

CHAPTER TWELVE

Rating the Net*

Jonathan Weinberg

I. INTRODUCTION

Internet filtering software is hot. Plaintiffs in *ACLU v. Reno*¹ relied heavily on the existence and capabilities of filtering software (also known as blocking software) in arguing that the Communications Decency Act was unconstitutional.² President Clinton has pledged to “vigorously support” the development and widespread availability of filtering software.³ Some free speech activists see this software as the answer to the dilemma of indecency regulation, making it possible “to reconcile free express of ideas and appropriate protection for kids.”⁴ Indeed, some of the strongest supporters of such software are First Amendment activists who sharply oppose direct government censorship of the Net.⁵

Internet filtering software, further, is here. As of this writing, the Platform for Internet Content Selection (PICS) working group has developed a common language for Internet rating systems, making it much easier to create and market such ratings.⁶ Already, two heavily promoted ratings systems (SafeSurf and RSACi) allow content providers to rate their own World Wide Web sites in a sophisticated manner. Microsoft’s World Wide Web browser incorporates a feature called Content Advisor that will block Web sites in accordance with the rules of any PICS-compliant ratings system, including SafeSurf and RSACi.⁷ Stand-alone blocking software—marketed under such trademarks as SurfWatch, Cyber Patrol, CYBERSitter, KinderGuard, Net Nanny, and Parental Guidance—is gaining increasing sophistication and popularity.

It is easy to understand the acclaim for filtering software. This software can do an impressive job at blocking access to sexually explicit material that a parent does not wish his or her child to see. The PICS standard for describing ratings systems is an important

technical achievement, allowing the development and easy use of a variety of sophisticated ratings schemes. In the midst of the general enthusiasm for Internet filtering software, it is worth trying to locate filtering technology's limitations and drawbacks. Blocking software is a huge step forward in solving the dilemma of sexually explicit speech on the Net, but it does have costs. People whose image of the Net is mediated through blocking software may miss out on worthwhile speech through deliberate exclusion, through inaccuracies in labeling inherent to the filtering process, and through the restriction of unrated sites.

II. BACKGROUND

Internet rating services respond to parents' and governments' concerns about children's access to sexually explicit material, and other adult content, available on the Net. The services focus greatest attention on children's access to the World Wide Web (Web). The Web consists of a vast collection of documents, each residing on a computer linked to the Internet. These documents may contain text, pictures, sound, and/or video. Any Web document may contain links to other Web documents or other Internet resources, so that a user with a Web browser can jump from one document to another with a single mouse click. It is easy for users without sophisticated equipment or expensive Internet connections to create Web pages that are then accessible to any other user with access to the Web.

Rating services have also paid special attention to Usenet newsgroups. Usenet newsgroups allow any user to post text, pictures, sound, or video to one of more than 15,000 different open forums, each devoted to a different topic. About 200,000 computer networks worldwide participate in the Usenet news system. A small number of Usenet newsgroups are devoted to sexually explicit material.

It is fairly easy for software to screen access to Usenet news. Because each newsgroup has a name describing its particular topic (such as `rec.music.folk`, `soc.culture.peru`, or `alt.tv.x-files`), software writers can do a reasonably effective job of blocking access to sexually explicit material by simply blocking access to those newsgroups (such as `alt.sex.stories`) whose names indicate that they include sexually explicit material.

Blocking access to sexually explicit material on the Web is much more difficult. There are millions of individual pages on the Web, and the number is increasing every day. An astonishingly small fraction of those pages contain sexually explicit material.⁸ Every Web page (indeed, every document accessible over the Internet) has a unique address, or "URL,"⁹ and the URLs of some Web pages do contain clues as to their subject matter. Because nothing in the structure or syntax of the Web *requires* Web pages to include labels advertising their content, though, identifying pages with sexually explicit material is not an easy task.

First-generation blocking software compiled lists of off-limits Web pages through two methods. First, the rating services hired raters to work through individual Web pages by hand, following links to sexually explicit sites and compiling lists of URLs to be deemed off-limits to children. Second, they used string-recognition software to automatically proscribe any Web page that contained a forbidden word (such as "sex" or "xxx") in its URL.¹⁰

The PICS specifications contemplate that a ratings system can be more sophisticated.

A rating service may rate a document along multiple dimensions. Instead of merely rating a document as “adult” or “child-safe,” it might give it separate ratings for violence, sex, nudity, and adult language. Further, along any given dimension, the rating service may choose from any number of values. Instead of simply rating a site “block” or “no-block” for violence, a rating service might assign it a rating of between 1 and 10 for increasing amounts of violent content. These features are important because they allow the creation of filtering software that is customizable by parents. A parent subscribing to such a rating service, for example, might seek to block only sites rated over 3 for violence and 8 for sex. Finally, the PICS documents note that ratings need not be assigned by the authors of filtering software.¹¹ They can be assigned by the content creators themselves or by third parties. One of the consequences of the PICS specifications is that varying groups—the Christian Coalition, say, or the Boy Scouts—can seek to establish rating services reflecting their own values, and these ratings can be implemented by off-the-shelf blocking software.¹²

Most rating services today follow the PICS specifications. Their particular approaches, however, differ. The Recreational Software Advisory Council (RSAC) has developed an Internet rating system called RSACi.¹³ Participating content providers rate their own sites along a scale of 0 through 4 on four dimensions: violence, nudity, sex, and language. RSAC does not itself market blocking software; instead, it licenses its service to software developers. SafeSurf is another system in which content providers rate their own speech.¹⁴ In that system, content providers choose from nine values in each of nine categories, from “profanity” through “gambling.”¹⁵

Rating services associated with individual manufacturers of blocking software include Cyber Patrol, Specs for Kids, and CYBERSitter. Cyber Patrol rates sites along fifteen dimensions, from “violence/profanity” to “alcohol & tobacco,” but assigns only two values within each of those categories: CyberNOT and CyberYES.¹⁶ Specs for Kids rates documents along eleven dimensions, including “advertising,” “alternative lifestyles,” “politics,” and “religion,” and assigns up to five values (including “no rating”) in each of those categories.¹⁷ CYBERSitter, by contrast, maintains a single list of objectionable sites; it affords users no opportunity to block only portions of the list.¹⁸

III. ACCURACY

Since blocking software first came on the market, individual content providers have complained about the ratings given to their sites. Not all of those complaints relate to problems inherent to filtering software. For example, some programs tend to block entire directories of Web pages simply because they contain a single “adult” file. That means that large numbers of innocuous Web pages are blocked merely because they are located near some *other* page with adult content.¹⁹ Some programs block entire domains, including all of the sites hosted by particular Internet service providers.²⁰ This may be a temporary glitch, though; over time, it is possible that the most successful rating services will—properly—label each document separately.²¹

Other problems arise from the wacky antics of string-recognition software. America Online’s software, ever alert for four-letter words embedded in text, refused to let users register from the British town of “Scunthorpe.”²² The University of Kansas Medical

Center installed SurfWatch in its Internet kiosk and discovered that users could not see the Web page of their own Archie R. Dykes Medical Library.²³ For sheer wackiness, nothing can match a CYBERSitter feature that causes Web browsers to white out selected *words* but display the rest of the page (so that the sentence “President Clinton opposes homosexual marriage” would be rendered “President Clinton opposes marriage”).²⁴ These problems too, though, may be addressed through proper software design.

Controversies over sites actually rated by humans are less amenable to technological solution. One dispute arose when Cyber Patrol blocked animal-rights Web pages because of images of animal abuse, including syphilis-infected monkeys; Cyber Patrol classed those as “gross depiction” CyberNOTs.²⁵ The situation was aggravated because Cyber Patrol, following the entire-directory approach described above, blocked *all* of the hundred or so animal welfare, animal rights, and vegetarian pages hosted at the Animal Rights Resource Site.²⁶ An officer of Envirolink, which had provided the Web space, responded: “Animal rights is usually the first step that children take in being involved in the environment. Ignoring companies like Mary Kay that do these things to animals and allowing them to promote themselves like good corporate citizens is a ‘gross depiction.’”²⁷

Sites discussing gay and lesbian issues are commonly blocked, even if they contain no references to sex. SurfWatch, in its initial distribution, blocked a variety of sites including the Queer Resources Directory, an archive of material on homosexuality in America,²⁸ and the International Association of Gay Square Dance Clubs. SurfWatch responded to protests by unblocking most of the contested sites.²⁹ Other blocking programs, on the other hand, still exclude them: Cyber Patrol blocks a mirror of the Queer Resources Directory, along with Usenet newsgroups including *clari.news.gays* (which carries AP and Reuters dispatches) and *alt.journalism.gay-press*.³⁰ CYBERSitter is perhaps the most likely to block any reference to sexual orientation, forbidding such newsgroups as *alt.politics.homosexual*. In the words of a CYBERSitter representative: “I wouldn’t even care to debate the issues if gay and lesbian issues are suitable for teenagers. . . . We filter anything that has to do with sex. Sexual orientation [is about sex] by virtue of the fact that it has sex in the name.”³¹

