to provide the public with unfiltered Internet

access, a theory that we nonetheless feel constrained to discuss (at length) in the margin.[36]

---

[36] Although in light of our disposition of the plaintiffs' *Dole* claim, we do not rule upon plaintiffs' contention that CIPA's conditioning of funds on the installation of filtering software violates the doctrine of unconstitutional conditions, we are mindful of the need to frame the disputed legal issues and to develop a full factual record for the certain appeal to the Supreme Court. *Cf. Ashcroft v. ACLU*, 2002 U.S. LEXIS 3421 (May 13, 2002) (remanding the case to the Court of Appeals to review the legal and factual bases on which the District Court granted plaintiffs' motion for a preliminary injunction after vacating its opinion that relied on a different ground from the ones used by the District Court). Although we do not decide the plaintiffs' unconstitutional conditions claim, we think that our findings of fact on public libraries, their use of the Internet, and the technological limitations of Internet filtering software, *see supra* Subsections II.D-E, and our framing of the legal issue here, would allow the Supreme Court to decide the issue if it deems it necessary to resolve this case.

The doctrine of unconstitutional conditions "holds that the government 'may not deny a benefit to a person on a basis that infringes his constitutionally protected . . . freedom of speech' even if he has no entitlement to that benefit." *Bd. of County Comm'rs v. Umbehr*, 518 U.S. 668, 674 (1996) (quoting *Perry v. Sindermann*, 408 U.S. 593, 597 (1972)). In this case, the plaintiffs argue that CIPA imposes an unconstitutional condition on libraries who receive E-rate and LSTA subsidies by requiring them, as a condition on their receipt of federal funds, to surrender their First Amendment right to provide the public with access to constitutionally protected speech. Under this theory, even if it does not violate the First Amendment for a public library to use filtering software, it nonetheless violates the First Amendment for the federal government to require public libraries to use filters as a condition of the receipt of federal funds.

The government contends that this case does not fall under the unconstitutional conditions framework because: (1) as state actors, the recipients of the funds (the public libraries) are not protected by the First Amendment, and therefore are not being asked to relinquish any constitutionally protected rights; and (2) although library patrons are undoubtedly protected by the First Amendment, they are not the funding recipients in this case, and libraries may not rely on their patrons' rights in order to state an unconstitutional conditions claim.

It is an open question in this Circuit whether Congress may violate the First Amendment by restricting the speech of public entities, such as municipalities or public libraries. The only U.S. Supreme Court opinion to weigh in on the issue is a concurrence by Justice Stewart, joined by Chief Justice Burger and Justice Rehnquist, in which he opined that municipalities and other arms of the state are not protected by the First Amendment from governmental interference with their expression. *See Colum. Broad. Sys., Inc. v. Democratic Nat'l Comm.*, 412 U.S. 94, 139 (1973) (Stewart, J., concurring)

("The First Amendment protects the press *from* governmental interference; it confers no analogous protection *on* the Government."); *see also id.* at 139 n.7 ("The purpose of the First Amendment is to protect private expression and nothing in the guarantee precludes the government from controlling its own expression or that of its agents.") (quoting Thomas Emerson, *The System of Freedom of Expression* 700 (1970) (internal quotation marks omitted)). The Court has subsequently made it clear, however, that it considers it to be an open question whether municipalities acting in their capacity as employers have First Amendment rights, suggesting that the question whether public entities are ever protected by the First Amendment also remains open. *See City of Madison Joint Sch. Dist. No. 8 v. Wisc. Employment Relations Comm'n*, 429 U.S. 167, 175 n.7 (1976) ("We need not decide whether a municipal corporation as an employer has First Amendment rights to hear the views of its citizens and employees.").

Several courts of appeals have cited Justice Stewart's concurrence in *Columbia Broadcasting Systems* and have, with little discussion or analysis, concluded that a "government . . . speaker is not itself protected by the first amendment." *Warner Cable Communications, Inc. v. City of Niceville*, 911 F.2d 634, 638 (11th Cir. 1990); *see also NAACP v. Hunt*, 891 F.2d 1555, 1565 (11th Cir. 1990) ("[T]he First Amendment protects citizens' speech only from government regulation; government speech itself is not protected by the First Amendment."); *Student Gov't Ass'n v. Bd. of Trustees of the Univ. of Mass.*, 868 F.2d 473, 481 (1st Cir. 1989) (concluding that the legal services organization run by a state university, "as a state entity, itself has no First Amendment rights"); *Estiverne v. La. State Bar Ass'n*, 863 F.2d 371, 379 (5th Cir. 1989) (noting that "the first amendment does not protect government speech").

