Chapter One -- INTRODUCTION

Filtering the Future?

For most of human history the word "filter" has had an entirely unambiguous meaning. Ask the average person on the street to name a filter, and they will likely point to one of the following mundane objects of everyday life. For those unfortunate enough to live in cities with poor tasting tap water (Boston and Philadelphia certainly come to mind), the dechlorinating, makes my tea tastes better "water filter" will likely be mentioned. Among the Starbucks, and XandO set -- or for that matter, any caffeine junkie -- the "coffee filter" will be mentioned as an irreplaceable invention for the mourning rush to work, or the late night cram session. Finally, for those unable to kick the nicotine habit, "Marlboro filtered cigarettes" will come to mind, as a cough comes to their mouth.

All of these everyday, common knowledge filters deal with physical, atom-based particles. The water filter traps chlorine and lead molecules, the coffee filter keeps ground rhines out of the final product, and the cigarette filter removes some of the harmful carcinogenic compounds about to be inhaled. The physical aspect of these filtering processes is reflected in the Oxford English Dictionary's definition of filter, "To pass (a liquid) through a filter, or some porous medium, for the purpose of removing *solid particles or impurities* (emphasis added)."

The use and definition of filters shows that they are employed to get rid of something unwanted. A byproduct of the last epoch of human history, the Industrial Revolution (focused on manufacturing atoms), has been heavy levels of air and water pollution. As such, we have developed advanced air and water filters to keep our environment more or less livable.

In this century, largely following World War II, the Industrial Revolution was replaced by the much hyped "Information Revolution" (Bell, 1973; Toffler, 1980). Negroponte (1995) notes that the central difference between the industrial and information revolutions is the shift from "atoms to bits." By this, Negroponte means, that the economic and cultural forces which shape our society are no longer governed by the manufacture of physical, atom-based goods (planes and cars), but rather the production and dissemination of vast amounts of information (news and entertainment). Due to incredible advances in computing, all of this information can be digitized, thus acquiring the unique characteristics of bits, namely convergence, compression, increased speed of dissemination, and intelligence in the channel (Neuman, 1991), or what Negroponte calls "bits about bits (1995: 18)". All of these factors have coalesced on the network of networks known as the Internet, and its graphical, multimedia counterpart, the World Wide Web. While the net and the web are relentlessly hyped as the answer to all of the world's problems by digital soothe sayers like Negroponte, Howard Rheingold (1993), and Bill Gates (1996, 1999), just like the pollution of the Industrial Revolution, the information society has its own unwanted byproducts.

Perhaps the most problematic of unwanted consequences in the Information Revolution, is an overabundance of information. Due to the characteristics of bits described above, literally anyone can become an information producer, and make his/her content, regardless of quality, accuracy, relevance, or appropriateness (all value judgments) available to a world-wide audience on the Internet. While such low barriers to entry may be seen as very democratic, they have produced a situation where the information consumer must sort through more than 5 million web sites (Netcraft, June 1999), 90,000 topical mailing lists (as indexed by Liszt.com, June 1999), 60,000 Usenet

newsgroups (as indexed by DejaNews, June 1999), and 51,000 Internet Relay Chat channels (Liszt.com, June 1999), to locate desired material. As anyone who has used an Internet search engine can testify, searching for topical information often produces an overwhelming number of links, many to entirely irrelevant sites. This trend towards more and more information, but less and less meaning and understanding (Baudrillard, 1983) has been called "information glut" by Postman (1992), "data smog" by Shenk (1997), and "garbage information" by Schiller (1976). "All told, the thesis is that enormous amounts of greatly increased information in the modern age are of dubious value. There undoubtedly is more information about today, but its informational quality is suspect in the extreme" (Webster, 1995: 125).

What is the solution to all of this unwanted, low quality information? Clearly the answer is filters. However, it is extremely important to note the difference between the physical filters needed for the Industrial Revolution, and the information filters we need today. Atom-based filters deal with physical world *objectively* defined atoms, molecules, particles, etc. If you do not want chlorine in you tap water, you study the properties of chlorine molecules, and develop a filter system which will prevent these molecules from passing through into the final product. This is in stark contrast to information filters which must sort through ideas which are inevitably *subjectively* defined artifacts of human experience and knowledge. In other words, describing a bit as relevant, truthful, accurate, appropriate, etc., means making value judgments about the digitized content it represents (with the exception of certain objective characteristics such as time, date, or geographic location). These largely subjective decisions are coded (as we shall see later, who does the coding makes a big difference) into the "headers" of electronic documents, so that machines/individuals on the receiving end of the information can choose what to do with it. Deciding what to do with

these bits, means using an information filter itself based on subjective rules about what content to let in, and what content to filter out. Problems arise in such a system when the senders description of his/her bits (an email with "URGENT, MUST READ NOW" as its subject line), does not square with the interpretation of the information filter on the receiving end (which finds the message to be anything but urgent). This information overabundance and description problem is certainly nothing new. Librarians and literary scholars have struggled for thousands of years about how to classify books. To aid in this process, librarians have developed card catalogs, and literary scholars developed the anthology. While these systems have worked well for some time, the advent of the Internet, and the absolute tidal wave of information now available, points to the incredible challenge for, and importance of information filters in the next millennium.

Indeed in an age of 500 cable channels, millions of web pages, thousands of printed publications, cell phones, and beepers, information filters will become an absolute necessity for the average citizen navigating his/her path through the wilds of the virtual and real worlds. Our growing dependence on this "filtered future" also means giving up a great deal of power to filters, to define what we will see, hear, and be in the digital future. This new reality points to a fundamental flaw in the logic of the new media mantra that information is power:

> In the Information Age, we were told, information would be power. It is turning out to be quite the opposite. In the Information Age, it seems, power does not rest with those who have access to information. It rests with those who filter it. (Balkin, 1996)

In seeding our information selection power to filters, battles over content definition will inevitably arise. Simply put, people will disagree that this bit means this, and that bit means that. Scaled to the millions of Internet users now on-line, the problem of subjectively defined information filters, means

disagreements about content will be pervasive. As such, information filters will become a public, political, legal, and technological problem of massive proportions.

The Internet Content Conundrum

This thesis will focus on one particular area where the nexus of information filters, public outrage, political policy making, jurisprudence, and technological solutions have converged into a contentious sociopolitical issue. This issue is the filtering of "objectionable" Internet content (mostly pornography) to protect children, an issue I will call the "Internet Content Conundrum." The conundrum is due to the fact that the Internet facilitates easy access to both large amounts of safe and useful information, as well as access to a much smaller amount of "dangerous" material. As Karen Jo Gounaud of Family Friendly Libraries notes, the Internet contains both "gigantic bottomless pits and wonderful playgrounds (cited in Hudson, 1998)."

Since the Internet came to the for of public attention around 1994, Americans have been obsessed with the scourge of easily accessed on-line pornography, violence, and hate speech. Newspaper and magazine articles have fed this fear with articles about pornographic web sites, hate groups, and on-line sexual predators (Turow, 1999). This perceived abundance of harmful Internet content, has led Congress to pass two laws, the Communications Decency Act (CDA), and the Child On-line Protection Act (COPA) aimed at defining, and criminalizing Internet content deemed harmful to minors. In conjunction with these legislative solutions, the software industry has developed its own technological solutions, namely content blocking filter software, and a content rating system known as the Platform for Internet Content Selection (PICS).

Over the past three years, courts have deemed both the CDA and COPA to be unconstitutional restraints of First Amendment protected speech. In overturning these legislative solutions, the courts pointed to the supposedly "less restrictive" alternative of software blocking and Internet content rating systems as the best way to keep the Internet a safe place for children. As a result, filter technologies have been championed as *the* solution for keeping inappropriate content at the edge of cyberspace, and away from children. These self regulatory, market driven technologies are seen as First Amendment friendly, and far preferable to direct government regulation. No less than the White House has endorsed this idea, noting that "Advanced blocking and filtering technology is doing a far more effective job of shielding children from inappropriate material than could any law (1997)." In keeping with this statement, the White House has aggressively pushed the development and implementation of blocking programs and PICS. This push has only intensified in the wake of the Littleton, Colorado shooting tragedy.

In the days following the massacre, the news media uncovered the fact that the shooters frequently used the Internet to access Neo-Nazi and bomb making web sites. In the rush to blame something, anything, for the inexplicable killing spree, both the public and politicians cast a collective pointing finger at the Internet. A CNN/USA Today poll conducted shortly after the killings found that 64 percent of respondents said the net contributed to the tragedy (cited in McCullagh, 1999). Similarly, Congress and the White House have drafted a flurry of new laws and proposals to curb access to "dangerous" Internet content. Several legislators are aggressively pushing the Childrens' Internet Protection Act (McCain, 1999) which will require all schools and libraries receiving federal funds for Internet access to install blocking software (discussed further in Chapter Six). Another proposed law would require any Internet Service

Provider (ISP) with more than 50,000 subscribers to distribute content blocking software (Bloomberg, 1999). Similarly, the executive branch has fully endorsed filters as the way to go. Speaking about Littleton at a recent conference, FCC chairman William Kennard noted "We need filtering software for families to use on their PC's. Just as you wouldn't send a child off alone in a big city, you wouldn't -- and shouldn't -- let them explore the vast landscape of the Internet without a chaperone (1999)." In a similar speech, announcing a joint industry - White House "Parents Protection Web Page", Vice President Gore noted that filters were the best tool parents could use to protect children from the "free-fire zones and red light districts of cyberspace (1999)."

While the public, Congress, and the White House may accept that content filters are the way to go, a growing number of scholars and civil libertarians have begun to ask whether these technologies are indeed the best solution to the Internet Content Conundrum. They point to the fact that content filtering technology tends to block a great deal more speech than even government regulation would deem off limits. Further, blocking decisions can be based upon nearly any criteria, and are not open to public or institutional review. In addition to blocking access to a great deal of constitutionally protected speech, filtering technologies can be invisibly implemented. Unlike "encoded" content laws of the physical world which punish ex post facto, cyberspace filtering laws are directly "coded" into Internet browsing software. As a result, end users potentially have no idea that their Internet access is being subjected to the rules and blocking decisions of a particular person, organization, or government. "One obeys these laws as code not because one should; one obeys these laws as code because one can do nothing else (Lessig, 1996)." The end result of "coded" cyberspace content filters is the potential for a perfect technology of censorship, hidden from view and accountable to no one. In short, software filters and

content ratings championed as First Amendment friendly, could prove to be anything but.

Which of these sides is correct? Are content blocking filters and rating systems a reasonable and First Amendment friendly solution to "dangerous" Internet content? Or are they an ineffective technological solution to an age old social problem? The goal of this thesis, is to answer these very questions. Stated formally:

> ***Research Question 1:*** *What social, economic, and legal costs are associated with adopting Internet content blocking filters and Internet rating systems as the preferred solution to the Internet Content Conundrum?*

A related question deals with the larger significance of content blocking and rating schemes as technological, "coded" solutions to larger social problems:

> ***Research Question 2:*** *What can Internet content blocking filters and Internet rating systems (social protocols) tell us about the power of extra-governmental Internet standards bodies? How can we ensure that these groups reflect the values of all Internet users?*

Significance and Justification

The development and implementation of content blocking filters and PICS is part of a broader trend on the Internet. As mentioned above, "social protocols" like content filters and PICS are "coded" into the very architecture of cyberspace. Unlike physical world laws, these protocols act upon Internet users invisibly, and perfectly enforce their rules. Thus, if a filter says access to a certain web site is prohibited, an end user will simply not be allowed to access the site, nor will he/she know why it is deemed off limits.

This situation arises, because social protocols are developed outside of traditional government, public policy, and constitutional oversight. Groups like the World Wide Web Consortium (the standards body for the web) and software

filter developers have limitless power to define the "reality" of cyberspace via the protocols that they develop. Yet unlike a law being debated in Congress, no CSPAN camera focuses on the software engineers of the W3C or the content filtering companies. Therefore, the standards developed by Internet infrastructure groups become the de facto laws of the Internet. Invisible and perfectly enforceable, these laws by protocol create a new type of sovereign entity. While these cyberspace laws may be perfectly enforceable, the may also be far from perfectly just.

The aim of this thesis is to understand how well these technological solutions work, and how they represent a new form of "cyber sovereign" law. Realizing that content blocking filters and PICS have the power to change the very nature of Internet access, it is essential that we understand the workings of these technologies, and the forces that are driving their adoption.

As mentioned at the outset of this chapter, filters will become more and more important in an information future that will have more and more information. As such, in identifying the elements of one type of filter already in use (the content blocking/rating system filter) it is hoped that this thesis will provide a framework for examining future filters like P3P, a privacy protocol also developed by the W3C. This roadmap will help ensure that future social protocols are developed and implemented within a larger framework of public debate and governmental oversight.

What's To Come

Chapter Two will take a long view of the problem of objectionable content and society. Perhaps since the invention of the spoken word, communities (political, religious, moral, etc.) have been concerned about the potentially harmful effects of content, especially upon the young. Such fears have often led

to massive state sponsored censorship. This chapter will briefly explore the history of censorship, and its antithesis, classical liberalism emerging out of the Enlightenment. From this discussion, we will gain an understanding of the root causes and mechanisms of censorship, as well as the powerful arguments against it which have resulted in the First Amendment freedoms we enjoy today. Using this knowledge as a base, we will explore "The Great Cyberporn Panic" that followed the emergence of the Internet and web as a major new medium of communication. This scare led directly to Congress's attempt to legislate Internet content controls, which in turn led to the current fixation with content blocking filters, and content rating systems.

Chapter Three will take an in-depth look at Internet content blocking filters, how they are marketed, their many features, how they work, and the plethora of problems associated with their use. This chapter will also describe the features and history of four popular Internet content blocking filters tested in this thesis.

In Chapter Four we will put the four filter programs mentioned in Chapter Three to the test. Combining a content analysis of randomly and purposively selected web sites, with the binary block, no block mechanism of the filters being tested, we will see just how effective these products really are.

Chapter Five will focus on the development, features, and implementation of the PICS Internet content rating system. We will look at the benefits and problems associated with this technology, and explore PICS as an example of a new form of world sovereign, the social protocol. The international implications of PICS will be used as a case study of the power of emerging social protocols.

Chapter Six will discuss the school and library filtering debate, a concrete example of where content blocking software, meaning, academic freedom, and community concerns have coalesced into a contentious policy issue.

Finally, Chapter Seven will conclude this thesis with a series of policy recommendations about how, when, and if to use Internet content blocking software and Internet content rating systems. These recommendations will be framed within a larger discussion of social protocols, and their importance in the filtered future of the Information Revolution.

Chapter Two -- FROM SOCRATES TO THE CDA

A Brief History of Censorship

The urge to censor that which is new, unpopular, and uncomfortable is one of the oldest and most basic of human urges. The desire to censor largely grows out of a perceived need to protect a community (especially children) from the supposedly harmful ideas espoused by those who dissent from conventional community norms. This sets up the classical debate between the rights of the

community to preserve its norms and the rights of the individual to self determination. As Garry (1993) frames the problem:

> There has historically existed a fear that individual liberties and community control are incompatible and even destructive of each other. Libertarians who seek expansion of individual freedom see censorship as the effort of an intolerant community to impose conformity and to diminish the range of freedom available to its individual members. Those who believe that too much individual freedom undermines community see censorship as a means of empowering community to deal with the destructive excesses of individual freedom. (107)

Perhaps the oldest and most famous example of censorship best illustrates this dilemma. Ancient Greece is often held up as a progressive and democratic society which valued free thought, and even political dissent. However, in 399 B.C. Socrates severely challenged these ideals. For questioning the existence of the gods and denouncing Athenian democracy, Socrates was charged with corrupting youth and offending the gods. Sticking to his ideals, Socrates chose hemlock and death, rather than bend to the mores of Athenian society (Stone, 1987; Riley, 1998).

Running contrary to Socrates truth seeking individuality, his philosophical counterpart, Plato, argued for the near total protection of the community from dissenting opinions. In *The Republic*, Plato argues the need for extensive censorship to protect the education of children, the morals of citizens, and to generally achieve a good and just society (Wolfson, 1997: 23). Indeed, Plato notes, "Then the first thing will be to establish a censorship of the writers of fiction, and . . . reject the bad (1977)." Plato goes on to argue for the censorship of playwrights, poets, and music. Warning of the influence of storytellers Plato comments:

> Children cannot distinguish between what is allegory and what isn't, and opinions formed at that age are usually difficult to

> eradicate or change; it is therefore of the utmost importance that the first stories they hear shall aim at producing the right moral effect. (1977)

Based on these arguments Plato even called for the censorship of Homer's *Odyssey*.

Yet another Greek philosopher, Aristotle, also laid the foundation for the suppression of ideas based on a concern for community. To Aristotle, the state was the ultimate embodiment of man's desire for the good life. Thus the state is the highest representation of community, and is therefore justified in curbing speech which detracts from the good life. As Smolla (1992) notes:

> When this Aristotelian impulse is the dominant mode of thinking in a society, there will be an inexorable tendency to think it reasonable for the state to exercise control over speech. Speech that promotes the good life, speech that affirms values of community, justice, and the rule of law, will be fostered and nurtured by the state, speech destructive of those ends will be condemned. (71)

While it is clear that Greek philosophers laid the foundation for, and even practiced censorship, it was the Romans who brought us the term, and bureaucratized its enforcement. In 443 B.C. the Romans established the office of the censor (from the Latin "censere") whose duty was to count citizens for political, military, and taxation purposes (Hoyt, 1970: 9). Additionally, Censors, appointed by the state to five year terms, established standards for citizenship. These included moral standards such as religious worship and general public conduct. Censors had the power to strip Romans of citizenship if they disapproved of public or private behavior. Cato the Elder was the most famous of Roman Censors (Jansen, 1988: 41). Under subsequent Roman rulers, the office of the censor was used to persecute Jews, Catholics, and the unpopular works of various Greek and Roman authors. Under the reign of Nero, censorship of

Christian proselytizers reached a bloody new peak. As recounted by Tacitus (cited in Jansen, 1988):

> They died in torments, and their torments were embittered by insult and derision. Some were nailed on crosses; others sewn up in the skins of wild beasts and exposed to the fury of dogs; others again, smeared over with combustible materials, were used as torches to illuminate the darkness of night. (43)

Following the rise of Christianity the Church became the main force behind the censorship of material. Contrary to popular belief, the early Church primarily censored literature deemed dangerous to religious or political authority, not immoral, filthy, or depraved writing. For example, the first act of Church censorship, the banning of *Acti Pauli* (about the life of St. Paul) in 150 A.D., was justified on doctrinal grounds (Jansen, 1988: 47). When the Church of Rome laid down its rules for the censorship of books in the fourth century A.D. it made no mention of public morals, but rather forbade Christians from circulating or possessing writings of the old pagans -- the unbelievers (Hoyt, 1970: 12).

Under this censorship regime, the Church came to control the vast majority of books in pre-printing press Europe. Lists of forbidden books would occasionally be distributed, again, largely aimed at religious heresies such as Gnosticism. The Church also maintained its control over the written word through its monopoly of medieval education. For the few who sought higher education in religion, philosophy, and science, the only books available were hand copied manuscripts (often transcribed by monks) already deemed acceptable by the Church (Hoyt, 1970: 12).

All of this radically changed when Johann Gutenberg invented the printing press and published his first bible around 1450. Within 20 years, some 255 European towns had printing presses churning out thousands of pamphlets and books. The Church's monopoly over the written word, and thus its

monopoly over the dissemination of ideas was destroyed. The printing press and Luther disintermediated the Catholic priest and laid the seeds for mass literacy, and mass political and religious dissent (Grendler, 1984; Eisenstein, 1980).

Responding this new technology of freedom, the Church developed one of the most comprehensive and long lasting censorship regimes in human history. In 1524, under Church guidance, Charles V of Belgium published a list of censored books. Forty years later in 1564, the Church formalized the listing of banned books by publishing the *Index librorum prohibitum (Index of Prohibited Books)*. The *Index* consisted of several parts: (1. a listing of outright banned authors (Luther, Zwingli, Calvin, etc.), (2. a listing of banned titles, (3. rules for expurgation of books with some "error" which were not all bad (for example the substituting of court nobility for clerics and priests in bawdy books such as Chuacer's *Cantebury Tales*), and (4. sweeping rules for the dissemination of printed works (Grendler, 1984: 30). Generally, the *Index* continued to punished doctrinal error, but it also expanded to include immoral and obscene works (from the Latin root, *obscensus*, meaning "filthy" or "repulsive"). As rule number eight of the original *Index* notes:

> Books which professedly deal with, narrate or teach things lascivious or obscene are absolutely prohibited, since not only the matter of faith but also that of morals, which are usually easily corrupted through the reading of such books, must be taken into consideration, and those who possess them are to be severely punished by the bishops. Ancient books written by heathens may by reason of their elegance and quality of style be permitted, **but may by no means be read to children**. (emphasis added, Modern History Sourcebook, 1999)

The *Index*, updated every fifty years and to eventually include more than 4,000 banned works (publication of the *Index* only ceased 33 years ago in 1966), was disseminated to Catholic countries like France who implemented licensing and

distribution controls over all printed material. Violators were jailed, tortured, and often put to death. Indeed, just before the French Revolution, the Bastille imprisoned more than 800 authors, printers, and book dealers (Cate, 1998). Despite these controls, and the prospect of death for violating them, a vast underground press flourished in Europe. For example, books banned by Catholic France were either published in France under the name of a foreign press, or were published in a foreign country like the Netherlands and smuggled in. In this way Europeans were exposed to the new political ideas of Locke, Milton, Rousseau, and other Enlightenment writers. Works that laid the theoretical and political foundations for the French Revolution, and other similar uprisings throughout Europe (Alter, 1984: 17).

Following the French Revolution, censorship entered a new phase in both its enforcement, and its favored topic. First, the late 18th century revolutions sweeping Europe and the new world severely curbed the political authority of the church. Thus the power of censorship was passed to secular parliaments and rulers. In doing so, the major target of censorship also changed (Hoyt, 1970: 14).

Concurrent with the revolutions mentioned above, was the rise of mass literacy and a flourishing press. Newspapers helped aggregate what was previously only separate local communities and opinions into a nationally "imagined community" with a collective voice expressed via public opinion (Tarde, 1898: Anderson, 1991: Carey 1995). No longer could rulers ignore the "will of the people." As such, they became obsessed with the potentially dangerous moral and ideological ideas spread though public media. Goldstein (1989) summarizes this trend in his book about 19th century political censorship:

> Censorship of the press and arts above all reflects the fact that, in an age of urban industrialization, widespread literacy and rapid transportation and communications, what average citizens think

> matters to political leaders. Much of the political struggle therefore consists of a battle for control of the minds of the population. (xiv)

Evidence of this shift away from religious censorship and towards state sponsored moral control of the public first emerged in 18th century England. In 1727, Richard Curl was convicted by an English court for publishing *Venus in the Cloister, or the Nun in Her Smock*. The lord chief justice, declared that "obscene libel" previously handled only by religious courts, was indeed a problem for secular authorities if it "reflects on religion, virtue, or morality" or "if it tends to disturb the civil order of society (Tedford, 1993: 12)." Thus obscenity became a crime under English common law. In 1857, Parliament officially recognized the crime of obscenity by passing the Obscene Publications Act which laid down the rules for the search, seizure, and destruction of obscene materials (Tedford, 1993: 13).

Helping English obscenity prosecutions along was one of the most famous censors of all time. Thomas Bowdler was an English doctor who sought to purify literature which might corrupt the morals of his fellow citizens. Bowdler took his cue from his father, who would orally "bowdlerize" morally questionable passages while reading from famous works of literature. Bowdler fondly remembers listening to his father read Shakespeare, "without knowing that those matchless tragedies containing expressions improper to be pronounced and without having any reason to suspect that any parts of the plays had been omitted (cited in Hoyt, 1970: 20)."

Following his desire to purify English morals, in 1802 Bowdler helped found the Society for the Suppression of Vice, whose goal was "To prevent the profanation of the Lord's Day, prosecute blasphemous publications, bring the trade in obscene books to a halt, close disorderly houses and suppress fortune

tellers (in St. John-Stevas, 1962: 104)." From 1802 to 1807, the Society successfully prosecuted between thirty and forty obscenity cases (Tedford, 1993: 13).