The list of blocked sites is sometimes both surprising and alarming. Cyber Patrol blocks Usenet newsgroups including *alt.feminism*, *soc.feminism*, *clari.news.women*, *soc.support.pregnancy.loss*, and *alt.support.fat-acceptance*.³² It blocks gun and Second Amendment Web pages (including one belonging to the NRA Members’ Council of Silicon Valley). It blocks the Web site of the League for Programming Freedom (a group opposing software patents). It blocked the Electronic Frontier Foundation’s censorship archive.³³ It blocked a site maintained by the U.S. Naval Academy Weapon Systems Engineering Department.³⁴ CYBERSitter blocks the National Organization of Women Web site.³⁵ It blocks the Penal Lexicon, an encyclopedic British site concerned with prisons and penal affairs.³⁶ It blocks some Web pages that criticize its blocking decisions,³⁷ and at one point demanded that a critic’s Internet service provider terminate the critic’s account or see all of the sites on its server blocked.³⁸ After the *Netly News*—a component of Time Warner Pathfinder—posted a search engine allowing viewers to find out whether the software blocked particular sites, CYBERSitter blocked the more than 150,000 pages on *pathfinder.com*.³⁹

One might think that a better answer lies in rating systems, such as RSACi and SafeSurf, in which content providers evaluate their own sites. An author, one might assume, could hardly disagree with a rating he chose himself. The matter, though, is not so clear. When an author evaluates his site in order to gain a rating from any PICS-compliant rating service, he must follow the algorithms and rules of that service. Jonathan Wallace, thus, in an article called *Why I Will Not Rate My Site*, asks how he is to rate “An Auschwitz Alphabet,”⁴⁰ his powerful and deeply chilling work of reportage on the Holocaust.⁴¹ The work contains descriptions of violence done to camp inmates’ sexual organs. A self-rating system, Wallace fears, would likely force him to choose between the unsatisfactory alternatives of labeling the work as suitable for all ages, on the one hand, or “lump[ing it] together with the Hot Nude Women page” on the other.⁴²

IV. RULES AND STANDARDS

At least some of the rating services’ problems in assigning ratings to individual documents are inherent. It is the nature of the process that no ratings system can classify documents in a perfectly satisfactory manner. Consider first how a ratings system designer might construct a ratings algorithm. She might provide an algorithm made up entirely of simple, focused questions, in which each question has a relatively easily ascertainable “yes” or “no” answer. (Example: “Does the file contain a photographic image depicting exposed male or female genitalia?”) Alternatively, she might seek to afford evaluators more freedom to apply broad, informal, situationally sensitive guidelines so as to capture the overall feel of each site. (Example: “Is the site suitable for a child below the age of 13?”)⁴³

In jurisprudential terms, the first approach relies on “rules” and the second on “standards.”⁴⁴ The RSACi system attempts to be rule based. In coding its violence levels, for example, to include “harmless conflict; some damage to objects”; “creatures injured or killed; damage to objects, fighting”; “humans injured or killed with small amount of blood”; “humans injured or killed; blood and gore”; and “wanton and gratuitous violence; torture; rape,” its designers have striven to devise simple, hard-edged rules, with results turning mechanically on a limited number of facts.⁴⁵ Not all RSAC categories are hard edged—the “revealing attire” nudity level requires a rater to decide whether a “reasonable person” would consider particular clothing sexually suggestive and alluring⁴⁶—but the system overall aims for rules.

Other rating systems rely more heavily on standards. The SafeSurf questionnaire, for example, requires the self-rater to determine whether nudity is “artistic” (levels 4 through 6), “erotic” (level 7), “pornographic” (level 8), or “explicit and crude” pornographic (level 9).⁴⁷ The Voluntary Content Rating self-rating system promoted by CYBERSitter is almost the model of a standards-based regime: it offers as its only guidance the instructions that self-raters should determine whether their sites are “not suitable for children under the age of 13,” and whether they include material “intended for an audience 18 years of age or older.”⁴⁸ Specs for Kids raters are instructed to distinguish between sites that: (1) refer to homosexuality “[i]mpartial[ly]”; (2) discuss it with “acceptance or approval”; or (3) “[a]ctive[ly] promot[e]” it or “attempt[] to recruit the viewer.”⁴⁹ Each of these classifications requires more judgment on the part of the evaluator, and is not so hard edged as the

RSACi categories. Individuals with different perspectives and values may disagree as to where the lines fall.⁵⁰ With respect to the Specs treatment of references to homosexuality, individuals disagree as to whether the categories are even coherent.⁵¹ These categories work only within a community of shared values, so that evaluators can draw on the same norms and assumptions in applying the value judgments embedded in the standards.

This distinction follows the more general rules-standards dichotomy in law, which focuses on the instructions lawmakers give to law-appliers in a variety of contexts.⁵² Legal thought teaches that rules and standards each have disadvantages. A problem with standards is that they are less constraining; relatively speaking, a standards-based system will lack consistency and predictability.⁵³ Rules become increasingly necessary as the universe of law-appliers becomes larger, less able to rely on shared culture and values as a guide to applying standards in a relatively consistent and coherent way.⁵⁴ One can see a parallel in problems the Yahoo! indexing service faces in seeking to classify the increasing number of Web sites. Yahoo!'s taxonomy embodies editorial judgments; the job is not amenable to resolution simply through rules. Consistent application of the taxonomy "comes from having the same 20 people classify every site, and by having those people crammed together in the same building where they are constantly engaged in a discussion of what belongs where."⁵⁵ As a result,

Yahoo! is faced with an unforgiving trade-off between the size and the quality of its directory. If Yahoo! hires another 50 or 60 classifiers to examine every last site on the Web, the catalog will become less consistent. . . . On the other hand, if Yahoo! stays with a small number of classifiers, the percentage of sites Yahoo! knows about will continue to shrink.⁵⁶

For this reason, the designers of RSACi attempted to be rule-like. They contemplate that the universe of ratings evaluators will include every content provider on the Web; that group can claim no shared values and culture. To accommodate that heterogeneous group, RSAC offers a rules-based questionnaire that (it hopes) all can understand in a similar manner. This, RSAC explains, will "provide[] fair and consistent ratings by eliminating most of the subjectivity inherent in alternative rating systems."⁵⁷ It seems plain that with a relatively large universe of evaluators—and it is hard to see how one could seek to map the entire Net without one—a ratings system relying too heavily on standards just won't work. The dangers of arbitrariness and inconsistency will be too great.⁵⁸

Rules, though, have their own problems. They direct law-appliers to treat complex and multifaceted reality according to an oversimplified schematic.⁵⁹ The point of rules, after all, is that by simplifying an otherwise complex inquiry, they "screen[] off from a decisionmaker factors that a sensitive decisionmaker would otherwise take into account."⁶⁰ They may thus generate results ill-serving the policies behind the rules.⁶¹ Consider the task of deciding which citizens are mature enough to vote. A rule that any person can vote if he or she has reached the age of eighteen has the advantage of administrability and avoids biased enforcement. Few of us would welcome a system in which a government bureaucrat examined each of us individually to determine whether we were mature enough to vote. Because the rule is much simpler than the reality it seeks to

govern, though, it is both over- and underinclusive: it bars from the franchise some people under eighteen who are mature, and grants the franchise to some people over eighteen who are not. Rules thus give rise to their own arbitrariness.⁶² At best, a rules-based filtering system will miss nuances; at worst, it will generate absurd results—as when America Online, enforcing a rule forbidding certain words in personal member profiles, barred subscribers from identifying themselves as “breast” cancer survivors.⁶³

V. RSACI AND ITS LIMITATIONS

Given this theoretical critique, one might think that the challenge facing ratings system designers is to devise really good rules-based systems, ones that track reality as well as possible, minimizing the difficulties noted above. That is what RSAC claims to have done in RSACi.⁶⁴ I think the product of any such effort, though, necessarily will be flawed.

Let's return to the choices facing a ratings system designer as she constructs blocking software. So far, this article has not addressed the most basic question confronting her: What sort of material should trigger ratings consequences? Should children have access to material about weapons making?⁶⁵ How about hate speech?⁶⁶ Or artistic depictions of nudity?⁶⁷ Again, she can take two different approaches. First, she can decide all such questions herself, so that the home user need only turn the system on and all choices as to what is blocked are already made. CYBERSitter adopts this approach.⁶⁸ This has the benefit of simplicity, but seems appropriate only if members of the target audience are in basic agreement with the rating service (and each other) respecting what sort of speech should and should not be blocked.⁶⁹

Alternatively, she can leave those questions for the user to answer. The ratings system designer need not decide whether to block Web sites featuring bomb-making recipes or hate speech. She can instead design the system so that the user has the power to block those sites if he chooses. Microsoft's implementation of the RSACi labels allows parents to select the levels of adult language, nudity, sex, and violence that the browser will let through.⁷⁰ Cyber Patrol allows parents to select which of the twelve CyberNOT categories to block.

Either approach, though, imposes restrictions on the categories chosen by the ratings system designer. If the system designer wishes to leave substantive choices to parents, she must create categories that correspond to the different sides of the relevant substantive questions. That is, if the designer wishes to leave users the choice whether to block sites featuring hate speech, she must break out sites featuring hate speech into a separate category or categories. If she wishes to leave the user the choice whether to block sites that depict explicit sexual behavior but nonetheless have artistic value, she must categorize those sites differently from those that do not have artistic value.⁷¹ On the other hand, if the system designer makes those substantive decisions herself, making her own value choices as to what material should and should not be blocked, she must create categories that correspond to those value choices.