We do not think that the question whether public libraries are protected by the First Amendment can be resolved as simply as these cases suggest. This difficulty is demonstrated by the reasoning of the Seventh Circuit in a case in which that court considered whether municipalities are protected by the First Amendment and noted that it is an open question that could plausibly be answered in the affirmative, yet declined to decide it:

> Only a few cases address the question whether municipalities or other state subdivisions or agencies have any First Amendment rights. . . . The question is an open one in this circuit, and we do not consider the answer completely free from doubt. For many purposes, for example diversity jurisdiction and Fourteenth Amendment liability, municipalities are treated by the law as if they were persons. *Monell v. Department of Social Services*, 436 U.S. 658, 690 (1978); *Moor v. County of Alameda*, 411 U.S. 693, 717-18 (1973). There is at least an argument that the marketplace of ideas would be unduly curtailed if municipalities could not freely express

themselves on matters of public concern, including the subsidization of housing and the demographic makeup of the community.

To the extent, moreover, that a municipality is the voice of its residents—is, indeed, a megaphone amplifying voices that might not otherwise be audible—a curtailment of its right to speak might be thought a curtailment of the unquestioned First Amendment rights of those residents. *See* Meir Dan-Cohen, "Freedoms of Collective Speech: A Theory of Protected Communications by Organizations, Communities, and the State," 79 Calif. L. Rev. 1229, 1261-63 (1991); *cf. Student Government Ass'n v. Board of Trustees*, *supra*, 868 F.2d at 482. Thus if federal law imposed a fine on municipalities that passed resolutions condemning abortion, one might suppose that a genuine First Amendment issue would be presented. Against this suggestion can be cited the many cases which hold that municipalities lack standing to invoke the Fourteenth Amendment against actions by the state. E.g., *Coleman v. Miller*, 307 U.S. 433, 441 (1939); *Williams v. Mayor & City Council of Baltimore*, 289 U.S. 36, 40 (1933); *City of East St. Louis v. Circuit Court for the Twentieth Judicial Circuit*, 986 F.2d 1142, 1144 (7th Cir. 1993). But it is one thing to hold that a municipality cannot interpose the Fourteenth Amendment between itself and the state of which it is the creature, *Anderson v. City of Boston*, 380 N.E.2d 628, 637-38 (Mass. 1978), appeal dismissed for want of a substantial federal question, 439 U.S. 1060 (1979), and another to hold that a municipality has no rights against the federal government or another state. *Township of River Vale v. Town of Orangetown*, 403 F.2d 684, 686 (2d Cir. 1968), distinguishes between these two types of cases.

Creek v. Village of Westhaven, 80 F.3d 186, 192-93 (7th Cir. 1996).

We also note that there is no textual support in the First Amendment for distinguishing between, for example, municipal corporations, and private corporations, which the Court has recognized have cognizable First Amendment rights. *First Nat'l Bank of Boston v. Bellotti*, 435 U.S. 765, 775-76 (1978). Unlike other provisions in the Bill of Rights, which the Supreme Court has held to be "purely personal" and thus capable of being invoked only by individuals, the First Amendment is not phrased in terms of who holds the right, but rather what is protected. *Compare* U.S. Const. amend V ("No *person* shall be held to answer . . .") (emphasis added) *with* U.S. Const. amend I ("Congress shall make no law . . . abridging the freedom of speech, or of the press . . . ."); *see also United States v. White*, 322 U.S. 694, 698-701 (1944) (holding that the privilege against self-incrimination applies only to natural persons).

The Supreme Court relied on this distinction (i.e., that the First Amendment protects a class of speech rather than a class of speakers) in a similar context in *Bellotti.* There, the Court invalidated a Massachusetts statute that prohibited corporations from spending money to influence ballot initiatives that did not bear directly on their "property, business or assets." *Id.* at 768. In so holding, the Court rejected the argument that the First Amendment protects only an individual's expression. The Court wrote:

> The Constitution often protects interests broader than those of the party seeking their vindication. . . . The proper question therefore is not whether corporations "have" First Amendment rights and, if so, whether they are coextensive with those of natural persons. Instead, the question must be whether [the government is] abridg[ing] expression that the First Amendment was meant to protect.