Bowdler's high point of "delicate" censorship was the 1807 publication of *The Family Shakespeare*, "bowdlerized" to exclude profanity, indecency, and blasphemy. A second edition published in 1817 went on to become a best seller (Hoyt, 1970: 21).

During this period of English obscenity prosecutions, one case in particular had a great impact upon the development of U.S. ideas about censorship and the constitutional protection of books. In 1868 Lord Cockburn ruled in the obscenity case of Regina v. Hicklin, and enunciated the "Hicklin rule" for determining obscenity: "Whether the tendency of the matter charged as obscenity is to deprave and corrupt those whose minds are open to such immoral influences, and into whose hands a publication of this sort may fall (cited in Bosmajian, 1976: 3)." This definition, latter adopted by U.S. courts, clearly appeals to protection of the community from "dangerous" and "impure" expression.

Like Bowdler in England, America's most infamous 19th century censor, Anthony Comstock, crusaded to save the morals of his fellow citizens. However, unlike Bowdler, Comstock didn't bother editing works he disagreed with, instead he lobbied for their outright censor.

Comstock's crusade against indecent literature began in 1867 when he moved to New York City where he worked in a dry-goods store. Appalled by the filthy literature his fellow employees were reading and passing around, he tracked down the supplier of the material in question, and had him arrested. Encouraged by his early success, Comstock set about on a censorious tizzy that would last nearly fifty years.

In 1872, at age 27, Comstock founded the New York Society for the Suppression of Vice, whose state given mandate was to suppress "obscene literature" including "vile weekly newspapers" and "licentious books (Hoyt, 1970: 22)." The Society received the support of several prominent New York industrialists including soap magnate Samuel Colgate, and financier J.P. Morgan (who ironically had one of the most extensive private collections of erotica in the nation).

One year after founding the New York Society, Comstock lobbied Congress to pass federal legislation outlawing the sending of "obscene or crime-inciting matter" through the mails. Prohibited material under what became known as the Comstock Law included, "every obscene, lewd, lascivious, or filthy book, pamphlet, picture, paper, letter, writing, print, or other publication of an indecent character" not to mention any material regarding contraception or abortion (Hoyt, 1970: 23). The Comstock Law, and the Vice Suppression Society served as models for similar laws and organizations in other U.S. cities like the New England Watch and Ward Society of Boston, and vice suppression societies in Philadelphia, Cincinnati, Chicago, and San Francisco. Many of these organizations continued their moral and legal crusades against obscenity well into the 20th Century.

Following passage of his federal anti-obscenity law, Comstock was appointed a special agent of the Post Office, a position which carried police powers. In this position, where he worked until his death in 1915, Comstock lived up to his crusading image by, according to his account, "convicting persons enough to fill a passenger train of 61 coaches, 60 coaches containing 60 passengers each, and the sixty-first almost full . . . and destroying over 160 tons of obscene literature (cited in Hoyt, 1970: 26)." During his reign, the U.S. Supreme Court in 1896 ruled that the Comstock Law was constitutional. In

doing so, the court accepted the "Hicklin Rule" for defining obscenity, and thus laid the legal foundation for the future banning of great literature like James Joyce's *Ulysses*, D. H. Lawrence's *Lady Chatterly's Lover*, and Hemingway's *For Whom the Bell Tolls* (Tedford, 1993: 40).

Debates about the banning of obscene material continued well into the 20th century. New groups like the National Organization for Decent Literature (founded in 1955) and The Citizens for Decent Literature (1956) gained widespread report. New types of media, including paper back books, comics, and films, also came under the scrutiny of these organizations. However, in the wake of two landmark obscenity cases Roth v. United States (1957) and Miller v. California (1973) which made the legal prosecution of obscenity much more difficult, morality crusaders had to turn to new censorship tactics. These new tactics mostly consisted of community pressure against distributors of "objectionable" material, and boycotts of offending book stores and movie theaters. Such community driven efforts often ended in promises of industry self regulation via conduct codes and content rating systems such as the Motion Picture Association of America's G, PG, PG-13, R, NC-17 system. Indeed today's debate over violence on television and pornography on the Internet have resulted in similar calls for industry regulation via the labeling and filtering of content (rating systems will be discussed further in Chapter Five).

The Mechanisms of Censorship

From the above discussion of the history of censorship it is possible for us to isolate out a number of elements, or mechanisms, by which censorship is bureaucratized and implemented:

Categorization -- this is the first and most difficult mechanism of censorship. Its aim is to identify broad or narrow categories of content which are deemed off limits. As seen above, these content categories can change over time, for example from an early concern with heresy to a more recent concern with obscenity and immorality. Additional categorizations can be added (violence), or old ones dropped (heresy) as social norms change over time.

Listing -- once authors and titles have been categorized as off limits, they must be listed and distributed to censors who can then enforce regulations against the enumerated offending works. Of great importance to the long term success of a censorship regime is the continued update of these lists to include the latest works created by pesky new authors. As a result of continual updating, lists can become extremely long (4,000 banned works in the *Index*) thus making them unwieldy and inflexible in their implementation.

Word Filtering -- for those works categorized as "not all bad," rules must be laid down for the expurgating, or "bowdlerizing" of offending passages. Word filtering rules may require simple omission, or more extensive character or plot modification.

Access and Distribution Control -- all points of access to content categorized as off limits must be controlled so as not to allow the censored material to be distributed to the public in its unadulterated form. For the Church and many European nations this meant licensing the use of the printing press, and for Comstock it meant controlling the mails.

These four mechanisms were all present in the first edition of the *Index*, likely the first comprehensive system of censorship. However, as we shall see in Chapter Three, these same ancient mechanisms serve as the base for today's "high-tech" software filters.

Arguing Against Censorship

> *I may disapprove of what you say, but I will defend to the death your right to say it. -- Voltaire*

While the call *for* censorship largely derives from a perceived need to protect community, the crusade *against* censorship derives from the inalienable rights of individuals and a profound doubt in the ability of a community, and its embodied power via the state, to infallibly determine the truth or the ultimate social good.

A foundation for these anti-censorship ideas was first laid by Socrates in his defense before Athenian censors. In one of history's greatest ironies, Socrates' stirring arguments for free thought and free speech, are recounted by censorship's good friend Plato, in his work the *Apology*. Socrates makes two main arguments in favor of free speech. The first deals with self determination and the right of individuals to follow their own ideas, not those prescribed by the state:

> If you propose to acquit me on condition that I abandon my research for truth, I will say: I thank you, O Athenians, but I will obey God, who I believe, set me this task, rather than you, and so long as I have breath and strength I will never cease from my occupation with philosophy . . . I do know that it is a bad thing to desert one's own post and I prefer what may be good to what I know is bad. (quoted in Jansen, 1988: 37)

Socrates' second argument is that the truth can only be obtained and tested through rigorous public debate:

> In me you have a stimulating critic, persistently urging you with persuasions and reproaches, persistently testing your opinions and trying to show you that you are really ignorant of what you suppose you know. Daily discussion of the matters about which you hear me conversing is the highest good for man. Life that is not tested by such discussion is not worth living. (quoted in Jansen, 1988: 38)

Socrates' foundational arguments for free speech would go unheeded for more than a thousand years, until they were wholeheartedly adopted by 17th and 18th century Enlightenment writers. The Enlightenment was based on ideas about individual natural rights (Locke), the use of reason, and the attainment of knowledge (Riley, 1998; Encyclopedia Britanica, 1999). Indeed the very word Enlightenment "means the free use of reason, the exercise of reason unfettered by external constraints (in Jansen, 1988: 4)." Within such an ideology, censorship (particularly by the state) was obviously anathema, as it prevented individuals from exercising and receiving reason.

Expressing these views, Englishman John Milton produced *Areopagitica* (1644), one of the cornerstones of later Enlightenment thinking and still one of the most important works of western, liberal, anti-censorship philosophy. In it, Milton argued against censorship, particularly licensing and prior restraint (the most common forms of censorship in 17th century England), because they hindered the discovery of truth. He argued that people tend to be comfortable with old ideas and fear new ones, thus leading to the censor of the new: "if it come to prohibiting, there is not aught more likely to be prohibited than truth itself, whose first appearance, to our eyes bleared and dimmed with prejudice and custom is more unsightly and unplausible than many errors (cited in Jansen, 1988: 72)." However, rather than censor new ideas which may be true, and will likely become known in spite of censorship, Milton proposes that people be allowed to hear both sides so that they can develop their own opinions: "Where

there is much desire to learn from there of necessity will be much arguing, much writing, many opinions; for opinion in good men is but knowledge in the making (cited in Riley, 1998: 7)." This system of competing ideas and opinions is widely referred to as "the marketplace theory of free speech", a theory that deeply effected the development of U.S. constitutional law.

Indeed the ideas of Milton and other Enlightenment theorists heavily influenced Thomas Jefferson while writing the First Amendment (1783), the cornerstone of free speech and liberty in the U.S. (Tedford, 1993). It's famous words state that "Congress shall make no law . . . abridging the freedom of speech, or of the press."

Among the firmament of anti-censorship works, perhaps none shines brighter than John Stuart Mill's *On Liberty* (1859), which many have called the finest defense of free speech ever written (Tedford, 1993: 374). Mill essentially takes Milton's marketplace theory and expands upon it. He makes three primary argument for the right to free speech. First, much like Milton, he argues that the censored idea may in fact be true, and that popular opinion is wrong: "if any opinion is compelled to silence, that opinion may, for aught we certainly know, be true (Mill in Berger, 1980: 39)." He further argues that the presumption made by censors is one of infallibility, that they know for certain what the truth is:

> The opinion which it is attempted to suppress by authority may possibly be true. Those who desire to suppress it, of course deny its truth; but they are not infallible. They have no authority to decide the question for all mankind, and exclude every other person from the means of judging. To refuse a hearing to an opinion because they are sure it is false, is to assume their certainty is the same thing as absolute certainty. All silencing of discussion is an assumption of infallibility. (in Berger, 1980: 44)

The logic of this argument lies behind U.S. jurisprudence's skepticism of view point based regulations of speech, an argument we will see again in our discussion of the CDA below and in Chapter Six.

Mill's second point is that all opinions likely have some element of truth in them, and therefore censorship should be avoided so that the truth can be refined through discussion and debate:

> Though the silenced opinion be an error, it may, and very commonly does, contain a portion of truth; and since the general or prevailing opinion on any subject is rarely or never the whole truth, it is only by the collision of adverse opinions that the remainder of the truth has any chance of being supplied. (in Berger, 1980: 39)

Finally, Mill argues that even if the truth can be ascertained with certainty, false opinions should still be allowed because they help to continually test and reaffirm the truth:

> However unwillingly a person who has a strong opinion may admit the possibility that his opinion may be false, he ought to be moved by the consideration that, however true it may be, if it is not fully, frequently, and fearlessly discussed, it will be held as a dead dogma, not a living truth. (in Tedford, 1993: 374)

While Milton and Mill and their market place theories are considered by many to be the bookends of free speech theory, other more recent scholars have proposed different free speech justifications.

In *Political Freedom* (1965), Alexander Meiklejohn argues that free speech is a necessary prerequisite for a functioning democracy, and that all forms of political speech should be free from censorship. He points to town hall meetings as an example of where citizens, exercising their right to free speech, become informed about issues that effect their self governance. Without unfettered political discussion, and minus an informed citizenry, democracy would fail to function. Greenwalt (1989) thusly summarizes Meiklejohn's argument from democracy:

> A liberal democracy rests ultimately on the choices of its citizens. Free speech can contribute to the possibility that they, and their representatives, can grasp truths that are significant for political life; it can enhance identification and accommodation of interests; and it can support wholesome attitudes about the relations of officials and citizens. (146)

Marketplace and democracy justifications for free speech are often described as utilitarian (Berger, 1980). In other words, free speech is a means to an end; finding the truth in marketplace theory, and maintaining a functioning democratic state in democracy theory. However within such utilitarian philosophies of speech, any expression which does not serve an ultimate purpose can be suppressed. Responding to this problem, C. Edwin Baker (1989) argues that free speech is a fundamental human liberty, justified in and of itself as an irreducible element of individual autonomy and self determination. Baker's model "holds that free speech protects not a marketplace, but rather an arena of individual liberty from certain types of governmental restrictions. Speech or other self-expressive conduct is protected not as a means to achieve a collective good but because of its value to the individual (1980: 5)." What values might individuals derive from free speech, and why should the government be prohibited from censoring such speech? Greenwalt (1989) summarizes:

> For the speaker, communication is a crucial way to relate to others; it is also an indispensable outlet for emotional feelings and a vital aspect of the development of one's personality and ideas. The willingness of others to listen to what one has to say generates self-respect. Limits on what people can say curtail all these benefits. If the government declares out of bounds social opinions that a person firmly holds or wishes to explore, he is likely to suffer frustration and affront to his sense of dignity. (145)

The eloquent justifications for free speech outlined above (marketplace, democracy, and individual autonomy) serve as the foundations

of U.S. First Amendment law. As such, they place a heavy burden on any governmental attempt to regulate speech. A burden which the CDA, described below, failed to meet. Yet beyond their value to the courts, these ideas will also inform our discussion of commercial content blocking software and rating systems as socially problematic solutions to the Internet Content Conundrum.

Don't Forget Market Censorship

The history of censorship described above largely revolved around the state's power to limit expression. However, due to the First Amendment, and its 20th century application, the state, both in the U.S. and in other western style democracies plays a very limited role in the censorship of content. Nevertheless, just because the First Amendment has greatly diminished the state's censorsorial power, does not mean that other powerful institutions have not implemented their own, less visible censorship regimes.

Indeed many scholars now point to the commercial marketplace (particularly media conglomerates) as the most powerful arbiter of speech (Jansen, 1988). Since the mass audience receives nearly all of its news and entertainment from the commercial media, the media, in essence have the power to define social reality. However, because the media are "for profit" institutions, they are incented to provide a certain sanitized view of reality which promotes endless consumption. In order to promote this view of reality, the media must censor out other competing messages, even if they are of high social importance. As Dallas Smythe (1981) succinctly summarizes:

> The act of modern censorship is essentially a decision as to what is to be mass produced in the cultural area. So long as current cultural production is in the hands of privately owned giant corporations, they must also make decisions as to what is to be mass produced in the cultural area and what will not be produced. It is accurate therefore to refer to corporate decision making in the

> cultural area as being censorship as it is to refer to government decision making by that pejorative term. (235)

The reality of market control of speech is likely to only intensify in the information age. While more and more channels of information become available, thus opening up a wider range of viewpoints, individuals will need to delegate information selection to commercially produced filters. An example of this is Negroponte's vision of the "Daily Me" an electronically compiled newspaper, tailored via information filters specifically to the end users wishes (1995: 153). Another prominent example of this trend is targeted and "one to one" marketing, which produces highly specialized advertising messages. While both of these technologies may be useful, they may also serve to integrate individuals into "consumption communities," thus lessening traditional social interactions, and "breaking up America" (Turow, 1997).

While filters like the Daily Me will seek out information that consumers want, Internet content blocking software will limit access to content that end users do not want to see. However, in seeding decisions about "objectionable" content to commercial software developers, information consumers loose their own autonomy to define what they view as off limits. As such, blocking decisions will represent market justified views of a sanitized world, where controversial topic matter is anathema to e-commerce and an increasingly commercialized Internet. In spite of this problem, the U.S. Supreme Court, and the White House, have "outsourced" the Internet Content Conundrum to the market, and its own unique brand of censorship.

Pornography Drives Technology -- Which Drives Censorship

Since the invention of the printing press, pornography has been a driving force behind the development of new media, which as a result has lead to efforts

to censor all new media. Two of the most popular books produced by Gutenberg's new invention were the pornographic tales of Pietro Aretino's *Postures* (1524) and Francois Rabelais' *Gargantua and Pantagruel* (1530-40). *Postures* consisted of a series of engravings depicting various sexual positions, each accompanied by a ribald sonnet. Rabelais' work was more satirical, including passages such as a playful governess introducing Gargantua to sex; Gargantua's horse pissing away an army, and a woman scaring away the devil by exposing her vagina (Kendrick, 1987; Findland, 1993).

Pornography next played an essential role in the development of the paperback book. In the late 19th century, printers began publishing books made of cheap "pulp" paper, thus the term "pulp fiction." One of the most popular genres of the paperback was pornography and erotica, a tradition which continues to this day, with cheap, Fabio covered novels sold in the local supermarket (Johnson, 1996).

In the 19th century, pornography also accompanied the development of photography. Civil War soldiers sought more than just letters from home. Through the mails they also received large quantities of pornographic photographs. The traffic in such images was so great, that Congress passed its first law prohibiting the sending of obscenity through the mails. However, by the time the bill passed in 1865 the war was over, and the soldiers returned home with pornography in their pockets (Johnson, 1996).

Several more modern media of communication can also attribute pornography as a factor in their success. Pay per-view cable television's first successful use was broadcasting X-rated films. The standards debate between VHS and Betamax was partially settled by early home video stores renting VHS recorded pornography. Pornography also helped prove the market for "900" phone services, and CD-ROMs (Johnson, 1996).

Pornography's integral role in the development of most modern media is likely attributable to two factors. First, put simply, humans enjoy sex. Secondly, entrepreneurs recognize this fact, and will use any medium open to them to distribute pornographic content to an eager consuming public. How eager is the public for such material? In 1998, Americans rented 686 million adult video tapes, representing a $5 billion dollar rental and sales market. Legal pornography is estimated to be a $56 billion global industry. Based on the brief history outlined above, and the vast size of its market, it should be no surprise that pornography has migrated on-line to the tune of $1 billion in annual Internet pornography sales (Morais, 1999).

What Can Social Science Research Tell Us About Censorship?

Social science understanding of censorship derives mostly from survey research attempting to measure support for free speech, and research into the third-person effect.

First, a number of studies have been conducted asking people how tolerant they are of unpopular viewpoints and their willingness to censor such content. For example, Wilson (1975) found that 62 percent of respondents did not believe that people should be allowed to make speeches against God, and 53 percent did not believe people should be allowed to publish books attacking our system of government. Generally speaking, many of these studies have found that despite the U.S.'s strong free speech tradition, citizens are surprisingly willing to censor certain types of unpopular speech. This willingness to censor has been found to be positively associated with age, authoritarianism, conservatism, feminism, and religiosity and negatively associated with income, education, and media use (Rojas et. al., 1996).

The second area of research into censorship is the so called third-person effect, which finds that "individuals exposed to a mass media message will expect the communication to have a greater effect on others than on themselves (Davison, 1983)." In simple English, Joe Smoe thinks that pornography is morally corrupting others but not himself. Several studies have attempted to tie the third-person effect to attitudes about censorship, and support for technological solutions to "dangerous" content like the V-chip. Rojas et. al. (1996) found that the third-person effect was associated with an increased desire to censor, however Nessinger (1997) found no connection between the effect and support for using the V-chip.

The third-person effect represents an intriguing potential explanation for why so many parents claim to be concerned about Internet pornography, but fail to use blocking software (discussed further in Chapter Three).

Fear, Cyberporn, and the March to Censor the Internet

Based on the history of censorship and pornography outlined above, as well as our historical fear of all forms of media content, it should be of no surprise that our newest medium, the Internet, has been similarly attacked as an "evil influence," poised to "contaminate the health and character of the nation's children (Starker, 1989: 5)." The moral danger inherent in the Internet has been defined as the availability of "cyberporn."

On July 3, 1995, *Time* magazine carried the following cover article: "On a Screen Near You: Cyberporn." The article, by *Time* senior writer Phillip Elmer-Dewitt, cited the soon to be published research of a Carnegie Mellon undergraduate student named Marty Rimm (Wallace and Mangan, 1996). Rimm's study, eventually published in the *Georgetown Law Review*, claimed to be an exhaustive look at the amount and types of pornography available on the

Internet. Rimm found that 83.5 percent of Usenet images were pornographic, and that over 70 percent of the sexual images on the newsgroups surveyed "originate from adult-oriented computer bulletin-board systems (BBS) whose operators are trying to lure customers to their private collections of X-rated material (Elmer-Dewitt, 1995)." Further, he found that many of the images analyzed were exceptionally kinky and violent.

Following the publication of the *Time* article and the actual Rimm study, many Internet pundits came forward to discredit Rimm's analysis. Taking the forefront in pointing out Rimm's weak methodology were Vanerdbilt University professors Donna Hoffman and Tom Novak. They argued that Rimm's selection of a few sex related newsgroups was simply not representative of the world of Usenet, or of the larger Internet. "Also, no information is provided on the degree to which these 32 newsgroups comprise the complete universe of Usenet imagery (Hoffman and Novak, 1995)." In addition to his poor sample of newsgroups (of which there are thousands mostly relating to news, recreation, and politics), he also used no clear definition of pornography to classify images as pornographic.

The onslaught of articles, emails, and Usenet posts discrediting the Rimm study led *Time* to "admit that grievous errors had slipped past their editorial staff, as their normally thorough research succumbed to a combination of deadline pressure and exclusivity agreements that barred them from showing the unpublished study to possible critics (Wilkins, 1997)." For all intents and purposes the Rimm study had been discredited, shown to be a methodologically weak investigation conducted by an attention seeking undergraduate student.

Despite this discreditation, the *Time* article and the Rimm study had stirred a wild moral panic about access to pornography on the Internet. In the months that followed, several mainstream newspapers and magazines including

the *New York Times, USA Today*, and *Newsweek* ran stories regarding the "threat" of Internet content. Electronic Freedom Foundation (EFF) lawyer Mike Goodwin referred to this situation as "The Great Cyberporn Panic of 1995 (1998: 206)."

Not ones to miss out on a moral crusade, several U.S. Senators and Congressmen weighed in with legislation to protect children from the scourge of easily accessed Internet pornography. As Margaret Seif notes, "the political football got blown up to gigantic proportions (1997)."

Senator Charles Grassley (Republican from Iowa) proposed the Protection of Children from Pornography Act of 1995. In support of his bill, Grassley introduced the entire *Time* article into the Congressional Record, and referred to Rimm's undergraduate research as "a remarkable study conducted by researchers at Carnegie Mellon University (Wilkins, 1997)." Grassley further noted that "There is a flood of vile pornography, and we must act to stem this growing tide (June 26, 1995)." Grassley's bill did not pass, but it led to several Internet censorship bills, culminating in the Communications Decency Act (CDA) sponsored by former Senator James Exon. The bill was attached to the Telecommunications Reform Act of 1996, which was passed by Congress and signed into law by President Bill Clinton in February, 1996.

Protecting Children On-line with the CDA

The CDA has two provisions aimed specifically at protecting minors from adult content. The first provision prohibits the knowing transmission of "any comment, request, suggestion, proposal, image or other communication which is obscene or indecent" to recipients younger than 18 years of age (47 U.S.C. 223a). The second provision prohibits the use of "an interactive computer service" to knowingly send or display "patently offensive" material that is available to a person under 18 years of age (47 U.S.C. 223d).

According to supporters of the CDA, these provisions would act like physical world zoning laws (a form of filter), ensuring that children could not access the "adult" section of the Internet. For example, Cathleen A. Cleaver of the Family Research Council equated the CDA to "blinder racks" which must be purchased by adult bookstores and newsstands to shield children from explicit magazine covers (Cleaver, 1996). Similarly, Lawrence Lessig notes that "what the CDA was trying to do was to rezone part of cyberspace: 'this part is not for kids' (quoted in Marshall, January 1998)."

When the CDA came under attack by free speech groups as being vague and overbroad, the Justice department used the cyberzoning claim to argue for the law's constitutionality:

> At bottom, plaintiffs are demanding that unlike physical space, cyberspace be free of any form of "cyberzoning" of indecent speech -- even if that means unlimited availability of pornography and indecency to minors in the home. This position flies in the face of a body of precedent in which the Supreme Court has upheld reasonable time, place, and manner limitations on indecency in "public" spaces. (Department of Justice, 1996)

Despite this argument, on June 26, 1997 the Supreme Court ruled in the case of Reno v. ACLU, that the CDA was an unconstitutional restriction on First Amendment freedoms. Why did the government's zoning argument fail to persuade the court? Let's take a look at the development of traditional, physical world zoning laws, and what constitutional test they must pass to regulate adult content.