The problem is that many of these questions cleave on lines defined by standards. Many users, for example, might like to block “pornography,” but allow other, more worthy speech, even if it is sexually explicit. SafeSurf responds to that desire when it

requires self-raters to determine whether nudity is “artistic,” “erotic,” “pornographic,” or “explicit and crude.” It gets high marks for attempting to conform its system to user intuitions, but its lack of rulishness means problems in application.⁷² Similarly, Specs’s distinction between “impartial reference,” “acceptance or approval,” and “active promotion” of homosexuality may well correspond to the intuitions of much of its target audience but will hardly be straightforward in actual application. The problem increases with the heterogeneity of the service’s audience: the more heterogeneous the audience, the more categories a rating system must include to accommodate different user preferences.

With this perspective, one can better appreciate the limitations of RSACi’s attempt to be rule-bound. RSACi ignores much content that some other ratings systems classify as potentially unsuitable, including speech relating to drug use, alcohol, tobacco, gambling, scatology, computer hacking and software piracy, devil worship, religious cults, militant or extremist groups, weapon making, tattooing and body piercing, and speech “grossly deficient in civility or behavior.”⁷³ For many observers (myself included), RSACi’s narrow scope is good news because it limits the ability to block access to controversial political speech. My point, though, is that RSACi *had to* confine its reach if it was to maintain its rule-bounded nature.

The problem appears as well in connection with the categories RSACi *does* address. Consider RSACi’s treatment of sex. It divides up sexual depictions into “romance, no sex,” “passionate kissing,” “clothed sexual touching,” “non-explicit sexual activity,” and “explicit sexual activity; sex crimes.”⁷⁴ But RSACi, in contrast to some other ratings systems, does not seek to distinguish educational, artistic, or crude depictions from others. There is no way, consistent with rulishness, that it can seek to distinguish the serious or artistic from the titillating. It achieves rule-boundedness and ease of administration, at the expense of nuance; it achieves consistent labeling but in categories that do not correspond to the ones many people want.

In sum, rating system designers face a dilemma. If a rating service seeks to map the Web in a relatively comprehensive manner, it must rely on a relatively large group of evaluators. Such a group of evaluators can achieve fairness and consistency only if the ratings system uses simple, hard-edged categories relying on a few, easily ascertainable characteristics of each site. Such categories, though, will not categorize the Net along the lines that home users will find most useful, and will not empower those users to heed their own values in deciding what speech should and should not be blocked. To the extent that ratings system designers allow evaluators to consider more factors in a more situationally specific manner to capture the essence of each site, they will ensure inconsistency and hidden value choices as the system is applied.

VI. UNRATED SITES

Blocking software can work perfectly only if all sites are rated. Otherwise, the software must either exclude all unrated sites, barring innocuous speech, or allow unrated sites, letting in speech that the user would prefer to exclude.⁷⁵ What are the prospects that a rating service will be able to label even a large percentage of the millions of pages on the Web? What are the consequences if it cannot?

First, consider rating services associated with individual manufacturers of blocking software, such as CYBERSitter and Cyber Patrol. These services hire raters to label the entire Web, site by site. The limits on their ability to do so are obvious. As the services get bigger, hiring more and more employees to rate sites, their consistency will degrade; that was one of the lessons of Part III of this article. Moreover, no service could be big enough to rate the entire Web. Too many new pages come online every day. The content associated with any given page is constantly changing.⁷⁶ Further, some of the sites most likely to be ephemeral are also among the most likely to carry sexually explicit material. A ratings service simply cannot keep tabs on every college freshman who gets to school and puts up a Web page, notwithstanding that college freshmen are of an age to be more interested in dirty pictures than most. A ratings service certainly cannot keep tabs on every Web page put up by a college freshman in Osaka, say, or in Amsterdam. So any such rating service must take for granted that there will be a huge number of unrated sites.

As a practical matter, providing access to all unrated sites is not an option for these rating services; it would let through too much for them to be able to market themselves as reliable screeners. Instead, they must offer users other options, dealing with unrated sites in one of two ways. First, they can seek to catch questionable content through string-recognition software. CYBERSitter, for example, offers this option. The problem with this approach, though, is that at least under current technology, string-recognition software simply doesn't work very well. This article has already mentioned America Online's travails with the town of Scunthorpe and the word "breast"; other examples are easy to find. SurfWatch, for example, blocked a page on the White House Web site because its URL contains the forbidden word "couples" (<http://www.whitehouse.gov/WH/kids/html/couples.html>).⁷⁷ The second option is for the rating services simply to block all unrated sites. Industry members seem to contemplate this as the necessary solution. Microsoft, for example, cautions Internet content providers that "[f]or a rating system to be useful, the browser application must deny access to sites that are unrated."⁷⁸ Other observers reach the same result.⁷⁹

What about self-rating approaches, like those of SafeSurf and RSACi? These services have the potential for near-universal reach, since they can draw on the services of an effectively unlimited number of evaluators. While the evaluators will be a diverse group (to say the least), rating service designers can try to cope with that diversity by constructing rule-bound questionnaires. While some evaluators may misrepresent their sites, rating services can try to devise enforcement mechanisms to cope with that as well. On the other hand, self-rating services will not achieve their potential unless content providers have a sufficient incentive to participate in the ratings process in the first place.⁸⁰

That incentive is highly uneven. Mass-market commercial providers seeking to maximize their audience reach will participate in any significant self-rating system, so as not to be shut out of homes in which parents have configured their browsers to reject all unrated sites.⁸¹ Many noncommercial site owners, though, may not participate. They may be indifferent to their under-eighteen visitors and may not wish to incur the costs of self-rating. It is still early to predict what those costs may be. For the owner of a large site containing many documents, supplying a rating for each page may be a time-consuming pain in the neck.⁸²

RSAC appears to have abandoned plans to charge Web sites for using its ratings,⁸³ but there may be other disincentives. Some content providers may not self-rate because they are philosophically opposed to the censorship a rating system enables⁸⁴ or are dissatisfied with the choices a rating system provides. More generally, why should a college or graduate student with a Web page bother to self-rate? He's not necessarily writing for people concerned about ratings, and if those people exclude him, the author may not much care.

VII. COMPULSORY SELF-RATING

It may be that the only way to ensure participation in a self-rating system even in a single country (let alone internationally) would be for the government to compel content providers to self-rate (or to compel Internet access providers to require their customers to do so). It is not obvious how such a requirement would work. The drafters of such a law would face the choice of forcing content providers to score their sites with reference to a particular rating system specified in the law, or allowing them leeway to choose one of a variety of PICS-compliant ratings systems. Neither approach seems satisfactory. The first, mandating use of a particular rating system, would freeze technological development by eliminating competitive pressures leading to the introduction and improvement of new searching, filtering, and organizing techniques. It would leave consumers unable to choose the rating system that best serve their needs. The second would be little better. Some government organ would have to assume the task of certifying particular self-rating systems as adequately singling out material unsuitable for children. It is hard to imagine how that agency could ensure that every approved system yielded ratings useful to most parents, while nonetheless maintaining a healthy market and allowing innovation.

In any event, a mandatory self-rating requirement would likely be held unconstitutional. In *Riley v. National Federation of the Blind*,⁸⁵ the Court considered a requirement that professional fundraisers disclose to potential donors the percentage of charitable contributions collected over the previous twelve months that were actually turned over to charity. The Court explained that "mandating speech that a speaker would not otherwise make" necessarily alters the content of the speech and thus amounts to content-based regulation.⁸⁶ Even when a compelled statement is purely factual, the compulsion burdens protected speech and is subject to "exacting" scrutiny, subject to the rule that government cannot "dictate the content of speech absent compelling necessity, and then, only by means precisely tailored."⁸⁷

The Court repeated that analysis in *McIntyre v. Ohio Elections Commission*,⁸⁸ striking down a requirement that persons distributing election materials state their names and addresses in those materials. The Court explained that the requirement was a "direct regulation of the content of speech" subject to "exacting" scrutiny.⁸⁹ Even though the compelled disclosure was useful to voters and uncontroversially factual, the state was requiring "that a writer make statements or disclosures she would otherwise omit"; the restriction, accordingly, could not stand unless narrowly tailored to serve an overriding state interest.⁹⁰

A requirement that Internet content providers provide ratings of their speech falls

straightforwardly under the rule of those cases.⁹¹ Even if the characterization of speech according to the taxonomy of a particular rating system were deemed factual and value-neutral, requiring a speaker to characterize her speech in that manner would require her to incorporate into her speech a “statement[] . . . she would otherwise omit.” Such a requirement must surmount exacting scrutiny.⁹²

In fact, mandatory self-rating is even more problematic. The Court has repeatedly recognized the impermissibility of requiring a speaker to associate herself with particular ideas she disagrees with.⁹³ Requiring self-rating does that, because rating is *not* factual and value-neutral. Mandatory self-rating compels the speaker to associate herself with the values and worldview embodied in the rating taxonomy. The drafters of RSACi, or SafeSurf, may view—and hence compartmentalize—the universe of speech in a way I reject. RSACi, for example, classifies sexually explicit speech without regard to its educational value or its crass commercialism; that choice is inconsistent with the values of many. Some taxonomies make the conflict more obvious than others; it would surely be offensive for many to be required to characterize their speech using Specs for Kids criteria, under which a message that expresses “acceptance” of homosexuality is by definition not “impartial.” But any taxonomy incorporates editorial and value judgments.

