IV. THE FIRST AMENDMENT AND CENSORSHIP OF INTERNET CONTENT

A. Sexually Explicit Speech

RENO v. AMERICAN CIVIL LIBERTIES UNION
521 U.S. 844 (1997)

JUSTICE STEVENS delivered the opinion of the Court.

At issue is the constitutionality of two statutory provisions enacted to protect minors from "indecent" and "patently offensive" communications on the Internet. Notwithstanding the importance of the goal of protecting children from harmful materials, we agree with the three-judge District Court that the statute abridges the First Amendment.

I

The District Court made extensive findings of fact. The findings describe the character and the dimensions of the Internet, the availability of sexually explicit material in that medium, and the problems confronting age verification for recipients of Internet communications. Because those findings provide the underpinnings for the legal issues, we begin with a summary of the undisputed facts.

The Internet

The Internet is an international network of interconnected computers. It is the outgrowth of what began in 1969 as a military program called "ARPANET," which was designed to enable computers operated by the military, defense contractors, and universities conducting defense-related research to communicate with one another by redundant channels even if some portions of the network were damaged in a war. While the ARPANET no longer exists, it provided an example for the development of a number of civilian networks that, eventually linking with each other, now enable tens of millions of people to communicate with one another and to access vast amounts of information from around the world. The Internet is "a unique and wholly new medium of worldwide human communication."

Anyone with access to the Internet may take advantage of a wide variety of communication retrieval methods. These methods are constantly evolving and difficult to categorize precisely. But, as presently constituted, those most relevant to this case are e-mail, automatic mailing list services (mail exploders, sometimes referred to as listservs), newsgroups, chat rooms, and the World Wide Web. All of these methods can be used to transmit text; most can transmit sound, pictures, and moving video images. Taken together, these tools constitute a unique medium--known to its users as "cyberspace"--located in no particular geographical location but available to anyone, anywhere in the world, with access to the Internet.

E-mail enables an individual to send an electronic message to another individual or to a group of addressees. A mail exploder is a sort of e-mail group. Subscribers can send messages to a common e-mail address, which then forwards the message to the group's other subscribers. Newsgroups also serve groups of regular participants, but these postings may be read by others as

well. There are thousands of such groups, each serving to foster an exchange of information or opinion on a particular topic. About 100,000 new messages are posted every day. In addition to posting a message that can be read later, two or more individuals wishing to communicate more immediately can enter a chat room to engage in real-time dialogue. It is "no exaggeration to conclude that the content on the Internet is as diverse as human thought."

The best known category of communication over the Internet is the World Wide Web, which allows users to search for and retrieve information stored in remote computers. In concrete terms, the Web consists of a vast number of documents stored in different computers all over the world. The Web is comparable, from the readers' viewpoint, to both a vast library including millions of readily available and indexed publications and a sprawling mall offering goods and services. From the publishers' point of view, it constitutes a vast platform from which to address and hear from a world-wide audience of millions of readers, viewers, researchers, and buyers. Any person or organization with a computer connected to the Internet can "publish" information. Publishers may either make their material available to the entire pool of Internet users, or confine access to a selected group, such as those willing to pay for the privilege. "No single organization controls any membership in the Web, nor is there any centralized point from which individual Web sites or services can be blocked from the Web."

Sexually Explicit Material

Sexually explicit material on the Internet includes text, pictures, and chat and "extends from the modestly titillating to the hardest-core." These files are created, named, and posted in the same manner as material that is not sexually explicit, and may be accessed either deliberately or unintentionally during the course of an imprecise search. "Once a provider posts its content on the Internet, it cannot prevent that content from entering any community."

Some of the communications over the Internet that originate in foreign countries are also sexually explicit. Though such material is widely available, users seldom encounter such content accidentally. "A document's title or a description of the document will usually appear before the document itself and in many cases the user will receive detailed information about a site's content before he or she need take the step to access the document. Almost all sexually explicit images are preceded by warnings as to the content." For that reason, the "odds are slim" that a user would enter a sexually explicit site by accident. Unlike communications received by radio or television, "the receipt of information on the Internet requires a series of affirmative steps more deliberate and directed than merely turning a dial. A child requires some sophistication and some ability to read to retrieve material and thereby to use the Internet unattended."

Systems have been developed to help parents control the material that may be available on a home computer with Internet access. A system may either limit access to an approved list of sources, block designated sites, or attempt to block messages containing identifiable objectionable features. "Although parental control software can screen for certain suggestive words or for known sexually explicit sites, it cannot now screen for sexually explicit images."

Age Verification

The District Court categorically determined that there "is no effective way to determine the

identity or the age of a user who is accessing material through e-mail, mail exploders, newsgroups or chat rooms." Moreover, even if it were technologically feasible to block minors' access to newsgroups and chat rooms containing discussions of art, politics or other subjects that potentially elicit "indecent" or "patently offensive" contributions, it would not be possible to block their access to that material and "still allow them access to the remaining content, even if the overwhelming majority of that content was not indecent."

Technology exists by which an operator of a Web site may condition access on the verification of requested information such as a credit card number or an adult password. Credit card verification is only feasible, however, either in connection with a commercial transaction in which the card is used, or by payment to a verification agency. Using credit card possession as a surrogate for proof of age would impose costs on non-commercial Web sites that would require many of them to shut down.

II

The Telecommunications Act of 1996 was an unusually important legislative enactment. As stated on the first of its 103 pages, its primary purpose was to reduce regulation and encourage "the rapid deployment of new telecommunications technologies" The Act includes seven Titles, six of which are the product of extensive committee hearings and the subject of Reports prepared by Committees of the Senate and House. Title V--known as the "Communications Decency Act of 1996" (CDA)--contains provisions that were either added in executive committee after the hearings were concluded or as amendments offered during floor debate. An amendment offered in the Senate was the source of the two statutory provisions challenged in this case. They are described as the "indecent transmission" provision and the "patently offensive display" provision.

The first, 47 U.S.C. § 223(a) (Supp. 1997), prohibits the knowing transmission of obscene or indecent messages to any recipient under 18 years of age. It provides in pertinent part:

> (a) Whoever--
> (1) in interstate or foreign communications–
> . . . .
> (B) by means of a telecommunications device knowingly--
> (i) makes, creates, or solicits, and
> (ii) initiates the transmission of,
> any comment, request, suggestion, proposal, image, or other communication which is obscene or indecent, knowing that the recipient of the communication is under 18 years of age, regardless of whether the maker of such communication placed the call or initiated the communication;
> . . . . .
> (2) knowingly permits any telecommunications facility under his control to be used for any activity prohibited by paragraph (1) with the intent that it be used for such activity,
> shall be fined under Title 18, or imprisoned not more than two years, or both.

The second provision, § 223(d), prohibits the knowing sending or displaying of patently offensive messages in a manner that is available to a person under 18 years of age. It provides:

(d) Whoever--

(1) in interstate or foreign communications knowingly--

(A) uses an interactive computer service to send to a specific person or persons under 18 years of age, or

(B) uses any interactive computer service to display in a manner available to a person under 18 years of age,

any comment, request, suggestion, proposal, image, or other communication that, in context, depicts or describes, in terms patently offensive as measured by contemporary community standards, sexual or excretory activities or organs, regardless of whether the user of such service placed the call or initiated the communication; or

(2) knowingly permits any telecommunications facility under such person's control to be used for an activity prohibited by paragraph (1) with the intent that it be used for such activity,

shall be fined under Title 18, or imprisoned not more than two years, or both."

The breadth of these prohibitions is qualified by two affirmative defenses. One covers those who take "good faith, reasonable, effective, and appropriate actions" to restrict access by minors to the prohibited communications. The other covers those who restrict access to covered material by requiring certain designated forms of age proof, such as a verified credit card or an adult identification number or code.

III

Immediately after the President signed the statute, 20 plaintiffs filed suit challenging the constitutionality of §§ 223(a)(1) and 223(d).

In its appeal, the Government argues that the District Court erred in holding that the CDA violated both the First Amendment because it is overbroad and the Fifth Amendment because it is vague. We begin our analysis by reviewing the authorities on which the Government relies.

IV

In arguing for reversal, the Government contends that the CDA is plainly constitutional under three of our prior decisions: (1) *Ginsberg v. New York*, 390 U.S. 629 (1968); (2) *FCC v. Pacifica Foundation*, 438 U.S. 726 (1978); and (3) *Renton v. Playtime Theatres, Inc.*, 475 U.S. 41 (1986). A close look at these cases, however, raises--rather than relieves--doubts concerning the constitutionality of the CDA.

In *Ginsberg*, we upheld the constitutionality of a New York statute that prohibited selling to minors under 17 years of age material that was considered obscene as to them even if not obscene as to adults. We rejected the defendant's broad submission that "the scope of the constitutional freedom of expression secured to a citizen to read or see material concerned with sex cannot be made to depend on whether the citizen is an adult or a minor." In rejecting that contention, we relied not only on the State's independent interest in the well-being of its youth, but also on our consistent recognition of the principle that "the parents' claim to authority in their own household to direct the rearing of their children is basic in the structure of our society." In

four important respects, the statute upheld in *Ginsberg* was narrower than the CDA. First, we 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. Second, the New York statute applied only to commercial transactions, whereas the CDA contains no such limitation. Third, the New York statute cabined its definition of material that is harmful to minors with the requirement that it be "utterly without redeeming social importance for minors." The CDA fails to provide us with any definition of the term "indecent" as used in § 223(a)(1) and, importantly, omits any requirement that the "patently offensive" material covered by § 223(d) lack serious literary, artistic, political, or scientific value. Fourth, the New York statute defined a minor as a person under the age of 17, whereas the CDA, in applying to all those under 18 years, includes an additional year of those nearest majority.

In *Pacifica*, we upheld a declaratory order of the Federal Communications Commission, holding that the broadcast of a recording of a 12-minute monologue entitled "Filthy Words" that had previously been delivered to a live audience "could have been the subject of administrative sanctions." The Commission had found that the repetitive use of certain words referring to excretory or sexual activities or organs "in an afternoon broadcast when children are in the audience was patently offensive" and concluded that the monologue was indecent "as broadcast." The respondent did not quarrel with the finding that the afternoon broadcast was patently offensive, but contended that it was not "indecent" within the meaning of the relevant statutes because it contained no prurient appeal. After rejecting respondent's statutory arguments, we confronted its two constitutional arguments: (1) that the Commission's construction of its authority to ban indecent speech was so broad that its order had to be set aside even if the broadcast at issue was unprotected; and (2) that since the recording was not obscene, the First Amendment forbade any abridgement of the right to broadcast it on the radio.

In the portion of the lead opinion not joined by Justices Powell and Blackmun, the plurality stated that the First Amendment does not prohibit all governmental regulation that depends on the content of speech. Accordingly, the availability of constitutional protection for a vulgar and offensive monologue that was not obscene depended on the context of the broadcast. Relying on the premise that "of all forms of communication" broadcasting had received the most limited First Amendment protection, the Court concluded that the ease with which children may obtain access to broadcasts, "coupled with the concerns recognized in *Ginsberg*," justified special treatment of indecent broadcasting.

As with the New York statute at issue in *Ginsberg*, there are significant differences between the order upheld in *Pacifica* and the CDA. First, the order in *Pacifica*, issued by an agency that had been regulating radio stations for decades, targeted a specific broadcast that represented a rather dramatic departure from traditional program content in order to designate when--rather than whether--it would be permissible to air such a program in that particular medium. The CDA's broad categorical prohibitions are not limited to particular times and are not dependent on any evaluation by an agency familiar with the unique characteristics of the Internet. Second, unlike the CDA, the Commission's declaratory order was not punitive; we expressly refused to decide whether the indecent broadcast "would justify a criminal prosecution." Finally, the

Commission's order applied to a medium which as a matter of history had "received the most limited First Amendment protection," in large part because warnings could not adequately protect the listener from unexpected program content. The Internet, however, has no comparable history. Moreover, the District Court found that the risk of encountering indecent material by accident is remote because a series of affirmative steps is required to access specific material.

In *Renton*, we upheld a zoning ordinance that kept adult movie theatres out of residential neighborhoods. The ordinance was aimed, not at the content of the films shown in the theaters, but rather at the "secondary effects"--such as crime and deteriorating property values--that these theaters fostered: "'It is the secondary effect which these zoning ordinances attempt to avoid, not the dissemination of "offensive" speech.'" According to the Government, the CDA is constitutional because it constitutes a sort of "cyberzoning" on the Internet. But the CDA applies broadly to the entire universe of cyberspace. And the purpose of the CDA is to protect children from the primary effects of "indecent" and "patently offensive" speech, rather than any "secondary" effect of such speech. Thus, the CDA is a content-based blanket restriction on speech, and, as such, cannot be "properly analyzed as a form of time, place, and manner regulation."

These precedents, then, surely do not require us to uphold the CDA and are fully consistent with the application of the most stringent review of its provisions.