Zoning Adult Content in Physical Space

State's zoning power, defined as the "regulation of land according to its nature and uses," has a long history in the United States (Tucker, 1997). Zoning developed as an outgrowth of common law nuisance principles, which sought to

maintain the physical and moral qualities of a particular place. In Euclid v. Ambler Realty Co. (1926), the Supreme Court recognized this interest by upholding a local zoning law which sought to separate industrial and residential areas. So long as a zoning ordinance was shown to relate to the "public health, safety, morals, or general welfare" of a town or city, the ordinance would be considered a constitutional time, place, and manner restriction (Turchi, 1983). Essentially, *Euclid* held that a town or city could proscribe the location of a shopping center, residential neighborhood, or factory district without impinging on a property owner's constitutional rights. However, *Euclid* did not speak to the validity of zoning laws whose primary purpose was the regulation of constitutionally protected speech. Instead, a series of cases have come to define the power to zone adult establishments.

A necessary prerequisite to zoning adult content, is the previously mentioned idea that such material is harmful to minors. The Supreme Court has recognized this concern, and agreed that it is within a state's power to protect minors from potentially harmful adult content. This idea was codified in the case of Ginsberg v. New York (1968).

In *Ginsberg*, the Court considered the constitutionality of a New York statute that banned the sale of material deemed "harmful to minors", where:

> "Harmful to minors" means that quality of any description or representation, in whatever form, of nudity, sexual conduct, sexual excitement, or sado-masochistic abuse, when it: (i) predominantly appeals to the prurient . . . interest of minors, and (ii) is patently offensive to prevailing standards in the adult community as a whole with respect to what is suitable material for minors, and (iii) is utterly without redeeming social importance for minors.

The Court upheld the statute, arguing that a state's interest in "the well being of its children" justified putting limitations on adults access to constitutionally protected speech (Coulter, 1987). "Because the burden on speech was relatively

slight, and because no cheaper discrimination seemed possible, the Court found this burden on adult speech constitutionally permissible (Lessig, 1998: 14)."

In 1972, presumably acting within the power of both the *Euclid* and *Ginsberg* precedents, the town of Jacksonville, Florida enacted an ordinance prohibiting the display of motion pictures depicting "the human male or female bare buttocks, human female bare breasts, or human bare pubic areas . . . , if such motion picture . . . is visible from any public street or public place." The city argued that like in *Euclid*, the ordinance was a reasonable time, place, and manner restriction, aimed at protecting "its citizens against unwilling exposure to materials that may be offensive." However, in Erznoznik v. City of Jacksonville (1975), the Supreme Court disagreed, and ruled the ordinance unconstitutional. The Court noted that:

> A state or municipality may protect individual privacy by enacting reasonable time, place, and manner regulations applicable to all speech irrespective of content. But when the government, acting as censor, undertakes selectively to shield the public from some kinds of speech on the ground that they are more offensive than others, the First Amendment strictly limits its power.

This helped establish the precedent that content-based regulation of speech could not be justified as a time, place, and manner restriction.

One year after the *Erznoznik* decision, the Court had its first encounter with an adult-use zoning ordinance. In Young v. American Mini Theatres, Inc. (1976), the Court considered the constitutionality of a Detroit "Anti-Skid Row Ordinance" which prohibited adult theaters from locating within five hundred feet of a residential area or within one thousand feet of two other such theaters or other "regulated uses," such as adult bookstores, taverns, hotels, and pawnshops. The ordinance defined an adult theater as one which presents "material characterized by an emphasis on 'specified sexual activities' or 'specified anatomical areas'." The city justified this regulation based on a study which

showed that the clustering of adult establishments in Detroit "tends to attract an undesirable quantity and quality of transients, adversely affects property values, causes an increase in crime, especially prostitution, and encourages residents and businesses to move elsewhere."

Two adult theater owners challenged the law which was overturned by a lower federal court which argued that the ordinance was a content-based regulation of speech and thus unconstitutional. However, the Supreme Court disagreed, and overturned the lower court's ruling. Writing for the majority, Justice Stevens reiterated the constitutional requirement of content neutral time, place, and manner restrictions: "above all else, the First Amendment means that government has no power to restrict expression because of its message, its ideas, its subject matter, or its content." In light of this, Stevens argued that the Detroit ordinance *was* content neutral because it sought to regulate the "secondary effects" of all adult theaters (increased crime, reduced property values, etc.), not the content of the films displayed. Further, the ordinance did not cause a "significant overall curtailment" of adult movies, nor did it place an outright ban on adult theaters.

In contrast to the Detroit ordinance, where adult theaters were still permitted although zoned, a 1975 Mt. Ephraim, New Jersey ordinance banned *all* forms of adult entertainment. This was challenged by the owner of an adult bookstore who had installed a coin-operated device that allowed customers to watch a nude dancer behind a glass panel. In Schad v. Borough of Mount Ephraim (1981), the Court struck down the ordinance as an unconstitutional prior restraint on speech. The Court refused to find the ordinance a valid time, place, and manner restriction under *Young*, because the *Young* ordinance "did not affect the number of adult movie theaters in the city; it merely dispersed them." Further, Mt. Ephraim had shown no evidence that it had a substantial interest in

banning all forms of live entertainment, or that such a ban was a reasonable measure to address the borough's zoning concerns. "The Borough has not established that its interests could not be met by restrictions that are less intrusive on protected forms of expression." Finally, the Court rejected the borough's argument that live adult entertainment was available in neighboring communities, and therefore the ordinance did not restrict peoples access to such speech.

> It would be a substantial step beyond *American Mini Theatres* to conclude that a town or county may legislatively prevent its citizens from engaging in or having access to forms of protected expression that are incompatible with its majority's conception of the "decent life" solely because these activities are sufficiently available in other locales.

Combined, the *Young* and *Schad* decisions put forth a constitutional framework for finding adult-use zoning acceptable. So long as an ordinance was aimed at the "secondary effects" of adult establishments and did not ban all such places, it would be considered a reasonable time, place, and manner restriction.

These ideas crystallized in the case of City of Renton v. Playtime Theatres, Inc. (1986) which today serves as the constitutional precedent by which adult-use zoning laws are tested. In 1981, after having reviewed the experiences of other cities, the City of Renton, Washington enacted a zoning ordinance prohibiting any adult movie theater from locating within 1,000 feet of any residential zone, dwelling, church, park, or school (Berger, 1996). Essentially the ordinance was identical to the one contested in *Young*. As such, Chief Justice Rhenquist stated that "the appropriate inquiry is whether the Renton ordinance is designed to serve a substantial governmental interest and allows for reasonable alternative avenues of communication." The Court found that Renton did have a substantial interest in regulating the potentially harmful "secondary effects" of adult establishments. The city established this interest by citing "secondary effect"

studies conducted in other cities which found adult establishments often brought urban decay. Further, because the regulation was not aimed at the content of the films displayed, but their secondary effects, the ordinance could be deemed content neutral. Finally, the Court found that Renton's ordinance left some 520 acres available for adult theaters, thus ensuring "alternative avenues of communication." While respondents argued that the land left was not commercially viable, the Court reasoned that adult theater owners "must fend for themselves in the real estate market." Justice Rhenquist concluded the court's opinion in the following manner:

> In sum, we find that the Renton ordinance represents a valid governmental response to the "admittedly serious problems" caused by adult theaters. Renton has not used the power to zone as a pretext for suppressing expression, but rather has sought to make some areas available for adult theaters and their patrons, while at the same time preserving the quality of life in the community at large by preventing those theaters from locating in other areas. This, after all, is the essence of zoning. Here, as in *American Mini Theaters*, the city has enacted a zoning ordinance that meets these goals while also satisfying the dictates of the First Amendment.

From *Young* to *Schad* and culminating in *Renton* the power to zone adult-use establishments has been established. In order for an adult-use ordinance to be deemed a constitutional time, place, and manner restriction the regulation must be: (1) unrelated to the suppression of speech, i.e. content neutral, (2) narrowly tailored to serve a substantial governmental interest, i.e. controlling the "secondary effects" of adult establishments, and (3) must leave open adequate alternative means of communication (Smith, 1991).

While the cases above describe the *law* which regulates adult establishments, it is important to realize that several other factors regulate adult speech as well. Lawrence Lessig (1998: 3) has noted that in addition to the law,

three other mechanisms regulate speech; the market, social norms, and the architecture of physical space.

The market regulates speech by setting a price on goods. In the case of adult entertainment, production costs especially for videos was once very high. However, with the invention of hand held recorders, production costs declined drastically. This reduction in price, has led to a greater number of options for consumers, and in turn the adult video market has boomed. Nevertheless, the real world distribution costs of pornography remain high (although the net is changing this), and therefore most porn establishments are commercial. This means that such content is inaccessible to minors because of cost, or because through entering a commercial transaction, a store owner can enforce age based legal restrictions.

Social norms regulate speech by guiding behavior. For example community norms may dictate that pornography is a taboo topic. As such, individuals who may wish to sell or consume such material are inhibited from doing so because they are afraid of the shame of being found out. Similarly, community norms dictate that minors should not have access to pornography. Even in the absence of *Ginsberg*-like regulation, the pornography industry recognizes this concern. "Even they understand that it is best if they don't exploit this market, and so even without laws, they will resist the sale of porn to kids (Lessig, 1998: 33)."

Finally, and perhaps most powerfully, the architecture of physical space regulates speech. Adult establishments use numerous forms of physical space regulation to ensure that children will not be exposed to explicit material. Perhaps the simplest of all of these controls is to place a dirty magazine behind the counter. Similarly, the magazine may be enclosed in a paper bag, or placed behind a blinder rack. In all of these instances, minors access to adult content is

constrained by physical world realities. The architecture of physical space also makes it very difficult to conceal age. "This is the fact that it is hard for a kid to hide that he is a kid. He can don a mustache, and walk into a porn shop on stilts, but this will not hide, at least perfectly, that he is a twelve year old boy (Lessig, 1998: 33)."

In sum, the physical world has developed a number of formal and informal ways to regulate adult establishments. Formally, towns can control adult-use property via zoning laws. Informally the market, social norms, and physical world architecture work in conjunction to limit minors access. "In countless ways, social life is regulated by these codes of zoning; in countless ways these codes achieve or interfere with social ends, whether enacted, or merely recognized (Lessig, 1996: 20)."

The Internet: Physical World Zoning Does Not Apply Here

While formal and informal zoning may do an excellent job of regulating adult establishments in the real world, the same can not be said for cyberspace. Both in terms of the law (in our case the CDA) and informal regulation, cyberspace poses uniquely new challenges to enforcing zoning controls. This section will examine why the CDA failed to qualify as a constitutional attempt at "cyberzoning" and also why the nature of the Internet nullifies many of the informal content controls we take for granted in the physical world.

As mentioned earlier, one of the governments primary defenses of the CDA, was that it fit within a well defined tradition of protecting minors from adult content via zoning. Specifically, the government argued that like *Ginsberg* the CDA was intended to protect minors from adult content. The government also argued that like *Renton*, the CDA would be constitutional as a form of

"cyberzoning." However, rather than serving as strengths, the Court used these very precedents to find the CDA unconstitutionally overbroad.

To begin with, the Court pointed out that the CDA was far broader than *Ginsberg* in three important ways. First, *Ginsberg* did not prohibit adult's from purchasing obscene material for their children, whereas the CDA would have applied despite parental consent. Second, *Ginsberg* applied only to commercial transactions. Finally, unlike the CDA, *Ginsberg* defined what it meant by the term "harmful to minors." The CDA contained no such definition of "indecent" and was therefore unconstitutionally vague.

With regards to *Renton* the Court found two flaws. First, unlike traditional zoning laws which apply to a specific neighborhood or area, the CDA applied to "the entire universe of cyberspace." Secondly, the stated intent of the CDA was to protect children from the effects of "indecent" and "patently offensive" speech. Therefore, the CDA constituted an unconstitutional content-based restriction on speech. As the Court noted:

> 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."

Next the Court addressed the Act's ambiguous language. One part of the act refers to "indecent" material, while another refers to "patently offensive" material. In both cases the terms are not defined, and could therefore lead to uncertainty among speakers. "This uncertainty undermines the likelihood that the CDA has been carefully tailored to the Congressional goal of protecting minors from potentially harmful materials."

The Court then suggests that the CDA's burden on free speech "is unacceptable if less restrictive alternatives would be at least as effective in

achieving the legitimate purpose of the statute," namely the protection of minors from adult speech. Pointing to both "tagging" content, and the use of software filters by parents, the Court found that the CDA was not "narrowly tailored."

A final argument with regards to zoning that the Court rejected was the governments assertion that the CDA leaves open ample "alternative channels" of communication. Because the CDA was found to be a content-based restriction on speech, the "alternative channels" argument was irrelevant. "The Government's position is equivalent to arguing that a statute could ban leaflets on certain subjects as long as individuals are free to publish books."

In short, the Court examined all three prongs of the *Renton* zoning ordinance test, and found all three wanting:

> 1. Is the regulation content neutral? No because the CDA's purpose was to protect children from the primary effects of "indecent" and "patently offensive" speech, rather than any "secondary" effects of such speech.
>
> 2. Is the regulation narrowly tailored to serve a substantial governmental interest? While the CDA's purpose of protecting children from adult speech may be a substantial government interest, its implementation was not narrowly tailored, nor could it be proven to be the "least restrictive" means of enforcing this interest.
>
> 3. Does the regulation leave open adequate alternative means of communication? This question is irrelevant, as the CDA is a blanket content-based restriction, thus forbidding speech in all forums.

Based on this logic, it is clear that the CDA was a poorly crafted attempt at zoning cyberspace. Failing all three prongs of the *Renton* adult-use zoning test, the CDA would have suppressed a great deal of constitutionally protected speech.

Despite its considerable flaws, two members of the Court refused to completely reject the governments attempt at regulating cyberspace. Dissenting

in part, Justice O'Connor joined by Chief Justice Rhenquist found the CDA's attempt at "cyberzoning" to have some merit. As O'Connor notes, "the CDA is 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 constitutional."

As Lawrence Lessig points out in *Reading the Constitution in Cyberspace* (1996) the CDA was an attempt to zone the Internet according to age. However, unlike the physical world, in cyberspace, age and other identifying characteristics can not be easily ascertained. Citing Lessig, O'Conner agrees, commenting that "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."

Once again citing Lessig, O'Conner comments that this need not be the case. Due to the Internet's "malleability", protocols and software can be developed to effectively screen by age, and thus make "cyberzoning" perfectly possible. Here O'Conner mentions software filters as well as content rating via the Platform for Internet Content Selection (PICS), as possible technologies by which cyber zoning could be achieved.

Although O'Conner found that Internet zoning could be possible in the future, she nevertheless agreed that the CDA was unconstitutional. Because Internet zoning technology was not widely available at the time of the decision, "the only way for a speaker to avoid liability under the CDA is to refrain from using indecent speech." O'Conner found this to be an unconstitutional restriction on adult speech, thus invalidating the CDA.

Technology to the Rescue!

Following the Court's rejection of the CDA, a number of pundits joyously described the decisions as a "legal birth certificate for the Internet" (Felsenthal and Sandberg, 1997) and as the "Bill of Rights for the 21st century (Schwartz and Biskupic, 1997)." The Internet did not need repressive government regulation, instead as the Court noted it merely needed better filtering and rating technologies to keep kids away from the "adult zones" of the Internet.

Picking up on this, immediately following the Court's decision President Clinton, who had supported the CDA, changed course and commented that "With the right technology and rating systems - we can help ensure that our children don't end up in the red light districts of cyberspace (1997)." One month later, the President followed up on his statement by convening an "Internet summit" with 40 industry executives to discuss filtering and rating solutions (Macavinta, 1997). The conference concluded with the President fully endorsing software filters, and calling upon the Internet content industry to voluntarily rate their web sites using the PICS standard. The President referred to these two solutions as forming an "Internet toolbox" for parents. Using the same metaphor, AOL president Steve Case commented, "You don't let your kids take a trip in a car without a safety belt. You shouldn't let your kids travel in cyberspace without this Internet toolbox (Vesely, 1997)."

Using his bully pulpit, President Clinton essentially convinced the Internet industry as well as concerned parents, that filters and ratings were far better than government regulation (Lasica, 1997). However, a small number of groups wondered if software filters and ratings were not in fact *more* harmful than the CDA. Groups like the ACLU who had pushed filters and content rating in their defeat of the CDA, pulled back from their earlier support and noted that these technologies often blocked far more than just adult content. As a result, software filters and content rating systems would not be "less restrictive" means

than the CDA. Chapter Three will examine these doubts in depth, and will more fully explain how software filters work. We will return to the issue of content rating systems and PICS in Chapter Five.

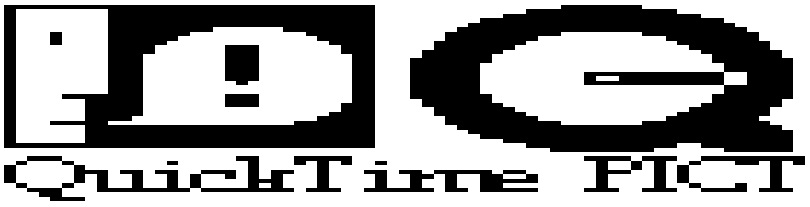
Chapter Three -- SOFTWARE FILTERS

The Moral Guardians of the Internet

When President Clinton and the Supreme Court referred to filters as a "less restrictive" alternative to the CDA, they were really pointing to a handful of commercially developed products aimed at protecting children from inappropriate content on the Internet. The four most popular of these titles are

Net Nanny, Solid Oak Software's CYBERsitter, The Learning Company's (now a division of Mattel) Cyber Patrol, and SpyGlass Inc.'s SurfWatch. All of these products were developed around 1995, directly coinciding with "The Great Cyberporn Panic" discussed in the previous chapter. All market themselves as having the most extensive lists of blocked sites, and as parental empowerment tools.

In its product literature, Net Nanny proudly claims that it will "protect your children and free speech on the Internet." It further advertises that due to its filters, Net Nanny will "ensure on-line safety for your users (Net Nanny, 1999)."



Solid Oak's CYBERsitter claims to offer "the safest way to explore cyberspace," for its 1.7 million users. It also claims to have "by far the most technologically advanced filtering product on the market" due to its use of an "intelligent 'content recognition' system," which "recognizes even brand new sites." Because of these technological advances, CYBERsitter is "guaranteed to block over 95 percent of all objectionable content (Solid Oak, 1999)!"

With six million users (Wallack, 1999), Cyber Patrol advertises itself as "the best way to manage children's computer use and safety on the Internet." It claims that all 50,000 plus sites on its blocked list are "reviewed by a team of Internet professionals, including parents and teachers (Cyber Patrol, 1999)." Cyber Patrol further claims that all blocked sites have been reviewed by human eyes (Censorware, 1997).

Finally, SurfWatch claims that more than eight million copies of its product have been downloaded, thus making it "the most popular, trusted product for harnessing the positive potential of the Internet." It's mission statement notes, "we **empower** people with the information, technology, and tools they need to harness the positive potential of the Internet (emphasis added)." With a blocked site list of more than 100,000 URL's, it claims to be "90-95 percent effective in blocking objectionable sites," and due to its "team of professional web surfers" the product will always remain up to date. SurfWatch also advertises that all blocked sites are seen by human eyes, and that difficult decisions are referred to an "Advisory Committee of parents, professionals, teachers, law enforcement, clergy and community members (SurfWatch, 1999)."

But do these products live up to their own hype? Do they protect children from dangerous content? Do they really empower parents? Are they 90-95

percent accurate in blocking dangerous content, and is it possible for their staff members to keep up with new material? Even more important than verifying product claims, what about the court's contention that these products are "less restrictive alternatives" which are "at least as effective in achieving the legitimate purpose" of the CDA, namely the protection of minors from "indecent" and "patently offensive" Internet material (Volokh, 1997)? This chapter, and Chapter Four will seek to answer these questions by explaining how filters work, citing examples of filter shortcomings, and actually testing their use.

The Index Reincarnated

The saying that everything old is new again is very accurate in describing the mechanisms by which modern day Internet content blocking software works. They employ the same four mechanisms -- categorization, listing, word filtering, and access/distribution control -- which the Catholic Church developed and perfected some 400 years ago with the *Index*. And just as people found ways to circumvent the *Index*, so too are there loopholes in our current technology of Internet censorship.

Categorization and Listing

The first and most important characteristic of all Internet filters, are the categories the products choose to focus on. Each company advertises its own unique categorization scheme, although all basically focus on pornography as their prime target. Some companies such as Cyber Patrol and SurfWatch are very explicit in their definitions for the content they evaluate. Others like CYBERsitter and Net Nanny offer no such information. One might call these category rules a rating system, and indeed they are. However, it is important to differentiate between the private, proprietary rating systems used internally by

the companies described here, and the public Internet content rating systems like PICS which will be described in greater detail in Chapter Five. What exactly do these categorizations look like? Let's take a look at Cyber Patrol and SurfWatch's described categories.

Cyber Patrol is very explicit in defining and describing the types of content it blocks. The program tailors its blocking decisions based on "the effect of the site on a typical twelve year old searching the Internet unaccompanied by a parent or educator (Cyber Patrol, 1999)." The product has twelve categories of blocked content: Violence/Profanity, Partial Nudity, Full Nudity, Sexual Acts, Gross Depictions, Intolerance, Satanic/Cult, Drugs/Drugs Culture, Militant/Extremist, Sex Education, Questionable/Illegal & Gambling, and Alcohol & Tobacco. Each of these categories carries an explicit definition, for example, Full Nudity is defined as "pictures exposing any or all portions of the human genitalia (definitions for all Cyber Patrol categories are available in Appendix 1)."

SurfWatch offers a very similar set of content categories, with explicit definitions, although it does not say which specific age group it is tailored for. Under its "Core Category Criteria" SurfWatch filters the following content: Sexually Explicit, Drugs/Alcohol, Gambling, Violence, and Hate Speech (definitions for SurfWatch categories are available in Appendix 2).

Once content is categorized along the stated criteria, it is added to a list of blocked sites, in Cyber Patrol this is called the "CyberNOT block list", which is then distributed to paying customers. Some companies like SurfWatch offer daily updates, while others offer weekly and monthly updates. As mentioned above, these blocked site lists can contain as many as 100,000 off limits URL's.

How do these companies go about categorizing the vast expanse of the web? All basically follow the same procedure, which includes the use of an

artificial intelligence web spider which flags potentially inappropriate content for company employees to review, categorize, and add to their blocked sites lists. For example, Cyber Patrol employs the use of its "Cyber Spyder" to aid in categorization:

> Cyber Spyder visits the sites and creates a report including 25 characters before and 25 characters after each occurrence of the keywords used in a particular search. The researchers start by reviewing this report. If necessary, the sites are visited and viewed by a human being before being added to the CyberNOT list. If not necessary, the sites are not viewed or added. For example, if the context of the word "breast" was the proper way to prepare chicken, that is a good indication that the site doesn't meet the CyberNOT criteria. (Cyber Patrol press release cited in Censorware, 1997)

Cyber Patrol employs 10 full-time employees to review and categorize the results from the web spider. SurfWatch claims to have a staff of four full-time content specialists and 12 freelance surfers (Roberts-Witt, 1998) who add blocked sites to SurfWatch's database at a rate of 400 sites per day (SurfWatch, 1999). Finally, CYBERsitter estimates that it spends $10,000 per month maintaining its list.

Problems With Categorization and Lists

To say their are major problems with the methods used to categorize and maintain lists of objectionable content is an understatement. Simply put, the blocking procedures followed by filter companies are awful, often capricious, and occasionally outright negligent.

The first problem with categorization is that despite precisely worded definitions, interpretation of such rules will inevitably involve subjective evaluations. For example, under its definition of "Sexually Explicit," SurfWatch

includes "erotic stories and textual descriptions of sexual acts." Would this therefore include Biblical stories such as that of Sodom and Gamora? The problem of subjective evaluation of content is best summed up by D.H. Lawrence, "what is pornography to one man is the laughter of genius to another (1936: 11)." In examining the blocking decisions of filter makers, their political biases become readily apparent.