Moreover, a self-rating requirement may otherwise chill protected speech. To the extent that rating criteria are less than wholly rule-like, their vagueness will lead Internet content providers to self-censor. Content providers will “steer far wider of the unlawful zone”⁹⁴ in order to avoid sanctions for misrating. “Vagueness and the attendant evils . . . are not rendered less objectionable because the regulation of expression is one of classification rather than direct suppression.”⁹⁵

I am doubtful that a self-rating requirement could survive exacting scrutiny. Even without a self-rating requirement, parents can restrict their children’s access to sexually explicit sites by using blocking programs, and instructing the software to block all unrated sites. Indeed, the wave of the future may well be Web browser add-ons, marketed by entities such as Disney, that collect a few tens of thousands of Web sites specifically chosen to be kid-friendly and block access to all others. A self-rating requirement would be helpful to parents only in that it would enable them to limit their children’s access in such a way that the kids could also view an uncertain number of *additional* sites, not containing sexually explicit material, whose providers would not otherwise choose to self-rate. In light of the First Amendment damage done by a compelled self-rating requirement, accomplishing that goal does not seem to be a compelling or overriding state interest.⁹⁶

The result, though, is that child-configured lenses will show only a limited, flattened view of the Internet. If many Internet content providers decline to self-rate, the only “safe” response may be to configure blocking software to exclude unrated sites. The plausible result? A typical home user, running Microsoft Internet Explorer set to filter using RSACi tags will have a browser configured to accept duly rated mass-market speech from large entertainment corporations, but to block out a substantial amount of quirky, vibrant individual speech from unrated (but child-suitable) sites. This prospect is disturbing.

The Internet is justly celebrated as “the most participatory form of mass speech yet developed.”⁹⁷ A person or organization with an Internet hookup can easily disseminate speech across the entire medium at low cost; the resulting “worldwide conversation”⁹⁸

features an immense number of speakers and “astoundingly diverse content.”⁹⁹ As Judge Dalzell noted in *ACLU v. Reno*, the Internet vindicates the First Amendment’s protection of “the ‘individual dignity and choice’ that arises from ‘putting the decision as to what views shall be voiced largely into the hands of each of us,’” because “every minute [Internet communication] allows individual citizens actually to make those decisions.”¹⁰⁰ But this prospect is threatened if widespread adoption of blocking software ends up removing much of the speech of ordinary citizens, leaving the viewer little to surf but mass-market commercial programming. One hardly needs the Internet for that; we get it already from the conventional media.

In sum, blocking software could end up blocking access to a significant amount of the individual, idiosyncratic speech that makes the Internet a unique medium of mass communication. Filtering software, touted as a speech-protective technology, may instead contribute to the flattening of speech on the Internet.

VIII. CHILDREN, ADULTS, AND BLOCKING SOFTWARE

You may protest that I am making much of little here. After all, blocking software is intended to restrict *children’s* access to questionable sites. It won’t affect what adults can see on the Internet—or will it? It seems to me that, in important respects, it will. The desire to restrict children’s access has spurred the recent development of filtering technology. Widespread adoption of that software, though, will not likely leave adults unaffected.

In a variety of contexts, we can expect to see adults reaching the Internet through approaches monitored by blocking software. In the home, parents may set up filters at levels appropriate for their children and not disable them for their own use.¹⁰¹ They may subscribe to an Internet access provider that filters out material at the server level, so that nobody in the household can see “objectionable” sites except by establishing an Internet access account with a new provider.¹⁰² If, as seems likely, future versions of the PICS specifications support the transmission of filtering criteria to search engines, then users running Internet searches will not even know which sites otherwise meeting their criteria were censored by the blocking software.¹⁰³

Other people get their Internet connections through libraries; indeed, some policy-makers tout libraries and other community institutions as the most promising vehicle for ensuring universal access to the Internet.¹⁰⁴ The American Library Association takes the position that libraries should provide unrestricted access to information resources; it characterizes the use of blocking programs as censorship.¹⁰⁵ This policy, however, is not binding on member libraries. It is likely that a substantial number of public libraries will install blocking software on their public-access terminals, including terminals intended for use by adults; indeed, some have already done so.¹⁰⁶ As one software vendor warns:

Unlimited Web Access is a Political Nightmare. Your library may spend tens of thousands of dollars on Internet hardware/training and then be closed down by an angry parent willing to go to the press and the town council because their child saw pornographic materials in the library.¹⁰⁷

Still other people get Internet access through their employers. Corporations too, wary of risk and wasted work time, may put stringent filters in place. Some large companies worry about the possibility of being cited for sexual harassment by virtue of material that came into the office via the Internet.¹⁰⁸ Even more are concerned about sports and leisure information they feel may detract from business productivity. One consultant sums up the corporate mood: “My kids went out on the Web to a museum and saw great artwork, but I don’t want my employees hanging out at the Louvre all day on my nickel.”¹⁰⁹

In sum, we may see home computers blocked for reasons of convenience, library computers blocked for reasons of politics, and workplace computers blocked for reasons of profit. Even one university temporarily installed blocking software in its computer labs, in aid of a policy “prohibit[ing] the display in public labs of pornographic material unrelated to educational programs.”¹¹⁰ The result may be that large amounts of content may end up off-limits to a substantial fraction of the *adult* population.¹¹¹

There are limits to this—sex sells. Many home Internet users will be loathe to cut themselves off from the full range of available speech. Most online services and Internet access providers, while attempting to make parents feel secure about their children’s exposure to sexually explicit material on the Internet, will still host such material for adults who wish to view it.¹¹² It seems safe to conclude, though, that blocking software will have the practical effect of restricting the access of a substantial number of adults.

This should affect the way we think about filtering software. Any filtering system necessarily incorporates value judgments about the speech being blocked. These value judgments are not so controversial if we think of the typical user of blocking software as a parent restricting his children’s access. It is part of a parent’s job, after all, to make value judgments regarding his own child’s upbringing. The value judgments are much more controversial, though, if we think of the typical “blockee” as an adult using a library computer, or using a corporate computer after hours. If we are concerned about these users’ access to speech, then we need to think hard about the way blocking software works, the extent to which it can be accurate, and the extent to which it is likely to exclude the sort of speech that makes the Internet worthwhile.

IX. CONCLUSION

Across the world, governments and industry are turning to filtering software as the answer to the problem of sexually explicit material on the Internet. In the United Kingdom, service providers and police have endorsed a proposal recommending that Internet service providers require users to rate their own Web pages, and that the providers remove Web pages that their creators have “persistently and deliberately misrated.”¹¹³ The European Commission has urged the adoption of similar codes of conduct to ensure “systematic self-rating of content” by all European content providers.¹¹⁴ Some U.S. companies have been leaning the same way: CompuServe has decided to “encourage” its users and other content providers to self-rate using RSACi.¹¹⁵

Ratings, though, come at a cost. It seems likely that a substantial number of adults, in the near future, will view the Internet through filters administered by blocking software. Intermediaries—employers, libraries, and others—will gain greater control over the

things these adults read and see. Sites may be stripped out of the filtered universe because of deliberate political choices on the part of rating service administrators, and because of inaccuracies inherent in the ratings process. If a rating service is to categorize a large number of sites, it cannot simultaneously achieve consistency and nuance; the techniques it must rely on to achieve consistency make it more difficult to capture nuance and make it less likely that users will find the ratings useful. The necessity of excluding unrated sites may flatten speech on the Net, disproportionately excluding speech that was not created by commercial providers for a mass audience.

This is not to say that ratings are bad. The cost they impose, in return for the comforting feeling that we can avert a threat to our children, is surely much less than that imposed by the Communications Decency Act. Ratings provide an impressive second-best solution. We should not fool ourselves, though, into thinking that they impose no cost at all.