V

In *Southeastern Promotions, Ltd. v. Conrad*, 420 U.S. 546 (1975), we observed that "each medium of expression . . . may present its own problems." Thus, some of our cases have recognized special justifications for regulation of the broadcast media that are not applicable to other speakers, see *Red Lion Broadcasting Co. v. FCC*, 395 U.S. 367 (1969); *FCC v. Pacifica Foundation*. In these cases, the Court relied on the history of extensive government regulation of the broadcast medium, the scarcity of available frequencies at its inception, and its "invasive" nature.

Those factors are not present in cyberspace. Neither before nor after the enactment of the CDA have the vast democratic fora of the Internet been subject to the type of government supervision and regulation that has attended the broadcast industry. Moreover, the Internet is not as "invasive" as radio or television. The District Court specifically found that "communications over the Internet do not 'invade' an individual's home or appear on one's computer screen unbidden. Users seldom encounter content 'by accident.'" It also found that "almost all sexually explicit images are preceded by warnings as to the content," and cited testimony that "'odds are slim' that a user would come across a sexually explicit sight by accident."

We distinguished *Pacifica* in *Sable Communications of Cal., Inc. v. FCC*, 492 U.S. 115 (1989), on just this basis. In *Sable*, a company in the business of offering sexually oriented prerecorded telephone messages (known as "dial-a-porn") challenged the constitutionality of an amendment to the Communications Act that imposed a blanket prohibition on indecent as well as obscene interstate commercial telephone messages. We held that the statute was invalid as applied to indecent messages. In attempting to justify the complete ban and criminalization of indecent commercial telephone messages, the Government relied on *Pacifica*, arguing that the

ban was necessary to prevent children from gaining access to such messages. We agreed that "there is a compelling interest in protecting the physical and psychological well-being of minors" which extended to shielding them from indecent messages that are not obscene by adult standards, but distinguished our "narrow holding" in *Pacifica* because it involved a different medium of communication. We explained that "the dial-it medium requires the listener to take affirmative steps to receive the communication." "Placing a telephone call," we continued, "is not the same as turning on a radio and being taken by surprise by an indecent message."

Finally, unlike the conditions that prevailed when Congress first authorized regulation of the broadcast spectrum, the Internet can hardly be considered a "scarce" expressive commodity. It provides relatively unlimited, low-cost capacity for communication of all kinds. The Government estimates that "as many as 40 million people use the Internet today, and that figure is expected to grow to 200 million by 1999." This dynamic, multifaceted category of communication includes not only traditional print and news services, but also audio, video, and still images, as well as interactive, real-time dialogue. 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. As the District Court found, "the content on the Internet is as diverse as human thought." We agree with its conclusion that our cases provide no basis for qualifying the level of First Amendment scrutiny that should be applied to this medium.

VI

Regardless of whether the CDA is so vague that it violates the Fifth Amendment, the many ambiguities concerning the scope of its coverage render it problematic for purposes of the First Amendment. For instance, each of the two parts of the CDA uses a different linguistic form. The first uses the word "indecent," while the second speaks of material that "in context, depicts or describes, in terms patently offensive as measured by contemporary community standards, sexual or excretory activities or organs." Given the absence of a definition of either term, this difference in language will provoke uncertainty among speakers about how the two standards relate to each other and just what they mean. Could a speaker confidently assume that a serious discussion about birth control practices, homosexuality, or the consequences of prison rape would not violate the CDA? This uncertainty undermines the likelihood that the CDA has been carefully tailored to the congressional goal of protecting minors from potentially harmful materials.

The vagueness of the CDA is a matter of special concern for two reasons. First, the CDA is a content-based regulation of speech. The vagueness of such a regulation raises special First Amendment concerns because of its obvious chilling effect on free speech. Second, the CDA is a criminal statute. The severity of criminal sanctions may well cause speakers to remain silent rather than communicate even arguably unlawful words, ideas, and images.

The Government argues that the statute is no more vague than the obscenity standard this Court established in *Miller v. California*, 413 U.S. 15 (1973). But that is not so. Having struggled for some time to establish a definition of obscenity, we set forth in *Miller* the test for obscenity that controls to this day:

> (a) whether the average person, applying contemporary community standards

would find that the work, taken as a whole, appeals to the prurient interest;

(b) whether the work depicts or describes, in a patently offensive way, sexual conduct specifically defined by the applicable state law; and

(c) whether the work, taken as a whole, lacks serious literary, artistic, political, or scientific value."

Because the CDA's "patently offensive" standard is one part of the three prong *Miller* test, the Government reasons, it cannot be unconstitutionally vague.

The Government's assertion is incorrect as a matter of fact. The second prong of the Miller test--the purportedly analogous standard--contains a critical requirement that is omitted from the CDA: that the proscribed material be "specifically defined by the applicable state law." This requirement reduces the vagueness inherent in the open ended term "patently offensive" as used in the CDA. Moreover, the *Miller* definition is limited to "sexual conduct," whereas the CDA extends also to include (1) "excretory activities" as well as (2) "organs" of both a sexual and excretory nature.

The Government's reasoning is also flawed. Just because a definition including three limitations is not vague, it does not follow that one of those limitations, standing by itself, is not vague. Each of *Miller's* additional two prongs--(1) that, taken as a whole, the material appeal to the "prurient" interest, and (2) that it "lac[k] serious literary, artistic, political, or scientific value"--critically limits the uncertain sweep of the obscenity definition. The second requirement is particularly important because, unlike the "patently offensive" and "prurient interest" criteria, it is not judged by contemporary community standards. This "societal value" requirement, absent in the CDA, allows appellate courts to impose some limitations and regularity on the definition by setting, as a matter of law, a national floor for socially redeeming value.

In contrast to *Miller* and our other previous cases, the CDA thus presents a greater threat of censoring speech that, in fact, falls outside the statute's scope. Given the vague contours of the coverage of the statute, it unquestionably silences some speakers whose messages would be entitled to constitutional protection. That danger provides further reason for insisting that the statute not be overly broad. The CDA's burden on protected speech cannot be justified if it could be avoided by a more carefully drafted statute.

VII

We are persuaded that the CDA lacks the precision that the First Amendment requires when a statute regulates the content of speech. In order to deny minors access to potentially harmful speech, the CDA effectively suppresses a large amount of speech that adults have a constitutional right to receive and to address to one another. That burden on adult speech is unacceptable if less restrictive alternatives would be at least as effective in achieving the legitimate purpose that the statute was enacted to serve.

In evaluating the free speech rights of adults, we have made it perfectly clear that "sexual expression which is indecent but not obscene is protected by the First Amendment." It is true that we have repeatedly recognized the governmental interest in protecting children from harmful materials. But that interest does not justify an unnecessarily broad suppression of speech

addressed to adults. As we have explained, the Government may not "reduce the adult population . . . to . . . only what is fit for children."

The District Court was correct to conclude that the CDA effectively resembles the ban on "dial a porn" invalidated in *Sable*. In *Sable*, this Court rejected the argument that we should defer to the congressional judgment that nothing less than a total ban would be effective in preventing enterprising youngsters from gaining access to indecent communications. *Sable* thus made clear that the mere fact that a statutory regulation of speech was enacted for the important purpose of protecting children from exposure to sexually explicit material does not foreclose inquiry into its validity. As we pointed out last Term, that inquiry embodies an "over arching commitment" to make sure that Congress has designed its statute to accomplish its purpose "without imposing an unnecessarily great restriction on speech."

In arguing that the CDA does not so diminish adult communication, the Government relies on the incorrect factual premise that prohibiting a transmission whenever it is known that one of its recipients is a minor would not interfere with adult to adult communication. The findings of the District Court make clear that this premise is untenable.

Given the size of the potential audience for most messages, in the absence of a viable age verification process, the sender must be charged with knowing that one or more minors will likely view it. Knowledge that, for instance, one or more members of a 100 person chat group will be minor--and therefore that it would be a crime to send the group an indecent message--would surely burden communication among adults.

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.

The breadth of the CDA's coverage is wholly unprecedented. Unlike the regulations upheld in *Ginsberg* and *Pacifica*, the scope of the CDA is not limited to commercial speech or commercial entities. Its prohibitions embrace all nonprofit entities and individuals posting indecent messages or displaying them on their own computers in the presence of minors. The general, undefined terms "indecent" and "patently offensive" cover large amounts of nonpornographic material with serious educational or other value. Moreover, the "community standards" criterion as applied to the Internet means that any communication available to a nation wide audience will be judged by the standards of the community most likely to be offended by the message. The regulated subject matter includes any of the seven "dirty words" used in the Pacifica monologue. It may also extend to discussions about prison rape or safe sexual practices, artistic images that include nude subjects, and the card catalogue of the Carnegie Library.

For the purposes of our decision, we need neither accept nor reject the Government's submission that the First Amendment does not forbid a blanket prohibition on all "indecent" and

"patently offensive" messages communicated to a 17 year old--no matter how much value the message may contain and regardless of parental approval. It is at least clear that the strength of the Government's interest in protecting minors is not equally strong throughout the coverage of this broad statute. Under the CDA, a parent allowing her 17 year old to use the family computer to obtain information on the Internet that she, in her parental judgment, deems appropriate could face a lengthy prison term. Similarly, a parent who sent his 17 year old college freshman information on birth control via e-mail could be incarcerated even though neither he, his child, nor anyone in their home community, found the material "indecent" or "patently offensive," if the college town's community thought otherwise.

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 as the CDA. It has not done so. Particularly in the light of the absence of any detailed findings by Congress, or even hearings addressing the problems of the CDA, we are persuaded that the CDA is not narrowly tailored.

VIII

In an attempt to curtail the CDA's facial overbreadth, the Government asserts that the "knowledge" requirement of both §§223(a) and (d), especially when coupled with the "specific child" element found in §223(d), saves the CDA from overbreadth. Because both sections prohibit the dissemination of indecent messages only to persons known to be under 18, the Government argues, it does not require transmitters to "refrain from communicating indecent material to adults." This argument ignores the fact that most Internet fora are open to all comers. The Government's assertion that the knowledge requirement somehow protects the communications of adults is therefore untenable. Even the strongest reading of the "specific person" requirement of §223(d) cannot save the statute. It would confer broad powers of censorship, in the form of a "heckler's veto," upon any opponent of indecent speech who might simply log on and inform the would be discoursers that his 17 year old child--a "specific person . . . under 18 years of age"--would be present.

IX

The Government's three remaining arguments focus on the defenses provided in §223(e)(5). First, relying on the "good faith, reasonable, effective, and appropriate actions" provision, the Government suggests that "tagging" provides a defense that saves the constitutionality of the Act. It is the requirement that the good faith action must be "effective" that makes this defense illusory. The Government recognizes that its proposed screening software does not currently exist. Even if it did, there is no way to know whether a potential recipient will actually block the encoded material. Without the impossible knowledge that every guardian in America is screening for the "tag," the transmitter could not reasonably rely on its action to be "effective."

For its second and third arguments concerning defenses--which we can consider together--the Government relies on the latter half of §223(e)(5), which applies when the transmitter has restricted access by requiring use of a verified credit card or adult identification. Such verification is used by commercial providers of sexually explicit material. These providers, therefore, would be protected by the defense. Under the findings of the District Court, however,

it is not economically feasible for most noncommercial speakers to employ such verification. Accordingly, this defense would not significantly narrow the statute's burden on noncommercial speech. Even with respect to the commercial pornographers that would be protected by the defense, the Government failed to adduce any evidence that these verification techniques actually preclude minors from posing as adults. Given that the risk of criminal sanctions "hovers over each content provider, like the proverbial sword of Damocles," the District Court correctly refused to rely on unproven future technology to save the statute. The Government thus failed to prove that the proffered defense would significantly reduce the heavy burden on adult speech produced by the prohibition on offensive displays.

We agree with the District Court's conclusion that the CDA places an unacceptably heavy burden on protected speech, and that the defenses do not constitute the sort of "narrow tailoring" that will save an otherwise unconstitutional provision. In *Sable* we remarked that the speech restriction at issue there amounted to "'burning the house to roast the pig.'" The CDA, casting a far darker shadow over free speech, threatens to torch a large segment of the Internet community.

JUSTICE O'CONNOR, with whom THE CHIEF JUSTICE joins, concurring in the judgment in part and dissenting in part.

I write separately to explain why I view the CDA as little more than an attempt by Congress to create "adult zones" on the Internet. Our precedent indicates that the creation of such zones can be constitutionally sound. Despite the soundness of its purpose, however, portions of the CDA are unconstitutional because they stray from the blueprint our prior cases have developed for constructing a "zoning law" that passes constitutional muster.

Appellees bring a facial challenge to three provisions of the CDA. The first, which the Court describes as the "indecency transmission" provision, makes it a crime to knowingly transmit an obscene or indecent message or image to a person the sender knows is under 18 years old. 47 U. S. C. §223(a)(1)(B). What the Court classifies as a single " `patently offensive display' " provision is in reality two separate provisions. The first of these makes it a crime to knowingly send a patently offensive message or image to a specific person under the age of 18 ("specific person" provision). §223(d)(1)(A). The second criminalizes the display of patently offensive messages or images "in a[ny] manner available" to minors ("display" provision). §223(d)(1)(B). None of these provisions purports to keep indecent material away from adults, who have a First Amendment right to obtain this speech. Thus, the undeniable purpose of the CDA is to segregate indecent material on the Internet into certain areas that minors cannot access.