Id. at 776. The Court thus concluded that corporations are entitled to assert First Amendment claims as speakers, noting that "[t]he inherent worth of the speech in terms of its capacity for informing the public does not depend upon the identity of its source, whether corporation, association, union, or individual." *Id.* at 777.

In view of the foregoing, the notion that public libraries may assert First Amendment rights for the purpose of making an unconstitutional conditions claim is clearly plausible, and may well be correct. But even if it is not, we think it plausible that they could rely on their patrons' rights, even though their patrons are not the ones who are directly receiving the federal funding. In similar cases, the Supreme Court has entertained unconstitutional conditions claims both by the organizations that receive federal funding and by their constituents. *See Legal Servs. Corp. v. Velazquez*, 531 U.S. 533, 537 (2001) ("Lawyers employed by New York City LSC grantees, together with private LSC contributors, LSC indigent clients, and various state and local public officials whose governments contribute to LSC grantees, brought suit . . . to declare the restriction [on LSC lawyers' ability advocate the amendment of or to challenge the constitutionality of existing welfare law] . . . invalid."); *Rust v. Sullivan*, 500 U.S. 173, 181 (1991) ("Petitioners are Title X grantees and doctors who supervise Title X funds suing on behalf of themselves and their patients. . . . Petitioners challenged the regulations on the grounds that . . . they violate the First and Fifth Amendment rights of Title X clients and the First Amendment rights of Title X health providers."); *FCC v. League of Women Voters of Cal.*, 468 U.S. 364, 370 n.6 (1984) (reviewing a First Amendment challenge to conditions on public broadcasters' receipt of federal funds, in which the plaintiffs included not only the owner of a public television station, but also viewers of the station's programs, including the League of Women Voters, and "Congressman Henry Waxman, . . . a regular listener and viewer of public broadcasting").

The question whether CIPA's requirement that libraries use filtering software constitutes an unconstitutional condition is not an easy one. The Supreme Court has held that it violates the First Amendment for the federal government to require public broadcasting stations that receive federal funds not to editorialize, *see League of Women Voters*, 468 U.S. at 366, 402; for states to subsidize "newspaper and religious, professional, trade, and sports journals," but not "general interest magazines," *Ark. Writers' Project, Inc. v. Ragland*, 481 U.S. 221, 223 (1987); for a state university to subsidize student publications only on the condition that they do not "primarily promote[] or manifest[] a particular belief in or about a deity or an ultimate reality," *Rosenberger v. Rector & Visitors of Univ. of Va.*, 515 U.S. 819, 823 (1995); and for the federal government to prevent legal services providers who receive federal funds from seeking to "amend or otherwise challenge existing welfare law." *Velazquez*, 531 U.S. at 537. On the other hand, the Supreme Court has held that it does not violate the First Amendment for the federal government to require healthcare providers who receive federal funds not to "encourage, promote or advocate abortion as a method of family planning," *Rust*, 500 U.S. at 180; for the federal government to subsidize charitable organizations only if they do not engage in lobbying activity, *see Regan v. Taxation with Representation*, 461 U.S. 540 (1983); and for the National Endowment for the Arts, in awarding grants on the basis of artistic excellence, to "take into consideration general standards of decency and respect for the diverse beliefs and values of the American Public." *NEA v. Finley*, 524 U.S. 569, 572 (1998).

In light of the facts that we discuss above regarding the operation of public libraries, and the limits of Internet filtering software, *see supra* Sections II.D-E, we believe that the plaintiffs have a good argument that this case is more analogous to *League of Women Voters*, *Arkansas Writers' Project*, and *Velazquez* than it is to *Rust*, *Finley* and *Taxation with Representation*. Like the law invalidated in *League of Women Voters*, which targeted editorializing, and the law invalidated in *Arkansas Writers' Project*, which targeted general interest magazines but not "religious, professional, trade, and sports journals," the law in this case places content-based restrictions on public libraries' possible First Amendment right to provide patrons with access to constitutionally protected material. *See Arkansas Writers' Project*, 481 U.S. at 229 ("[T]he basis on which Arkansas differentiates between magazines is particularly repugnant to First Amendment principles: a magazine's tax status depends entirely on its *content*. Above all else, the First Amendment means that government has no power to restrict expression because of its message, its ideas, its subject matter, or its content.") (internal quotation marks and citations omitted); *League of Women Voters*, 468 U.S. at 383 ("[T]he scope of [the challenged statute's] ban is defined solely on the basis of the content of the suppressed speech."). *See generally Rosenberger*, 515 U.S. at 828 ("It is axiomatic that the government may not regulate speech based on its substantive content or the message it conveys."). Because of the

technological limitations of filtering software described in such detail above, Congress's requirement that public libraries use such software is in effect a requirement that public libraries block a substantial amount of constitutionally protected speech on the basis of its content.