Notes

- * I am grateful to Jessica Litman, whose comments greatly improved this article. An earlier version of this article was presented at the 1996 Telecommunications Policy Research Conference; I am indebted to the participants in that conference, in particular Paul Resnick and Rivkah Sass, for their perspectives. This article attempts to take a snapshot of an extraordinarily fast-moving field; it reflects developments through the spring of 1997.
- 1. 117 S. Ct. 2329 (1997).
- 2. See Brief of Appellees at Part II.B.2, *Reno v. ACLU*, 117 S. Ct. 2329 (1997), <<http://www.aclu.org/court/renovaclu.html>>.
- 3. The White House Office of the Press Secretary, Statement by the President (June 12, 1996) <http://www.eff.org/pub/Legal/Cases/EFF_ACLU_v_DoJ/960612_clinton_cda_decision.statement>.
- 4. Peter H. Lewis, Microsoft Backs Ratings System for Internet, N.Y. TIMES, Mar. 1, 1996, at D5 (quoting Daniel Weitzner, Deputy Director, Center for Democracy and Technology); see Jerry Berman & Daniel J. Weitzner, Abundance and User Control: Renewing the Democratic Heart of the First Amendment in the Age of Interactive Media, 104 YALE L.J. 1619, 1634-35 (1995).
- 5. Antipornography activists, by contrast, have been decidedly less enthusiastic. Some express concern that such software leaves "the parent . . . responsible to go out and buy the software, become educated about how to apply it, how to install it, how to use it, and how to then monitor it to make sure your child or his friends have not gotten around it." Pornography on the Internet: Straight Talk from the Family Research Council (radio broadcast transcript) (last modified July 3, 1996) <<http://www.townhall.com/townhall/FRC/netst96g1.html>> (statement of Colby May, Senior Counsel, American Center for Law and Justice). To say that blocking software obviates the need for government speech restrictions is "saying . . . that we are free to pollute our cultural environment, and parents have to buy the gas masks." Id. (Statement of Kristi Hamrick, moderator).
- 6. See Paul Resnick & James Miller, PICS: Internet Access Controls Without Censorship, 39 COMMUNICATIONS OF THE ACM 89 (1996). PICS was developed by the World Wide Web Consortium, the body responsible for developing common protocols and reference codes for the evolution of the Web, with the participation of Apple, America Online, AT&T, the Center for Democracy and Technology, Compuserve, DEC, IBM, MCI, the MIT Laboratory for Computer Science, Microsoft, Netscape, Prodigy, the Recreational Software Advisory Council, SafeSurf, SurfWatch, Time Warner Pathfinder, and others.
- 7. Microsoft calls its World Wide Web browser Internet Explorer; Content Advisor first appeared in Internet Explorer's version 3.0. Content Advisor makes it easiest to use RSACi ratings. RSACi is an Internet ratings system established by the Recreational Software Advisory Council (RSAC), which was created by the Software Publishers Association in 1994 to create a rating system for computer games. RSAC formed a working party in late 1995, including representatives from Time Warner Pathfinder, AT&T, PICS and Microsoft, to develop RSACi. See *infra* note 13 and accompanying text.

For Content Advisor to use ratings from a PICS-compliant rating service other than RSACi, the user must copy that service's .RAT file into his Windows System folder and then click on "Add A New

Rating service" in the IE Options menu. See SafeSurf News (visited Feb. 7, 1997) <<http://www.safesurf.com/nletter/summ96.htm>>.

8. *Shea v. Reno*, 930 F.Supp. 916, 931 (S.D.N.Y. 1996):

While it is difficult to ascertain with any certainty how many sexually explicit sites are accessible through the Internet, the president of a manufacturer of software designed to block access to sites containing sexually explicit material testified in the Philadelphia litigation that there are approximately 5,000 to 8,000 such sites, with the higher estimate reflecting the inclusion of multiple pages (each with a unique URL) attached to a single site. The record also suggests that there are at least thirty-seven million unique URLs. Accordingly, even if there were twice as many unique pages on the Internet containing sexually explicit materials as this undisputed testimony suggests, the percentage of Internet addresses providing sexually explicit content would be well less than one tenth of one percent of such addresses.

Id. (citations omitted).

9. "URL" is an acronym for "Uniform Resource Locator." See Internet Engineering Task Force, Uniform Resource Locators [RFC-1738] (Dec. 1994) <<http://ds.internic.net/rfc/rfc1738.txt>>.
10. See *Shea*, 930 F.Supp. at 932.
11. See Resnick & Miller, *supra* note 6.
12. See id.
13. The heavy hitters behind RSACi have been RSAC, established in 1994 by the Software Publishers Association, and such industry players as Microsoft, AT&T, and Time Warner Pathfinder. See *supra* note 6. As of April 15, 1996, content providers have been able to rate their own sites using the RSACi system by completing a questionnaire at the RSAC Web site, <<http://www.rsac.org>> (visited March 27, 1997).
14. SafeSurf describes itself as an "international no-fee parents' organization formed to protect children on the Internet and the rights of parents through technology and education." SafeSurf press release (Apr. 18, 1996) <<http://www.safesurf.com/press/press12.htm>>. It uses the CyberAngels, an offshoot of Curtis Sliwa's Guardian Angels, to patrol sites whose owners have rated them as suitable for "All Ages," verifying that the sites do not contain adult content. E-mail from Wendy Simpson, President, SafeSurf to Declan McCullagh (Apr. 28, 1996) (on file with author).
15. The categories are: profanity, heterosexual themes, homosexual themes, nudity, violence, intolerance, glorifying drug use, other adult themes, and gambling. See SafeSurf Rating System (visited Feb. 7, 1997) <<http://www.safesurf.com/classify/index.html>>.
16. See CyberNOT List Criteria (last modified May 9, 1996) <http://www.microsys.com/cyber/cp_list.htm>.
17. See Specs Glossary (visited Feb. 7, 1997) <http://www.newview.com/cust/ss_sg_lv13a_cf_fcs.html>.
18. See CYBERSitter Product Information (visited Feb. 7, 1997) <<http://solidoak.com/cysitter.htm>>. CYBERSitter characterizes its customers as "strong family-oriented people with traditional family values." The product is sold by Focus on the Family. See Brock N. Meeks & Declan B. McCullagh, *Jacking In from the 'Keys to the Kingdom' Port, CYBERWIRE DISPATCH* (July 3, 1996) <http://www.fff.org/pub/Publications/Declan_McCullagh/cwd.keys.to.the.kingdom.0796.article>.
19. For the most part, Cyber Patrol drops all but the first three characters of the file name in the URL, thus blocking innocuous pages. See Meeks & McCullagh, *supra* note 18. In some instances, Cyber Patrol blocks at a higher level, so that, for example, it excluded all of Jewish.com because personal ads were not stored in a separate subdirectory. Eric Berlin & Andrew Kantor, *Who Will Watch the Watchmen?*, *INTERNET WORLD* (Oct. 1996) <<http://www.iw.com/1996/11/surf.html>>.
20. According to an article in the electronic version of *Internet World*, CYBERSitter blocks all sites hosted by cris.com. A CYBERSitter representative suggests that Internet service providers "are responsible for their content," and that the owners of cris.com are to blame because they "will not monitor their [customers'] sites." Berlin & Kantor, *supra* note 19. According to another recent report, CYBERSitter now blocks all sites at a variety of Internet service providers including the WELL, the pioneering California electronic community. See K.K. Campbell, *Who's Watching the 'Watchers'?*, *TORONTO STAR*, Jan. 30, 1997, at J3. Cyber Patrol blocks all pages hosted by crl.com (including a real estate agency's Web pages). A Cyber Patrol representative says that the company is reviewing its policy of blocking entire domains. Berlin & Kantor, *supra* note 19.
21. The RSACi and SafeSurf systems allow content providers to label each page individually. At a recent PICS developers' workshop, the prevailing view was that filtering software should expect to find PICS-compliant labels only in the individual documents, not in the directories or elsewhere in the site. See PICS Developers' Workshop Summary (visited Feb. 7, 1997) <<http://www.w3.org/pub/WWW/>

PICS/picsdev-wkshp1.html>. This makes sense only in the context of software that makes the blocking decision for each page individually.

The more difficult question is whether the problem will persist in connection with third-party rating services. At least one third-party rating service (Specs for Kids) does rate on the document level, and such a service should be more attractive to many users; the question is whether the increased sales will outweigh the added expense of that granularity.