An excellent case study in the problem of subjective content categorization comes from the evolution of Cyber Patrol. In 1995 Cyber Patrol was found to block a number of gay web sites including the Queer Resource Directory. This decision should be of no surprise considering that on Cyber Patrol's content review board at the time were members of the conservative National Rifle Association and the right-wing anti-pornography group Morality in Media (Arthur, 1996). Following protests from GLAAD (the Gay and Lesbian Alliance Against Defamation), Cyber Patrol unblocked the site, and appointed GLAAD members to its content review board. Subsequently, Cyber Patrol has added an "Intolerance" category, defined as "pictures or text advocating prejudice or discrimination against any race, color, national origin, religion, disability or handicap, gender of sexual orientation. Any picture or text that elevates one group over another. Also includes intolerant jokes or slurs." At the urging of GLAAD and other gay rights groups, Cyber Patrol now blocks as intolerant the conservative American Family Association (AFA), whose web site includes statements such as "we want to outlaw public homosexuality" and "we believe that homosexuality is immoral and leads ultimately to personal and social decay (cited in Peters, 1998)." The AFA, which actively supports the use of filters, argues that its content is espousing a political and religious viewpoint, and not advocating prejudice against gays. This example clearly shows that blocking decisions are largely based on who defines what sex and intolerance is. In both

cases, the political bent of Cyber Patrol's review board determined what was in and what was out.

Even more blatant than Cyber Patrol's early conservative bent is CYBERsitter, which blocks numerous gay web sites including GLAAD, and the National Organization for Women's site for its discussion of lesbian issues. CYBERsitter even blocks sites critical of its product! CYBERsitter was at one point the preferred filter of the ultra-conservative Focus on the Family, of which CYBERsitter president Brian Milburn is an alleged member (GLAAD, 1998). Responding to criticism of blocking homosexual sites, a CYBERsitter representative commented, "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 (cited in Weinberg, 1997)."

Another problem with these political categorizations is the way in which they are implemented. A web site may be made up of hundreds even thousands of web pages. Within a web domain, say www.upenn.edu, some pages may pertain to sex, violence, etc., while others have nothing to do with such off limits categories. Ideally a filter should only block those pages with prohibited category content. Yet in practice, this is not the case, with filter companies blocking access to entire domains, thus creating "collateral damage." Three gross examples of such "overbroad blocking" come from Cyber Patrol. In 1997, Cyber Patrol was informed of sexual content on some web pages within the GeoCities (a free web hosting service) "West Hollywood" neighborhood, which is a gay and lesbian community. Rather than search for the specific problematic sites, Cyber Patrol blocked the entire neighborhood, composed of more than 50,000 web pages, under its Full Nude Sex Acts category. After complaints from groups like GLAAD, Cyber Patrol's CEO, Dick Gorgens admitted to prejudicial blocking:

"we took the 'easier' approach to blocking the small number of actionable non-nudity publishers in that area rather than individually sanctioning them (cited in Censorware, 1997)." Cyber Patrol also took the "easier approach" with two other major web sites. Due to isolated instances of problematic content on Tripod's web site (a similar service to GeoCities), Cyber Patrol blocked all 1.4 million pages within the site as violating all twelve Cyber Patrol content categories. For similar reasons, Cyber Patrol blocks access to all of Deja News, a site which archives 80,000 Usenet discussion groups posts. Despite the fact that Deja News does not archive images uploaded to Usenet, and that only a tiny fraction of Usenet posts are pornographic, Cyber Patrol still feels the need to block access to the entire database of more than 250 million messages dating back to 1995 (Censorware, 1998).

While the examples just described derive from a political bent, which the companies do not exactly advertise, even more troublesome are the completely erroneous categorizations regularly made by filters. In addition to the incorrect categorization of sub-pages due to overbroad blocking, individual web sites are routinely misclassified. Jamie McKenzie of *From Now On*, an adult education web journal, whose site has been incorrectly blocked by SurfWatch, calls such decisions "SL@Ps" which he describes as "an electronic insult -- an unfounded and defamatory label applied to a web page without looking (1999)." Once again, Cyber Patrol provides us with a number of outrageous examples:

> The "Creature's Comfort Pet Care Service" web page devoted to pets -- blocked by Cyber Patrol under Full Nude Sex Acts.
>
> The "Air Penny" web site run by Nike to glamorize basketball player Penny Hardaway -- blocked by Cyber Patrol under Full Nude Sex Acts.
>
> The "MIT Project on Mathematics and Computations -- blocked by Cyber Patrol under Full Nude Sex Acts.

> "The National Academy of Clinical Biochemistry" web site -- blocked by Cyber Patrol under Full Nude Sex Acts.
>
> The "U.S. Army Corps of Engineers Construction Engineering Research Laboratories" web site -- blocked by Cyber Patrol under Full Nude Sex Acts.
>
> "We the People of Ada" web site devoted to politics in Ada, Michigan -- blocked by Cyber Patrol under Full Nude Sex Acts.

All of these sites were reviewed by the Censorware (1997) project and found to contain no sexually explicit material meeting Cyber Patrol's categories for Full Nude Sex Acts. Based on its study of banned Cyber Patrol pages, the Censorware project estimates the filter's accuracy (number of correctly banned pages divided by total number of pages banned) as less than 1 percent (Sims, 1998). How could such outrageous miscategorizations and low accuracy rates occur?

The answer lies in the methods which filter makers use to review the vast amount of content available on the web. As mentioned earlier, all use some form of artificial intelligence web searching spider. The "advanced" artificial intelligence that these companies use mostly means looking for "improper" flag words like breast, sex, xxx, gay, etc. (described further below). These spiders, which companies claim index 90-95 percent of the web, then create content reports which are supposedly reviewed by individual humans who make the ultimate decisions about whether to block a site. Unfortunately, the realities of the web make such claims highly dubious.

An estimate published in *Science* magazine placed the size of the web at roughly 320 million pages. This is compounded by the fact that the web is growing by several hundred percent per year. Further, in a March, 1997 *Scientific American* article, Brewster Kahle estimates that the average life span of a web

page is 75 days. These figures translate into about 250,000 web pages changing every single hour of every single day, all while overall growth increases exponentially (Censorware, 1998). Combining the shear size of the web, with its ever changing nature, it is clearly impossible for a filter company with 12 employees to review 90-95 percent of web content. Even if they were able to review such a large percent of web content, they would have to continually re-review sites that have updated their content (for example candyland.com was originally a pornography web site until Hasbro bought the domain and converted it to a Candyland board game product site). As Censorware (1997) researchers summarize the problem:

> Common sense tells us that, to stay ahead of the web, censorware vendors must drastically reduce their human workload by making blanket judgments about thousands of pages at once, and by providing their employees so little data that they must make snap decisions based on almost nothing. And this is exactly what we have seen in practice: the blocking of thousands of web sites because they are gay-oriented, and the blocking of sites which have no explicit content whatsoever.

Comparing filter advertising with the efforts of major Internet search engines provides another example of shaky filter maker claims. The AltaVista search engine uses 28 top of the line Digital AlphaServer 8400 5/440's super computers, each with 8 gigabytes of memory, and costing roughly $35,000,000 (Sims, 1998). These machines use a 25 Gigabyte per second connection to the net, and index content 24 hours per day. Even with this astonishing amount of technology, AltaVista only indexes 125,000,000 unique web pages, representing about 38 percent of the entire web (AltaVista, 1999). If a well funded, multi-million dollar corporation, with limitless technology can only index 38 percent of the web, what is the likelihood that much smaller filter companies can review 90-95 percent of objectionable web content? The answer is slim to none. As a result,

filters which claim to make the net safe for children, will miss vast swaths of potentially dangerous material, and as we shall see in Chapter Four, this fact means that filters allow through surprisingly large amounts of hardcore pornography and other objectionable content.

Compounding the problem of political and miscategorized blocks mentioned above are three additional factors. First, none of the filter makers notify sites who have been blocked. As such, site developers have no idea that their content is being kept from the view of between six and eight million web users. Nor can they know why their site has been blocked. Once a site operator learns of a blocking decision, usually due to the work of anti-filter groups like Censorware, they are not guaranteed a due process review of their site. While Cyber Patrol and SurfWatch to their credit both have formal site review procedures, Net Nanny and CYBERsitter have none. In response to a journalist's question about a site operator finding out why his/her site had been blocked, CYBERsitter president Brian Milburn answered "They would be out of luck (in Arthur, 1997)."

Second, even if a site operator is successful in appealing a blocking decision, the site may not be removed from the blocked sites list due to a lack of time or an extensive backlist. Further, once removed, the same site may be flagged again by a filter company's web spider, thus banning it all over again! These problems point to the difficulty in effectively managing a list of 50,000 plus sites (remember that the *Index* only had 4,000 banned works).

Finally, and most egregiously CYBERsitter, Cyber Patrol, and SurfWatch do not make their lists of blocked sites publicly available. The lists are considered proprietary trade secrets and are encrypted to ensure that no one can gain access to them. As Theresa Marcroft of SurfWatch notes, "If we publish the list, we would be shooting ourselves in the foot and giving ammunition to

competitors (in Guernsey, 1999)." Due to such secrecy, public review of the vast majority of blocking decisions is made impossible. Lawrence Lessig equates such lists with past book censorship: "The lists are our day's banned books, yet unlike the past, we never see the actual list of books banned (1998: 33)."

All filters claim to be "parental empowerment tools", but the secretive nature of their blocked site lists prevents parents from taking control of the content they want their children to view. While all programs do allow parents to override blocking decisions, they can not do so until they learn that a particular site is blocked through direct experience. This approach also assumes that parents will have the technological savvy to unblock a site (consider that many adults can not program a VCR).

Even if all filters made their blocked site lists public, like Net Nanny, this would not necessarily solve anything. Net Nanny's public list of blocked sites contains thousands of web pages. It would therefore take a parent days to scan through the entire list of sites, and unblock those which he/she deemed safe. This notion is backed up by Kevin Britt, product manager for CompuServe's Internet in a Box for Kids package, who notes that "Parents don't want to know about configuration settings, they just want the stuff to work (O'Brien, 1996)." In light of these realities, it is doubtful that parents will take the time to customize their filters, and will therefore seed their parental judgment about "what little Johnny can read" to filter makers, and their less than stellar record of content categorization.

21st Century Bowdlerizing -- Word Filters and Their Problems

The second method used by filter companies to block objectionable content is the use of word filters, also known as string recognition software. Word filters are used by filter companies in one of two ways. First they can

block out or overwrite "objectionable" words found on a particular web page. So for example, if a page is not outright blocked by a filter program, but contains the word "shit", the filter will replace the swear with ### on the page as it is displayed by a web browser. Unfortunately, word filters are rarely advanced enough to understand context, and thus block out words such as "Essex" and "Anne Sexton" because they contain the dirty little word "sex." In one hilarious example of this problem, CYBERsitter's blocking of the word "homosexual" would render "President Clinton opposes homosexual marriage" to say "President Clinton opposes marriage (Weinberg, 1997)." Similarly, AOL got into trouble for blocking the word "breast", thus also forbidding "chicken breast", "turkey breast," and more importantly "breast cancer ." More recently, AOL has been chided for pointing customers of its ICQ chat service, to download a very conservative word filter offered by the ClickChoice Company. Its DirtyWords filter blocks out your usual sexually oriented terms, but also goes much further to block "popculture, lesbian, accounting.com, safesex, and now.org ." The filter also blocked the phrase "Don't by CYBERsitter," a peculiar rule for a separate filtering company. As it turns out, ClickChoice simply stole CYBERsitter's list of banned words, and sold it as its own. CYBERsitter is now pursuing a copyright infringement case against ClickChoice (Macavinta, 1999). Finally, Net Nanny makes the FCC and George Carlin's "seven dirty words" look quaint with its list of 118 off-limits words (see Table 3.1)! In addition to the usual sexually oriented terms Net Nanny also finds fault with "anarchy" and "spunk"? Net Nanny also word blocks 53 email addresses, including numerous gay and lesbian oriented list serves.

Table 3.1: NetNanny Blocked Words List

Adult Check	dildos	nympho
adult entertainment	doobie	nymphomania
adult gif	drugs	nymphomaniac
Adult ID	ejaculate	oral
adult images	ejaculation	orgasm
adult links	erection	orgy
adult movies	erotic	penis
adult pics	erotica	perversion
AdultCheck	exhibitionism	perverted
AdultSights	exhibitionist	porn
amateur sex	exhibitionists	porno
amateur videos	fellatio	pornography
amateur women	fetish	prick
anal	fistfuck	pussies
anarchy	fisting	pussy screw
ass	flesh	S&M
asshole	fuck	screwing
beastiality	fucked	sex
bestiality	fuckers	sex toys
blowjob	fucking	sexual
blowjobs	gangbang	sexually
bomb	groupsex	slut
bondage	hard-on	sluts
boob	hardcore	smut
buttfucking	hardon	spunk
cannibalism	horniest	suck
clit	horny	teen movies
cock	incest	teen pics
cocks	intercourse	teen videos
coitus	jism	threesome
copulate	kinky	tit
copulation	live couples	tits
cum	lust nudity	twat
cumshot	lusting	voyeurism
cumshots	marijuana	whore
cunnilingus	masturbate	XXX
cunt	masturbation	zoophile
cunts	nude	zoophilia
dicks	nudes	
dildo	nudity	

As mentioned earlier word filters are also implemented in the automated, artificial intelligence web spiders that filter companies use to identify potentially

off limits material. However, once again these word filtering rules run into the problem of context. If a spider comes across a site with some permutation of the word "sex" or other off limits word, the robot will block the site. In a particularly embarrassing example, SurfWatch blocked access to the White House web site because of a page containing the allegedly indecent word "couple" in reference to Al and Tipper Gore (Einstein, 1996). Similarly, Cyber Patrol blocked access to GeoCities music area "Sunset Strip" presumably because of the word "strip," and "LezliSoft" a shareware developer's page, presumably due to the presence of "Lez." And as described earlier, it is highly unlikely that human reviewers will correct any of these mistakes unless they are brought to the company's attention.

The numerous examples of silly word blocking decisions are all attributable to the fact that "intelligent content recognition software" as CYBERsitter describes it, simply do not work. Indeed, the U.S. government and the computer industry have spent billions of dollars over the past thirty years funding research into artificial intelligence. Still it was only two years ago that a computer defeated the world's best chess player. More importantly, a computer has yet to consistently passed the "Turing test," a measure of a computer's ability to carry on a seamless conversation with a human (Turkle, 1997). Given that the world's best and brightest artificial intelligence researchers, spending billions of dollars of grant money, have yet to come up with an "artificial intelligence," the likelihood that a small filter company could develop a truly context sensitive word filter are very slim. As the Censorware Project (1998) concludes: "Artificial intelligence -- computers that read like humans do -- isn't coming any time soon. When it does it will rock the world. But it hasn't come. And no $24.95 software is going to even come close to what billion dollar research projects have failed at for thirty years."

Upstream -- Downstream: Proxies, Clients and Access Control

Just as Bishops controlled information access points in the time of the *Index*, so too do today's content filters. And, as we shall see, where a filter is implemented within an information access and distribution chain makes all the difference.

Under the *Index*, Bishops essentially controlled the views allowed to enter their own regional diocese. As such, they stood above individual printers, book stores, libraries, etc., and claimed to represent and protect the views of the community. The same top down thinking is represented by modern filters which are implemented through "upstream" proxy filtering. Within an upstream filtering system, all incoming and outgoing information is channeled through a powerful proxy computer which sits atop the network (see Figure 3.1).

Figure 3.1: Upstream Proxy Filtering

The proxy may be programmed to deny access requests to certain web sites, and to forbid the dissemination of certain types of messages (swear laden emails, credit card numbers, etc.) . The rules programmed into a proxy server therefore have tremendous power to define the reality of the Internet and its possibilities to network users. Who defines these proxy rules is obviously of tremendous importance. Proxy systems are usually employed within large networks with numerous points of access. The proxy helps cut down on costs associated with implementing access rules on every computer within the network. However in doing so, the proxy also centralizes control over the definition of what types of information are acceptable. This centralization is not necessarily a bad thing if all network users agree and understand the proxy's filtering rules. So for example, several Internet Service Providers (ISPs) now provide concerned parents with the

option of proxy filtered access, which blocks pornography and the like. In this situation network users opt in to the filtering (although all of the same problems associated with delegating filtering to third parties remains). Much more problematic is invisible upstream filtering, where network users have no idea that their information requests are being filtered by an upstream proxy, nor do they know the proxy's programmed content rules. In this situation, the rules determined by the proxy administrator (who supposedly represents the community) affect the individual information decisions of all network users. As we shall see in our discussion of library and school Internet access, upstream filtering is the norm, and the values programmed into these proxies may well violate First Amendment and academic freedom rights. All of the programs described above offer proxy filtering solutions which they primarily market to large organizations like libraries, schools, and businesses.

More pertinent to individual home users is "downstream" client filtering. Client filtering simply means that a parent or computer owner purchases a copy of Cyber Patrol, SurfWatch, etc. to install on his/her individual home computer. With client filtering, the content decisions of one user do not affect everyone else on the network (see Figure 3.2). As such, despite its many problems, client filtering presents less of an ethical and legal dilemma than proxy filtering.

Figure 3.2: Downstream Client Filtering

Other Content Filter Issues

Beyond issues with the four main mechanisms by which filters work, three other problems effect their use. The first is security, or lack there off. One of the truisms of the computer revolution is that children know far more about computers than their parents do. This situation makes it easy for kids to override parental installed filters by using any of a number of computer savvy workarounds. First, a child can simply guess the override security word/number set by a parent to switch a filter off for adult use (how many parents set their password to their birth date or license plate number). If that does not work, a child can choose to simply uninstall the program. Finally, if both options fail to work, a child can download "cracker" software which will provide a valid override password, or outright disable the program. For

example Bennett Hasselton of the anti-filter group Peacefire, has developed "CPCrack" which generates an override password for Cyber Patrol 4.0 (Macavinta, 1999).

Even if kids can not override a filter's controls, this still does not mean they will be unable to find objectionable material on the net. As mentioned earlier, filter programs allow through quite a bit of objectionable material, and with a little effort using search engines, kids can easily locate such unblocked content.

Finally, despite two years of White House, Congressional, and industry support for Internet content filters, few parents actually use them. In a 1998 survey, *Family PC* magazine found that only 20 percent of parents used filters built into their browser or provided by their ISP. Additionally, only 6 percent of parents used commercially available software like CYBERsitter, Cyber Patrol, etc. In a more recent survey, Turow (1999) found that only 32 percent of parents used some form of Internet filter. To date, no studies have investigated why parents, many of whom are afraid of dangerous Internet content, fail to use filters. Two likely answers are complexity and the third person effect. Many parents who have Internet access may not feel they have the technical ability to install and configure content blocking software. Further, although such options are built into popular browsers, they are difficult to locate and configure (remember that the vast majority of web users do not even know how to change their start page). Second, parents may feel that filters are a good idea for others, but that their children do not need such protection. Both of these potential explanations need systematic study. Without a deeper understanding of what leads people to use filters, they may end up being a "dead on arrival" solution to the Internet Content Conundrum.

Filters, Public Policy, and Democracy

This chapter set out by asking whether the Supreme Court and the White House were correct in endorsing content blocking filters as "less restrictive alternatives" which are "at least as effective in achieving the legitimate purpose" of the CDA (Volokh, 1997)? Unfortunately, the answer would seem to be no, and in both directions. First off, content blocking filters are clearly not less restrictive than the CDA. While the CDA would have declared vast portions of the net "indecent", it would likely have left alone innocuous material and political speech. However, the filters described above have gone beyond the CDA's mandate and blocked access to sites with absolutely no objectionable material -- remember Cyber Patrol's decision to block the "Creature's Comfort Pet Care Service" web page?! Even more troubling, content filters have been found to block important political speech such as the entire White House web site, the Starr Report, and any political organization with controversial views (GLAAD and the AFA for example). These decisions would seem to run counter to a democracy which can only thrive when its citizens are well informed (Meiklejohn, 1965). As Lawrence Lessig sagely notes, "Democracy doesn't work if you can turn off anyone you don't want to hear from (in Sacramento Bee, 1997)."

Not only are filters *overinclusive*, thus failing the first prong of the courts logic, but they are also not "at least as effective" in achieving the CDA's goal of protecting children from indecent material. Because it is impossible for filters, or any other technology, to keep up with the vast size of the web, they will inevitably be *underinclusive*, and fail to protect children from harmful Internet content.

Based on these problems, it does not seem particularly appropriate for the White House, the FCC, libraries, schools, etc. to promote filters as First

Amendment friendly, parental empowerment tools which will protect children from dangerous content. Filters, especially within the context of public institutions are not First Amendment friendly, as they block large amounts of constitutionally protected speech (see Chapter 6). To this, lawyers and parents respond that privately installed client filters pose no First Amendment issues because they enforce the legitimate right of parents to limit their child's access to content they do not approve of. However, this argument assumes that filters are empowering and adequately reflect parental attitudes about content. Yet, as described above, parents have little ability to truly tailor filters to their own values. Finally, government support for filters gives people the false sense that they actually work. Unfortunately, as we shall see in Chapter Four, they in fact still fail to block a significant amount of inappropriate content.

In light of these factors, it would seem the government should take a harder look at its support for filters as *the* solution to the Internet Content Conundrum. We will look further at potential policy improvements to filters, and other alternatives in Chapter Seven.

Chapter Four -- SOFTWARE FILTER PERFORMANCE

The majority of reports of Internet content filters being both underinclusive (failing to block the worst pornography), and overinclusive (blocking non-sexual, non-violent content), have come from journalists and anti-

censorship groups. Both have used largely unscientific methods to arrive at the conclusion that such filters are deeply flawed. The goal of this chapter is to apply social science methods of randomization and content analysis to examine the effectiveness of Internet content blocking filters.

Hypotheses

Based on our extended discussion of the problems with Internet content blocking software in the previous chapter, the following hypotheses are put forward for analysis:

1. Internet content blocking software will be underinclusive. They will fail to block access to sites with "objectionable material."

2. Internet content blocking software will be overinclusive. They will block access to sites with no "objectionable material."

Methods

The hypotheses above beg the question of what is "objectionable" Internet content? To answer this question I used the Recreational Software Advisory Council's Internet rating system or RSACi. RSAC was originally developed by Stanford Communication professor, Donald F. Roberts, to rate the content of video games, and provide parents with a way to protect their children from excessive violence. However, with the advent of the Internet the system was adapted to allow web site owners to self rate their content. Currently, RSACi is the most popular system for rating content on the Internet, with more than 100,000 web sites using it to self rate (RSAC, 1999).

RSACi contains four content categories (language, nudity, sex, and violence) each with five levels of severity (0, 1, 2, 3, 4). So for example, within the language category, a site may be rated 0 if it contains no objectionable language,

1 if it contains mild expletives, 2 if it has profanity, 3 with strong language, and 4 if it contains crude, vulgar language. Table 4.1 gives a summary of RSACi's rating categories. The full definitions for each category and level are provided in Appendix 3.

Table 4.1: The RSACi Rating System

	Violence	Nudity	Sex	Language
Level 4	rape or wanton, gratuitous violence	provocative frontal nudity	explicit sexual acts or sex crimes	crude, vulgar language or extreme hate speech
Level 3	aggressive violence or death to humans	frontal nudity	non-explicit sexual acts	strong language or hate speech
Level 2	destruction of realistic objects	partial nudity	clothed sexual touching	moderate expletives or profanity
Level 1	injury to human beings	revealing attire	passionate kissing	mild expletives
Level 0	none of the above or sports related	none of the above	none of the above or innocent kissing; romance	none of the above

This system was used to rate the content of 200 web sites drawn from three web page samples described below. Only the first page of all sites was rated. Links were not followed to subsidiary pages. The only exception to this rule was on pages that had no other content than an "Enter this site" link, in which case the link was followed, and the first fully developed page was rated.

RSACi rating decisions were then compared to the actual filter performance -- i.e. site blocked, site not blocked -- of CYBERsitter, Cyber Patrol, Net Nanny, and SurfWatch. A site was considered blocked, if the filter programs

completely denied access to it. Partial blocks, such as word masking were not considered, as they still allow access to the majority of a page.

Each of these filter products was purchased or downloaded, and all were left with their default settings on. Default settings were used due to the theory discussed in the last chapter, that few parents customize filter software. The only change made to these programs was to download the most recent blocked sites list from each company (see Appendix 4 for filter defaults and blocked site list dates). Filters were tested against selected web sites in June 1999.