The creation of "adult zones" is by no means a novel concept. States have long denied minors access to certain establishments frequented by adults. The Court has previously sustained such zoning laws, but only if they respect the First Amendment rights of adults and minors. That is to say, a zoning law is valid if (i) it does not unduly restrict adult access to the material; and (ii) minors have no First Amendment right to read or view the banned material. As applied to the Internet as it exists in 1997, the "display" provision and some applications of the "indecency transmission" and "specific person" provisions fail to adhere to the first of these limiting principles by restricting adults' access to protected materials in certain circumstances. Unlike the

Court, however, I would invalidate the provisions only in those circumstances.

Our cases make clear that a "zoning" law is valid only if adults are still able to obtain the regulated speech. If they cannot, the law interferes with the rights of adults to obtain constitutionally protected speech and effectively "reduce[s] the adult population . . . to reading only what is fit for children." *Butler v. Michigan*, 352 U.S. 380, 383 (1957). The First Amendment does not tolerate such interference. If the law does not unduly restrict adults' access to constitutionally protected speech, however, it may be valid. In *Ginsberg v. New York*, 390 U.S. 629, 634 (1968), for example, the Court sustained a New York law that barred store owners from selling pornographic magazines to minors in part because adults could still buy those magazines.

The Court in *Ginsberg* concluded that the New York law created a constitutionally adequate adult zone simply because, on its face, it denied access only to minors. The Court did not question that an adult zone, once created, would succeed in preserving adults' access while denying minors' access to the regulated speech. Before today, there was no reason to question this assumption, for the Court has previously only considered laws that operated in the physical world, a world that with two characteristics that make it possible to create "adult zones": geography and identity. A minor can see an adult dance show only if he enters an establishment that provides such entertainment. And should he attempt to do so, the minor will not be able to conceal completely his identity (or, consequently, his age). Thus, the twin characteristics of geography and identity enable the establishment's proprietor to prevent children from entering the establishment, but to let adults inside.

The electronic world is fundamentally different. Cyberspace allows speakers and listeners to mask their identities. Since users can transmit and receive messages on the Internet without revealing anything about their identities or ages, it is not currently possible to exclude persons from accessing certain messages on the basis of their identity.

Cyberspace differs from the physical world in another basic way: Cyberspace is malleable. Thus, it is possible to construct barriers in cyberspace and use them to screen for identity, making cyberspace more like the physical world and, consequently, more amenable to zoning laws. This transformation of cyberspace is already underway. Internet speakers have begun to zone cyberspace itself through the use of "gateway" technology. Such technology requires Internet users to enter information about themselves--perhaps an adult identification number or a credit card number--before they can access certain areas of cyberspace, much like a bouncer checks a person's driver's license before admitting him to a nightclub. Internet users who access information have not attempted to zone cyberspace itself, but have tried to limit their own power to access information in cyberspace, much as a parent controls what her children watch on television by installing a lock box. This user based zoning is accomplished through the use of screening software or browsers with screening capabilities, both of which search for keywords that are associated with "adult" sites and, if the user wishes, blocks access to such sites.

Despite this progress, the transformation of cyberspace is not complete. Although gateway technology has been available on the World Wide Web for some time now, it is not available to all Web speakers, and is just now becoming technologically feasible for chat rooms and USENET newsgroups. Gateway technology is not ubiquitous in cyberspace, and because without

it "there is no means of age verification," cyberspace still remains largely unzoned--and unzoneable. User based zoning is also in its infancy. For it to be effective, (i) an agreed upon code (or "tag") would have to exist; (ii) screening software would have to be able to recognize the "tag"; and (iii) those programs would have to be widely available--and widely used--by Internet users. At present, none of these conditions is true.

Although the prospects for the eventual zoning of the Internet appear promising, we must evaluate the constitutionality of the CDA as it applies to the Internet as it exists today. Given the present state of cyberspace, I agree with the Court that the "display" provision cannot pass muster. A speaker cannot be reasonably assured that the speech he displays will reach only adults. Thus, the only way for a speaker to avoid liability is to refrain completely from using indecent speech. But this forced silence impinges on the First Amendment right of adults and, for all intents and purposes, "reduce[s] the adult population [on the Internet] to reading only what is fit for children." As a result, the "display" provision cannot withstand scrutiny.

The "indecency transmission" and "specific person" provisions present a closer issue. The "indecency transmission" provision makes it a crime to transmit knowingly an indecent message to a person the sender knows is under 18. The "specific person" provision proscribes the same conduct, although it does not as explicitly require the sender to know that the intended recipient is a minor. Appellant urges the Court to construe the provision to impose a knowledge requirement, and I would do so.

So construed, both provisions are constitutional as applied to a conversation involving only an adult and one or more minors--e.g., when an adult speaker sends an email knowing the addressee is a minor, or when an adult and minor converse by themselves or with other minors in a chat room. In this context, these provisions are no different from the law we sustained in *Ginsberg*. Restricting what the adult may say to the minors in no way restricts the adult's ability to communicate with other adults.

The analogy to *Ginsberg* breaks down, however, when more than one adult is a party to the conversation. If a minor enters a chat room otherwise occupied by adults, the CDA effectively requires the adults in the room to stop using indecent speech. If they did not, they could be prosecuted under the "indecency transmission" and "specific person" provisions for any indecent statements they make to the group. The absence of any means of excluding minors from chat rooms in cyberspace restricts the rights of adults to engage in indecent speech in those rooms. The "indecency transmission" and "specific person" provisions share this defect.

But these two provisions do not infringe on adults' speech in all situations. I agree with the Court that the provisions are overbroad in that they cover any and all communications between adults and minors, regardless of how many adults might be part of the audience to the communication. This conclusion does not end the matter, however. I would sustain the "indecency transmission" and "specific person" provisions to the extent they apply to the transmission of Internet communications where the party initiating the communication knows that all of the recipients are minors.

Whether the CDA substantially interferes with the First Amendment rights of minors, and thereby runs afoul of the second characteristic of valid zoning laws, presents a closer question.

The Court neither "accept[s] nor reject[s]" the argument that the CDA is facially overbroad because it substantially interferes with the First Amendment rights of minors. I would reject it. *Ginsberg* established that minors may be denied access to material that is obscene as to minors. As *Ginsberg* explained, material is obscene as to minors if it (i) is "patently offensive to prevailing standards in the adult community as a whole with respect to what is suitable . . . for minors"; (ii) appeals to the prurient interest of minors; and (iii) is "utterly without redeeming social importance for minors." Because the CDA denies minors the right to obtain material that is "patently offensive"--even if it has some redeeming value for minors and even if it does not appeal to their prurient interests--Congress' rejection of the Ginsberg "harmful to minors" standard means that the CDA could ban some speech that is not obscene as to minors.

I do not deny this possibility, but to prevail in a facial challenge, our cases require proof of "real" and "substantial" overbreadth. In my view, the universe of speech constitutionally protected as to minors but banned by the CDA is a very small one. Accordingly, in my view, the CDA does not burden a substantial amount of minors' constitutionally protected speech.

Thus, the constitutionality of the CDA as a zoning law hinges on the extent to which it substantially interferes with the First Amendment rights of adults. Because the rights of adults are infringed only by the "display" provision and by the "indecency transmission" and "specific person" provisions as applied to communications involving more than one adult, I would invalidate the CDA only to that extent. Insofar as the "indecency transmission" and "specific person" provisions prohibit the use of indecent speech in communications between an adult and one or more minors, however, they can and should be sustained.

UNITED STATES V. AMERICAN LIBRARY ASSN., INC.

539 U.S. 194 (2003)

Chief Justice Rehnquist announced the judgment of the Court and delivered an opinion, in which Justice O’Connor, Justice Scalia, and Justice Thomas joined.

To address the problems associated with the availability of Internet pornography in public libraries, Congress enacted the Children’s Internet Protection Act (CIPA). Under CIPA, a public library may not receive federal assistance to provide Internet access unless it installs software to block images that constitute obscenity or child pornography, and to prevent minors from obtaining access to material that is harmful to them. The District Court held these provisions facially invalid on the ground that they induce public libraries to violate patrons’ First Amendment rights. We now reverse.

To help public libraries provide their patrons with Internet access, Congress offers two forms of federal assistance. First, the E-rate program established by the Telecommunications Act of 1996 entitles qualifying libraries to buy Internet access at a discount. In the year ending June 30, 2002, libraries received $58.5 million in such discounts. Second, pursuant to the Library Services and Technology Act (LSTA), the Institute of Museum and Library Services makes grants to state library administrative agencies to “electronically lin[k] libraries with educational, social, or

information services," "assis[t] libraries in accessing information through electronic networks," and "pa[y] costs for libraries to acquire or share computer systems and telecommunications technologies." In fiscal year 2002, Congress appropriated more than $149 million in LSTA grants. These programs have succeeded greatly in bringing Internet access to public libraries: By 2000, 95% of the Nation's libraries provided public Internet access.

By connecting to the Internet, public libraries provide patrons with a vast amount of valuable information. But there is also an enormous amount of pornography on the Internet. The accessibility of this material has created serious problems for libraries, which have found that patrons of all ages, including minors, regularly search for online pornography.

Upon discovering these problems, Congress became concerned that the E-rate and LSTA programs were facilitating access to illegal and harmful pornography. But Congress also learned that filtering software that blocks access to pornographic Web sites could provide a reasonably effective way to prevent such uses of library resources. A library can set such software to block categories of material, such as "Pornography" or "Violence." When a patron tries to view a site that falls within such a category, a screen appears indicating that the site is blocked. But a filter set to block pornography may sometimes block other sites that present neither obscene nor pornographic material, but that nevertheless trigger the filter. To minimize this problem, a library can set its software to prevent the blocking of material that falls into categories like "Education," "History," and "Medical." A library may also add or delete specific sites from a blocking category, and anyone can ask companies that furnish filtering software to unblock particular sites.

Responding to this information, Congress enacted CIPA. It provides that a library may not receive E-rate or LSTA assistance unless it has "a policy of Internet safety for minors that includes the operation of a technology protection measure … that protects against access" by all persons to "visual depictions" that constitute "obscen[ity]" or "child pornography," and that protects against access by minors to "visual depictions" that are "harmful to minors." The statute defines a "[t]echnology protection measure" as "a specific technology that blocks or filters Internet access to material covered by" CIPA. CIPA also permits the library to "disable" the filter "to enable access for bona fide research or other lawful purposes." Under the E-rate program, disabling is permitted "during use by an adult." Under the LSTA program, disabling is permitted during use by any person.

Appellees are a group of libraries, library associations, library patrons, and Web site publishers. They sued the United States, challenging the constitutionality of CIPA's filtering provisions. The District Court ruled that CIPA was facially unconstitutional. The District Court held that Congress had exceeded its authority under the Spending Clause because "any public library that complies with CIPA's conditions will necessarily violate the First Amendment." The court held that the filtering software contemplated by CIPA was a content-based restriction on access to a public forum, and was therefore subject to strict scrutiny. Applying this standard, the District Court held that, although the Government has a compelling interest "in preventing the dissemination of obscenity, child pornography, or, in the case of minors, material harmful to minors," the use of software filters is not narrowly tailored to further those interests. We reverse.

Congress has wide latitude to attach conditions to the receipt of federal assistance in order to

further its policy objectives. *South Dakota v. Dole*, 483 U.S. 203, 206 (1987). But Congress may not "induce" the recipient "to engage in activities that would themselves be unconstitutional." To determine whether libraries would violate the First Amendment by employing the filtering software that CIPA requires, we must first examine the role of libraries in our society.

Public libraries pursue the worthy missions of facilitating learning and cultural enrichment. To fulfill their traditional missions, public libraries must have broad discretion to decide what material to provide to their patrons. Although they seek to provide a wide array of information, their goal has never been to provide "universal coverage." Instead, public libraries seek to provide materials "that would be of the greatest direct benefit or interest to the community." To this end, libraries collect only materials deemed to have "appropriate quality."

We have held in two analogous contexts that the government has broad discretion to make content-based judgments in deciding what private speech to make available to the public. In *Arkansas Ed. Television Comm'n v. Forbes*, 523 U.S. 666 (1998), we held that public forum principles do not generally apply to a public television station's editorial judgments regarding the private speech it presents to its viewers. "[B]road 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."

Similarly, in *National Endowment for Arts v. Finley*, 524 U.S. 569 (1998), we upheld an art funding program that required the National Endowment for the Arts (NEA) to use content-based criteria in making funding decisions. We explained that "[t]he very assumption of the NEA is that grants will be awarded according to the 'artistic worth of competing applicants,' and absolute neutrality is simply inconceivable."

The principles underlying *Forbes* and *Finley* also apply to a public library's exercise of judgment in selecting the material it provides to its patrons. Just as forum analysis and heightened judicial scrutiny are incompatible with the role of public television stations and the role of the NEA, they are also incompatible with the discretion that public libraries must have to fulfill their traditional missions. Public library staffs necessarily consider content in making collection decisions and enjoy broad discretion in making them.