22. The on-line service solved the problem, to its own satisfaction, by advising its customers from that city to pretend they were from "Sconthorpe" instead. See Clive Feather, AOL Censors British Town's Name!, 18 RISKS DIGEST, Issue 7 (Apr. 25, 1996) <<http://catless.ncl.ac.uk/Risks/18.07.html#subj3.1>>. On string-recognition software, see *infra* notes 63 and 77 and accompanying text.
23. See Internet Censorship and Blocking Software, WEB4LIB ARCHIVE (visited Mar. 18, 1997) <<http://www.lib.berkeley.edu/Web4Lib/archive/9703/0120.html>>.
24. See e-mail from Solid Oak Software Technical Support to Bob Stock (Oct. 24, 1996) (on file with author).
25. See Meeks & McCullagh, *supra* note 18; Cyber Patrol Censors Animal Rights Web Sites (visited Feb. 7, 1997) <<http://www.mit.edu/activities/safe/labeling/cp-bans-animal-rights>>.
26. *Id.*
27. *Id.*
28. Queer Resources Directory (visited Feb. 9, 1997) <<http://www.qrd.org>>. The Health/AIDS directory at QRD, for example, contains information from the Centers for Disease Control and Prevention, the AIDS Book Review Journal, and AIDS Treatment News. See Meeks & McCullagh, *supra* note 18.
29. See SurfWatch Censorship Against Lesbigan WWW Pages (visited Feb. 7, 1997) <<http://www.utopia.com/mailings/censorship/SurfWatch.Censorship.Against.Lesbigan.WW>>; e-mail from Chris Kryzan for wide distribution (June 15, 1995) (on file with author).
30. See Meeks & McCullagh, *supra* note 18.
31. *Id.*
32. *Id.* Indeed, Cyber Patrol apparently blocks all of the alt.support groups (including, for example, alt.support.shyness and alt.support.depression), along with such groups as alt.war.vietnam and alt.fan.frank-zappa. E-mail from Declan McCullagh to the fight-censorship mailing list (Oct. 4, 1996) (on file with author); CyberPatrol: The Truth (visited Feb. 7, 1997) <<http://www.canucksoup.net/CYBERWHY.HTM>>.
33. Meeks & McCullagh, *supra* note 18. Among the other WWW sites blocked by Cyber Patrol is that of the Campaign for Real Ale, a British consumer group dedicated to preserving and promoting traditional pubs and independent breweries. Cyber Patrol lists it as an alcohol & tobacco CyberNOT. Charles Arthur, Real Ale is Too Strong for the American Moralists, INDEPENDENT (London), July 22, 1996, at 11.
34. See e-mail from Ari Herzog to the fight-censorship mailing list, Feb. 27, 1997 (on file with author).
35. Meeks & McCullagh, *supra* note 18. It also refuses any site whose URL contains "sinnfein" or "fascism." Berlin & Kantor, *supra* note 19.
36. See The Penal Lexicon: What's New Page (visited Mar. 18, 1997) <<http://www.penlex.org.uk/wnarc51.html>>.
37. See Campbell, *supra* note 20; Pamela Mendels, Publishers Say CYBERSitter Filter is Screening Out Their Criticism (Feb. 9, 1997) <<http://www.nytimes.com/web/docsroot/library/cyber/week/020997cybersitter.html>>.
38. See David Pescovitz, Site-Filtering Controversy Likely to Heat Up, L.A. TIMES, Jan. 6, 1997, at D3.
39. See Censorware Search Engine (visited Mar. 18, 1997) <<http://www.pathfinder.com/netly/spoofcentral/censored>>.
40. Jonathan Wallace, An Auschwitz Alphabet (visited Feb. 7, 1997) <<http://www.spectacle.org/695/ausch.html>>.
41. Jonathan Wallace, Why I Will Not Rate My Site (visited Feb. 7, 1997) <<http://www.spectacle.org/cda/rate.html#report>>.
42. *Id.*
43. Or she could take an approach falling somewhere in between. The polar models I describe in the text, though, provide a useful way of looking at the problem.
44. See Duncan Kennedy, Form and Substance in Private Law Adjudication, 89 HARV. L. REV. 1685, 1685, 1688-89 (1976); Pierre Schlag, Rules and Standards, 33 UCLA L. REV. 379, 379-80 (1985); Kathleen Sullivan, The Supreme Court, 1991 Term—Forward: The Justices of Rules and Standards, 106 HARV. L. REV. 22, 58-59 (1992); JONATHAN WEINBERG, Broadcasting and Speech, 81 CAL. L. REV. 1101, 1167-69 (1993); see also Cass R. Sunstein, Problems with Rules, 83 CAL. L. REV. 953, 956 (1995) (adopting somewhat different terminology, but contrasting "two stylized conceptions of legal judgment":

- “clear, abstract rules laid down in advance of actual applications” and “law-making at the point of application through case-by-case decisions, narrowly tailored to the particulars of individual circumstances”).
45. See Jim Miller et al., *Rating Services and Rating Systems (and their Machine Readable Descriptions)* (last modified Oct. 31, 1996) <<http://www.w3.org/pub/WWW/PICS/services.html>>, at Appendix B. There is a slightly different description of the RSACi categories at *Rating the Web* <<http://www.rsac.org/why.html>>.
 46. See *The Net Labeling Delusion: Protection or Oppression* (visited Jan. 14, 1997) <<http://www.thehub.com.au/~rene/liberty/label3.html>>.
 47. See *SafeSurf Rating System* (visited Feb. 7, 1997) <<http://www.safesurf.com/classify/index.html>>.
 48. See *Solid Oak Software, Inc. VCR Rating System* (visited Feb. 7, 1997) <<http://www.solidoak.com/vcr.htm>>.
 49. *Specs Glossary* (visited Feb. 7, 1997) <http://www.newview.com/cust/ss_sg_lvl3a_cf_fcs.html>.
 50. It is inevitable that people will disagree as to the consequences of an item of speech being pigeonholed in a particular category—whether, for example, youngsters should be exposed to scenes of murder and mayhem. My point about the examples in the text is that individuals will come to different conclusions regarding which pigeonhole a given item of speech should be deemed to occupy in the first place.
 51. Elsewhere in the Specs rating system, one can find definitions that seem standard-like because it is doubtful that they mean what they say. For example, the Specs default settings do not allow persons under eighteen to view Web sites that “[a]ttempt[] to persuade the viewer to join a specific political group.” *Specs Glossary* (visited Feb. 7, 1997) <http://www.newview.com/cust/ss_sg_lvl3a_cf_fcs.html>. If this is not to exclude the Democratic and Republican parties (say), the test must embody some unarticulated assumptions about which political appeals are the pernicious ones—rendering the de facto category standard-like and unconstrained.
 52. See sources cited *supra* note 44.
 53. See Kennedy, *supra* note 44, at 1688–89; Sullivan, *supra* note 44, at 62–63; Sunstein, *supra* note 44, at 972–77.
 54. See Frederick Schauer, *Formalism*, 97 *YALE L.J.* 509, 512 n.8 (1988) [hereinafter Schauer, *Formalism*]:

[Consider] the transformation of the “honor codes” at various venerable universities. These codes were phrased in quite general terms at their inception in the 18th and 19th centuries because these schools contained homogenous student bodies who shared a common conception of the type of conduct definitionally incorporated within the word “honor.” If a person thought that purchasing a term paper from a professional term paper service was consistent with being honorable, then that person simply did not know what “honor” meant. As values have changed and as student bodies have become less homogenous, however, shared definitions of terms such as “honor” have broken down. Some people now do think that buying a term paper can be honorable, and this breakdown in shared meaning has caused general references to “honor” to be displaced in such codes by more detailed rules. There may now be little shared agreement about what the precept “be honorable” means, but there is considerable agreement about what the rule “do not purchase a term paper” requires.
- See also *id.* at 539–40.
55. Steve G. Steinberg, *Seek and Ye Shall Find (Maybe)*, *WIRED*, May 1996, at 108, 112–13.
 56. *Id.* at 113; see also Leslie Walker, *On the Web, a Catalogue of Complexity*, *WASH. POST*, Nov. 20, 1996, at F17; *The Total Librarian*, *ECONOMIST* (visited Feb. 7, 1997) <<http://www.economist.com/review/rev9/rv12/review.html>>.
 57. *RSAC Specifics About the Rating Process, Questionnaire, the PICS Standard and Granularity* (visited Feb. 7, 1997) <<http://www.rsac.org/start.html>>.
 58. Indeed, for just that reason, First Amendment philosophy largely proscribes standards on the level of operative First Amendment doctrine. Speech-regulatory law, the Supreme Court has explained, must be expressed in hard-edged, nondiscretionary terms so as to minimize the possibility of government arbitrariness or bias. Situationally sensitive judgment by government officials, making speech-regulatory decisions turn on “the exercise of judgment and the formation of an opinion,” is forbidden. *Forsyth County v. Nationalist Movement*, 112 S.Ct. 2395, 2401–02 (1992) (quoting *Cantwell v. Connecticut*, 310 U.S. 296, 303 (1940)); see Weinberg, *supra* note 44, at 1169–70; see also Frederick Schauer, *The Second-Best First Amendment*, 31 *W.M. & MARY L. REV.* 1, 14–17 (1989).
 59. See Kennedy, *supra* note 44, at 1689.
 60. Schauer, *Formalism*, *supra* note 44, at 510.