A site is deemed to contain "objectionable" material if any of its content received an RSACi rating of 2, 3, or 4. Such sites should theoretically be blocked by filter software. Conversely, a site is deemed "not objectionable" if the highest score in all content categories is either 0 or 1. Such sites should theoretically not be blocked. For example, a site with an RSACi score of 0 - language, 4 - nudity, 3 - sex, and 1 - violence, would be deemed "objectionable" because its highest rating was a 4, and it should therefore be blocked.

Using these RSACi-based definitions of "objectionable - not objectionable" our inclusiveness hypotheses can be clarified. A filter will be deemed underinclusive if it fails to block a site with a 2, 3, or 4 RSACi rating. A filter will be deemed overinclusive if it blocks a site with only a 0 or 1 as its highest RSACi rating. Tables 4.2 and 4.3 summarize these rules:

Table 4.2: Objectionable Definitions

	Highest RSACi score in any category
objectionable	2, 3, or 4
not objectionable	0 or 1

Table 4.3: Inclusiveness

	Filter Performance
underinclusive	fails to block "objectionable" content
overinclusive	blocks "not objectionable" content

Web Page Samples

Internet users, including children, come across content through numerous surfing techniques. People stumble across pages through serendipitous surfing, by using search engines, and by using indexes such as Yahoo. As such, I choose to select three different samples of web content to rate for objectionable content, and to test filters against.

The first sample, roughly analogous to serendipitous surfing is a set of 50 randomly generated web pages. On April 15th and 16th, 1999, I used the Webcrawler search engine's, random links feature to produce a sample of 50 English language web sites. Although these sites were randomly provided by Webcrawler, this does not mean they are a random sample of all web content. As described previously, even the most powerful search engines can only index about half of the web. Thus, the random sample produced by Webcrawler is only representative of the percentage of the web indexed by the search engine.

The second sample, roughly analogous to typical search engine use, is a set of 50 popular search term results. In April 1999, Searchterms.com, a site which tracks the most frequently searched for terms on major search engines, listed yahoo, warez, hotmail, sex, and MP3 as the five most searched for terms. I took each of these terms and entered them into the AltaVista search engine. For each search result, I took only the first ten links generated by AltaVista, thus producing an overall sample of 50 sites. In terms of "objectionable" material, it is

interesting to note that search engines have been singled out as one way that children are intentionally and unintentionally exposed to adult material. If children are actively seeking out pornography they need only enter the terms "sex" or "porn" into any search engine to receive thousands of links to such sites. However, search engines also expose children to adult material through the most innocuous of searches. For example, searching for the term "toys" on several major search engines produces links to sex toy stores and pornography web pages. Similar objectionable and unintended results are even produced by searches for current events topics such as "Monica Lewinski" or "Columbine." These results occur due to the way that search engines index content. Most search engines read a web page's "meta tag," a piece of HTML which describes the content of a particular page or site. Unfortunately, several less reputable site owners place keywords they know to be popular in their meta tags, even if such words bear no relevance to the content of their site. Therefore, pornography sites seeking increased traffic will include keywords such as toys, play, Columbine, etc. in their meta tags. Thus, when a child searches for toys, expecting to be transported to Toys-R-Us, he/she might be linked off to a pornography web site that included toys in its meta tag. As a result of these characteristics, rating and testing search engine results provides a very good test of filtering software.

The final sample, roughly analogous to using a web index, is a set of 100 purposively selected web sites. I intentionally choose a number of web content categories that filters have been shown to have problems with. First I selected the 36 web sites of organizations who filed amicus briefs in the ACLU's challenge of the CDA and COPA. These organizations argued that Congressional legislation would place their content off-limits. However, seeing as some of these sites deal with touchy issues such as homosexuality and safe sex, filters

may also deem them inappropriate and thus accomplish the same end as legislation. In addition to the ACLU litigants, I used the Yahoo web site to select content in the following areas: Internet portals, political web sites, feminist web sites, hate speech sites, gambling sites, religious sites, gay pride/homosexual sites, alcohol, tobacco, and drug sites, pornography sites, news sites, violent game sites, safe sex sites, and pro and anti-abortion sites. Five links were selected in each category except pro and anti-abortion sites, where I only selected four to round out the overall sample to 100 sites. Keep in mind that these links are easily found by surfing through the Yahoo index. (see Appendix 5 for a list of all sites tested)

Reliability

I tested the reliability of my use of the RSACi rating system by having four colleagues rate a 21 site subset of the larger 200 site sample. Overall, use of the RSACi rating system was found to be highly reliable. Coders rated sites with perfect reliability seventy-three percent of the time. Additionally, coders only differed by one rating point 12 percent of the time (see Table 4.4).

Table 4.4: Coder Percentage Agreement Among All Sites

	Frequency	**Percent**
exact agreement	61	72.6
differed by one	10	11.9
differed by more than one	13	15.5
total	84	100

Within the 21 sites tested, 7 were rated exactly the same across all categories, and 5 only differed by one rating point across all categories.

Intercoder reliability for each individual RSACi content category; language (Alpha = .92), nudity (Alpha = .98), sex (Alpha = .96), and violence (Alpha = .82), was also extremely high. Finally, intercoder reliability across all RSACi content categories and web sites was found to be excellent (Alpha = .94).

While these results point to a highly reliable coding scheme they may be artificially high due to the large amount of non-objectionable content in the sample. In other words, since the vast majority of sites were rated 0 for all categories by coders, there was little variation in the amount of objectionable content across the sites. This reduces the room for error among coders.

Random Link Results

Perhaps the most interesting finding derived from rating the 50 Webcrawler randomly generated links is the very low percentage of objectionable material (see Table 4.5).

Table 4.5: Random Link Sample (N=50) Objectionable Content

	objectionable	**not objectionable**
language	3 (6%)	47 (94%)
nudity	1 (2%)	49 (98%)
sex	1 (2%)	49 (98%)

violence	1 (2%)	49 (98%)
any objectionable (all categories)*	4 (8%)	46 (92%)

* Derived from highest RSACi score obtained in any content category

These statistics support the conclusion that there is very little dangerous content on the Internet as a whole.

In accordance with such little objectionable content, the filters tested left the vast majority of sites unblocked. CYBERsitter blocked 2 sites (4 percent), Cyber Patrol blocked 2 sites (4 percent), SurfWatch blocked 1, and Net Nanny blocked no sites. Taken all together, filters only blocked 3 out of 50 sites (6 percent). (Note: All filter blocks combined is not additive, i.e. multiple filters can block the same site.) While these results are encouraging for filters -- they blocked roughly the percentage of objectionable material -- evidence of both under and overinclusive blocking can be found.

Underinclusive blocking

CYBERsitter, Cyber Patrol, and SurfWatch all failed to block 2 of the 3 sites (67 percent) with objectionable language and Net Nanny missed all 3. Net Nanny also failed to block the one site with objectionable nudity and sexual content. Finally, all four filters failed to block the one site with objectionable violence.

Overinclusive blocking

It is impossible to determine whether a filter is overinclusive within a particular RSACi category because for example, a filter may block a site with a 0 for language, but a 4 for nudity. Without knowing this, one might be led to

believe that the filter is being overinclusive on language because the site had a 0 language score. However, it is not the language but the presence of nudity that got the site properly blocked. As such, to test overinclusiveness we must rely on the highest overall RSACi score a site receives. In other words, a site with a 3 for violence, but zeros for all other content, would have an overall high rating of 3. Knowing this, any filter which blocks a site with a 0 or 1 overall high RSACi score is deemed overinclusive.

Both CYBERsitter and Cyber Patrol are guilty of overinclusive blocking within the random link sample. CYBERsitter blocked one site with a 0 as its highest rating, and Cyber Patrol blocked one site with 1 as its highest rating. Combined, CYBERsitter and Cyber Patrol's overinclusive blocking reached 4 percent of sites.

What type of content did these filters improperly deem off limits? CYBERsitter blocked "Sharktagger.com", a site devoted to fishing and tagging sharks. Cyber Patrol blocked "WebCastro Hotlinks", which contains numerous links to gay resources on the web.

Search Term Results

Largely due to the presence of "sex" as one of the search terms, this sample of pages had a much higher percentage of objectionable content (see Table 4.6).

Table 4.6: Search Term Results Sample (N=50) Objectionable Content

	objectionable	not objectionable

language	13 (26%)	37 (74%)
nudity	11 (22%)	39 (78%)
sex	10 (20%)	40 (80%)
violence	1 (2%)	49 (98%)
any objectionable (all categories)	15 (30%)	35 (70%)

These numbers support the general proposition that search engines provide an easy way for children to access improper material.

Overall, CYBERsitter blocked 28 percent of search term sites, Cyber Patrol 22 percent, Net Nanny 6 percent, and SurfWatch 24 percent. Taken together, filters blocked 17 of 50 sites (34 percent).

Underinclusive Blocking

Once again, all filters tested failed to block some form of objectionable content. CYBERsitter failed to block 1 of 13 objectionable language sites. Other filters faired much worse with SurfWatch missing 3, Cyber Patrol missing 5, and Net Nanny missing a whopping 10 of 13 objectionable language sites (77 percent). With regards to objectionable nudity, Cyber Patrol missed 4 of 10 sites, and Net Nanny missed 7. Among sexually objectionable sites, Cyber Patrol missed 3 of 10, and Net Nanny 7. The one objectionable violence site was only correctly blocked by Cyber Patrol.

Overinclusive Blocking

CYBERsitter and SurfWatch each blocked 1 of 35 non objectionable sites, and Cyber Patrol blocked 2 (5 percent). Combined, filters blocked 3 of 35 non objectionable sites. Or in other words, 9 percent of popular search term results may be inappropriately blocked by filter use.

What sites did filters go overboard to block? CYBERsitter blocked the "Yahoo! Local Events" page because it contained a reference to an upcoming concert by the musical band the "Bare Naked Ladies"?! Both Cyber Patrol and SurfWatch blocked "warez" sites. This is not surprising however, considering that "warez" trading is considered software piracy, and thus an illegal activity. Both Cyber Patrol and SurfWatch have their own internal categories for illegal activity.

Purposive Sample Results

Due to the presence of controversial topic areas like pornography, hate speech, violence, and safe sex, the purposive sample contained a relatively high percentage of objectionable material (see Table 4.7).

Table 4.7: Purposive Sample (N=100) Objectionable Content

	objectionable	not objectionable
language	11 (11%)	89 (89%)
nudity	7 (7%)	93 (93%)

sex	6 (6%)	94 (94%)
violence	5 (5%)	95 (95%)
any objectionable (all categories)	17 (17%)	83 (83%)

While the percentages of objectionable material are somewhat high, the percentage of content blocked by some filters is even higher. CYBERsitter blocked 33 percent of purposive sample pages, Cyber Patrol 22 percent, SurfWatch 15 percent, and Net Nanny 8 percent. These percentages would seem to indicate that CYBERsitter and Cyber Patrol are being overinclusive. Even more indicative of overinclusive blocking is the fact that all filters combined, blocked 42 percent of purposive sample sites.

Underinclusive Blocking

CYBERsitter failed to block 1 of 11 sites with objectionable language, Cyber Patrol 2, SurfWatch 7, and Net Nanny 8 (73 percent). Cyber Patrol missed 1 of 7 objectionable nudity sites, while SurfWatch and Net Nanny performed atrociously missing 6 and all 7 respectively. With regards to objectionable sexual content, Cyber Patrol missed 2 of 6 sites, SurfWatch 5, and again Net Nanny missed 100 percent of objectionable content. Finally, all four filters failed to block all five sites containing objectionable violence. These results show that once again, each filter missed at least one category of objectionable material.

Overinclusive Blocking

Overinclusive blocking is to be expected within the purposive sample of sites because I intentionally selected content types such as gay material that filters have been shown to block despite containing no off limits content. Indeed all four filters tested did not disappoint.

Net Nanny only blocked 6 percent of non-objectionable sites, SurfWatch 13 percent, Cyber Patrol 14 percent, and CYBERsitter blocked an incredible 22 of 83 sites (27 percent) with no objectionable material. Taken as a whole, filters blocked 30 of 83 non-objectionable sites, or 36 percent of the purposively selected sample. As mentioned above, this percentage is artificially high due to the fact that Cyber Patrol and SurfWatch both specifically block gambling and alcohol sites, all of which received non-objectionable RSACi ratings. However even minus these 10 sites, taken together, filters still blocked 27 percent of non-objectionable content.

The types of sites overinclusively blocked confirm the image of filters as extremely socially conservative. CYBERsitter blocked 7 of the 36 ACLU plaintiff web sites despite the fact that they had no RSACi measured objectionable content. Within this group, CYBERsitter particularly targeted gay web sites including "A Different Light Bookstore: Gay and Lesbian Literature" , "Planet Out", the "Queer Resources Directory" and "Gay Wired Wildcat Press." Cyber Patrol also blocked the "Gay Wired Wildcat Press," and Net Nanny joined CYBERsitter in blocking the "Queer Resources Directory." Among the five other gay sites within the purposive sample, all of which received 0 RSACi ratings, CYBERsitter blocked 4 and Cyber Patrol 2.

CYBERsitter also found objection with several feminist sites, blocking "Planned Parenthood" , the "National Organization for Women," and "Guerrilla Girls" a site devoted to feminist art. Once again, all of these sites had no RSACi rated objectionable content.

The five safe sex/Aids prevention web sites within the purposive sample were also blocked by several filters despite the absence of RSACi rated objectionable material. CYBERsitter blocked 4 of these sites, Cyber Patrol 2, and Net Nanny 1.

Off all of these overinclusive blocks, perhaps the most outrageous, and politically/educationally unjustified is Net Nanny's blocking of the White House web site!? Apparently one of the supreme representations of U.S. democracy is too dangerous for young Net Nanny users to access.

Combined Results

Combining all three of the web site samples described above into one large 200 site sample gives us an excellent overview of filter performance. As mentioned earlier, each sample is meant to represent one way in which average Internet users find information. As such, combining all three web site samples represents a rough approximation of the types of information a typical Internet user might come across in the process of surfing the web. While this combined sample is roughly reflective of average Internet use, the generalizability of results is limited due to low sample size, and a lack of completely randomized sites tested.

Among all 200 sites, a relatively high percentage had some form of objectionable content. Again, this is due to the presence of search term, and category areas relating to sex, hate sites, and violent games (see Table 4.8).

Table 4.8: All Samples Combined (N=200) Objectionable Content

	objectionable	**not objectionable**
language	27 (13.5%)	173 (86.5%)

nudity	19 (9.5%)	181 (90.5%)
sex	17 (8.5%)	183 (91.5%)
violence	7 (3.5%)	193 (96.5%)
any objectionable (all categories)	36 (18%)	164 (82%)

As shown in Table 4.8, 18 percent of sites contained some form of objectionable material. Based on this number, a perfectly operating filter should block the 18 percent of objectionable sites within the sample. In terms of overall percentage of sites blocked, Cyber Patrol achieves this goal, by blocking 18 percent of content. However, as we shall see, among this 18 percent, Cyber Patrol blocked a substantial proportion of non-objectionable sites. In other words, its 18 percent of blocked sites are not the 18 percent of objectionable sites in the sample. CYBERsitter is by far the most restrictive filter, blocking 25 percent of all content. SurfWatch and Net Nanny would seem to be underinclusive, blocking 14 and 6 percent of content respectively. Finally, 31 percent of sites were blocked by at least one filter.

Underinclusive and Overinclusive Blocking

Using highest RSACi score obtained as the independent variable, we can see how under and overinclusive each filter was in blocking content in the 200 site sample.

CYBERsitter did the best job of all filters by properly blocking 69 percent of objectionable material. Still this falls well short of its 90-95 percent

objectionable content block product claim. While CYBERsitter may do the best job blocking inappropriate content, it carries with it the worst record for overinclusive blocks. It blocked 15 percent of sites with no RSACi rated objectionable material (see Table 4.9).

Table 4.9: CYBERsitter Over - Underinclusive

	not objectionable	**objectionable**	**total**
not blocked	140 (85.4%)	11 (30.6%)	151 (75.5%)
blocked	***24*** ***(14.6%)***	***25*** ***(69.4%)***	49 (24.5%)
total	164 (100%)	36 (100%)	200 (100%)

Cyber Patrol places second in correctly blocking objectionable material 56 percent of the time. However, it also overinclusively blocked 9 percent of content with no objectionable material (see Table 4.10). Once again the caveat applies that Cyber Patrol includes gambling and alcohol categories in its blocking scheme, both content areas that received low RSACi ratings.

Table 4.10: Cyber Patrol Over - Underinclusive

	not objectionable	**objectionable**	**total**
not blocked	149 (90.9%)	16 (44.4%)	165 (82.5%)
blocked	***15*** ***(9.1%)***	***20*** ***(55.6%)***	35 (17.5%)

total	164 (100%)	36 (100%)	200 (100%)

SurfWatch failed to block 56 percent of objectionable content (see Table 4.11). A woeful score considering SurfWatch's product literature claims to block 90-95 percent of objectionable material. On the flip side, SurfWatch improperly blocked 7 percent of non-objectionable web sites, although this percentage may be artificially high because SurfWatch contains internal categories for gambling and alcohol.

Table 4.11: SurfWatch Over - Underinclusive

	not objectionable	**objectionable**	**total**
not blocked	152 (92.7%)	20 (55.6%)	172 (86%)
blocked	***12*** ***(7.3%)***	***16*** ***(44.4%)***	28 (14%)
total	164 (100%)	36 (100%)	200 (100%)

Finally, Net Nanny performed horrendously in blocking a measly 17 percent of objectionable content. However, of all filters, it blocked the least appropriate material, only blocking 3 percent of non-objectionable content (see Table 4.12).

Table 4.12: Net Nanny Over - Underinclusive

	not objectionable	**objectionable**	**total**
not blocked	159 (97%)	30 (83.3%)	189 (94.5%)

blocked	***5*** ***(3%)***	***6*** ***(16.7%)***	11 (5.5%)
total	164 (100%)	36 (100%)	200 (100%)

With all blocking decisions combined, filters correctly blocked objectionable material 75 percent of the time. On the other hand, they also overinclusively blocked 21 percent of non-objectionable material (see Table 4.13).

Table 4.13: All Filter Combined Over - Underinclusive

	not objectionable	**objectionable**	**total**
not blocked	129 (78.7%)	9 (25%)	138 (69%)
blocked	***35*** ***(21.3%)***	***27*** ***(75%)***	62 (31%)
total	164 (100%)	36 (100%)	200 (100%)

Discussion

Support for both of my under and overinclusive hypotheses was found in all three web page samples. Put simply, taken all together, filters fail to block objectionable content 25 percent of the time, while on the other hand, they improperly block 21 percent of benign content. If we assume the web has 320 million unique documents, filters would incorrectly block approximately 67 million pages (note: this inference has limited validity due to the lack of a truly random sample). Just imagine the outrage if your local library incorrectly removed 21 percent of its books, and then gave no explanation for their removal,

nor made public the book titles removed! This is exactly the reality created by the filters reviewed above.

These results point to a profound conflict for parents and policy makers considering the adoption of content blocking filters. They can purchase filters such as CYBERsitter and Cyber Patrol which correctly block large percentages of objectionable web content, but at the same time also block significant amounts of appropriate Internet material. These overinclusive filters cause particular damage to any content dealing with gays, safe sex information, and left leaning political groups.

If parents and policy makers are unhappy with overinclusive blocking they could go with SurfWatch and Net Nanny. Unfortunately, these products let through a tremendous amount of objectionable material.

This catch-22 situation brings the Supreme Court and President Clinton's support for content filtering into question. In Reno v. ACLU the Court noted that content filters were an effective, and less restrictive means for shielding children from objectionable content, while maintaining access to other non-dangerous content. Yet, as the results above show, filters are (1. not effective, and (2. not less restrictive. They fail to block access to significant amounts of pornography, hate speech, violence, etc., but at the same time make indefensible blocks of political sites such as the White House. Further, if sites have anything to do with important but controversial topics such as gay rights or safe sex, assume that they will be blocked.

Based on these tremendous problems, governmental outsourcing of the Internet Content Conundrum to filter makers should be seriously reconsidered. Similarly, parents should think twice about the benefit of spending $30, plus update fees, for products which will not protect children from significant portions of "dangerous" Internet material.

Methodological Improvements

To my knowledge, no other study has attempted to combine a content analysis with the blocking performance of Internet filters. As such, the results presented above represent a first attempt at using such a methodology. Future uses of this methodological framework would greatly benefit from several improvements.

First, a larger random sample of web pages (say 1,000+) would improve the generalizability of results. While this sounds straight forward, future researchers must develop a better way of achieving a truly random sample of pages. As mentioned earlier, the web is vast, and even the most powerful search engines can not index all of its content. Therefore, random links generated by search engines are only representative of the relatively small portion of the web indexed by a particular search engine.

Also associated with the idea of a larger random sample, is the fact that such a sample would likely contain little "objectionable" material that parents would want filtered. As such, it would fail to test filters against pornographic or violent content that filters are meant to block. This would point to the use of a second purposive sample, perhaps derived from usage statistics of what sites adolescents attempt to access. This test, although less representative of the overall universe of web pages, would be representative of the universe of pages that adolescents -- the group that filters are meant to protect -- typically attempt to view.

With regards to rating web content for "objectionable" material, it is possible that RSACi is not the best system. It only covers four categories, and some of its definitions are not particularly clear. This problem becomes evident when evaluating blocking decisions about alcohol and gambling related sites by

Cyber Patrol and SurfWatch. Both types of sites received non-objectionable RSACi ratings, but were blocked due to internal off limits categories in both filters. Basically, RSACi failed to capture the fact that alcohol and gambling sites may be dangerous to children. To remedy this flaw, a more inclusive system for rating Internet content should be developed. Similarly, future studies using RSACi as the coding system, should have better controls for additional, internal blocked content categories used by filters. Such controls would allow for a better assessment of overinclusive blocking.

A Note to Consumers

Compounding the failure of filters to live up to their claims of blocking 90-95 percent of objectionable Internet material, is the fact that most of these applications caused significant installation, use, and removal problems. It is important to note that the experiences described below were derived from personal experience on one computer, not a rigourous, multi-computer usability test that one might find in computer software trade magazines such as *PC World* or *MacWorld*.

From a use standpoint, CYBERsitter was by far the worst program. It crashed the computer it was installed on during installation. Once working (if that's the word for it) it constantly crashed when it encountered off limits sites. Finally, the program failed to remove properly, forcing a reinstallation of Internet protocols. Similar problems were encountered with Net Nanny, which after installation failed to properly import updated blocked site lists, and failed to work properly with the latest version of Netscape Communicator. Worst of all, Net Nanny failed to remove properly, and as a result corrupted my Windows NT operating system to the point that the machine could not boot properly. Compounding all of these problems, Net Nanny does not offer free technical

support! Cyber Patrol installed properly, but was unable to import updated blocked site lists. The only filter which experienced no problems during installation, use, and removal was SurfWatch.

If I were to recommend any of the filters tested above, I would point to SurfWatch as the best option. As just mentioned, it installed and operated with no problems. Further, it was extremely easy to set up. But most importantly, it struck the best balance between blocking objectionable content, and letting through benign material. SurfWatch performed admirably in not blocking the vast majority of sites related to gay rights, feminism, safe sex, and other controversial topic areas. Despite this endorsement, keep in mind that SurfWatch failed to block 56 percent of objectionable web sites.

When it comes to currently available commercial Internet filter software, the best advice is to have low expectations.

Chapter Five -- THE PICS PARADOX

Rating the Internet: Is PICS Any Better?

Another proclaimed solution to the Internet Content Conundrum, one supported by the Court, the White House, and industry was the development of

a descriptive universal rating system for content on the Internet. President Clinton compared the benefits of such a system to mandated "food safety labels."

Indeed informational labels are a part of everyday life. We see them at the grocery store, on cigarette packages, at the movies, and on video game and music album covers. Supporters of ratings claim that they merely objectively describe the content of what's inside a package, and therefore do not run afoul of the First Amendment, or contribute to censorship. Opponents however, argue that rating systems applied to subjective matters like media content, are inevitably biased, and when combined with market and government forces lead to wide-spread self and overt censorship. This chapter will look at the issue of rating systems through the lens of the Platform for Internet Content Selection (PICS), a protocol developed specifically to aid in the rating of Internet content.