Plaintiffs' argument that the federal government may not require public libraries who receive federal funds to restrict the availability of constitutionally protected Web sites solely on the basis of the sites' content finds further support in the role that public libraries have traditionally served in maintaining First Amendment values. As evidenced by the many public libraries that have endorsed the Freedom to Read Statement and the Library Bill of Rights, *see supra* Subsection II.D.1, public libraries seemingly have a duty to challenge prevailing orthodoxy and make available to the public controversial, yet constitutionally protected material, even if it means drawing the ire of the community. *See Bd. of Educ. v. Pico*, 457 U.S. 853, 915 (1982) (Rehnquist, J., dissenting) (noting that "public libraries" are "designed for freewheeling inquiry").

By interfering with public libraries' discretion to make available to patrons as wide a range of constitutionally protected speech as possible, the federal government is arguably distorting the usual functioning of public libraries as places of freewheeling inquiry. The *Velazquez* Court, in invalidating the federal government's restrictions on the ability of federally funded legal services providers to challenge the constitutionality of welfare laws, relied on the manner in which the restrictions that the federal government placed on legal services' attorneys' speech distorted the usual functioning of the judicial system:

> [T]he Government seeks to use an existing medium of expression and to control it, in a class of cases, in ways which distort its usual functioning. . . . The First Amendment forb[ids] the Government from using the forum in an unconventional way to suppress speech inherent in the nature of the medium.

531 U.S. at 543. By the same token, CIPA arguably distorts the usual functioning of public libraries both by requiring libraries to: (1) deny patrons access to constitutionally protected speech that libraries would otherwise provide to patrons; and (2) delegate decision making to private software developers who closely guard their selection criteria as trade secrets and who do not purport to make their decisions on the basis of whether the blocked Web sites are constitutionally protected or would add value to a public library's collection.

At all events, CIPA clearly does not seem to serve the purpose of limiting the extent of government speech given the extreme diversity of speech on the Internet. Nor can Congress's decision to subsidize Internet access be said to promote a governmental message or constitute governmental speech, even under a generous understanding of the concept. As the Court noted in *Reno v. ACLU*, 521 U.S. 844 (1997), "[i]t is no

Having determined that CIPA violates the First Amendment, we would usually be required to determine whether CIPA is severable from the remainder of the statutes governing LSTA and E-rate funding. Neither party, however, has advanced the argument that CIPA is not severable from the remainder the Library Services and Technology Act and Communications Act of 1934 (the two statutes governing LSTA and E-rate funding, respectively), and at all events, we think that CIPA is severable.

"The inquiry into whether a statute is severable is essentially an inquiry into legislative intent." *Minn. v. Mille Lacs Band of Chippewa Indians*, 526 U.S. 172, 191 (1999). "Unless it is evident that the legislature would not have enacted those provisions which are within its power, independently of that which is not, the invalid part may be

---

exaggeration to conclude that the content on the Internet is as diverse as human thought." *Id.* at 852 (internal quotation marks omitted). Even with software filters in place, the sheer breadth of speech available on the Internet defeats any claim that CIPA is intended to facilitate the dissemination of governmental speech. Like in *Velazquez*, "there is no programmatic message of the kind recognized in *Rust* and which sufficed there to allow the Government to specify the advice deemed necessary for its legitimate objectives." *Velazquez*, 531 U.S. at 548.

In sum, we think that the plaintiffs have good arguments that they may assert an unconstitutional conditions claim by relying either on the public libraries' First Amendment rights or on the rights of their patrons. We also think that the plaintiffs have a good argument that CIPA's requirement that public libraries use filtering software distorts the usual functioning of public libraries in such a way that it constitutes an unconstitutional condition on the receipt of funds. We do not decide these issues, confident that our findings of fact on the functioning of public libraries, their use of the Internet, and the technological limitations of Internet filtering software, *see supra* Sections II.D-E, would allow the Supreme Court to decide the unconstitutional conditions claim if the Court deems it necessary.

dropped if what is left is fully operative as a law." *Buckley v. Valeo*, 424 U.S. 1, 108 (1976) (internal quotation marks and citation omitted). There is no doubt that if we were to strike CIPA from the sections of the United States Code where it is currently codified, the remaining statutory sections, providing eligible public libraries with E-rate discounts and LSTA grants, would be fully operative as law. Indeed, the LSTA and E-rate programs existed prior to the enactment of CIPA in substantially the same form as they would exist were we to strike CIPA and leave the rest of the programs intact.