61. See *id.* at 534–37; Sunstein, *supra* note 44, at 992–93.
62. See Kennedy, *supra* note 44, at 1689; Sullivan, *supra* note 44, at 62; Sunstein, *supra* note 44 at 994; Weinberg, *supra* note 44, at 1168–69.
63. See Richard A. Knox, Women Go On Line to Decry Ban on ‘Breast,’ BOSTON GLOBE, Dec. 1, 1995, at A12. This incident was likely the result of string-identification software. String-identification programs are excellent examples of rules-based filtering systems.
64. In fact, RSACi is seriously flawed for reasons having nothing to do with rules and standards. The original RSACi rating system was designed for video games. RSACi carries over the categories and language of the earlier video game rating system even where they are completely inappropriate. Thus, for example, RSACi’s definition of “aggressive violence” on a Web page excludes acts of nature “such as flood, earthquake, tornado, hurricane, etc., unless the act is CAUSED by Sentient Beings or Non-sentient Objects in the game or where the game caused the act.” See RSACi Ratings Dissected (visited Mar. 18, 1997) <<http://www.antipope.demon.co.uk/charlie/nonfiction/rant/rsaci.html>>. One consequence of RSACi’s approach is that the Internet rating system nowhere acknowledges a distinction between images and text.
65. In the wake of recent political speculation about bomb-making recipes on the Internet, five major rating services agreed to work together to “ensure that parents can block Internet sites containing weapons and bomb making information and recipes.” Press Release, SafeSurf Enables Parents to Block Internet Bomb Sites (Aug. 1, 1996) <<http://www.safesurf.com/press/press16.htm>>.
66. The Specs default settings, for example, would deny to persons under eighteen any “[m]aterial defaming one or more social groups or members of such groups.” See Specs Glossary (visited Feb. 9, 1997) <http://www.newview.com/cust/ss_sg_lvl3a_cf_fcs.html>; Specs: Age Defaults (visited Feb. 9, 1997) <http://www.newview.com/cust/ss_stsp_lvl2_fcs.html>.
67. Specs classes all nudity as either “in an artistic or educational context,” or “with the principal purpose of exciting the viewer.” Specs Glossary, *supra* note 66.
68. See *supra* text accompanying note 19.
69. To the extent that a user does not agree, the service will block sites he would want admitted, or let through sites he would want shut out, or both.
70. See Using Content Advisor (visited Feb. 9, 1997) <<http://microsoft.com/ie/most/howto/ratings.htm>>.
71. As a ratings system multiplies parental choice, it becomes more complex and, perhaps, harder to use. As a practical matter, rating system designers will have to balance fine differentiation of the ratings system against ease of use. See J.M. Balkin, Media Filters, the V-Chip, and the Foundations of Broadcast Regulation, 45 DUKE L.J. 1131, 1172 (1996). Cf. Solid Oak Software’s Voluntary Web Site Rating System (visited Feb. 9, 1997) <<http://www.solidoak.com/vcr.htm>> (arguing self-rating system should be “extremely simple,” in contrast to “PICS compliant ratings systems where there are several dozen possible ratings”).
72. The Federal Communications Commission relies on an emphatically standard-like guide to determine whether speech broadcast on television and radio is “indecent.” The resulting uncertainties have subjected the agency to critical attack. See generally JONATHAN WEINBERG, Vagueness and Indecency, 3 VILL. SPORTS & ENT. L.J. 221 (1996). The FCC, though, is a single entity; its choices will display far more consistency than those of millions of disconnected content providers each evaluating their own sites.
73. All of these areas of speech trigger Cyber Patrol blocking (except for “tattooing and body piercing,” which constitute a CyberNOT only to the extent they result in “gross depictions”). See Cyber Patrol Cyber NOT List Criteria (visited Feb. 9, 1997) <http://www.microsys.com/cyber/cp_list.htm>. Tattooing and body piercing are specifically blocked by Specs (in a category, called “subjects of maturity,” that lumps them in with “illegal drugs, weapon making . . . [and] some diseases.” Specs Glossary, *supra* note 66. Cf. Balkin, *supra* note 71, at 1166–68 (discussing competing images of “what characteristics count in making programming unsuitable for children”).
74. RSACi Rating the Web (visited Feb. 9, 1997) <<http://www.rsac.org/why.html>>.
75. If unrated sites are either all innocuous or all verboten, we have an exceptional case; blocking software can then treat all according to a single rule.
76. Rating services are only beginning to confront the issue of updating ratings for particular sites as their contents change. RSACi provides one-year expiration dates for its labels. SafeSurf is providing no expiration dates, instead simply enjoining content providers to update their ratings if there is a material change in the content of their speech. See PICS Developers’ Workshop Summary, *supra* note 21.
77. See Douglas Bailey, Couplegate, BOSTON GLOBE, Feb. 22, 1996, at 54. The page displays pictures of Bill and Hillary Clinton and Al and Tipper Gore.

78. The PICS Standard⁷ (visited Feb. 7, 1997) <<http://www.microsoft.com/intdev/sdk/docs/ratings/ratng002.htm>>.
79. See Whit Andrews, Site-Rating System Slow to Catch On, WEB WEEK (July 8, 1996) <<http://www.webweek.com/96July8/comm/rating.html>> (quoting Compuserve representative Jeff Shafer); Specs FAQs: Quick Quest: General Info (visited Feb. 9, 1997) <http://www.newview.com/cust/ss_qq_lvl3a_reg.html> (recommending users select option of blocking all unrated sites “to ensure a safe Internet environment”); e-mail from Andy Oram, O’Reilly and Associates, to telecomreg mailing list (May 21, 1996) (on file with author).
80. Few Web sites today carry self-rating labels. See Andrews, *supra* note 80 (only two of the “more than 50” sites listed in the Entertainment Magazine: Sex category at Yahoo! carry self-ratings); see also Hiawatha Bray, Rated P for Preemptive: System to Shield Kids From Adult Web Material Also Seeks to Keep Censors Off Net, BOSTON GLOBE, Jul. 25, 1996, at E4 (“only a tiny percentage” of Web sites have RSACi ratings).
81. See Lewis, *supra* note 4; RSAC Rating the Web (visited Feb. 9, 1997) <<http://www.rsac.org/why.html>>. Cf. Balkin, *supra* note 71, at 1164 (discussing the V-chip).
82. See Andrews, *supra* note 79. There are two separate problems here. The less important one is the technical issue of affixing a rating to each individual page. As noted *supra* note 21, the prevailing view at a recent PICS developers’ workshop was that filtering software should expect to find PICS-compliant labels in each document; content providers cannot get away with supplying “blanket” ratings at the directory level or higher. On the other hand, it should be easy to develop software that will automatically insert labels into Web pages, so long as all of the pages on a site carry the same rating.
- The more important problem arises when a content provider must audit each page of a large archive to determine what rating that page should receive. Robert Croneberger, director of the Carnegie Library in Pittsburgh, testified at the *ACLU v. Reno* trial that he would have to hire 180 additional staff in order to search the library’s online materials (in particular, its online card catalogue) so as to be able to tag individual, potentially indecent items. Trial Transcript for Mar. 22, 1996 at 101–02, *ACLU v. Reno*, 929 F.Supp. 824 (E.D. Pa. 1996) (No. 96-963) <http://www.eff.org/pub/Legal/Cases/EFF_ACLU_v_DoJ/960322_croneberger.testimony>. It would be a huge task for MSNBC, say, to rate its news stories individually for descriptions or pictures of violent behavior—and perhaps for that reason, as of this writing, MSNBC does not provide RSACi ratings. See Declan McCullagh, RSACi-Hacky, NETLY NEWS (Mar. 18, 1997) <<http://cgi.pathfinder.com/ALRDzgcACqLjhGnr/netly/1,1039,740,00.html>>.
83. See e-mail from Stephen Balkam, RSACi, to Irene Graham (Feb. 14, 1997) (on file with author).
84. See 3 Trial Transcript at 192:3–4, *ACLU v. Reno*, 929 F.Supp. 984 (E.D. Pa. 1996) (No. 96-963) (testimony of Barry Steinhardt), and *Reno v. ACLU*, 117 S. Ct. 2329 (1997).
85. 487 U.S. 781 (1988).
86. *Id.* at 795.
87. *Id.* at 798, 800. The Court noted that “[p]urely commercial speech is more susceptible to compelled disclosure requirements.” *Id.* at 796 n.9 (citing *Zauderer v. Office of Disciplinary Counsel*, 471 U.S. 626 (1985)); see also *Hurley v. Irish-American Gay, Lesbian and Bisexual Group*, 115 S.Ct. 2338, 2347 (1995). A self-rating requirement, though, would affect noncommercial as well as commercial speech. The Justices have noted that a state can compel doctors to make certain disclosures as part of the practice of medicine, see *Planned Parenthood v. Casey*, 505 U.S. 833, 884 (1992) (opinion of O’Connor, Kennedy, & Souter, JJ.), but that isn’t this case either.
88. 115 S.Ct. 1511 (1995).
89. *Id.* at 1518.
90. *Id.* at 1519–20.
91. See also *Hurley*, 115 S.Ct. at 2347–48:

[O]ne important manifestation of the principle of free speech is that one who chooses to speak may also decide what not to say. . . . [Except in the context of commercial advertising,] this general rule, that the speaker has the right to tailor the speech, applies not only to expressions of value, opinion, or endorsement, but equally to statements of fact the speaker would rather avoid. . . . Nor is the rule’s benefit restricted to the press, being enjoyed by business corporations generally and by ordinary people engaged in unsophisticated expression as well as by professional publishers. Its point is simply the point of all speech protection, which is to shield just those choices of content that in someone’s eyes are misguided, or even hurtful.

Id. (citations and internal quotation marks omitted).