PICS was developed by the World Wide Web Consortium (W3C) in 1995, and released in 1996. It was a direct response to the threat of CDA-like government regulation, a prospect the W3C, whose members are primarily drawn from the Internet industry, hoped to avoid. As the W3C notes, "PICS was spearheaded as a practical alternative to global governmental censorship of the Internet. In particular, it was created as a way to allow parents to select information that they consider acceptable for their children (W3C, 1996)."

How PICS Works

The Platform for Internet Content selection is in fact a number of protocols, which work in tandem to allow users to develop rating systems, distribute labels, write filtering rules, and digitally sign labels for verification and security. Each of these four functions is outlined by its own protocol, all of which are described below.

It is important to note that PICS is not itself a rating system or a filter. Instead, it merely puts forth a shared universal language for developing these tools. As W3C developer Jim Miller notes, "PICS establishes Internet conventions for label formats and distribution methods, without dictating a labeling vocabulary. It is analogous to specifying where on a package a label should appear, and in what font it should be printed, without specifying what it should say (W3C, 1996)."

Rating Services and Rating Systems (and Their Machine Readable Descriptions)

The most basic element needed to rate content on the Internet is some form of rating system. Such a system can be extremely simple, for example one which rates content by age appropriateness. Alternatively, a more advanced system, such as RSACi, can rate content along multiple categories, and multiple levels of severity. The PICS Rating Services and Rating Systems protocol allows for the description of such rating systems in a universally understood format (W3C, 1996). Within this protocol, a distinction is made between a rating system, which specifies the dimensions for rating content, and a rating service, which distributes content labels based on a rating system (labels and distribution are described below). So what does a PICS described rating system look like? Let's take a look at how RSACi's system is formatted using PICS.

Figure 5.1: RSACi Rating System Described in PICS format

```
1       ((PICS-version 1.1)
2       (rating-system "http://www.rsac.org/ratingsv01.html")
3       (rating-service "http://www.rsac.org/")
4       (name "The RSAC Ratings Service")
5       (description "The Recreational Software Advisory Council rating service.")
6       (default (label-only true))

7       (category
```

```
        (transmit-as "n")
        (name "Nudity")

8               (label
                        (name "None")
                        (description "No nudity or revealing attire")
                        (value 0))

9               (label
                        (name "Revealing Attire")
                        (description "Revealing attire")
                        (value 1))

10              (label
                        (name "Partial Nudity")
                        (description "Partial nudity")
                        (value 2))

11              (label
                        (name "Frontal Nudity")
                        (description "Non-sexual frontal nudity")
                        (value 3))

12              (label
                        (name "Explicit")
                        (description "Provocative frontal nudity")
                        (value 4)))
```

Lines 1-5 give basic descriptive information about the protocol version (PICS 1.1), and rating system/service (RSACi) to be described. Line 6 specifies that all labels must be accompanied by a description. Line 7 describes the RSACi category named "Nudity" which is to be transmitted as "n". Finally, lines 8-12 describe the 4 levels of RSACi defined nudity, and the corresponding value for each. The three other RSACi categories -- language, violence, sex -- are described in a similar fashion.

PICS Label Distribution Label Syntax and Communication Protocols

A rating system is of little use, unless its decisions can be expressed via content labels which can then be distributed to interested parties. The PICS Label Distribution Label Syntax and Communication Protocols specify the form which labels must take, and multiple methods for their distribution (W3C, 1996). Below is an example of a RSACi content label. This particular label is distributed via the use of a "Meta-tag", a piece of HTML which describes the contents of a page.

Figure 5.2: PICS Expressed RSACi Content Label

```
1   <META http-equiv="PICS-Label"
2   content='(PICS-1.1 "http://www.rsac.org/ratingsv01.html"
3   l gen false comment "RSACi North America Server"
4   for "http://www.rsactest.com/" on "1999.06.21T20:49-0800"
5   r (n 1 s 2 v 4 l 3))'>
```

Line 1 specifies that this Meta tag will describe a PICS label. Lines 2 and 3 describe the protocol version (PICS 1.1), and the rating system used. Line 4 specifies the site which has been rated and when it was rated. Finally, line 5 contains the actual RSACi rating; a 1 for nudity, 2 for sex, 4 for violence, and a 3 for language.

Two other options are available for the distribution of labels. First, rather than be embedded in the HTML of a particular web page, a label can be stored in a server side database. When a user requests a particular document, and also requests a label for that document, the web server hosting the page exchanges the label within the HTTP transaction.

The final method for distributing content labels is through the use of a label bureau. A label bureau is a server which contains PICS labels of *other* sites

on the Internet. For example, the Chris Hunter label bureau, which resides at http://www.upenn.edu/ , contains content labels for other sites such as http://www.sex.com/ . If a parent is wary of a page, he/she can turn to a trusted label bureau (say developed by the PTA) which will deliver a label for that page. Note that label bureaus, much like traditional blocking software described previously, can rate a site without the developer of that site having any input. Below is an example of a label bureau request.

Figure 5.3: Label Bureau Query

Client sends request to server:

```
1       GET /ratings?opt=normal&format=full&
2       u="http%3A%2F%2Fwww.w3.org%2Fpub%2FWWW%2F+&"
3       s="http%3A%2F%2Fwww.rsac.org%2Fv1.0&"
```

Server responds to client:

```
4       HTTP/1.0 200 OK
5       Content-Length: 569
6       Content-Type: application/pics-labels
7       Server: Jigsaw 0/0
8       Date: 15 Apr 1996 18:20:54 GMT

9               (PICS-1.1 "http://www.rsac.org/v1.0"
10              labels for "http://www.w3.org/pub/WWW"
11              generic true
12              by "abaird@w3.org"

13              ratings (v 0 s 0 n 0 l 0)
```

Line 1 requests that a label be obtained for the site listed in line 2, using the label bureau (RSACi) specified in line 3. Once the request is made, the RSACi label bureau responds with a rating for the requested site, lines 4-13.

PICSRules

Solely labeling web content is not enough to prevent access to a particular page or site. Instead, filters must be written which understand PICS-based labels, and can make blocking decisions based on those labels. PICSRules specifies the format for writing PICS compliant filters (W3C, 1997). Figure 5.4 displays a sample PICS-based filter rule.

Figure 5.4: PICSRules Described Filter

```
1       (PicsRule-1.1
2       ( name    (rulename "Example 4"
3               description "Example 4 from PICSRules spec; simply shows
                how PICSRules rules are formed.")

4       ServiceInfo ("http://www.rsac.org/ratingsv01.html"
5               shortname "RSACi")

6       Policy (RejectByURL
                ("http://*@www.badnews.com:*/*"
                "http://*@www.worsenews.com:*/*"
                "*://*@18.0.0.0!8:*/*"))

7       Policy (RejectIf "(RSACi.violence >= 3)"
                Explanation "Excessive violence.")

8       Policy (AcceptIf "otherwise") ) )
```

Line 1 states the protocol to be used (PicsRule 1.1). Lines 2 and 3 note the rule to be developed, and a brief description of it. Line 4 notes the rating system the filter rule will use (RSACi). Line six describes a set of outright blocked URL's. These sites will be blocked regardless of their RSACi label. Line 7 states that any site with a RSACi score equal or greater than 3 will be blocked. Finally, line 8 specifies than any site not meeting the above criteria will be let through.

Far more complex filter rules can be written using PICSRules. For example, in addition to using embedded ratings within a self rated site, a filter

could request alternative ratings from a third party label bureau. A filter could also be programmed to block all pages not rated using a particular rating system.

PICS Signed Labels (DSig)

Two problems can occur with the security of a PICS label. First, a label could be tampered with so that its rating does not match the initial rating provided by a self rated page or by a third partly label bureau. Second, it could be possible for a malicious server to forge the labels of another group, and pass them off as originals. Both of these problems are solved by a cryptographic extension to PICS known as DSig (W3C, 1998). DSig allows label creators to (1. sign a label to verify its internal accuracy, and (2. sign a label to verify that it came from a particular web server.

PICS in Plain English

The above discussion of how PICS works may be overly complex and confusing for non-computer scientists, non-engineers, and Internet novices. As such, a much simpler description of what PICS does, and how it actually works in practice is provided.

The PICS standard basically creates a universal language to describe Internet content. The PICS standard allows for a number of features:

1. The development of numerous rating systems to label content along any number of criteria. (the *Rating Services and Rating Systems* protocol)

2. Individual web content providers can select a PICS enabled rating system and voluntarily self rate their site. (using labels specified by the *PICS Label Distribution Label Syntax and Communication Protocols*)

3. Third parties like the Christian Coalition, or the ACLU can create label bureaus to label sites according to a PICS enabled rating

system. (again using the *PICS Label Distribution Label Syntax and Communication Protocols,* but using a different distribution method; a label bureau)

4. Software developers (Netscape, Microsoft, Cyber Patrol, etc.) can use PICSRules to write filters that understand and process PICS-based labels.

5. Verification of label accuracy and source. (the *DSig* protocol)

If a software filter is programmed to interpret PICS labels, it can make blocking decisions based on the description of a web page's content. As of 1999, both Netscape Communicator (in its NetWatch feature) and Microsoft Internet Explorer (via Content Advisor) support PICS-based filtering. Of the filters reviewed in the last chapter, both Cyber Patrol and SurfWatch can process RSACi labeled sites.

A parent would use PICS to filter a child's access in the following way: Using a PICS compatible filter, the parent selects a trusted rating system, say the MPAA's. The child then begins to surf the web and requests a self rated site labeled G. The filter grants access to the site because the parent has told it that G rated material is allowable. The child continues to surf, and requests a site that has not self rated. The filter program then requests a rating of that site (if it is available) from the MPAA's third party label bureau. The MPAA bureau returns an R label for the requested site, and the site is blocked because the filter was configured to deny access to R labeled sites.

This example shows the flexibility of PICS, which allows for both self and third party content rating. On the user's end, the software filter can be programmed to use any PICS enabled rating system. Further, if a requested site is not self rated, the filter can then request a rating from a third party label bureau. Figure 5.5 (Resnick, 1998) gives a graphical representation of how a

PICS enabled filter might work. Figure 5.6 (Salamonsen & Yeo, 1996) shows how a PICS enabled proxy server can filter Internet access for downstream network users.

Figure 5.5: PICS Enabled Client Filter

Figure 5.6: PICS Enabled Proxy Filter

Problems With PICS

While the benefits of PICS are many, especially for end users who can potentially choose from numerous rating systems, PICS also raises a number of troubling concerns.

First, just like private blocking software, PICS enabled filters are still quite difficult to use. While PICS is promoted for its ability to allow the end user to select from a wide range of rating systems, actually installing and configuring these systems is not as easy as it may seem. Therefore, users are likely to accept the default rating system that comes with the filter. As Michael Froomkin notes, "Users are empowered to choose who will make their choices, but the system is

sufficiently complex to discourage the average person from making their own choices (cited in Stutz, 1997)."

Another problem with PICS "user choice" argument, is that there really are not that many rating systems to choose from. So far, only RSACi and SafeSurf have created well known rating systems (Lasica, 1997). In fact, Communicator and Internet Explorer filter modules are by default set to accept RSACi and SafeSurf labels. This situation is unlikely to change as there are no great economic incentives for groups to develop PICS based rating systems. For example, RSACi initially hoped to charge web sites who rated their content with RSACi's system, but they have since dropped this business model.

The same argument is true for third party label bureaus. Simply put, it requires a great deal of time and effort to label the millions of sites available on the web. The vast size of the web creates an economic disadvantage for the very groups that the W3C hopes will develop label bureaus. For example, the W3C speaks of a liberal ACLU-like label bureau developing to offset the effects of a conservative Christian Coalition-like label bureau (Resnick, 1998). However, it is likely that very few groups will have the time and the money to develop extensive label bureaus. As a result, the Internet industry may standardize around one rating system and one label bureau, thus implicitly accepting the biases of that system and the organization behind it. As mentioned earlier, industry is already leaning towards RSACi which is an outgrowth of the Software Publishers Association (SPA) and received start up money from IBM and Microsoft. Therefore, it is not too much of a stretch to argue that RSACi will aim for a homogenized, business friendly version of the Internet that pushes "messy" and controversial forms of content to the periphery.

Continuing with the theme of rating systems and label bureaus, PICS does not force either of these to reveal the criteria by which they rate content.

Although the W3C encourages such disclosure, there is nothing built into the PICS specification which requires it (Reagle and Weitzner, 1998).

Yet another problem that stems from one particular rating system like RSACi gaining too much power, is the fact that sites may feel compelled to self rate. The W3C promotes PICS as a voluntary standard, but this may well be wishful thinking (Reagle and Weitzner, 1998). For a filter to be truly effective, it must block access to all sites that are not rated, as well as sites rated using a different standard. Thus, if RSACi gains the upper hand as a rating system, a web site developer may feel compelled to rate according to the standard, even if he/she would rather rate using another standard. If the developer chooses not to rate or to use a different system, he/she risks being blocked by the majority of software filters.

This brings up another troubling point about rating systems. Again consider that RSACi has become the industry standard. As a result, site developers are basically compelled to self rate if they want their site to be seen by a wide audience. But how should a site dealing with the Holocaust rate itself? RSACi provides four classification categories: violence, nudity, sex, and language. Pictures and content regarding Nazi death camps are likely to contain a good deal of both violence and nudity. However, if a site operator rates this information accordingly, it will likely be blocked by most filters. After all, parents will try to shield their children from sites with excessive nudity and violence. But would parents really want to block access to a Holocaust information web page based on these overly simplistic criteria? As Jonathan Wallace, the creator of a Holocaust information page notes, "ratings systems which lump an Auschwitz Alphabet together with the Hot Nude Women Page ignore this distinction (1996)."

This problem would likely present itself with all sorts of controversial material. How should a gay rights page be rated? What about a safe sex site? What about the news? It certainly contains plenty of sex and violence. This very problem was confronted by MSNBC, which in 1996 pledged to use RSACi to rate all of its news content. However, MSNBC editors soon came to the conclusion that "news is not something that can be rated (Lasica, 1997)." To ameliorate the problem of news content, the Internet Content Coalition, an organization representing Internet content producers such as MSNBC and the New York Times, proposed creating a new RSACi "news" category which would be exempt from ratings. On the surface, this may seem logical, but who decides what is news and what is entertainment? As Joshua Quittner of Pathfinder comments, "You can't define news on the web since everyone with a home page is a global town crier (in Lasica, 1997)." Once again, rating systems can not account for such subtleties. Adding to the strange character of Internet content rating, is the fact that in the physical world, all of these topics would not need to rate themselves to be available. As the ACLU notes, "Imagine being forced to wear a sandwich board that says 'violent and sexual content' if you want to stand on the street and hand out a pamphlet on domestic abuse (1997)."

Based on these concerns, it is reasonable to conclude that like blocking software, PICS is not a "less restrictive alternative" to the CDA. PICS has the potential to block far more speech than would the CDA, and again no justification would need to be given for these decisions.

An analogy to the dangers of PICS, are the experiences of the movie (MPAA ratings), music (Parental Advisory Labels), and video game industries (RSAC and others), each of which uses a "voluntary" rating system. All of these industries adopted ratings due to intense social and political pressure to limit access to bad language, sexual content, and excessive violence. While these

rating systems are referred to as voluntary, each industry essentially felt compelled to adopt ratings to avoid direct governmental regulation. A similar situation has recently occurred with the V-chip for television programming. Congress essentially told the television industry that if they did not create an acceptable rating system (acceptable to the FCC and thus the government), that it would impose its own system. How voluntary is a system where the government tells you "do this or else?" As Smolla notes, "If there is a case to be made against what the FCC did with regards to children's television, it must be not the goal but the method of using governmental power and leverage to exact concessions from the private sector (1997)."

Once these concessions, in the form of ratings, are made, proponents claim that they are merely "intended to provide information for parents (cited in Roberts, 1997)." However, such systems have been combined with market forces and state regulations to outright censor media content. In the U.S. record industry, about 10 percent of all music is sold by Walmart, which will not carry records that have advisory labels. This has forced many popular musicians to rewrite their songs in order to be "approved" by Walmart. Similarly, several states including Georgia, Washington, and Tennessee have attempted to pass laws banning the sale of labeled records to minors. As Lasica notes, Parental Advisory Labels which "started out as a tool for parental empowerment turned into an effective means of censorship (1997)." A similar situation has occurred in the movie industry where any film given an NC-17 rating will not be carried by theaters. This has led numerous directors to "soften" their work to receive an acceptable R-rating (Taylor, 1998). Additionally, many states are now considering laws that would make it illegal for underage children to be admitted to R-rated films. Once again, "informational" and "voluntary" ratings may lead

to state sanctioned censorship. Could PICS be the technology that will send the Internet down this same road?

While content advisory labels on records and movies may have led to some censorship, they do not compare with the massive censorship that PICS makes possible at all levels of implementation. As Lawrence Lessig comments, PICS is "the devil" because:

> It not only allows any number of filters to be selected among; it also allows these filters to be imposed — invisibly — at any level in the distributional chain. The filter can be imposed at the level of the individual's computer. But it can also be imposed at the level of the ISP. Or at the level — in principle — of a nation-state. PICS doesn't discriminate in favor of local control, or against centralized control. (1998, p. 40)

Because PICS contains no assurance that it will only be used at the individual user's level (downstream filtering), it will almost definitely be used by upstream network groups like ISPs, schools, or governments. When implemented upstream, the end user has no idea what he/she is missing while surfing. Instead, blocking decisions occur automatically and invisibly, perfectly enforcing the rules of the upstream organization. While this may sound a bit dramatic, several countries are already looking into implementing PICS as a global content filtering mechanism. Both China and Singapore, who already have state sponsored Internet filtering regimes, have shown great interest in PICS. So has the European Union (EU), which is seeking to create its own PICS based rating system. The EU will then force all member nations ISPs and content providers to rate according to this standard, and to distribute PICS compliant filters to end users (EU Green Paper, 1996). Finally, and most drastically, Australia recently passed the Online Services Act which legally forces Australian ISP's to remove any native Internet content rated X or RC (refused classification) by the Australian Broadcasting Authority (ABA), their equivalent of the FCC (Taggart,

1999). The law further calls for Australian ISP's to develop procedures to monitor, filter, and block international content that may not be acceptable to the ABA. While the law does not specifically call for the use of PICS, the ABA has in the past endorsed it as the best technology for developing national proxy servers and content filters (Kruger, 1998). As such, it would seem quite possible that Australian ISP's will create PICS-proxies, and PICS enabled label bureaus to aid in filtering international content.

If nation states and intergovernmental groups do choose to move forward with implementing their own PICS based rating systems, this raises a serious problem for the international flow of data across the Internet. The reason being that different nations may adopt different rating systems, and as a result their filters will be forced to block the unknown rating systems of other countries. This situation would run directly counter to the ideal of the Internet as an international communications network which ignores physical borders. Indeed, PICS could make borders in cyberspace just as tangible and enforceable as real world borders.

Governments using PICS to build borders in cyberspace points to what I call the PICS Paradox. The paradox is that the W3C developed PICS to avoid "global governmental censorship." However, left only to the market, PICS has failed miserably as a protocol. Because few rating systems and rating bureaus have developed, few web sites have self rated their content. RSACi, by far the most popular rating system, claims that only 100,000 sites have self rated using the standard, less than one percent of the web. Corresponding to this lack of rated sites, is a lack of PICS compliant filters. This shows that on its own, PICS will fail as a market alternative to government action. Therefore, governments will be incented to step into this vacuum and require that web sites and ISP's self rate and develop filters using the PICS standard. In other words, the only way

for PICS to be widely implemented is if governments, via regulation, require its use. In essence, the W3C's logic behind PICS has been turned on its head. Given the right circumstances, like what is happening in Australia and the EU, PICS would seem the perfect tool of government censorship, not an alternative to it.

While nation level "upstream" PICS filtering has yet to occur in practice, the same can not be said for search engine filtering. Search engines like AltaVista, Excite, Lycos, etc., are at the very heart of the Internet, and in a way their query results define the universe of the Internet, and thus where net citizens can travel. It is therefore very troubling that one of the most popular search engines, AltaVista, has implemented PICS filtered search results. Using the PICS enabled rating database of Net Shepherd (which claims to have rated 97 percent of English language web sites), a special "Family Search" AltaVista will only return results which meet an end users filtering criteria (AltaVista, 1997). This results in 95-99 percent of Internet sites otherwise available via an unfiltered AltaVista search being blocked by Net Shepherd. For example, an unfiltered AltaVista search for "Thomas Edison" produced 11,522 hits. Using "Family Search" only 9 hits were returned (EPIC, 1997). Although "Family Search" is a specialized version of AltaVista, it demonstrates that PICS-based search result filtering is possible. This represents yet another form of invisible upstream filtering, where the end user will have no idea what he/she is missing (Lessig and Resnick, 1998, p. 18).

In short "A fully PICS enabled world will be a world with more censorship of speech than a fully CDA enabled world (Lessig, 1998, p. 41)." Just as with blocking programs, PICS is not a "less restrictive alternative." Instead, "PICS could be the most effective global censorship technology ever designed (Garfinkel, 1997)." Despite this all to real potential, President Clinton and the

W3C continue to push PICS as a parental empowerment tool that will work far better than any government regulation.

The Great W3C Cop Out: PICS, Values, and Poor Assumptions

The W3C claims that PICS is a value neutral technology (Resnick & Miller, 1996). To a certain extant this is quite true. Essentially PICS creates an alphabet that others can use to develop their own rating languages. While it is true that an alphabet is value neutral, what is not, are the assumption that the W3C had about how PICS would be implemented. The W3C assumed that multiple ratings systems and label bureaus would arise, and that this would counter secretive and overzealous censoring groups. However, as discussed above, their are no economic incentives for groups to develop multiple rating systems, and already the web community is coalescing around RSACi. The W3C should have studied the example of movie ratings, where for the past 30 years, we have had one, and only one rating system, the MPAA's. This fatal flaw in the W3C's logic shows that PICS is not really value neutral. Combined with assumptions about use, PICS takes on a sociopolitical reality that has consequences. Unfortunately, much like the NRA's argument that people kill people, not guns, the W3C says "we created the technology, its not our fault that mean governments and businesses use it to censor expression." However, it is the very failed assumptions made by the W3C that make PICS a potential tool for global censorship. This reality would seem to run counter to the W3C's stated mission to "realize the full potential of the web (1998)."

In developing PICS, a social protocol which makes assumptions about human use and values, the W3C essentially legislated by code. Yet, this legislation was written by engineers representing industry, with no public, legal, or governmental oversight. As such, the W3C acted as an extra-governmental

sovereign, writing laws and rules that effect all nations using the Internet (Reidenberg, 1998). But unlike traditional sovereigns who are responsible to their citizens and to other nations, the W3C operates without such checks (Garfinkel, 1998). This lack of openness and responsibility at an increasingly powerful organization does not bode well for the future of democracy and free speech in the digital future. A potential answer to this problem is transparency, a topic we will explore in greater depth in Chapter Seven.

Chapter Six -- LIBRARY AND SCHOOL FILTERING

Cyberspace Filtering Meets the Real World

The many problems associated with filters and PICS make them less than perfect parental empowerment tools. However, when these filtering technologies are introduced into public, government sponsored institutions, tremendous ethical and constitutional problems are raised. Perhaps the most interesting and instructive example of where cyberspace technologies meet real world information use is occurring in our nations public libraries and schools.

These cornerstones of our democracy are currently engaged in a debate about the use of filters to protect minors from potentially harmful material. More than a decision about what filter program to use, the debate over filters in libraries and schools raises fundamental questions about the core nature and purposes of these institutions. Therefore, decisions made about filtering Internet access will have profound implications for information access, education, and academic freedom.