The public forum principles on which the District Court relied are out of place in the context of this case. Internet access in public libraries is neither a "traditional" nor a "designated" public forum. First, this resource did not exist until quite recently. We have "rejected the view that traditional public forum status extends beyond its historic confines." The doctrines surrounding traditional public forums may not be extended to situations where such history is lacking.

Nor does Internet access in a public library satisfy our definition of a "designated public forum." To create such a forum, the government must make an affirmative choice to open up its property for use as a public forum. A public library does not acquire Internet terminals in order to create a public forum for Web publishers to express themselves, any more than it collects books in order to provide a public forum for the authors of books to speak. It provides Internet access, not to "encourage a diversity of views from private speakers," but for the same reasons it offers other library resources: to facilitate research, learning, and recreational pursuits by furnishing materials of requisite and appropriate quality.

The District Court disagreed because, whereas a library reviews and affirmatively chooses to acquire every book in its collection, it does not review every Web site that it makes available. We do not find this distinction constitutionally relevant. A library's need to exercise judgment in making collection decisions depends on its traditional role in identifying suitable and worthwhile material; it is no less entitled to play that role when it collects material from the Internet than when it collects material from any other source. Most libraries already exclude pornography from their print collections because they deem it inappropriate for inclusion. We do not subject these decisions to heightened scrutiny; it would make little sense to treat libraries' judgments to block online pornography any differently, when these judgments are made for just the same reason.

Moreover, because of the vast quantity of material on the Internet and the rapid pace at which it changes, libraries cannot possibly segregate, item by item, all the Internet material that is appropriate for inclusion from all that is not. It is entirely reasonable for public libraries exclude certain categories of content, without making individualized judgments that everything they do make available has requisite and appropriate quality.

Like the District Court, the dissents fault the tendency of filtering software to "overblock"–that is, to erroneously block access to constitutionally protected speech that falls outside the categories that software users intend to block. Due to the software's limitations, "[m]any erroneously blocked [Web] 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.' " Assuming that such erroneous blocking presents constitutional difficulties, any such concerns are dispelled by the ease with which patrons may have the filtering software disabled. When a patron encounters a blocked site, he need only ask a librarian to unblock it or (at least in the case of adults) disable the filter. As the District Court found, libraries have the capacity to permanently unblock any erroneously blocked site, and the Solicitor General stated at oral argument that a "library may eliminate the filtering with respect to specific sites at the request of a patron." With respect to adults, CIPA also authorizes library officials to "disable" a filter altogether "to enable access for bona fide research or other lawful purposes." The Solicitor General confirmed that a "librarian can, in response to a request from a patron, unblock the filtering mechanism altogether," and further explained that a patron would not "have to explain … why he was asking a site to be unblocked or the filtering to be disabled.," The District Court viewed unblocking and disabling as inadequate because some patrons may be too embarrassed to request them. But the Constitution does not guarantee the right to acquire information at a public library without any risk of embarrassment.

Because public libraries' use of Internet filtering software does not violate their patrons' First Amendment rights, CIPA does not induce libraries to violate the Constitution, and is a valid exercise of Congress' spending power. Therefore, the judgment of the District Court is Reversed.

Justice Kennedy, concurring in the judgment.

If, on the request of an adult user, a librarian will unblock filtered material or disable the Internet software filter without significant delay, there is little to this case. The Government represents this is indeed the fact. If some libraries do not have the capacity to unblock specific

Web sites or to disable the filter, that would be the subject for an as-applied challenge, not the facial challenge made in this case.

The interest in protecting young library users from material inappropriate for minors is legitimate, and even compelling. Given this interest, and the failure to show that the ability of adult library users to have access to the material is burdened in any significant degree, the statute is not unconstitutional on its face. For these reasons, I concur in the judgment of the Court.

Justice Breyer, concurring in the judgment.

Filtering software does not function perfectly, for to some extent it also screens out constitutionally protected materials that fall outside the scope of the statute (i.e., "overblocks") and fails to prevent access to some materials that the statute deems harmful (i.e., "underblocks"). In determining whether the statute's conditions consequently violate the First Amendment, the plurality first finds the "public forum" doctrine inapplicable, and then holds that the statutory provisions are constitutional. I agree with both determinations. But I reach the plurality's ultimate conclusion in a different way.

In my view, the First Amendment does not here demand application of the most limiting constitutional approach–that of "strict scrutiny." The statutory restriction in question is, in essence, a kind of "selection" restriction (a kind of editing). It affects the kinds and amount of materials that the library can present to its patrons. And libraries often properly engage in the selection of materials, either as a matter of necessity (i.e., due to the scarcity of resources) or by design (i.e., in accordance with collection development policies). To apply "strict scrutiny" to the "selection" of a library's collection would unreasonably interfere with the discretion necessary to create, maintain, or select a library's "collection." Strict scrutiny implies too limiting and rigid a test for me to believe that the First Amendment requires it in this context.

Instead, I would examine the constitutionality of the Act's restrictions here as the Court has examined speech-related restrictions in other contexts where circumstances call for heightened, but not "strict," scrutiny. Typically the key question in such instances is one of proper fit. In such cases the Court has asked whether the harm to speech-related interests is disproportionate in light of both the justifications and the potential alternatives. It has considered the legitimacy of the statute's objective, the extent to which the statute will tend to achieve that objective, whether there are other, less restrictive ways of achieving that objective, and ultimately whether the statute works speech-related harm that, in relation to that objective, is out of proportion.

The Act's restrictions satisfy these constitutional demands. The Act seeks to restrict access to obscenity, child pornography, and, in respect to access by minors, material that is comparably harmful. These objectives are "legitimate," and indeed often "compelling." As the District Court found, software filters "provide a relatively cheap and effective" means of furthering these goals. Due to present technological limitations, however, the software filters both "overblock" and "underblock." But no one has presented any clearly superior or better fitting alternatives.

At the same time, the Act contains an important exception that limits the speech-related harm that "overblocking" might cause. The Act allows libraries to permit any adult patron access to an "overblocked" Web site; the adult patron need only ask a librarian to unblock the specific Web

site or, alternatively, ask the librarian, "Please disable the entire filter."

The Act does impose upon the patron the burden of making this request. But it is difficult to see how that burden (or any delay associated with compliance) could prove more onerous than traditional library practices associated with segregating library materials in closed stacks, or with interlibrary lending practices that require patrons to make requests that are not anonymous and to wait while the librarian obtains the desired materials. Perhaps local library practices could further restrict the ability of patrons to obtain "overblocked" Internet material. But we are not now considering any such local practices. We here consider only a facial challenge to the Act itself.

Given the comparatively small burden that the Act imposes upon the library patron seeking legitimate Internet materials, I cannot say that any speech-related harm that the Act may cause is disproportionate in relation to the Act's legitimate objectives. I therefore agree with the plurality that the statute does not violate the First Amendment, and I concur in the judgment.

Justice Stevens, dissenting.

"To fulfill their traditional missions, public libraries must have broad discretion to decide what material to provide their patrons." Accordingly, I agree with the plurality that it is neither inappropriate nor unconstitutional for a local library to experiment with filtering software as a means of curtailing children's access to Internet Web sites displaying sexually explicit images. I also agree with the plurality that the 7% of public libraries that decided to use such software on all of their Internet terminals in 2000 did not act unlawfully. Whether it is constitutional for the Congress of the United States to impose that requirement on the other 93%, however, raises a vastly different question. The Children's Internet Protection Act (CIPA) operates as a blunt nationwide restraint on adult access to "an enormous amount of valuable information" that individual librarians cannot possibly review. Most of that information is constitutionally protected speech. In my view, this restraint is unconstitutional.

I

The unchallenged findings of fact made by the District Court reveal fundamental defects in filtering software. Because the software relies on key words or phrases to block undesirable sites, it does not have the capacity to exclude a precisely defined category of images.

Given the quantity and ever-changing character of Web sites offering free sexually explicit material, it is inevitable that a substantial amount of such material will never be blocked. Because of this "underblocking," the statute will provide parents with a false sense of security without really solving the problem that motivated its enactment. Conversely, the software's reliance on words to identify undesirable sites necessarily results in the blocking of thousands of pages that "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.' " In my judgment, a statutory blunderbuss that mandates this vast amount of "overblocking" abridges the freedom of speech protected by the First Amendment.

The effect of the overblocking is the functional equivalent of a host of individual decisions excluding hundreds of thousands of individual constitutionally protected messages from Internet

terminals located in public libraries throughout the Nation. Neither the interest in suppressing unlawful speech nor the interest in protecting children justifies this overly broad restriction on adult access to protected speech. "The Government may not suppress lawful speech as the means to suppress unlawful speech."

Although CIPA does not permit any experimentation, the District Court expressly found that a variety of alternatives less restrictive are available at the local level:

"[L]ess restrictive alternatives exist that further the government's interest. 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. 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."

The plurality does not reject any of those findings. Instead, "[a]ssuming that such erroneous blocking presents constitutional difficulties," it relies on the Solicitor General's assurance that the statute permits individual librarians to disable filtering mechanisms whenever a patron so requests. In my judgment, that assurance does not cure the constitutional infirmity in the statute.

Until a blocked site or group of sites is unblocked, a patron is unlikely to know what is being hidden and therefore whether there is any point in asking for the filter to be removed. It is as though the statute required a significant part of every library's reading materials to be kept in unmarked, locked rooms or cabinets, which could be opened only in response to specific requests. Some curious readers would in time obtain access to the hidden materials, but many would not. A law that prohibits reading without official consent, like a law that prohibits speaking without consent, "constitutes a dramatic departure from our constitutional tradition."

II

The plurality incorrectly argues that the statute does not impose "an unconstitutional condition on public libraries." On the contrary, it impermissibly conditions the receipt of Government funding on the restriction of significant First Amendment rights.

The plurality explains the "worthy missions" of the public library. It then asserts that in order to fulfill these missions, "libraries must have broad discretion to decide what material to provide to their patrons." Thus the selection decision is the province of the librarians, a province into which we have hesitated to enter. As the plurality recognizes, we have always assumed that libraries have discretion when making decisions regarding what to include in, and exclude from, their collections. That discretion is comparable to the " 'business of a university … to determine for itself on academic grounds who may teach, what may be taught, how it shall be taught, and who may be admitted to study.' " Given our Nation's deep commitment "to safeguarding

academic freedom" and to the "robust exchange of ideas," a library's exercise of judgment with respect to its collection is entitled to First Amendment protection.

A federal statute penalizing a library for failing to install filtering software on every one of its Internet-accessible computers would unquestionably violate that Amendment. Cf. *Reno v. American Civil Liberties Union*, 521 U.S. 844 (1997). I think it equally clear that the First Amendment protects libraries from being denied funds for refusing to comply with an identical rule. An abridgment of speech by means of a threatened denial of benefits can be just as pernicious as an abridgment by means of a threatened penalty.

The plurality's reliance on *National Endowment for Arts v. Finley*, 524 U.S. 569 (1998), is misplaced. Unlike this case, the Federal Government was not seeking to impose restrictions on the administration of a nonfederal program. Further, *Finley* did not involve a challenge by the NEA to a governmental restriction on its ability to award grants. Instead, the respondents were performance artists who had applied for NEA grants but were denied funding. If this were a case in which library patrons had challenged a library's decision to install and use filtering software, it would be in the same posture as *Finley*. Because it is not, *Finley* does not control this case.

Also unlike *Finley*, the Government does not merely seek to control a library's discretion with respect to computers purchased with Government funds or those computers with Government-discounted Internet access. CIPA requires libraries to install filtering software on every computer with Internet access if the library receives any discount from the E-rate program or any funds from the LSTA program. Under this statute, if a library attempts to provide Internet service for even one computer through an E-rate discount, that library must put filtering software on all of its computers with Internet access, not just the one computer with E-rate discount.

This Court should not permit federal funds to be used to enforce this kind of broad restriction of First Amendment rights, particularly when such a restriction is unnecessary to accomplish Congress' stated goal. The abridgment of speech is equally obnoxious whether a rule like this one is enforced by a threat of penalties or by a threat to withhold a benefit.

Justice Souter, with whom Justice Ginsburg joins, dissenting.

I agree in the main with Justice Stevens. I also agree with the library appellees on a further reason to hold the blocking rule invalid in the exercise of the spending power: the rule mandates action by recipient libraries that would violate the First Amendment's guarantee of free speech if the libraries took that action on their own. I respectfully dissent on this further ground.

I

Like the other Members of the Court, I have no doubt about the legitimacy of governmental efforts to put a barrier between child patrons of public libraries and the raw offerings on the Internet, and if the only First Amendment interests raised here were those of children, I would uphold application of the Act.

Nor would I dissent if I agreed with the majority of my colleagues that an adult library patron could, consistently with the Act, obtain an unblocked terminal simply for the asking. I realize the Solicitor General represented this to be the Government's policy. But the Federal

Communications Commission, in its order implementing the Act, pointedly declined to set a federal policy on when unblocking by local libraries would be appropriate under the statute. Moreover, the District Court expressly found that "unblocking may take days, and may be unavailable, especially in branch libraries, which are often less well staffed than main libraries."