The second question, whether Congress would in this case have chosen to repeal the LSTA and E-rate subsidy programs instead of continuing to fund them if it had known that CIPA's limitations on these programs were constitutionally invalid, is less clear. CIPA contains "separability" clauses that state that if any of its additions to the statutes governing the LSTA and E-rate programs are found to be unconstitutional, Congress intended to effectuate as much of CIPA's amendments as possible.[37] We interpret these clauses to mean, for example, that if a court were to find that CIPA's requirements are unconstitutional with respect to adult patrons, but permissible with respect to minors, that

---

[37] CIPA § 1712(a)(2) contains a provision titled "Separability," which is codified in the Library Services and Technology Act, 20 U.S.C. § 9134(f)(6), and provides: "If any provision of this subsection is held invalid, the remainder of this subsection shall not be affected thereby." CIPA section 1721(e) also contained a similar provision that applied to E-rate funding, although it was not codified in the Communications Act. That section, also titled "Separability," provided: "If any provision of paragraph (5) or (6) of section 254(h) of the Communications Act of 1934, as amended by this section, or the application thereof to any person or circumstance is held invalid, the remainder of such paragraph and the application of such paragraph to other persons or circumstances shall not be affected thereby." CIPA § 1721(e).

Congress intended to have the court effectuate only the provisions with respect to minors. These separability clauses do not speak to the situation before us, however, where we have found that CIPA is facially unconstitutional in its entirety.

Nevertheless, the government has not pointed to anything in the legislative history or elsewhere to suggest that Congress intended to discontinue funding under the LSTA and E-rate programs unless it could effectuate CIPA's restrictions on the funding. And Congress's decision, prior to CIPA's enactment, to subsidize Internet access through the LSTA and E-rate programs without such restrictions, counsels that we reach the opposite conclusion. At bottom, we think that it is unclear what Congress's intent was on this point, and in the absence of such information, we exercise a presumption in favor of severability. *Regan v. Time, Inc.*, 468 U.S. 641, 653 (1984) ("[T]he presumption is in favor of severability."); *cf. Velazquez v. Legal Servs. Corp.*, 164 F.3d 757, 773 (2d Cir. 1999), *aff'd* 531 U.S. 533 (2001) (applying a presumption in favor of severability in the face of uncertainty whether Congress intended to fund the Legal Services Corporation even if a restriction on the funding was to be declared invalid).

For the foregoing reasons, we will enter a final judgment declaring Sections 1712(a)(2) and 1721(b) of the Children's Internet Protection Act, codified at 20 U.S.C. § 9134(f) and 47 U.S.C. § 254(h)(6), respectively, to be facially invalid under the First Amendment and permanently enjoining the defendants from enforcing those provisions.

_____

Edward R. Becker, Chief Circuit Judge

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA

AMERICAN LIBRARY ASSOCIATION, INC., et al.	:	CIVIL ACTION
v.	:	
UNITED STATES, et al.	:	NO. 01-1303
MULTNOMAH COUNTY PUBLIC LIBRARY, et al.	:	CIVIL ACTION
v.	:	
UNITED STATES OF AMERICA, et al.	:	NO. 01-1322

ORDER

AND NOW, this day of May, 2002, based on the foregoing findings of fact and conclusions of law, it is hereby ORDERED that:

(1) judgment is entered in favor of the plaintiffs and against the defendants, declaring that §§ 1712(a)(2) and 1721(b) of the Children's Internet Protection Act, 20 U.S.C. § 9134(f) and 47 U.S.C. § 254(h)(6), are facially invalid under the First Amendment to the United States Constitution; and

(2) the United States, Michael Powell, in his official capacity as Chairman of the Federal Communications Commission, the Federal Communications Commission, Beverly Sheppard, in her official capacity as Acting Director of the Institute of Museum

and Library Services, and the Institute of Museum and Library Services are permanently enjoined from withholding federal funds from any public library for failure to comply with §§ 1712(a)(2) and 1721(b) of the Children's Internet Protection Act, 20 U.S.C. § 9134(f) and 47 U.S.C. § 254(h)(6).

BY THE COURT:

_____
Ch. Cir. J.

_____
J.

_____
J.