92. *Meese v. Keene*, 481 U.S. 465 (1987), is not to the contrary. The Court in that case approved statutory provisions pursuant to which the Justice Department characterized speech distributed by foreign agents as “political propaganda.” The disseminator of the speech, however, was not required to characterize it in that manner. The case was about the extent to which the government can pejoratively characterize a person’s speech, not about the extent to which government can force a person to characterize her own speech, pejoratively or otherwise.
93. See *Hurley*, 115 S.Ct. at 2347–48; *Pacific Gas & Elec. Co. v. Public Utils. Comm’n*, 475 U.S. 1, 15 (1986) (plurality opinion) (holding government may not “require [speakers] to associate with speech with which [they] may disagree,” nor force them to “alter their speech to conform with an agenda they do not set”); *Wooley v. Maynard*, 430 U.S. 705, 714 (1977) (holding government may not compel citizen to “be an instrument for fostering public adherence to an ideological point of view he finds unacceptable”); *West Va. State Bd. of Educ. v. Barnette*, 319 U.S. 624, 642 (1943) (holding government may not prescribe an orthodoxy and “force citizens to confess [it] by word”).
94. *Baggett v. Bullitt*, 377 U.S. 360, 372 (1964) (quoting *Speiser v. Randall*, 357 U.S. 513, 526 (1958)).
95. *Interstate Circuit, Inc. v. City of Dallas*, 390 U.S. 676, 688 (1968); see also *Motion Picture Ass’n of Am., Inc. v. Specter*, 315 F.Supp. 824 (E.D. Pa. 1970).
96. The Court followed a similar reasoning process in *McIntyre*. The state in that case supported its ban on anonymous election materials by pointing to its interest in policing fraudulent statements and libel in election campaigns. The Court noted, though, that other provisions of state election law barred the making or dissemination of false statements. The value of the challenged provision was merely incremental. That incremental benefit could not justify the damage the provision did to free speech. *McIntyre v. Ohio Elections Comm’n*, 115 S.Ct. 1511, 1520–22 (1995).
97. *ACLU v. Reno*, 929 F.Supp. 824, 883 (E.D. Pa.) (Dalzell, J.), prob. juris. noted, 117 S.Ct. 554 (1996).
98. *Id.* at 883.
99. *Id.* at 877.
100. *Id.* at 881–82 (quoting *Leathers v. Medlock*, 499 U.S. 439, 448–49 (1991)).
101. This concern is most salient in connection with blocking programs, such as Microsoft’s Content Advisor, that block *any* access to restricted sites through the computer on which the program is installed unless the program is disabled. Other programs, including Cyber Patrol, offer a more advanced feature known as “multiple user profiles.” Each family member can have his or her own password, and the program can be configured at the start to grant the different password holders different levels of access. These programs make it easy for a parent to access the sites he seeks to exclude his child from. See PICS Developers’ Workshop Summary, supra note 21 (noting formation of working group to specify formats for describing PICS user profiles). Parents may be wary of this feature, though, since the exclusion is only as secure as the parent’s (frequently used) password.
102. See, e.g., BESS.NET: The Service (visited Feb. 9, 1997) <http://demo.bess.net/about_bess/the_service.html>. SafeSurf is now providing technology—the SafeSurf Internet Filtering Solution—that allows any ISP to offer parents this easy option. See Rose Aguilar, Site Filters Criticized, THE NET (Oct. 18, 1996) <<http://www.news.com/News/Item/0,4,4609,00.html>>. Even some households without children, if blocking software comes bundled with their Web browser, may choose to enable that software because they believe that otherwise they may be confronted with smut.
103. When a user running blocking software seeks to conduct a search using an Internet search engine such as Alta Vista, the software will transmit the user’s filtering rules to the search engine. The search engine will tailor its search so as not to return any sites excluded by the filter. Participants at the recent PICS Developers’ Workshop agreed that this was the preferable approach, in part because it would be undesirable for users to get search results like “here’s the first 10 responses, but 9 of them were censored by your browser.” PICS Developers’ Workshop Summary; see also PICS Frequently Asked Questions (visited Feb. 9, 1997) <<http://www.w3.org/pub/WWW/PICS>>.
104. See, e.g., Gary Chapman, Universal Service Must First Serve Community, L.A. TIMES, June 3, 1996, at D1. See generally ROBERT H. ANDERSON ET AL., UNIVERSAL ACCESS TO E-MAIL: FEASIBILITY AND SOCIETAL IMPLICATIONS (1995) (discussing pros and cons of locating devices for e-mail access in home, at work, in schools, and in libraries, post offices, community centers, and kiosks).
105. See QUESTIONS AND ANSWERS: Access to Electronic Information, Services, and Networks: An Interpretation of the Library Bill of Rights (visited Feb. 9, 1997) <<http://ala1.ala.org:70/0/alagophx/alagophxfreedom/electacc.qa>>; Access to Electronic Information, Services, and Networks: An Interpretation of the Library Bill of Rights (visited Feb. 9, 1997) <<http://ala1.ala.org:70/0/alagophx/alagophxfreedom/electacc.fin>>.
106. See, e.g., Alan Boyle, Resolving the Information Battle (visited Mar. 17, 1997) <<http://www.msncb>

- com.news/59459.asp> (explaining that Bakersfield, Cal. public libraries have installed blocking software on all terminals); Pamela Mendels, *Censoring Web Sites Poses Dilemma for Librarians* (Mar. 9, 1997) <<http://nytimes.com/library/cyber/week/030997libraries.html>> (Austin Tex. and Connetquot, N.Y.; same); Rebecca Vesely, *Library Blocks Porn, and May Block Rights*, WIRED NEWS (visited Jan. 7, 1997) <<http://www.wired.com/news/story/1289.html>> (Orange County, Fla.; same). I do not want to overplay this point. Many libraries have decided not to install blocking software. See, e.g., Ramon McLeod & Carolyn Zinko, *Online Smut in the Reading Room*, S.F. CHRON., Mar. 1, 1997, at A1. Other libraries have installed the software only on terminals intended for use by children. See, e.g., Geeta Anand, *Library Ok's Limits on 'Net Access*, BOSTON GLOBE, Mar. 22, 1997, at A1. I am grateful to Linda Mielke, President of the Public Library Association and Director of the Carroll County (Maryland) Public Library, Kathleen Reif, Director of the Wicomico County (Maryland) Free Library, and Naomi Weinberg, President, Board of Trustees, Peninsula Public Library Lawrence, New York for educating me on these issues.
107. *Pornography and Gambling are Inappropriate in a Library* (visited Feb. 9, 1997) <<http://www.librarysafe.com/library.html>> (typeface in original). The vendor is the Library Safe Internet System. Librarians have shown great courage in their decisions to carry controversial books and artworks. They have repeatedly demonstrated their willingness to carry items of sexually explicit material that they consider valuable. Recent cases litigated by the Freedom to Read Foundation include *Lowe v. Kiesling*, 882 P.2d 91 (Or. Ct. App. 1994), rev. dismissed, 889 P.2d 916 (Or. 1995), challenging a proposed Oregon ballot measure that, among other things, would have forbidden public libraries from collecting any materials on homosexuality written for children, and *Ong v. Salt Lake City Public Library*, in which plaintiffs sought to bar a public library from exhibiting art including nudity. See Freedom to Read Foundation Annual Report For 1994-1995, 20 Freedom to Read Foundation News, Nos. 3-4 (1995). (visited Apr. 17, 1997) <<http://www.sirs.com/partner/read/v20n3.htm>>; Reports to Council, 19 Freedom to Read Foundation News, Nos. 3-4 (1994). (visited Apr. 17, 1997) <<http://www.sirs.com/partner/read/v19n2.htm>>. By providing an uncensored Internet feed, though, a library makes available material much more difficult to defend in a political context.
108. See Rosilind Retkwa, *Corporate Censors, INTERNET WORLD*, Sept. 1996, at 60; see also, e.g., *Microsystems Announces Immediate Availability of Cyber Patrol Proxy for Microsoft's Proxy Server* (July 31, 1996) <<http://www.microsys.com/prfiles/proxy796.htm>>.
109. Retkwa, *supra* note 108, at 61.
110. The university was the University of Arkansas at Monticello. See e-mail from Carl Kadie to fight-censorship mailing list (Oct. 22, 1996); e-mail from Tyrone Adams to amend1-L mailing list (Oct. 22, 1996); e-mail from Stephen Smith to Jonathan Weinberg (Oct. 22, 1996) (all on file with author).
111. It is possible that Disney or a similar entity will get a large market share with a kid-centered interface limiting users to a specific list of kid-friendly sites, and that that interface will be so aggressively child-oriented that adults won't use it (and can't be suckered into using it). Even so, employers and similar entities using the Internet will still have an interest in installing a grown-up interface with blocking capabilities and, presumably, the market will respond to that.
112. Consider America Online. AOL markets itself as a family-friendly service. It allows parents to confine their children to a "Kids Only" area, or to disallow their access to chat rooms and Usenet news. AOL monitors the use of forbidden words in various contexts. It censors messages posted in the advertisers' area called "Downtown AOL," removing advertisements that its manager thinks do not have "the look and feel that best fits [AOL]'s environment." At the same time, though, it allows its members to create chat rooms with names like "m needs bj now," "bond and gaged f4f," and "M4Fenema."
113. R3 Safety-Net: Rating Reporting Responsibility For Child Pornography and Illegal Material on the Internet (last modified Sept. 23, 1996) <<http://dtiinfo1.dti.gov.uk/safetynet/r3.htm>>. Under the initial proposal, users were to rate with RSACi. See *id.* The proponents apparently have backed away from that position. The proposal also recommends that Internet service providers take steps to support rating and filtering of Usenet newsgroups. For an explanation of the mechanics of the Usenet proposal, see Turnpike Newsgroups (last modified Sept. 24, 1996) <<http://www.turnpike.com/ratings>>.
114. See *Restricting Access to Illegal and Harmful Content on the Internet: Communication to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions* (Oct. 16, 1996) <<http://www2.echo.lu/legal/en/internet/content/communic.html>>. A recent EU working group document recommends research into new, non-RSAC rating systems, so as to "take account of Europe's cultural and linguistic diversity" and "guarantee respect of [users'] convictions." Report of Working Party on Illegal and Harmful Material on the Internet (visited Mar. 7, 1997) <<http://www2.echo.lu/legal/en/internet/ientent/wpen.html>>. Other countries have adopted more drastic approaches. See, e.g.,

Kathy Chen, China Bars Access To as many as 100 Internet Web Sites, WALL ST. J., Sept. 5, 1996, at B5; James Kyng, Singapore Cracks Down on Internet, FIN. TIMES (London), July 12, 1996, at 6.

115. See RSAC Press Release, Compuserve to Rate Internet Content by July 1 (May 9, 1996) <<http://www.rsac.org/press/960509-1.html>>.

Page Intentionally Left Blank

Page Intentionally Left Blank