In any event, we are here to review a statute, and the unblocking provisions simply cannot be construed to say that a library must unblock upon adult request, no conditions imposed and no questions asked. We therefore have to take the statute on the understanding that adults will be denied access to a substantial amount of nonobscene material harmful to children but lawful for adult examination, and a substantial quantity of text and pictures harmful to no one. This is the inevitable consequence of the indiscriminate behavior of current filtering mechanisms, which screen out material to an extent known only by the manufacturers of the blocking software.

We likewise have to examine the statute on the understanding that the restrictions on adult Internet access have no justification in the object of protecting children. Children could be restricted to blocked terminals, leaving other unblocked terminals in areas restricted to adults and screened from casual glances. And of course the statute could simply have provided for unblocking at adult request, with no questions asked. The statute could, in other words, have protected children without blocking access for adults or subjecting adults to anything more than minimal inconvenience. Instead, the Government's funding conditions engage in overkill to a degree illustrated by their refusal to trust even a library's staff with an unblocked terminal, one to which the adult public itself has no access.

The question for me, then, is whether a local library could itself constitutionally impose these restrictions on the content otherwise available to an adult patron through an Internet connection, at a library terminal provided for public use. The answer is no. A library that chose to block an adult's Internet access to material harmful to children would be imposing a content-based restriction on communication of material in the library's control that an adult could otherwise lawfully see. This would simply be censorship. True, the censorship would not necessarily extend to every adult, for an Internet user might convince a librarian that he was a true researcher or had a "lawful purpose." But as to those who did not qualify for discretionary unblocking, the censorship would be complete and, like all censorship by the Government, presumptively invalid owing to strict scrutiny in implementing the Free Speech Clause of the First Amendment.

II

The Court's plurality does not treat blocking affecting adults as censorship, but chooses to describe a library's act in filtering content as simply an instance of the kind of selection from available material that every library must perform. But this position does not hold up.

Public libraries are indeed selective in what they acquire to place in their stacks, as they must be. There is only so much money and so much shelf space, and the necessity to choose some material and reject the rest justifies the effort to be selective with an eye to demand, quality, and the object of maintaining the library as a place of civilized enquiry by widely different sorts of people. Selectivity is thus necessary and complex, and these two characteristics explain why review of a library's selection decisions must be limited.

At every significant point, however, the Internet blocking here defies comparison to the process of acquisition. Whereas traditional scarcity of money and space require a library to make choices about what to acquire, blocking is the subject of a choice made after the money for Internet access has been spent. Blocking is not necessitated by scarcity of either money or space. In the instance of the Internet, the choice to block is a choice to limit access that has already been acquired. The proper analogy therefore is not to passing up a book that might have been bought; it is either to buying a book and then keeping it from adults lacking an acceptable "purpose," or to buying an encyclopedia and then cutting out pages thought to be unsuitable for all adults.

After a library has acquired material, the variety of possible reasons that might legitimately support an initial rejection are no longer in play. Removal of books or selective blocking by controversial subject matter is not a function of limited resources and less likely than a selection decision to reflect an assessment of esthetic or scholarly merit. Removal (and blocking) decisions being so often obviously correlated with content, they tend to show up for just what they are, and because such decisions tend to be few, courts can examine them without facing a deluge. The difference between choices to keep out and choices to throw out is thus enormous.

III

There is no good reason to treat blocking of adult enquiry as anything different from censorship. For this reason, I would hold in accordance with strict scrutiny that a library's practice of blocking would violate an adult patron's First Amendment right to be free of Internet censorship, when unjustified (as here) by any legitimate interest in screening children from harmful material. On that ground, the Act's blocking requirement is unconstitutional.

Ashcroft v. American Civil Liberties Union
542 U.S. 656 (2004)

Justice Kennedy delivered the opinion of the Court.

This case presents a challenge to a statute enacted by Congress to protect minors from exposure to sexually explicit materials on the Internet, the Child Online Protection Act (COPA). In enacting COPA, Congress gave consideration to our earlier decisions on this subject, in particular *Reno v. American Civil Liberties Union*. For that reason, "the Judiciary must proceed with caution before invalidating the Act." The imperative of according respect to Congress, however, does not permit us to depart from well-established First Amendment principles.

Content-based prohibitions, enforced by severe criminal penalties, have the constant potential to be a repressive force in the lives and thoughts of a free people. To guard against that threat the Constitution demands that content-based restrictions on speech be presumed invalid, and that the Government bear the burden of showing their constitutionality. *United States v. Playboy Entertainment Group, Inc.*, 529 U.S. 803, 817 (2000). This is true even when Congress twice has attempted to find a constitutional means to restrict, and punish, the speech in question.

This case comes to the Court on certiorari review of an appeal from the decision of the

District Court granting a preliminary injunction. We affirm the decision of the Court of Appeals upholding the preliminary injunction, and we remand the case so that it may be returned to the District Court for trial.

I

COPA is the second attempt by Congress to make the Internet safe for minors by criminalizing certain Internet speech. The first attempt was the Communications Decency Act of 1996. The Court held the CDA unconstitutional because it was not narrowly tailored to serve a compelling governmental interest and because less restrictive alternatives were available.

In response to the Court's decision in *Reno*, Congress passed COPA. COPA imposes criminal penalties for the knowing posting, for "commercial purposes," of World Wide Web content that is "harmful to minors." Material that is "harmful to minors" is defined as:

> any communication, picture, image, graphic image file, article, recording, writing, or other matter of any kind that is obscene or that–
>
> "(A) the average person, applying contemporary community standards, would find, taking the material as a whole and with respect to minors, is designed to appeal to, or is designed to pander to, the prurient interest;
>
> (B) depicts, describes, or represents, in a manner patently offensive with respect to minors, an actual or simulated sexual act or sexual contact, an actual or simulated normal or perverted sexual act, or a lewd exhibition of the genitals or post-pubescent female breast; and
>
> (C) taken as a whole, lacks serious literary, artistic, political, or scientific value for minors.

"Minors" are defined as "any person under 17 years of age." A person acts for "commercial purposes only if such person is engaged in the business of making such communications." "Engaged in the business," in turn,

> means that the person who makes a communication, or offers to make a communication, by means of the World Wide Web, that includes any material that is harmful to minors, devotes time, attention, or labor to such activities, as a regular course of such person's trade or business, with the objective of earning a profit as a result of such activities (although it is not necessary that the person make a profit or that the making or offering to make such communications be the person's sole or principal business or source of income). §231(e)(2).

While the statute labels all speech that falls within these definitions as criminal speech, it also provides an affirmative defense to those who employ specified means to prevent minors from gaining access to the prohibited materials on their Web site. A person may escape conviction under the statute by demonstrating that he

> has restricted access by minors to material that is harmful to minors–
>
> (A) by requiring use of a credit card, debit account, adult access code, or adult

personal identification number;

(B) by accepting a digital certificate that verifies age, or

(C) by any other reasonable measures that are feasible under available technology.

II

"This Court, like other appellate courts, has always applied the abuse of discretion standard on the review of a preliminary injunction." If the constitutional question is close, therefore, we should uphold the injunction and remand for trial on the merits. Applying this mode of inquiry, we agree with the Court of Appeals that the District Court did not abuse its discretion.

The District Court, in deciding to grant the preliminary injunction, concentrated primarily on the argument that there are plausible, less restrictive alternatives to COPA. When plaintiffs challenge a content-based speech restriction, the burden is on the Government to prove that the proposed alternatives will not be as effective as the challenged statute.

In considering this question, a court assumes that certain protected speech may be regulated, and then asks what is the least restrictive alternative that can be used to achieve that goal. The purpose of the test is not to consider whether the challenged restriction has some effect in achieving Congress' goal, regardless of the restriction it imposes. The purpose of the test is to ensure that speech is restricted no further than necessary to achieve the goal, for it is important to assure that legitimate speech is not chilled or punished. For that reason, the test does not begin with the status quo of existing regulations, then ask whether the challenged restriction has some additional ability to achieve Congress' legitimate interest. Any restriction on speech could be justified under that analysis. Instead, the court should ask whether the challenged regulation is the least restrictive means among available, effective alternatives.

In deciding whether to grant a preliminary injunction stage, a district court must consider whether the plaintiffs have demonstrated that they are likely to prevail on the merits. As the Government bears the burden of proof on the ultimate question of COPA's constitutionality, respondents must be deemed likely to prevail unless the Government has shown that respondents' proposed less restrictive alternatives are less effective than COPA. Applying that analysis, the District Court concluded that respondents were likely to prevail. That conclusion was not an abuse of discretion, because on this record there are a number of plausible, less restrictive alternatives to the statute.

The primary alternative considered by the District Court was blocking and filtering software. Blocking and filtering software is an alternative that is less restrictive than COPA, and, in addition, likely more effective as a means of restricting children's access to materials harmful to them. The District Court, in granting the preliminary injunction, did so primarily because the plaintiffs had proposed that filters are a less restrictive alternative to COPA and the Government had not shown it would be likely to disprove the plaintiffs' contention at trial.

Filters are less restrictive than COPA. They impose selective restrictions on speech at the receiving end, not universal restrictions at the source. Under a filtering regime, adults without children may gain access to speech they have a right to see without having to identify themselves

or provide their credit card information. Even adults with children may obtain access to the same speech on the same terms simply by turning off the filter on their home computers. Above all, promoting the use of filters does not condemn as criminal any category of speech, and so the potential chilling effect is eliminated, or at least much diminished. All of these things are true, moreover, regardless of how broadly or narrowly the definitions in COPA are construed.

Filters also may well be more effective than COPA. First, a filter can prevent minors from seeing all pornography, not just pornography posted to the Web from America. The District Court noted in its factfindings that one witness estimated that 40% of harmful-to-minors content comes from overseas. COPA does not prevent minors from having access to those foreign harmful materials. That alone makes it possible that filtering software might be more effective in serving Congress' goals. Effectiveness is likely to diminish even further if COPA is upheld, because the providers of the materials that would be covered by the statute simply can move their operations overseas. It is not an answer to say that COPA reaches some amount of materials that are harmful to minors; the question is whether it would reach more of them than less restrictive alternatives. In addition, the District Court found that verification systems may be subject to evasion and circumvention, for example by minors who have their own credit cards. Finally, filters also may be more effective because they can be applied to all forms of Internet communication, including e-mail, not just communications available via the World Wide Web.

That filtering software may well be more effective than COPA is confirmed by the findings of the Commission on Child Online Protection, a commission created by Congress in COPA itself. Congress directed the Commission to evaluate the relative merits of different means of restricting minors' ability to gain access to harmful materials on the Internet. It unambiguously found that filters are more effective than age-verification requirements. See Commission on Child Online Protection, Report to Congress (score for Effectiveness of 7.4 for server-based filters and 6.5 for client-based filters, as compared to 5.9 for independent adult-id verification, and 5.5 for credit card verification). Thus, not only has the Government failed to carry its burden of showing that the proposed alternative is less effective, but also a Government Commission appointed to consider the question has concluded just the opposite. That finding supports our conclusion that the District Court did not abuse its discretion in enjoining the statute.

Filtering software, of course, is not a perfect solution to the problem of children gaining access to harmful-to-minors materials. It may block some materials that are not harmful to minors and fail to catch some that are. Whatever the deficiencies of filters, however, the Government failed to introduce specific evidence proving that existing technologies are less effective than the restrictions in COPA. In the absence of a showing as to the relative effectiveness of COPA and the alternatives proposed by respondents, it was not an abuse of discretion for the District Court to grant the preliminary injunction. The Government's burden is not merely to show that a proposed less restrictive alternative has some flaws; its burden is to show that it is less effective. The Government having failed to carry its burden, it was not an abuse of discretion for the District Court to grant the preliminary injunction.

One argument to the contrary is worth mentioning–the argument that filtering software is not an available alternative because Congress may not require it to be used. That argument carries little weight, because Congress undoubtedly may act to encourage the use of filters. We have

held that Congress can give strong incentives to schools and libraries to use them. *United States v. American Library Assn., Inc.*, 539 U. S 194 (2003). It could also take steps to promote their development by industry, and their use by parents. It is incorrect, for that reason, to say that filters are part of the current regulatory status quo. The need for parental cooperation does not automatically disqualify a proposed less restrictive alternative. COPA presumes that parents lack the ability, not the will, to monitor what their children see. By enacting programs to promote use of filtering software, Congress could give parents that ability without subjecting protected speech to severe penalties.

The closest precedent on the general point is our decision in *Playboy Entertainment Group*. *Playboy Entertainment Group*, like this case, involved a content-based restriction designed to protect minors from viewing harmful materials. The choice was between a blanket speech restriction and a more specific technological solution that was available to parents who chose to implement it. Absent a showing that the proposed less restrictive alternative would not be as effective, we concluded, the more restrictive option preferred by Congress could not survive strict scrutiny. In the instant case, too, the Government has failed to show, at this point, that the proposed less restrictive alternative will be less effective. The reasoning of Playboy Entertainment Group, and the holdings and force of our precedents require us to affirm the preliminary injunction. To do otherwise would be to do less than the First Amendment commands. "The starch in our constitutional standards cannot be sacrificed to accommodate the enforcement choices of the Government."