The Library Filter Debate

Long before computers or the Internet, libraries were faced with the challenge of providing access to "adult" books and material, while at the same time protecting the morals of children and having to answer to the concerns of their larger community. Libraries in the 1920's struggled with purchasing decisions regarding "pornographic" fiction like *Lady Chatterley's Lover*, *Ulysses*, *Madame Bovary*, and *The Arabian Nights* (Cornog and Perper, 1991). In more recent times, libraries have debated the purchase of adult magazines like *Playboy*, and in the case of the Library of Congress, the translation of *Playboy* into braille (Cornog, 1991). And now, with over 60 percent of U.S. public libraries having access to the Internet (NCLIS, 1998), libraries are faced with yet another "tough call"; allow unfettered access to information on the net, or use filters to block minors access to sexually explicit material. This situation is further complicated by the fact that public libraries are governmental institutions.

Those who support filtering Internet access in libraries note that libraries have always acted as filters. Through purchasing decisions, librarians "evaluate, analyze, and authenticate" information and materials. They further choose how that information will be displayed within a library. These "information quality" decisions are at the very core of the library profession (Bastian, 1997).

Advocates of library filtering also argue that libraries make selection choices which reflect prevailing community norms. Further, these choices are supported by the tax dollars of community members. As such, library filtering advocates argue that libraries should block material that the communities they serve find harmful or offensive. Expressing this opinion, Robert Peters of Morality in Media notes, "If libraries allow access to porn, even for adults, then the public will be subsidizing a peep-show booth (in Macavinta, 1997)." Similarly, K.I.D.S., a group of concerned parents in California argues that "allowing use of public facilities for the display and distribution of pornography is a disorder and violation of public trust (1998)."

So, if librarians traditional role has been as a community sensitive information filter for tangible books, magazines, etc., why shouldn't they filter Internet access?

The simple answer, as abundantly illustrated in previous chapters, is that blocking programs take information selection decisions out of the hands of librarians, and put them into the unknown blocking criteria of a particular program. As discussed earlier, blocking software makers often refuse to reveal which sites they choose to block and the criteria by which such sites are deemed off limits. Michael Sims of the Censorware Project dramatically illustrating this problem in the following hypothetical:

> Imagine if you had written your Great American Novel, and found it banned from public libraries because it contained full frontal nudity and graphic description of sexual acts. But it didn't. And this gross error couldn't be corrected. The library told you they subscribed to a list, managed by a private company, which even they couldn't look at, which determined what books they would make available, and it seems that your novel wasn't on it. Every morning, the company employees came in with two big black bags. They put some books on the shelves from the one bag, and removed unknown books from the shelves and took them away in the other, and wouldn't respond to any queries about why

> YOUR book was called "pornography" and had been taken off the shelves. You would be fighting mad in short order, I imagine. This is precisely the situation with implementing censorware in libraries today. (1998)

At a more fundamental level, many library's argue that their purpose is to promote free speech, a goal they achieve by providing free books to individuals regardless of their age or income. However, using software filters which they have no control over, libraries will inevitably block access to a wide range constitutionally protected speech. This runs afoul of both library tradition and the First Amendment. Realizing this potential danger, the American Library Association (ALA) has come out strongly against filtered library Internet access:

> Libraries are places of inclusion rather than exclusion. Current blocking/filtering software prevents not only access to what some may consider "objectionable" material, but also blocks information protected by the First Amendment. The result is that legal and useful material will inevitably be blocked. (July 1997)

Despite this stance, local public libraries in Massachusetts, California, Texas, and Virginia have decided to install blocking software (Hafner, 1998), and according to the 1998 National Survey of Public Library Outlet Internet Connectivity, 15 percent of libraries use some form of Internet filter. This decision is usually in response to public pressure regarding the easy availability of sexually explicit speech on the Internet.

By far the most publicized case of library filtering occurred in Loudoun County, Virginia where in October 1997, the library's board of trustees decided to install blocking software on all public Internet terminals. They did so in fear of legal prosecution for making obscene material available to minors, as well as sexual harassment suits by employee's forced to view "objectionable" material on library computer screens (Macavinta, 1998). In its final form, the library's "Policy on Internet Sexual Harassment" stated that county public libraries would

provide Internet access to patrons subject to the following restrictions: (1) the library would not provide e-mail, chat rooms, or pornography; (2) all library computers would be equipped with site-blocking software to block all sites displaying: (a) child pornography and obscene material; and (b) material deemed harmful to juveniles; (3) all library computers would be installed near and in full view of library staff; and (4) patrons would not be permitted to access pornography and, if they do so and refuse to stop, the police may be called to intervene (cited in Mainstream Loudoun, et. al. v. Board of Trustees of the Loudoun County Library, 1998).

In order to implement its new policy, the library choose to purchase Log-On Data's "X-Stop" filtering program. According to X-Stop marketing material specifically targeting libraries, the program only blocked sites deemed legally obscene under the Supreme Court's *Miller* (1973) test. Doubting the accuracy of such claims, a local community group, Mainstream Loudoun, asked lawyer Jonathan Wallace to test the program. Similar to results discussed in previous chapters, Wallace found that X-Stop blocked far more than legally obscene Internet material. In his "The X-Stop Files (1997)", Wallace found that the program blocked the following non-obscene, non-pornographic, and non-violent material:

- The University of Chicago's Fileroom project, which tracks acts of censorship around the world.
- The National Journal of Sexual Orientation Law, which describes itself as devoted to "legal issues affecting lesbians, gay men and bisexuals."
- The Banned Books page at Carnegie Mellon, which gives a historical account of the travails of books such as Candide and Ulysses.

- The American Association of University Women, which describes itself as a national organization that "promotes education and equity for all women and girls."

- The AIDS Quilt site, for people interested in learning more about HIV and AIDS, with statistics on the disease and links to other relevant sites.

- The Heritage Foundation, a conservative thinktank whose mission is to "formulate and promote conservative public policies based on the principles of free enterprise, limited government, individual freedom, traditional American values, and a strong national defense."

- The Religious Society of Friends, better known as the Quakers.

- Quality Resources Online, a clearinghouse for books and other materials relating to quality in business operations.

Angered by such decisions, four months after the passage of the library access policy, People for the American Way, representing Mainstream Loudoun, filed suit claiming the new policy was an unconstitutional restriction of patrons free speech rights. The ACLU joined the suit, Mainstream Loudoun, et. al. v. Board of Trustees of the Loudoun County Library, which was settled in Federal District Court in November 1998.

In the Court's decision, Judge Leonie M. Brinkema struck down the library's filtering policy, arguing that it failed a number of First Amendment tests designed to protect free speech. First, Judge Brinkema concluded that the policy was a government sponsored content based regulation of speech which must meet the "strict scrutiny test" to be deemed constitutional. Much like the *Renton* test described in Chapter Two, strict scrutiny asks if a government regulation (1. serves a compelling state interest, (2. whether the limitation is necessary to further those interests, and (3) whether the limitation is narrowly drawn to achieve those interests. As in the CDA, the court found that protecting children

from pornography was indeed a compelling interest. Despite this, the Loudoun County policy was not necessary, because as the court found, only one library patron had complained about a child viewing pornography. Further, an expert witness at the trial could only cite three other examples of such problems occurring in libraries outside of Virginia. As Judge Brinkema notes:

> As a matter of law, we find this evidence insufficient to sustain defendant's burden of showing that the policy is reasonably necessary. No reasonable trier of fact could conclude that three isolated incidents nationally, one very minor isolated incident in Virginia, no evidence whatsoever of problems in Loudoun County, and not a single employee complaint from anywhere in the country establish that the policy is necessary to prevent sexual harassment or access to obscenity or child pornography.

Finally, and akin to the argument made throughout this thesis, the court found that X-Stop was not the least restrictive method of implementing the county's desire to protect children from Internet pornography. Instead, Judge Brinkema listed privacy screens, librarian monitoring, and installing filters on selected child access computers (as opposed to all computers), as less restrictive alternatives.

Not only did the Loudoun County policy fail strict scrutiny, it was also deemed a prior restraint, as it blocked access to constitutionally protected speech without giving any blocking criteria, nor a well defined procedural mechanism for reviewing blocking decisions. Noting the complete lack of blocking criteria Judge Brinkema concludes:

> The degree to which the policy is completely lacking in standards is demonstrated by the defendant's willingness to entrust all preliminary blocking decisions -- and, by default, the overwhelming majority of final decisions -- to a private vendor, Log-On Data Corp. Although the defendant argues that X-Stop is the best available filter, a defendant cannot avoid its constitutional obligation by contracting out its decision making to a private

> entity. Such abdication of its obligation is made even worse by the undisputed facts here. Specifically, defendant concedes that it does not know the criteria by which Log-On Data makes its blocking decisions. It is also undisputed that Log-On Data does not base its blocking decisions on any legal definition of obscenity or even on the parameters of defendant's policy.

Anti-library filtering advocates have claimed the Loudoun decision as a major victory. However, a closer look reveals that it only settled a relatively narrow issue. The Loudoun County policy required that *all* library computers utilize filters, regardless of whether they were used by adults or children. The Court overturned this rule as overbroad, but in its own ruling noted that filters may be appropriate if installed on computers designated only for children. This raises the question of how many computers in a library should be filtered. What if a library in a particularly conservative area installed filters on all but one computer, and the sole unfiltered computer was placed directly adjacent to the head librarian's office? Would this regulation, which would likely intimidate adults from accessing controversial material be constitutional?

Also unanswered is the constitutionality of filters installed only on child access computers. As we have seen, filter programs block large amounts of completely innocuous material. Is the court willing to accept this collateral damage to protect children from the much smaller percentage of pornographic and obscene material on the Internet? Also, should filters be tailored for certain age groups? For example, a teenager would likely benefit from access to a safe sex page, but would such access be appropriate for younger users? At what age should this distinction be made? In many conservative communities parents might even conclude that teenagers should not access safe sex sites at all.

Another alternative to filtering, not mentioned in the Loudoun case, but supported by the ACLU, the ALA, and the NCLIS is the utilization of

"Acceptable Use Policies." The NCLIS, whose mission is to asses the library needs of U.S. citizens, has gone so far as to pass a resolution urging the use of such policies:

> The U.S. National Commission on Libraries and Information Science feels strongly that the governing body of every school and public library, in order to meet its trustee responsibilities, should establish, formally approve, and periodically review a written acceptable use policy statement on Internet access. (1998)

Acceptable use policies generally outline a series of requirements which users must agree to in order to use library Internet facilities. Such policies are in place at 62 percent of U.S. public libraries (NCLIS, 1998). For example, my home town library, which does not filter access, requires all patrons who wish to use the Internet to agree to the following rules:

> Regulations Governing Patron Use of Computer Workstations at Lincoln Public Library:
>
> 1. All users must have a valid library card.
>
> 2. Computers may be used by the public age 10 and over. Younger children must be supervised by an adult.
>
> 3. A parent or guardian's signature is required for those under 18.
>
> 4. All users must sign up at the circulation desk prior to using one of the workstations.
>
> 5. Misuse or abuse of the computer workstations will result in suspension of the user's computer access privileges.

On the surface, these rules seem quite reasonable. However, rules 4 and 5 present troubling free speech issues. First, why should patrons be forced to sign up before using the Internet? This could allow librarians to develop profiles of what this or that patron accesses. In turn, this could create a chilling effect for

patrons who research controversial material that librarians might frown upon. More troubling is the complete lack of definition of "misuse or abuse" in rule 5. What does this mean? Would viewing pornography, or hate speech, or bomb making sites be considered an abuse?

While not included in Lincoln Library's policy, many others including the Boston and New York public libraries contain a rule forbidding computer use for illegal activities. Presumably this includes accessing obscenity and child pornography. But how is a librarian to know if such material is obscene? For any content to be found obscene it must meet the *Miller* test in a court trial. Despite this, one can envision a situation where an overzealous librarian will claim that a merely pornographic web site is in fact obscene, and then revoke a patron's Internet privileges.

These examples, taken directly from currently existing library acceptable use policies, show that such rules are often inherently vague. In many ways, this vagueness is equivalent to the opaque categorization rules used by filter makers. In a sense, acceptable use policies, if not well defined, merely substitute vague code with vague written policy.

All of these problems will only get worse as the remaining 40 percent of U.S. public libraries come on-line. As such, the wrenching debate illustrated in the Loudoun case, will likely be repeated many times over in the years to come.

The School Filter Debate

Like libraries, public schools are confronted by multiple goals which are often in direct conflict. The primary goal of education, and the reason it is compulsory, is the creation of informed citizens, capable of the autonomous thought and action necessary for a vibrant democracy. To achieve this goal, schools must provide students with wide access to ideas, even those which may

be offensive and contrary to prevailing opinion. Schools must also give students the chance to explore any topic and ask any question, practices enshrined in the ideal of "academic freedom." Through such open access and inquiry, education allows students to define their own ideas and beliefs, and to critically weigh those of others.

Competing with the notion of open inquiry is the responsibility schools have to local communities and local values. This responsibility is set forth by the thousands of local school boards, who representing the views of their community, choose which topics to teach and what books to buy. Given this system, liberal school districts may teach sex education and evolution, while more conservative districts have the latitude to exclude such subjects as contrary to community norms. In this way, education is also about indoctrination into the norms and values of the surrounding community. Indoctrination clearly seems antithetical to open inquiry, where nothing is sacred and all norms are open to investigation. The Court has noted this paradox, commenting in James v. Board of Education (1972) :

> Society must indoctrinate children so they may be capable of autonomy. They must also be socialized to the norms of society while remaining free to modify or even abandon those norms. Paradoxically, education must promote autonomy while simultaneously denying it by shaping and constraining present and future choices.

Given these somewhat contradictory goals, what are schools to do about the Internet? The Internet clearly facilitates near limitless access to information of all stripes and colors. At the same time, this very access has the potential to expose students to content which is contrary to community norms. Not surprisingly, many schools have turned to filters as a way of balancing access with indoctrination. As of 1998, 89 percent of public schools had access to the

Internet (National Center for Education Statistics, 1999), of which 39 percent used filtering software (Quality Education Data, 1998). As we have seen first hand, filtering programs block significant amounts of constitutionally protected speech in the process of blocking the "harmful" material that school systems rightly purchase filters to deal with. But is this situation constitutional? Is it a violation of students free speech rights to block whitehouse.com (a pornography site), while also blocking whitehouse.gov? What latitude do school administrators have in determining what Internet content is not acceptable to community norms and therefore subject to blocking?

A partial answer, or at the very least a guide to these questions is provided by a case settled before any schools had Internet access. In Board of Education v. Pico (1982), a New York school board removed a number of books from a school library for being "anti-American, anti-Christian, anti-Semitic, and just plain filthy." Students sued the school for violating their First Amendment right to information. The Court affirmed this right, noting that "just as access to ideas makes it possible for citizens generally to exercise their rights of free speech and press in a meaningful manner, such access prepares students for active and effective participation in the pluralistic, often contentious society in which they will soon be adult members." The Court further recognized that especially within the context of a school library, "a student can literally explore the unknown, and discover areas of interest and thought not covered by the prescribed curriculum . . . The student learns that a library is a place to test or expand upon ideas presented to him, in or out of the classroom." While the court did note that schools have wide discretion in selecting material appropriate for classroom curriculum, it could not exercise this power "beyond the compulsory environment of the classroom, into the school library and the regime of voluntary inquiry that there holds sway."

The *Pico* case would seem to imply that school administrators can filter access to the Internet if it is part of a predefined classroom curriculum. In essence, filters would mirror a school board's power to decide what text books are appropriate. However, if schools grant students unsupervised time to simply "surf the net" for research purposes, therefore not part of a predefined lesson plan, than filtering would not be permissible. As Kubota (1997) notes, "The freedom of choice enjoyed by students while browsing the Internet is analogous to students searching the library and voluntarily choosing books of interest. Schools can not claim to have any real curricular control over such an open-ended, free wheeling, and unsupervised activity (713)."

No case has yet challenged the constitutionality of school filtering. Despite this, a fascinating case study of Utah schools raises the question if schools need to filter access at all? In 1996, the Utah Education Network (UEN), which represents all 40 Utah public school districts and 8 public libraries, implemented SmartFilter, a proxy based content filtering program. These schools and libraries all gain access to the Internet through this proxy system. To examine SmartFilter's utility, and the general need for such a product, the Censorware project obtained UEN Internet log files using Utah's equivalent of the Freedom of Information Act. The log files obtained were for one month of public school Internet access from September 10 to October 10, 1998. Examination of the files revealed that less than one percent, or about one out of every 260 requests was blocked. For days when school was not in session, the figure nearly doubled to one in 120 requests blocked. As Censorware (1999) concludes, "One can view this in two ways: high school students are much less likely to access banned material, or adults are more likely to (7)." These results seriously question the need for schools to purchase expensive, difficult to operate, and potentially unconstitutional filter software. Given that students

access less than one percent of "objectionable" sites, and the fact that filters are overinclusive, thus blocking some legitimate content, schools may want to reevaluate the need to limit access to the Internet.

The Future of the School and Library Filtering Debate

Playing off parents fears of the Internet, a number of prominent politicians are calling for mandatory filtering in public schools and libraries. In 1998, Vice President Gore urged Congress to pass school filtering legislation, commenting "As we connect every school and classroom to the Internet, we must protect our children from the red-light districts of cyberspace (in Mosquera, 1998)." Most recently, presidential candidate Elizabeth Dole has come out in favor of filtering pornography in public libraries. According to Dole, "Federal tax dollars should never be used to poison our children or provide free pornography for adults. To protect our families and to protect the taxpayers, we shouldn't let pornography gain access to federally funded libraries through an electronic back door (in McCullagh, 1999)."

Answering such calls for legislation are two Congressional bills currently working their way towards the White House. In June 1999, the House passed HR 368, "The Safe Schools Internet Act," which requires public schools and libraries who use "e-rate" funding (federal grants for Internet access) to install filters to block access to content deemed "harmful to minors." A nearly identical bill, S.97, "The Childrens' Internet Protection Act" has made its way out of the Senate Commerce Committee, and will likely be voted on in the fall. According to the act's author, and presidential candidate, John McCain, "Parents have the

right to feel safe that, when they send their child to school, when they drop their child off at the public library, someone is going to be looking out for their children, protecting them. That's what this bill is all about (Senate Testimony, 1999)." The act achieves these goals through the following requirements (see Appendix 6 for the full text of S.97):

- Schools would have to certify with the FCC that they are using or will use a filtering or blocking system on computers with Internet access so that students will not be exposed to harmful material on the Internet. A school will not be eligible to receive universal service support for Internet access unless they do this.

- In order to be eligible for universal service, libraries would only have to certify that they are using a filtering or blocking system for one or more of their computers so that at least one computer will be suitable for minors' use.

- School and library administrators are free to choose any filtering or blocking system that would best fit their community standards and local needs. In providing for universal service discounts for Internet access, no federal governmental body can make any qualitative judgments about the system nor the material to be filtered that the school or library has chosen. (McCain, 1999)

According to the bill's supporters, it is a necessary and constitutional way to protect children from dangerous Internet content. They point out that the bill does not force filtering on all library computers (a concession made after the *Loudoun* case), and that decisions about what content is deemed harmful and what product to use, are left to local communities to decide (Taylor, 1999). Opponents however, note that S.97 forces one and only one solution to the Internet Content Conundrum on all libraries. Rather than use alternatives such as acceptable use policies, privacy screens, etc., under S.97 all libraries would be forced to use filtering software (Morgan, 1999). Opponents also point out that

under the logic of the *Reno* and *Loudoun* cases the bill would likely be found unconstitutional. First, S.97 fails to define "harmful to minors." Instead, it leaves this decision up to local communities. However, very similar language found in the CDA was deemed unconstitutionally vague and overbroad. Next, in *Loudoun* the Court found that less restrictive alternatives to filters were available, and therefore the one size fits all solution provided in S.97 may be found overly stringent. The most powerful constitutional argument against S.97 is the *Loudoun* Court's finding that filtering represented a prior restraint on speech because it provided no specific standards as to what content was blocked, nor a due process procedure for appealing blocking decisions. Nowhere in S.97 are provisions made for such procedural safeguards (Mincberg, 1999).

Despite the many practical and constitutional concerns over "The Childrens' Internet Protection Act", the bill will likely pass the Senate. If it does, it will be reconciled with the House version and eventually sent to the White House. A White House that passed the CDA, COPA, and has called for school and library filtering. As such, beginning in 2000, expect mandatory filtering to be in place at many of the nations schools and libraries. Such regulation will almost certainly face a constitutional challenge. One which may finally lay down clear rules about what options schools and libraries may permissibly use to deal with the Internet Content Conundrum.

Chapter Seven -- CONCLUSION

This thesis set out by asking whether Internet content filters and rating systems were indeed the First Amendment friendly solution to the Internet Content Conundrum that the judicial, legislative, and executive branches claimed. Clearly the evidence presented throughout this thesis, severely calls this assertion into question.

The best way of illustrating the shortcomings of filters and rating systems is to use the Supreme Court's own logic in ACLU v. Reno, where the Court found that filters and ratings were "at least as effective" and "a less restrictive alternative" to government regulation intended to protect minors from harmful Internet content. Unfortunately, as discussed in past chapters, filters and rating systems fail both prongs of this test.

First, filters are not "at least as effective," as they let through a substantial portion of "objectionable" Internet content, including hard core pornography, hate speech, and violence. According to the filter test performed in Chapter Four, taken as a whole, filters will fail to block "objectionable" material 25 percent of the time! The situation is similar for rating systems which have not been widely adopted. As such, very few sites have self rated, and very few PICS compliant filters have been written. This ensures that a majority of content will be let through.

More troubling than the fact that filters are not 100 percent effective, is their overinclusive blocking of completely innocuous material. As discussed in

Chapters Three and Four, filters blocked access to pet care web sites, home pages devoted to music, academic institutions, research tools, etc. , all content with no off limits material as defined by the filter companies own blocking rules. Even more troubling, several filters blocked access to important political content, including political advocacy groups like the AFA, GLAAD, and NOW, and most egregiously, the White House web site. According to Chapter Four's test, on average, filters will "overinclusively" block innocuous material 21 percent of the time. Given this reality, it is clear that filters are not a "less restrictive alternative" to government regulation like the CDA, which would likely have left such material untouched. Although not yet widely used, a PICS enabled web would suffer from the same problems. Independent third party label bureaus could block content for any reason whatsoever, including the fact that a page had not self rated.

By promoting the potential for wide spread censorship, these solutions fall outside of a First Amendment tradition of narrowly tailored regulations on constitutionally protected speech. Therefore, it would seem that President Clinton, the Court, Congress, and the Internet industry are pushing an unconstitutional technological solution. As Lawrence Lessig lays out the problem:

> If the government has a legitimate interest in filtering speech of kind X, but not speech of kind Y and Z, and there are two architectures, one that would filter speech X, Y and Z, and one that would filter only speech of kind X, then Congress may constitutionally push technologies of the second kind, but not the first. It may push architectures that filter speech of kind X only, and not architectures that facilitate the filtering of speech of kind X, Y, and Z. (1998, p. 48)

Unfortunately a technology of type X has yet to develop. As a result, we run the risk of developing an Internet where censorship, rather than information exchange becomes the default setting.

Filtering Policy For the 21st Century

Despite the numerous problems outlined above, filters and rating systems will likely become more, not less prevalent in the coming years. Why? Because legislators realize that blaming societies ills on Internet pornography is an easy way to score points. This has resulted in support for filters coming from the Chairman of the FCC, presidential candidates, the Vice President, and the Commander in Chief himself. This is even more so in the wake of the Littleton tragedy. Such support resonates due to communities traditional fears of all form of new media, and a general hysteria about pornography.

Another reason for filter support is that parents remain very afraid about the harmful effects of the Internet. As Turow (1999) found, 76 percent of parents are concerned that their children might view sexually explicit images on the Internet. This fear is fanned by the media, which portray the Internet as full of sexual predators, pornography, hate, and bomb making sites. As Ann K. Symons of the ALA comments, " It's not news to say that millions of kids had a safe rewarding experience on-line today (1999)."

Given such strong support, filters and ratings systems, and legislation requiring these technologies, are likely to remain the preferred solution to the Internet Content Conundrum in the eyes of the public policy community. As such, what is the best way to ensure that future Internet filtering policies are

parentally empowering and sensitive to the First Amendment concerns of groups like the ALA, ACLU, and Censorware? I would propose that the answer is transparency.