There are also important practical reasons to let the injunction stand pending a full trial on the merits. First, the potential harms from reversing the injunction outweigh those of leaving it in place by mistake. Second, there are substantial factual disputes remaining in the case. As mentioned above, there is a serious gap in the evidence as to the effectiveness of filtering software. By allowing the preliminary injunction to stand and remanding for trial, we require the Government to shoulder its full constitutional burden of proof respecting the less restrictive alternative argument, rather than excuse it from doing so.

Third, and on a related point, the factual record does not reflect current technological reality. The technology of the Internet evolves at a rapid pace. Yet the factfindings of the District Court were entered in February 1999, over five years ago. It is reasonable to assume that technological developments important to the First Amendment analysis have occurred during that time. More and better filtering alternatives may exist than when the District Court entered its findings.

Delay between the time that a district court makes factfindings and the time that a case reaches this Court is inevitable, with the necessary consequence that there will be some discrepancy between the facts as found and the facts at the time the appellate court takes up the question. We do not mean, therefore, to set up an insuperable obstacle to fair review. Here, however, the usual gap has doubled because the case has been through the Court of Appeals twice. The additional two years might make a difference. By affirming the preliminary injunction and remanding for trial, we allow the parties to update and supplement the factual record to reflect current technological realities.

On this record, the Government has not shown that the less restrictive alternatives proposed

by respondents should be disregarded. Those alternatives, indeed, may be more effective than the provisions of COPA. The District Court did not abuse its discretion when it entered the preliminary injunction.

Justice Stevens, with whom Justice Ginsburg joins, concurring.

In registering my agreement with the Court's less-restrictive-means analysis, I wish to underscore just how restrictive COPA is. COPA is a content-based restraint on the dissemination of constitutionally protected speech. It enforces its prohibitions by way of the criminal law, threatening noncompliant Web speakers with a fine of as much as $50,000, and a term of imprisonment as long as six months, for each offense. And because implementation of the various adult-verification mechanisms described in the statute provides only an affirmative defense, even full compliance with COPA cannot guarantee freedom from prosecution.

COPA's criminal penalties are strong medicine for the ill that the statute seeks to remedy. To be sure, our cases have recognized a compelling interest in protecting minors from exposure to sexually explicit materials. As a parent, grandparent, and great-grandparent, I endorse that goal without reservation. As a judge, however, I must confess to a growing sense of unease when the interest in protecting children from prurient materials is invoked as a justification for using criminal regulation of speech as a substitute for adult oversight of children's viewing habits.

In view of the gravity of the burdens COPA imposes on Web speech, the possibility that Congress might have accomplished the goal of protecting children by other, less drastic means is a matter to be considered with special care. With that observation, I join the opinion of the Court.

Justice Scalia, dissenting.

I agree with Justice Breyer's conclusion that COPA is constitutional. Both the Court and Justice Breyer err, however, in subjecting COPA to strict scrutiny. Nothing in the First Amendment entitles the type of material covered by COPA to that exacting standard of review.

Justice Breyer, with whom The Chief Justice and Justice O'Connor join, dissenting.

Like the Court, I would subject the Act to "the most exacting scrutiny," requiring the Government to show that any restriction of nonobscene expression is "narrowly drawn" to further a "compelling interest" and that the restriction amounts to the "least restrictive means" available to further that interest. Nonetheless, my examination of (1) the burdens the Act imposes on protected expression, (2) the Act's ability to further a compelling interest, and (3) the proposed "less restrictive alternatives" convinces me the Court is wrong. I cannot accept its conclusion that Congress could have accomplished its objective in other, less restrictive ways.

I

Although the Court rests its conclusion upon the existence of less restrictive alternatives, I must first examine the burdens that the Act imposes upon protected speech. That is because the term "less restrictive alternative" is a comparative term. An "alternative" is "less restrictive" only

if it will work less First Amendment harm than the statute itself, while at the same time similarly furthering the "compelling" interest that prompted Congress to enact the statute. Unlike the majority, I do not see how it is possible to make this comparative determination without examining both the extent to which the Act regulates protected expression and the nature of the burdens it imposes on that expression. That examination suggests that the Act, properly interpreted, imposes a burden on protected speech that is no more than modest.

The Act's definitions limit the material it regulates to material that does not enjoy First Amendment protection, namely legally obscene material, and very little more. The only significant difference between the present statute and Miller's definition consists of the addition of the words "with respect to minors," §231(e)(6)(A), and "for minors," §231(e)(6)(C). But the addition of these words to a definition that would otherwise cover only obscenity expands the statute's scope only slightly.

The "lack of serious value" requirement narrows the statute yet further–despite the presence of the qualification "for minors." That is because one cannot easily imagine material that has serious literary, artistic, political, or scientific value for a significant group of adults, but lacks such value for any significant group of minors. Thus, the statute, read literally, insofar as it extends beyond the legally obscene, could reach only borderline cases.

These limitations on the statute's scope answer many of the concerns raised by those who attack its constitutionality. Respondents fear prosecution for the Internet posting of material that does not fall within the statute's ambit as limited by the "prurient interest" and "no serious value" requirements; for example: an essay about a young man's experience with masturbation and sexual shame; "a serious discussion about birth control practices, homosexuality, . . . or the consequences of prison rape"; an account by a 15-year-old, written for therapeutic purposes, of being raped when she was 13; a guide to self-examination for testicular cancer; a graphic illustration of how to use a condom; or any of the other postings of modern literary or artistic works or discussions of sexual identity, homosexuality, sexually transmitted diseases, sex education, or safe sex, let alone J. D. Salinger's Catcher in the Rye, or, as the complaint would have it, "Ken Starr's report on the Clinton-Lewinsky scandal."

These materials are not both (1) "designed to appeal to, or . . . pander to, the prurient interest" of significant groups of minors and (2) lacking in "serious literary, artistic, political, or scientific value" for significant groups of minors. §§231(e)(6)(A), (C). Thus, they fall outside the statute's definition of the material that it restricts.

I have found nothing elsewhere in the statute's language that broadens its scope. Other qualifying phrases, such as "taking the material as a whole" and "for commercial purposes," limit the statute's scope still more. In sum, the Act's definitions limit the statute's scope to commercial pornography. It affects unprotected obscene material. Given the inevitable uncertainty about how to characterize close-to-obscene material, it could apply to a limited class of borderline material that courts might ultimately find is protected.

The Act does not censor the material it covers. Rather, it requires providers of the "harmful to minors" material to restrict minors' access to it by verifying age. They can do so by inserting screens that verify age using a credit card, adult personal identification number, or other similar

technology. In this way, the Act requires creation of an internet screen that minors, but not adults, will find difficult to bypass.

I recognize that the screening requirement imposes some burden on adults who seek access to the regulated material, as well as on its providers. The cost is, in part, monetary. The parties agreed that a Web site could store card numbers or passwords at between 15 and 20 cents per number. And verification services provide free verification to Web site operators, while charging users less than $20 per year. In addition to the monetary cost, the identification requirements inherent in age-screening may lead some users to fear embarrassment. Both monetary costs and potential embarrassment can deter potential viewers and, in that sense, the statute's requirements may restrict access to a site. But this Court has held that in the context of congressional efforts to protect children, restrictions of this kind do not automatically violate the Constitution. See, e.g., *United States v. American Library Assn., Inc.*, 539 U.S. 194, 209 (2003) (plurality opinion).

In sum, the Act at most imposes a modest additional burden on adult access to legally obscene material, perhaps imposing a similar burden on access to some protected borderline obscene material as well.

II

I turn next to the question of "compelling interest," that of protecting minors from exposure to commercial pornography. No one denies that such an interest is "compelling." Rather, the question here is whether the Act, given its restrictions on adult access, significantly advances that interest. In other words, is the game worth the candle?

The majority argues that it is not, because of the existence of "blocking and filtering software." The majority refers to the presence of that software as a "less restrictive alternative." But that is a misnomer. Conceptually speaking, the presence of filtering software is not an alternative legislative approach to the problem of protecting children from exposure to commercial pornography. Rather, it is part of the status quo, i.e., the backdrop against which Congress enacted the present statute. It is always true, by definition, that the status quo is less restrictive than a new regulatory law. It is always less restrictive to do nothing than to do something. But "doing nothing" does not address the problem Congress sought to address–namely that, despite the availability of filtering software, children were still being exposed to harmful material on the Internet.

Thus, the relevant constitutional question is not the question the Court asks: Would it be less restrictive to do nothing? Of course it would be. Rather, the relevant question posits a comparison of (a) a status quo that includes filtering software with (b) a change in that status quo that adds to it an age-verification screen requirement. Given the existence of filtering software, does the problem Congress identified remain significant? Does the Act help to address it? These are questions about the relation of the Act to the compelling interest. Does the Act, compared to the status quo, significantly advance the ball?

The answers to these intermediate questions are clear: Filtering software, as presently available, does not solve the "child protection" problem. It suffers from four serious inadequacies. First, its filtering is faulty, allowing some pornographic material to pass through

without hindrance. Just last year, in *American Library Assn.*, Justice Stevens described "fundamental defects in filtering software." He pointed to the problem of underblocking: "It does not have the capacity to exclude a precisely defined category of images." In the absence of words, the software cannot distinguish between the most obscene image and the Venus de Milo.

Second, filtering software costs money. Not every family has the $40 or so necessary to install it. By way of contrast, age screening costs less.

Third, filtering software depends upon parents willing to decide where their children will surf the Web and able to enforce that decision. As to millions of American families, that is not a reasonable possibility. More than 28 million school age children have both parents or their sole parent in the work force, at least 5 million children are left alone at home without supervision each week, and many of those children will spend afternoons and evenings with friends who may well have access to computers and more lenient parents.

Fourth, software blocking lacks precision, with the result that those who wish to use it to screen out pornography find that it blocks a great deal of material that is valuable. Indeed, the ACLU told Congress that filtering software "block[s] out valuable and protected information, such as information about the Quaker religion, and web sites including those of the American Association of University Women, the AIDS Quilt, the Town Hall Political Site (run by the Family Resource Center, Christian Coalition and other conservative groups)." The software "is simply incapable of discerning between constitutionally protected and unprotected speech."

Nothing in the District Court record suggests the contrary. No party has suggested, for example, that technology allowing filters to interpret and discern among images has suddenly become, or is about to become, widely available. Indeed, the Court concedes that "[f]iltering software, of course, is not a perfect solution to the problem."

In sum, a "filtering software status quo" means filtering that underblocks, imposes a cost upon each family that uses it, fails to screen outside the home, and lacks precision. Thus, Congress could reasonably conclude that a system that relies entirely upon the use of such software is not an effective system. And a law that adds to that system an age-verification screen requirement significantly increases the system's efficacy.

The upshot is that Congress could reasonably conclude that, despite the current availability of filtering software, a child protection problem exists. It also could conclude that a precisely targeted regulatory statute, adding an age-verification requirement for a narrow range of material, would more effectively shield children from commercial pornography.

III

I turn, then, to the actual "less restrictive alternatives" that the Court proposes. The Court proposes two real alternatives. First, the Government might "act to encourage" the use of blocking and filtering software. Any argument that rests upon this alternative proves too much. If one imagines enough government resources devoted to the problem and perhaps additional scientific advances, then, of course, the use of software might become as effective and less restrictive. Obviously, the Government could give all parents, schools, and Internet cafes free computers with filtering programs already installed, hire federal employees to train parents and

teachers on their use, and devote millions of dollars to the development of better software. The result might be an alternative that is extremely effective.

But the Constitution does not, because it cannot, require the Government to disprove the existence of magic solutions, i.e., solutions that, put in general terms, will solve any problem less restrictively but with equal effectiveness. A "judge would be unimaginative indeed if he could not come up with something a little less 'drastic' or a little less 'restrictive' in almost any situation, and thereby enable himself to vote to strike legislation down." Perhaps that is why no party has argued seriously that additional expenditure of government funds to encourage the use of screening is a "less restrictive alternative."

Second, the majority suggests decriminalizing the statute. To remove a major sanction, however, would make the statute less effective, virtually by definition.

IV

My conclusion is that the Act risks imposition of minor burdens on some protected material–burdens that adults wishing to view the material may overcome at modest cost. At the same time, it significantly helps to achieve a compelling congressional goal, protecting children from exposure to commercial pornography. There is no serious, practically available "less restrictive" way similarly to further this compelling interest. Hence the Act is constitutional.

CENTER FOR DEMOCRACY & TECHNOLOGY v. PAPPERT

337 F. Supp. 2d 606 (E.D. Pa. 2004)

MEMORANDUM OPINION
JUDGE JAN E. DUBOIS

In February of 2002, Pennsylvania enacted the Internet Child Pornography Act, 18 Pa. Cons. Stat. §§ 7621-7630, ("the Act"). The Act requires an Internet Service Provider ("ISP") to remove or disable access to child pornography items "residing on or accessible through its service" after notification by the Pennsylvania Attorney General. It is the first attempt by a state to impose criminal liability on an ISP which merely provides access to child pornography through its network and has no direct relationship with the source of the content.

Plaintiffs argue that, due to the technical limitations of the methods used by ISPs to comply with the Act, the efforts of ISPs to disable access to child pornography in response to requests by the Attorney General have led to the blocking of more than one and a half million innocent web sites not targeted by the Attorney General. Plaintiffs filed suit claiming that this blocking of innocent content, or "overblocking," violates the First Amendment to the Constitution.

Defendant responds by arguing that the suppression of protected speech is not required by the Act and is the result of action taken by ISPs. According to defendant, ISPs have options for disabling access that would not block content unrelated to child pornography. Based on the evidence presented by the parties at trial, the Court concludes that, with the current state of technology, the Act cannot be implemented without excessive blocking of innocent speech in

violation of the First Amendment.

The elimination of child pornography is an important goal. To that end, all of the ISPs involved in the case have given defendant their complete cooperation. Notwithstanding this effort, there is little evidence that the Act has reduced the production of child pornography or the child sexual abuse associated with its creation. On the other hand, there is an abundance of evidence that implementation of the Act has resulted in massive suppression of speech protected by the First Amendment. For these reasons, the Act is unconstitutional.

FINDINGS OF FACT

Shared Domain Names

Within the United States alone, there are tens of millions of separate domain names used for web sites that are, for the most part, independent of each other. Web publishers can also publish on the World Wide Web without obtaining their own unique domain names. For example, a web publisher can place content with a provider that offers to host web pages on the provider's own web site (as a sub-page under the provider's domain name). Thus, hypothetically, the Example Corporation could have a web site at the URL http://www.webhostingcompany.com/example. Some web hosts allow users to create web sites using individualized subdomains of the web hosts' primary domain. Thus, hypothetically, the Example Corporation web site might be at the URL http://example.webhostingcompany.com, while another customer site might be at the URL http://acehardware.webhostingcompany.com. Web sites hosted as sub-pages or sub-domains are usually independent of the provider and of each other.

IP Addresses and the Domain Name System

A URL such as http://www.attorneygeneral.gov provides enough information for a user to access the desired web site. However, the URL alone is not sufficient for the user's computer to locate the web site. A user's computer must first determine the numeric Internet Protocol Address or IP address of the desired web site.

When a user seeks to access a particular URL, the user's computer initiates a look up through a series of global databases known as the domain name system ("DNS") to determine the IP Address of the Web Server that can provide the desired web pages. To search for the requested URL's IP address, the user's web browser must query a domain name system server ("DNS server") that has been assigned or selected within the user's computer. If that DNS server cannot find the IP address in its own database, it queries other DNS servers until it receives the correct IP address. It then returns that address to the user's computer.

Typically, an ISP gives its customers the IP addresses of DNS servers controlled by the ISP. Some ISPs assign a new IP address identifying a different DNS server each time the user establishes a connection to the ISP. This is called dynamic assignment.

The numeric IP address of the DNS server provides the user's computer with the Internet address of the Web Server to which the user's computer then sends a request for the particular URL entered in the user's web browser. IP addresses are generally expressed as four sets of numbers separated by periods, e.g., 207.102.198.176.

IP addresses are assigned by several registries covering various parts of the world. The party to whom the registry assigns an IP address may subassign the address.

Although a specific URL refers only to one specific web site, many different web sites (each with different domain names and URLs) are hosted on the same physical Web Server, and all the web sites on a server share the same IP Address.

It is common for web hosting companies to offer virtual web hosting under which many web sites are hosted on the same Web Server and thus share the same IP address. Research by plaintiffs' expert Michael Clark empirically confirms the prevalence of shared IP addresses. "At the time the data was collected (October 2003), at least fifty percent of domains shared an IP address with at least fifty other domains."

One cannot determine with any certainty - using technical means - whether a given web site shares its IP address with another web site. The most reliable method of determining whether a particular web site uses an IP address shared by other sites is to contact the web hosting entity.

Internet Child Pornography Act ("The Act")

On February 21, 2002, Pennsylvania enacted the Internet Child Pornography Act. The Act permits defendant or a district attorney in Pennsylvania to seek a court order requiring an ISP to "remove or disable items residing on or accessible through" an ISP's service upon a showing of probable cause that the item constitutes child pornography. The application for a court order must contain the Uniform Resource Locator providing access to the item. Child pornography is defined as images that display a child under the age of 18 engaged in a "prohibited sexual act."

The court order may be obtained on an ex parte basis with no prior notice to the ISP or the web site owner and no post-hearing notice to the web site owner. Under the Act, a judge may issue an order directing that the challenged content be removed or disabled from the ISP's service upon a showing that the items constitute probable cause evidence of child pornography. A judge does not make a final determination that the challenged content is child pornography.

Once a court order is issued, the Pennsylvania Attorney General notifies the ISP and provides a copy of the court order. The ISP then has five days to block access to the specified content or face criminal liability, including fines of up to $ 30,000 and a prison term of up to seven years.

Implementation of the Act

To implement the Act, the OAG formed a Child Sexual Exploitation Unit. Starting in April 2002, agents investigated complaints by citizens regarding child pornography on the Internet and also searched the Internet for child pornography using ISPs to which the OAG subscribed.

Soon after the Act was enacted, ISPs contacted the OAG to express concern about the Act. "The major complaint is that it is technologically impossible for an ISP to comply with a notice to deny access to a URL to Pennsylvania residents only on which child pornography has been accessed. The ISPs indicate they can deny access to their entire customer base nationwide."

Representatives of ISPs conferred with representatives of the Attorney General regarding implementation of the Act. At these conferences, the participants discussed (1) informal

implementation of the Act to avoid issuance of court orders to ISPs, and (2) technical methods of blocking or disabling access to sites. Representatives of the OAG advanced the use of DNS filtering, URL filtering, and IP filtering as methods that ISPs could use to comply with the Act.

Informal Notices

Starting in late April 2002, when an agent or citizen complainant identified a suspected child pornography web site and Agent Guzy reviewed the site and concluded that it displayed child pornography, an agent sent a document titled "Informal Notice of Child Pornography" to the ISP through whose service the agent or the citizen complainant had accessed the site. Each Notice identified the URL (or URLs) of the site(s) to which the Notice was directed. The ISPs generally responded to the Informal Notices by stating, in writing, that they had complied. The Informal Notices were issued in lieu of court orders.

ISP Compliance with Court Orders or Informal Notices
Methods of Implementation

According to the ISPs, on most occasions, they attempted to comply with the Informal Notices by implementing either IP filtering or DNS filtering. These methods were either used alone or together. Use of IP filtering, DNS filtering, or URL filtering to block content accessible through the service of an ISP only affects Internet users who access the Internet through that ISP's service. Thus, Internet users that do not use the service of an ISP that blocked a web site would still have access to the blocked content.

DNS Filtering

"To perform DNS filtering, an ISP makes entries in the DNS servers under its control that prevent requests to those servers for a specific web site's domain name from resolving to the web site's correct IP address. The entries cause the DNS servers to answer the requests for the IP addresses for such domain names with either incorrect addresses or error messages.

IP Filtering

To implement IP filtering, an ISP first determines the IP address to which a specific URL resolves. It then makes entries in routing equipment that it controls that will stop all outgoing requests for the specific IP address.

URL Filtering

URL filtering involves the placement of an additional device, or in some cases the reconfiguration of an existing "router" or other device, in the ISP's network to (a) reassemble the packets for Internet traffic flowing through its network, (b) read each http web request, and (c) if the requested URL in the web request matches one of the URLs specified in a blocking order, discard or otherwise block the http request.

Comparison of Filtering Methods
Ease of Implementation and Cost

Because the market for Internet access is "very competitive," if an ISP were to implement a [filtering method] which adversely affected [its] network performance, it would be incentive for

[its] customers to jump ship." Most ISPs already have the hardware needed to implement IP filtering and IP filtering is a fairly routine aspect of the management of a network. IP filtering is used to respond to various types of attacks on a network, such as denial of service attacks and spam messages. IP filtering generally does not require ISPs to purchase new equipment and it does not have any impact on network performance.

Most ISPs would not be required to purchase new equipment to implement DNS filtering. If the ISP's staff is familiar with this method of filtering, the necessary entries in the DNS servers require no expenditure of money and little staff time. Almost all ISPs that do not outsource Internet access can utilize DNS filtering for customers that use their DNS servers. Compared to IP filtering, DNS filtering is a "much more specialized technique" within the network security field. With the exception of AOL and WorldCom and other ISPs that do not currently perform DNS filtering, the cost of implementing IP filtering and DNS filtering is "approximately equal." More generally, the difficulty of implementation, financial cost, and performance impact of DNS filtering and IP filtering are similar.

No ISPs known to either plaintiffs' or defendant's experts utilize URL filtering to screen all World Wide Web traffic. AOL engineer Patterson explained that to undertake URL filtering for all AOL members would require expenditures for development, installation, new hardware and software, management costs, performance assessments, customer support, and further re-engineering of the network. It would take years to implement and be "extraordinarily expensive." Mr. Stern acknowledged that any implementation of URL filtering would require extensive research and testing. Mr. Stern also admitted that most ISPs do not have the hardware or software required to implement URL filtering. If an ISP did not purchase substantially more switches and routers, URL filtering would "significantly degrade" the performance of an ISP's network. Such degradation is caused by the fact that the technical process of comparing all of the URLs in the web traffic flowing through an ISP's network with a list of URLs to be blocked is "expensive" in the computational sense - it requires a significant amount of computing power. Performing these computations would slow down each switch and router substantially and decrease the overall capacity of the network. The purchase and testing of the equipment necessary to perform URL filtering would require a significant investment by ISPs. It would cost Verizon "well into seven figures" to implement URL filtering across its entire network. "Money aside, the current [URL filtering] technology . . . would not be able to even operate in [WorldCom's] network" because the current URL filtering products (a) cannot support the speeds needed in WorldCom's network and (b) do not connect to the type of physical wiring (such as fiber optic and coaxial copper cable) that WorldCom uses.

Relative Effectiveness

An ISP's use of DNS filtering does not impact customers that do not use the ISP's DNS servers. "Large businesses often operate their own [DNS servers]. Because DNS filtering is not effective for all of their customers, some ISPs chose not to use this method.

IP filtering would be effective even where a user did not rely on the ISP's DNS server.

A child pornography web site can evade an IP filter by obtaining a new IP address for the web site. A web site's IP address can change without the URL changing. If, however, the ISP

implementing the IP filter monitors the web site for a new IP address and changes the IP address being filtered to block the new address, the IP filtering is still effective.

Because DNS filtering stops a request for the domain name before it has been resolved to an IP address, it continues to prevent access to the identified child pornography item even if the offending site changes its IP address.

IP filtering is more effective than DNS filtering because IP filtering blocks content for all users, including those who do not use DNS servers under an ISP's control. Although a web host can evade IP filtering by changing a web site's IP address - a technique that will not defeat DNS filtering - an ISP can track these changes and block the new IP address. Thus, it is reasonable for an ISP to chose IP filtering as a method of compliance over DNS filtering.

Overblocking

DNS filtering stops requests for all sub-pages under the blocked domain name. Thus, if the domain name included in the URL identified by an Informal Notice is of a Web Hosting Service that allows users to post their independent content as sub-pages on the service's site, the DNS server entries will stop requests for all of the independent pages on the service, not just the page that displays the targeted child pornography item.

DNS filtering stops requests for the domain name, not the IP address for the domain name; it does not disable access to any domain names that share an IP address with the targeted site unless they also share a domain name.

DNS filtering stops requests only for the domain name specified, it does not stop requests for parent domains or sibling sub-domains of the domain name. Thus, if the filtering stops requests for subdomaina.da.ru, it will not stop requests for da.ru or subdomainb.da.ru. However, if the parent domain is filtered, requests for sub-domains would be blocked. Thus, if da.ru was blocked, subdomaina.da.ru and subdomainb.da.ru would also be blocked.

IP filtering leads to a significant amount of overblocking. IP filtering leads to blocking, of innocent web sites, because of the prevalence of shared IP addresses.

URL filtering filters out URLs down to the specific subpage. It presents no risk of disabling access to untargeted sites. Although URL filtering results in the least amount of overblocking, no ISPs are currently capable of implementing this method. Both DNS filtering and IP filtering result in overblocking.

Blocking of Innocent Web Sites

Based on the evidence compiled by Mr. Clark, the total number of innocent web sites blocked by the Informal Notices discussed in this section is approximately 1,190,000. This number does not include the "upwards of 500,000" web sites hosted by Terra.es that were blocked by Verizon.

Methods of Evasion
Anonymous Proxy Servers

Internet users who want to keep their identity secret can use anonymous proxy servers or anonymizers. In the context of visiting web sites, these services route all requests through the

proxy server or anonymizer, which in turn sends the request to the desired web site. Requests using these services appear to the ISP routing the request as if they are requests directed to the proxy service, not to the underlying URL to which the user actually seeks access.

The use of anonymous proxy services or anonymizers completely circumvents both of the technical blocking methods - IP filtering and DNS filtering - used by the ISPs to comply with the Informal Notices and would circumvent URL filtering as well.

Individuals attempting to evade a DNS filter can do so by manually entering the IP address for a DNS server that is not controlled by their ISP.

The Ability of Child Pornographers to Evade Filters

Child pornographers can determine that blocking actions are being used - and that circumvention measures are needed. IP filtering can be evaded by operators of child pornography sites by changing the IP address of the web site.

Operators of child pornography sites can use a range of methods to evade DNS filtering, including: (1) using an IP address (or string of numbers) as the URL instead of a domain name; or (2) changing a portion of a domain name and promulgating the new domain name in hyperlinks to the web site in advertisements, search engines or newsgroups.

Office of the Attorney General Response to Overblocking

The ISPs told the OAG at the April 2002 meetings that, with any method of blocking, they faced the problem of blocking non-child pornography content on the Internet. Specifically, they reported that DNS filtering would block everything behind a given domain, and IP filtering would block everything associated with a given IP address.

CONCLUSIONS OF LAW

FIRST AMENDMENT ISSUES

The Supreme Court has stated, "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 v. ACLU, 521 U.S. 844, 870 (1997). As a result, the Court has ruled that there is "no basis for qualifying the level of First Amendment scrutiny that should be applied to this medium."

1. Burden on Speech

This case is unusual in that the Act, on its face, does not burden protected speech. Facially, the Act only suppresses child pornography, which can be completely banned from the Internet. However, the action taken by private actors to comply with the Act has blocked a significant amount of speech protected by the First Amendment. *United States v. Playboy Entertainment Group*, 529 U.S. 803 (2000), relied upon by both parties, is the case that comes closest to addressing how this type of burden on protected speech should be addressed.

The federal statute at issue in *Playboy* required cable operators which provided sexually

oriented programing to either fully scramble or block the channels that provided this programming, or limit the transmission of such programming to the hours between 10:00 P.M., and 6:00 A.M., referred to as "time channeling." The Supreme Court determined that the statute was unconstitutional because the government failed to establish that the two methods for compliance identified in the challenged section were the least restrictive means for achieving the government's goal. In addressing the statute, the *Playboy* Court applied strict scrutiny because the speech targeted was defined by its content--"sexually explicit content."

The analysis of the *Playboy* Court is instructive. That is so because the majority of cable operators chose to comply with the statute by using time channeling notwithstanding the fact that it silenced a significant amount of protected speech, whereas the other method of compliance, scrambling, did not. On that issue, the Court ruled that a reasonable cable operator could choose not to use scrambling because the available scrambling technology was "imprecise" and portions of the scrambled programs could be heard or seen by viewers, a phenomenon known as "signal bleed." Thus, "[a] rational cable operator, faced with the possibility of sanctions for intermittent bleeding, could well choose to time channel." The Court also noted that digital technology would have solved the signal bleed problem, but it was "not in wide-spread use."

The basis for the *Playboy* Court's determination that the statute was not the least restrictive means for achieving the government's goal was the fact that time channeling, deemed to be a reasonable method of compliance for cable operators, silenced "protected speech for two-thirds of the day in every home in a cable service area, regardless of the presence or likely presence of children or of the wishes of viewers." In making this statement, the Court determined that "targeted blocking" at the request of a customer was a "less restrictive" and feasible means of furthering the government's compelling interest. Targeted blocking required cable operators to block sexually-oriented channels at individual households. It was less restrictive in that it enabled parents who did not want their child exposed to the program to block the offending channels without depriving willing viewers of the opportunity to watch a particular program.

The Act in this case has resulted in the blocking of in excess of 1,190,000 web sites that were not targeted by the Informal Notices. Defendant argues that this overblocking does not violate the First Amendment because it resulted from decisions made by ISPs, not state actors. According to defendant, ISPs have "options for disabling access that would and will not block any, or as many, sites as Plaintiffs claim were blocked in the past" and the choice of which filtering method to use was "completely the decision of the ISPs."

The Court rejects this argument. Like the statute analyzed in *Playboy*, the Act in this case provides ISPs with discretion to choose a method of compliance. Like the time channeling in *Playboy*, the court concludes that ISPs could reasonably choose IP filtering and DNS filtering to comply with Act. And, like *Playboy*, the alternatives reasonably available to the ISPs block protected speech to a significant degree.

The two filtering methods used by the ISPs to comply with the Informal Notices and the court order - IP filtering and DNS filtering - both resulted in overblocking. IP filtering blocks all web sites at an IP address and, given the prevalence of shared IP addresses, the implementation of this method results in blocking a significant number of sites not related to the alleged child

pornography. As an example, access to Ms. Blain's web sites and over 15,000 other sites was blocked to Epix users as a result of the IP Filtering Epix implemented to comply with Informal Notice 2545. DNS filtering also results in overblocking when the method is used to block a web site on an online community or a Web Hosting Service, or a web host that hosts web sites as sub-pages under a single domain name. Specifically, Verizon blocked hundreds of thousands of web sites unrelated to the targeted child pornography when it used DNS filtering to block access to a sub-page of the Terra.es web site, a large online community, in response to Informal Notice 5924. Although a small subset of web hosts, Web Hosting Services host a large number of web sites and the OAG admitted that they are not always identifiable based on the URL. In fact, the OAG continued to issue notices to Web Hosting Services after it was aware of the overblocking problem and had implemented a new procedure to deal with these services.

Moreover, contacting the web host is not a legitimate alternative to use of technical filtering methods. ISPs will not always be able to contact the host within the time period provided by the Act. Even if they can contact a host, the host may not be willing to remove the offending content. In addition, an ISP using this method of compliance risks criminal prosecution if the host decides to place the offending content back on the Internet. Thus, it is rational for an ISP to implement a method of compliance that is not based on the actions of a third party.

The Court will evaluate the constitutionality of the Act with respect to the technology that is currently available. The *Playboy* Court did not consider digital technology a feasible alternative because it was not "economical" for cable operators to use this technology. Similarly, in *Reno v. ACLU*, 521 U.S. 844 (1997), the Supreme Court rejected an argument that Internet content providers could rely on "tagging" or credit card verification technology because the proposed screening software did not exist at that time.

The URL filtering technology recommended by the OAG was not available to any ISPs that received Informal Notices or a court order, with the exception of AOL. AOL's use of URL filtering was limited; it could not use URL filtering on its entire network. The evidence establishes that it would not be economical for ISPs to develop and implement URL filtering technology. Even if the ISPs invested in this technology, it would take significant research and testing to implement this filtering method. Given the uncertain nature of the research, it is difficult to predict the cost of developing this technology. However, one expert estimated that it would cost Verizon "well into seven figures" to implement URL filtering across its entire network. Thus, URL filtering is not a feasible alternative to DNS filtering and IP filtering.

As this Court reads *Playboy*, if a statute regulating speech provides distributors of speech with alternatives for compliance and the majority of distributors reasonably choose an alternative that has the effect of burdening protected speech, the statute is subject to scrutiny as a burden on speech. Both of the filtering methods used by the ISPs in this case resulted in the blocking of innocent speech. The method of filtering recommended by defendant at trial - URL filtering - was rejected by the ISPs as infeasible. As a result, the Court concludes that the Act burdens speech and is subject to First Amendment scrutiny.

2. Level of Scrutiny

In determining whether a statute's burden on protected speech is constitutional, a Court must

generally first decide whether to apply strict or intermediate scrutiny. Plaintiffs argue that strict scrutiny applies because the Act is a content based restriction on speech. Defendant argues that intermediate scrutiny is more appropriate because the Act only applies to child pornography, which has no protection, and the burden on protected expression is a collateral consequence of the Act. In addition, defendant argues that intermediate scrutiny applies because the Act regulates conduct - child sexual abuse - or the secondary effects of the manufacture of child pornography - also child sexual abuse.

The Supreme Court generally subjects "regulations that suppress, disadvantage, or impose differential burdens upon speech because of its content" to strict scrutiny. "In contrast, regulations that are unrelated to the content of speech are subject to an intermediate level of scrutiny because in most cases they pose a less substantial risk of excising certain ideas or viewpoints from the public dialogue." "Strict scrutiny requires that a statute (1) serve a compelling governmental interest; (2) be narrowly tailored to achieve that interest; and (3) be the least restrictive means of advancing that interest." Intermediate scrutiny is more difficult to define. According to the Third Circuit, "admittedly, the intermediate scrutiny test applied varies to some extent from context to context, and case to case. As set forth by the Supreme Court in *United States v. O'Brien*, 391 U.S. 367 (1968), intermediate scrutiny requires that a regulation "(1) furthers an important or substantial governmental interest; (2) the governmental interest is unrelated to the suppression of free expression; and (3) the incidental restriction on alleged First Amendment freedoms is no greater than is essential to the furtherance of that interest."

The Supreme Court has acknowledged that "deciding whether a particular regulation is content-based or content-neutral is not always a simple task." In Turner Broadcasting Systems, the Court stated that "principal inquiry in determining content-neutrality . . . is whether the government has adopted a regulation of speech because of [agreement or] disagreement with the message it conveys."

Even if a statute is content-based, it is not always subject to strict scrutiny because this general rule is subject to "narrow and well-understood exceptions." There are exceptions for obscenity, as defined in *Miller v. California*, 413 U.S. 15 (1973), and child pornography, detailed in *New York v. Ferber*, 458 U.S. 747 (1982). Based on these exceptions, defendant could "completely ban obscenity and child pornography from the Internet.

The Act at issue, on its face, only regulates material that is "outside the protection of the First Amendment." If it were not for the fact that the implementation of the Act resulted in the suppression of protected speech, the Act would not be subject to First Amendment scrutiny. Furthermore, there is no evidence that the innocent content blocked by implementation of the Act is suppressed because of its content or a disagreement with the message it conveys. To the contrary, there is no evidence that the OAG knew the content of the innocent web sites blocked by the ISPs. As a result, the traditional justifications for strict scrutiny do not apply.

Defendant has a strong argument that intermediate scrutiny should apply. The Act is aimed at a legitimate subject of regulation - child pornography - but has the incidental or collateral effect of burdening speech. This statute's collateral or incidental effect on protected speech is similar to the burden on speech in cases in which intermediate scrutiny was applied. For example, the

burden on speech is similar to the one upheld in a secondary effects case, *Renton v. Playtime Theatres, Inc.*, 475 U.S. 41, 48 (1986). In *Renton*, a statute providing for the zoning of adult movie theaters was justified as an attempt to reduce the "adverse effects" such theaters had on the surrounding area. Similarly, the Act is aimed at the "adverse effects" of the production of child pornography - the exploitation and abuse of children. Moreover, the Act is not aimed at suppressing the message communicated by child pornography, it is justified by Pennsylvania's interest in protecting children from sexual exploitation. Thus, the regulation is based on how the material "[is] made, not on what it communicates."

Although there are strong arguments for the application of strict and intermediate scrutiny, the Court need not choose between the two because, even under the less demanding standard - intermediate scrutiny - the Act does not pass Constitutional muster. Under *O'Brien*, a regulation must further an important government interest unrelated to the suppression of free expression and the incidental restriction on First Amendment freedoms must be no greater than is essential to the furtherance of that interest. The government has the burden of proving that the "regulation will in fact alleviate [the] harms [addressed by the regulation] in a direct and material way," and it has not met that burden in this case. In addition, the Act suppresses substantially more protected material than is essential to the furtherance of the government's interest.

Although the prevention of child exploitation and abuse is a state interest unrelated to the suppression of free expression, defendant has not produced any evidence that the implementation of the Act has reduced child exploitation or abuse. The Act does block some users' access to child pornography; however, the material is still available to Internet users accessing the material through ISPs other than the one that blocked the web site. In addition, there are a number of methods that users and producers of child pornography can implement to avoid the filtering methods. For example, both IP filtering and DNS filtering can be avoided by a person using an anonymous proxy server or an anonymizer. A child pornographer can evade an IP filter by moving his web site to another IP address without having to change the content or the URL identifying the site. A user attempting to evade a DNS filter can manually enter the IP address for a DNS server not controlled by his ISP to avoid the block. Moreover, there is no evidence that any child pornographers have been prosecuted as a result of enforcement of the Act. In fact, the OAG did not investigate the entities that produce, publish, and distribute the child pornography. Although the inference could be drawn that making it more difficult to access child pornography reduces the incentive to produce and distribute child pornography, this burden on the child pornography business is not sufficient to overcome the significant suppression of expression that resulted from the implementation of the Act.

More than 1,190,000 innocent web sites were blocked in an effort to block less than 400 child pornography sites, and there is no evidence that the government made an effort to avoid this impact on protected expression. As discussed in this Memorandum, all the currently available technical methods of disabling access to a web site accessible through an ISP's service result in significant overblocking. The Act fails to specify any means of compliance, let alone provide guidance as to which method will minimize suppression of protected speech. This burden on protected expression is substantial whereas there is no evidence that the Act has impacted child sexual abuse. Thus, the Act cannot survive intermediate scrutiny.