To understand what I mean by transparency, it is instructive to first describe its opposite, complexity. Technological complexity is hidden from view by the graphical user interface of the modern operating system (Windows 95/98/NT, Mac OS), and today's advanced consumer software products such as word processors, electronic mail clients, and web browsers. Operating systems and applications present a clean, comprehensible interface to what behind the scenes is an otherwise incomprehensible set of rules, procedures, and complex mathematical operations. As such, these technologies may be considered opaque. In other words, it is not particularly easy to understand what is happening behind the scenes of a double click, a file transfer, or a web page request. This situation is by no means unique to computers, for example how many automobile drivers can claim knowledge of how their high performance engine manages to propel them down the highway? With a car, the technological complexity of the engine is hidden from view by the hood, and controlled via the simple mechanism of a gas peddle (like the mouse is to an operating system).

Opaque applications are not necessarily a bad thing. After all, how many people prefer the line mode operating system of DOS to the simple to use graphical user interface of a Macintosh or Windows 95? In these situations a double click has no bearing on how other people come to know and understand you, or how you participate in a larger public sphere. Instead, the interface merely facilitates the intended use of the application. However, opaque applications/protocols are dangerous, when those things which are hidden or

not readily apparent to an end user can be used in ways contrary to the end user's wishes.

This is clearly the case with many filtering and rating solutions. As mentioned earlier, most filtering companies refuse to publish the list of sites which they block. Many also fail to fully explain their filtering criteria. Thus, parents have a very limited ability to customize the software. This renders filters less than parentally empowering, and when applied to libraries and schools, outsources content selection decisions to secretive filter makers and label bureaus. Compounding these problems is the fact that no filter makers notify sites who have been blocked, and few provide a due process review procedure for site owners who feel they have been unjustly blocked.

The answer to these problems is transparency (Brin, 1998). Transparency means peeling away the layers of technological and procedural complexity to understand how blocking decisions are made and implemented. By understanding, and sometimes seeing through this complexity, filter users will be better able to ensure that their software use is directed towards their ends, not those of a politically motivated filter maker.

Therefore, transparency is truly about empowerment. The ability to control one's own information, and one's own Internet experience. These goals are consistent with the ideals of individual liberty and autonomy that serve as the building blocks for our democracy, both in the physical and virtual world.

So what specific recommendations would make filters and rating systems more transparent, and therefore truly empowering?:

- Filter makers and label bureaus should publicly publish their blocked sites lists. Due to the large number of blocked URL's, an easy to use search function should be made available so that parents, educators, etc. can quickly find individual sites.

- All filter makers, rating systems, and label bureaus should publicly post their filtering criteria, including a notice that some blocking decisions are made without human review.

- Filters must be completely customizable. Parents, teachers, and librarians should have the unlimited ability to add and remove sites from the blocked list.

- By default, PICS-based filters should not block unrated web sites. As the ACLU comments, the default setting should be set to "free speech (ACLU, 1997)."

- Filter makers and label bureaus should notify via email the owners of all sites deemed off limits. The message should include the reason for the blocking decision.

- Filter makers and label bureaus should have a clear written policy for appealing blocking decisions. This process should be expeditious and open to public review. Both site owners and end users should be able to contest blocking decisions.

While these transparency enhancing recommendations are useful for private, parental filter use, they are absolutely essential for government sanctioned filtering in libraries and schools. In the *Loudoun* case, the Court found that filters were a prior restraint because they provided no way of knowing what sites had been blocked, why they were blocked, and no procedure for appealing blocking decisions. If filter makers want to expand into library and educational markets, they must accept the burdens of constitutional review, which forbid arbitrary, capricious, and secretive decisions about limiting access to constitutionally protected speech. This means abandoning the argument that blocked sites lists are copyrighted, proprietary trade secrets. If filter makers accept this tradeoff, their products *may* be found suitable for public institutions.

The Future of Filters in Public Institutions

Increased filter transparency would go a long way towards showing that filters are a reasonable and constitutionally acceptable method of protecting children from harmful Internet content. However, even with these changes, public filter use faces serious legal challenges. First, even the most transparent of filters may be found unnecessary to fulfill the state's legitimate purpose of protecting children from harmful content. In the *Loudoun* case only one example of inappropriate access was raised. Similarly, Censorware's study of Utah public school filtering found that less than one percent of Internet requests were blocked. These findings point to the conclusion that the Internet Content Conundrum is not as bad as it seems. This is likely due to the fact that library and school Internet terminals are located in open public spaces, where others can see what an individual may be accessing. Thus, social pressure keeps children, and even adults from accessing controversial content like pornography or hate speech.

Even if public institutions found that the Internet Content Conundrum was a major problem, it is not clear that filters would be the least restrictive way of limiting access to inappropriate material. Several other options such as privacy screens, monitoring, kids safe search engines/portals, acceptable use policies, and time limits would seem less onerous than filtering (ACLU, 1998).

Given these problems it is entirely unclear if public filter use will be found constitutional. Within the context of libraries, these problems may be insurmountable. However, within schools, particularly when applied to curricular activities, filters may be found acceptable.

The Limits of Transparency

In theory, transparency is a great idea. It places information selection decisions back in the hands of end users. Unfortunately, due to the vast size of

the web, transparency has significant limitations. For example, above I suggest that filter makers and label bureaus publish their lists of blocked sites. But who will have the time to dig through the hundreds of thousands of URL's on these lists to ensure that they square with a user's values? Even with a search feature, an end user can only identify one site at a time. In this way, transparency could become a convenient bureaucratic excuse for filter makers. They will say "hey, we make all our blocking decisions public, therefore it's your problem to find the decisions you disagree with." Hiding behind this excuse, filter makers like CYBERsitter will feel no public pressure to stop making politically motivated blocking decisions. After all, if an end user doesn't like them, he/she can find and unblock them.

A similar problem occurs with the suggestion that filter makers notify all blocked site owners, and provide them with an appeals process. First, not all web pages contain an email address identifying the creator of the page. Next, undoubtedly most site owners who have been successfully notified will want to appeal the blocking decision. This could mean tens of thousands of appeal requests for filter companies who already can not keep up with the ever expanding web.

Forget the Code of Law, Here Comes the Law of Code

Precisely due to the problems of information overabundance, software products like filters, and protocols like PICS will become incredibly important in the 21st century. They will help define the very nature of the on-line world, and the possibilities that exist within in it. In the real world, the limits of human action are constrained by physical reality (gravity for example) and by laws which are encoded into constitutions, criminal codes, and local ordinances. In democracies, these laws are developed and implemented within a vibrant public

sphere, which includes governmental and public oversight. Therefore, at least in theory, laws are meant to represent the will of the people.

The same can not be said for the on-line world, were computer code and the speed of electrons defines reality. Unlike the encoded laws of the real world, the code of cyberspace is developed within closed institutions like the W3C and the Internet Corporation for Assigned Names and Numbers (ICANN), the new governing body for Internet domain names (like www.whatever.com). As evidenced by their memberships, these groups primarily represent the interests of the Internet industry, not those of the general Internet using public. As such, the protocols they develop, although they effect all Internet users, only reflect the values of their computer industry members.

This is clearly a problem when such groups wade into contentious sociopolitical issues such as content appropriateness and privacy. Their closed structures prevent full and open public debate about the underlying good of the protocols being developed. As we have seen with PICS, this results in poor assumptions about human use. Assumptions which have consequences, like global censorship with PICS, for all Internet users.

The solution to this problem is to require a far more open structure for Internet standards setting bodies. Governments, public interest groups, and the general public should have an oversight role in the development of social protocols. One way of achieving this goal would be to place groups like the W3C and ICANN under the auspices of an open international governing body, much like the International Telecommunications Union is governed by the United Nations.

Conclusion

In the end, it is clear that there is no one solution to the Internet Content Conundrum. Both filters and rating systems have significant performance, ethical, and constitutional problems associated with them. However, within a transparent and open framework, these problems can be ameliorated. Still, even the most transparent piece of Internet filtering software will not solve the Internet Content Conundrum. After all, people have been arguing about meaning and appropriateness since the beginning of the written word. Well designed software and protocols can not hope to settle the eternal debate between a communities desire to protect its members from supposedly harmful content, and the individuals right to self determination and autonomy.

To answer the question posed by the title of this thesis, yes, the future will be filtered. It will be a necessity. What remains to be seen, is whether these code governed filters will reflect the values of industry, or those of transparency and democracy. If the latter is true, free speech will indeed become the default setting for the Information Revolution.

Appendix 1: Cyber Patrol Content Categories and Definitions

Any on-line content that contains more than 3 instances in 100 messages. Any easily accessible pages with graphics, text or audio which fall within the definition of the categories below will be considered sufficient to place the source in the category.

Violence/Profanity:

Violence: pictures exposing, text or audio describing extreme cruelty, physical or emotional acts against any animal or person which are primarily intended to hurt or inflict pain. Profanity: is definded as obscene words or phrases either audio, text or pictures.

Partial Nudity:

Pictures exposing the female breast or full exposure of either male or female buttocks except when exposing genitalia. The Partial Nudity category does not include swimsuits (including thongs).

Full Nudity:

Pictures exposing any or all portions of the human genitalia.

Please note: The Partial Nudity and Full Nudity categories do not include sites containing nudity or partial nudity of a non-prurient nature. For example: web sites for publications such as National Geographic or Smithsonian Magazine or sites hosted by museums such as the Guggenheim, the Louvre, or the Museum of Modern Art.

Sexual Acts:

Pictures, descriptive text or audio of anyone or anything involved in explicit sexual acts and or lewd and lascivious behavior, including masturbation, copulation, pedophilia, intimacy involving nude or partially nude people in heterosexual, bisexual, lesbian or homosexual encounters. Also includes phone sex ads, dating services, adult personal ads, CD-ROM's and videos.

Gross Depictions:

Pictures, descriptive text or audio of anyone or anything which are crudely vulgar or grossly deficient in civility or which show scatological impropriety. Includes such depictions as maiming, bloody figures, autopsy photos or indecent depiction of bodily functions.

Intolerance:

Pictures or text advocating prejudice or discrimination against any race, color, national origin, religion, disability or handicap, gender, or sexual orientation. Any picture or text that elevates one group over another. Also includes intolerant jokes or slurs.

Satanic/Cult:

Satanic material is defined as: Pictures or text advocating devil worship, an affinity for evil, or wickedness. A cult is defined as: A closed society, often headed by a single individual, where loyalty is demanded, leaving may be punishable, and in some instances, harm to self or others is advocated. Common elements may include: encouragement to join, recruiting promises, and influences that tend to compromise the personal exercise of free will and critical thinking.

Drugs/Drug Culture:

Pictures or text advocating the illegal use of drugs for entertainment. Includes substances used for other than their primary purpose to alter the individual's state of mind, such as glue sniffing. This category does not include material about the use of illegal drugs when they are legally prescribed for medicinal purposes (e.g., drugs used to treat glaucoma or cancer).

Militant/Extremist:

Pictures or text advocating extremely aggressive and combative behaviors, or advocacy of unlawful political measures. Topics include groups that advocate violence as a means to achieve their goals. Includes “how to” information on weapons making, ammunition making or the making or use of pyrotechnics materials. Also includes the use of weapons for unlawful reasons.

Sex Education:

Pictures or text advocating the proper use of contraceptives. This topic would include condom use, the correct way to wear a condom and how to put a condom in place. Also included are sites relating to discussion about the use of the Pill, IUD's and other types of contraceptives. In addition to the above, this category will include discussion sites on how to talk to your partner about diseases, pregnancy and respecting boundaries. The Sex Education category is uniquely assigned; sites classified as Sex Education are not classified in any other category. This permits the user to block or allow the Sex Education category as appropriate, for example, allow the material for an older child while restricting it for a younger child.

Not included in the category are commercial sites that sell sexual paraphernalia. These sites are typically found in the Sex Acts category.

Questionable/Illegal & Gambling:

Pictures or text advocating materials or activities of a dubious nature which may be illegal in any or all jurisdictions, such as illegal business schemes, chain letters, copyright infringement, computer hacking, phreaking (using someone's phone lines without permission) and software piracy. Also includes text advocating gambling relating to lotteries, casinos, betting, numbers games, on-line sports or financial betting, including non-monetary dares and "1-900" type numbers.

Alcohol & Tobacco:

Pictures or text advocating the sale, consumption, or production of alcoholic beverages or tobacco products, including commercial sites in which alcohol or tobacco products are the primary focus. Pub and restaurant sites featuring social or culinary emphasis, where alcohol consumption is incidental are not in this category.

Note: Web sites which post "Adult Only" warning banners advising that minors are not allowed to access material on the site are automatically added to the CyberNOT list in their appropriate category.

Appendix 2: SurfWatch Content Categories and Definitions

Evaluation Policies

SurfWatch criteria are reviewed with our Advisory Committee on a monthly basis to ensure responsible filtering. A site will be blocked if it meets the following guidelines:

1. A disclaimer indicating restricted access; a screen or warning that identifies the site as adult-oriented or containing information unsuitable for those underage

2. The publisher has requested that his/her site be blocked

3. A site which publishes information on how to bypass SurfWatch filtering or render SurfWatch inoperable in a manner which violates the software license agreement or is otherwise unauthorized by the original purchaser of the software

4. Any page or site which predominantly contains links to sites matching the following criteria:

Sexually Explicit

• sexually-oriented or erotic full or partial nudity

• depictions or images of sexual acts, including animals or other inanimate objects used in a sexual manner

• erotic stories and textual descriptions of sexual acts

• sexually exploitive or sexually violent text or graphics

• bondage, fetishes, genital piercing

• adult products including sex toys, CD-ROMs, and videos

• adult services including videoconferencing, escort services, and strip clubs

NOTE: We do not block on the basis of sexual preference, nor do we block sites regarding sexual health, breast cancer, or sexually transmitted diseases (except in graphic examples).

Drugs/Alcohol

• recipes or instructions for manufacturing or growing illicit substances, including alcohol, for purposes other than industrial usage

• sites that glamorize, encourage, or instruct on the use of alcohol, tobacco, illegal drugs, or other substances that are illegal to minors

• alcohol and tobacco manufacturers' commercial Web sites

• sites detailing how to achieve "legal highs": glue sniffing, misuse of prescription drugs or abuse of other legal substances

• sites that make available alcohol, illegal drugs, or tobacco free or for a charge displaying, selling, or detailing use of drug paraphernalia

NOTE: We do not block sites discussing medicinal drug use, industrial hemp use, or public debate on the issue of legalizing certain drugs. Nor do we block sites sponsored by a public or private agency that provides educational information on drug use. The term "illegal" is defined according to United States law.

Gambling

• online gambling or lottery web sites that invite the use of real money

• sites that provide phone numbers, online contacts or advice for placing wagers, participating in lotteries, or gambling real money

• newsgroups or sites discussing number running

• virtual casinos and offshore gambling ventures

• sports picks and betting pools

Violence

• sites portraying or describing physical assault against humans, animals, or institutions

• depictions of torture, mutilation, gore, or horrific death

• sites advocating suicide or self-mutilation

• instructions or recipes for making bombs or other harmful or destructive devices

• sites that make available guns, artillery, other weapons, or poisonous substances

• excessive use of profanity or obscene gesticulation

NOTE: We do not block news, historical, or press incidents that may include the above criteria (except in graphic examples).

Hate Speech

• sites advocating or inciting degradation or attack of specified populations or institutions based on

• associations such as religion, race, nationality, gender, age, disability, or sexual orientation

• sites which promote a political or social agenda which is supremacist in nature and exclusionary of others

• based on their race, religion, nationality, gender, age, disability, or sexual orientation

• Holocaust revision/denial sites

• coercion or recruitment for membership in a gang* or cult**

NOTE: We do not block news, historical, or press incidents that may include the above criteria (except in graphic
examples).

*A gang is defined as: a group whose primary activities are the commission of felonious criminal acts, which has a common name or identifying sign or symbol, and whose members individually or collectively engage in criminal activity in the name of the group.

**A cult is defined as: a group whose followers have been deceptively and manipulatively recruited and retained through undue influence such that followers' personalities and behavior are altered. Leadership is all-powerful, ideology is totalistic, and the will of the individual is subordinate to the group. Sets itself outside of society.

Appendix 3: RSACi Content Categories and Definitions

RSACi Rating Language

In order to determine the appropriate advisory level for language, you will be asked to go through a checklist of very specific terms to determine whether or not your content contains language, expressions, images, portrayals, etc., which some viewers might potentially consider objectionable. The RSACi rating addresses two kinds of speech; 'hate speech' and 'objectionable speech'; that is, language ranging from mild expletives or profanity to crude, vulgar, and obscene statements and gestures. You are urged to review the Definitions before submitting your answer.

Moving through the list below in order from top to bottom, please click the first button of the content descriptor that applies to your content. Does your content portray:

(l4) crude, vulgar language
(l4) explicit sexual references
(l4) extreme hate speech
(l4) epithets that advocate violence or harm against a person or group
(l3) strong language
(l3) obscene gestures
(l3) hate speech or strong epithets against any person or group
(l2) profanity
(l2) moderate expletives
(l1) non-sexual anatomical reference
(l1) mild expletives
(l1) mild terms for body functions

(l1) slang
(l0) none of the above

Definitions for RSACi Language Questions

GUIDING PRINCIPLE
The construction of a list of every word, action, innuendo, and gesture that a reasonable person would consider as crude, slang, profane or explicit is a never-ending task. Times change. Words change. Gestures change. New street slang is constantly evolving. Language considered inoffensive in one culture may be considered vulgar in another culture. It is therefore your responsibility to properly interpret and classify any slang, profanity or vulgarity according to the usage in the title and the general category definitions below. Words or expressions in the title that fit a definition or
categorization, but do not appear on a word list, should be treated as if they do appear on the list.

CONTAIN
The inclusion of specific content in any form or manner, including but not limited to printed words, written descriptions, oral recitations, and other audio sounds.

CRUDE LANGUAGE; EXPLICIT SEXUAL REFERENCES
Crude references, direct or indirect to intercourse: Fuck, bugger, mother-fucker, cock-sucker, penis-breath. Crude references to genitalia: prick, cock, pussy, twat, cunt. Explicit street slang for intercourse or genitalia.

EXTREME HATE SPEECH
The combination of vulgar language with hate speech or epithets; advocating violence or harm against a person or group.

HATE SPEECH
Any portrayal (words, speech, pictures, etc.) which strongly denigrates, defames, or otherwise devalues a person or group on the basis of race, ethnicity, religion, nationality, gender, sexual orientation, or disability is considered to be hate speech. Any use of an epithet is considered hate
speech. Any description of one of these groups or group members that uses strong language, crude language, explicit sexual references, or obscene gestures is considered hate speech.

EPITHET
A disparaging or abusive word or phrase used in the place of the name of any person or group. There are many examples of slang terms which, in any given

historical period, function almost exclusively as epithets: e.g., honky, nigger, coon, spic, greaser, chink, slant, faggot, etc. In addition, sometimes a word which is not in and of itself an epithet functions as one because of context. For example, in some contexts the word "pig" may be used in place of "police officer," thus becoming an epithet. In other contexts, and at different times, the word "monkey" has been used as an epithet to refer to individuals of Asian descent and to individuals of African descent.

OBSCENE GESTURES
Any visual or described gestures, body movements, such as flipping the bird, mooning, non-verbal indications of sexual insult, etc., indicating any of the above. Any visual or described innuendo, euphemisms, street slang, double-entendre for any of the above.

STRONG LANGUAGE
Strong, but not crude, language for genitalia: asshole, butthole, dork, dong, pecker, schlong, dick. Strong language for bodily functions or elimination: Shit, piss, cum, asswipe, buttwipe. Strong language for sexual functions or intercourse: jerk-off, balling, shtupping, screwing, boffing, cumming. References to genitalia used in a sexual setting including the use of penis, vagina, rectum, semen.

PROFANITY
To treat something regarded as sacred with abuse, irreverence, or contempt. To use the name of a deity with contempt or as a curse.

MODERATE EXPLETIVES
The words bastard and bitch (when used as epithets rather than biological terms), son-of-a-bitch, turd, crap.

MILD EXPLETIVES
The words hell and damn, ass and horse's ass, BUT NOT asshole, assface, asswipe; butthead and buttface BUT NOT butthole and buttwipe.

NON-SEXUAL ANATOMICAL REFERENCES
Words such as penis, vagina, rectum, semen used in a non-sexual context.

MILD TERMS FOR BODY FUNCTIONS
Words such as piss and poop not used in a sexual context.

SLANG
No profanity, expletives, vulgar gestures, innuendo, double-entendre, vulgar street slang other than listed below.

A. Inoffensive slang: darn, drat, golly, gosh, dang, rats, sheesh, geeze, gee wiz.
B. Screw to indicate cheated or harmed, BUT NOT screw in any sexual context.
C. Butt to indicate one's rear end as in "get your butt out of here, or "I'm going to paddle your butt," or "he fell on his butt.," BUT NOT butthead, butthole, buttface, buttwipe, etc.
D. Ass when referring to the animal, but not "Horse's ass."
E. Dork used in a non-sexual context as in, "He's a dork."
F. Sucks used in a non-sexual contest as in, "That sucks," or "He sucks."

RSACi Rating Nudity

In order to determine the level of nudity, if any, in your content, please go through the checklist of very specific terms about how nudity is portrayed. Definitions are provided for all terms that must be understood to make the determinations necessary to answer the questions. The definitions are highly specific and the objectivity of the labeling system depends on using them correctly.

Moving through the list below in order from top to bottom, please click the first button of the content descriptor that applies to your content. Does your content portray:

(4) frontal nudity that qualifies as a provocative display of nudity
(3) frontal nudity
(2) partial nudity
(1) revealing attire
(0) none of the above

Definitions for RSACi Nudity Questions

PORTRAYAL
Any presentation including, but not limited to, pictures, no matter how crudely drawn or depicted, written descriptions, oral recitations and or audio sounds.

HUMAN or HUMAN-LIKE BEINGS
Any sentient being, no matter how portrayed (photographed or drawn) or how crudely drawn (including stick figures) understood by any reasonable person as human or humanoids in form including alien sentient beings that have human-like form (head AND arms AND torso AND legs AND walking upright).

NUDITY
Any portrayal of a human's buttocks (other than the exception below), genitalia, or female breasts, or of humanoid genitalia or female breast(s), including such portrayals as see-through blouses, the pasties of a topless dancer, or other types of clothing which do not prevent exposure of those parts of the body. This definition also includes nudity in widely recognized works of art and nudity in documentary context. NOTE: An exception is made for portrayals of the buttocks of characters which a reasonable person would consider as BOTH (a) something other than a true human being or representation thereof, AND (b) a character that normally is expected to be unclothed and whose natural state is undressed. If the portrayal is such that it would not cause a reasonable person to comment upon or take notice of the exposed buttocks, then, for this one exception, the characters require no rating for nudity.

PROVOCATIVE DISPLAY OF FRONTAL NUDITY
Any portrayal of genitalia that might reasonably imply sexual arousal, or the display of frontal nudity in what might be reasonably considered a sexual context.

FRONTAL NUDITY
Any portrayal of a nude sentient being which shows pubic hair or genitalia, excluding known animals in their natural state of undress.

PARTIAL NUDITY
Partial nudity is a subset of nudity. Any portrayal of a human buttocks or female breasts, or of humanoid female breast(s), including such portrayals as see-through blouses and other types of clothing which do not prevent exposure of the body and portrayals with minimal covering, such as pasties on the breasts of a topless dancer. In the case of non-humans, portraying buttocks does not constitute partial nudity IF AND ONLY IF one can surmise that the creature is natural state is undressed.

REVEALING ATTIRE
Any portrayal of a human/humanoid that does not portray nudity, yet portrays outlines through tight clothing, or clothing that otherwise emphasizes male or female genitalia, female nipples or breasts (including the display of cleavage that is more than one half of the possible length of such

cleavage), or clothing on a male or female which a reasonable person would consider to be sexually suggestive and alluring.

RSACi Rating Sex

In order to determine the level of sexual activity, if any, in your content, you will be asked to go through a checklist of very specific terms about how sex is portrayed. Definitions are provided for all terms that must be understood to make the determinations necessary to answer the questions. The definitions are highly specific and the objectivity of the labeling system depends on using them correctly. You are urged to review the definitions before submitting your answer.

Moving through the list below in order from top to bottom, please click the first button of the content descriptor that applies to your content. Does your content portray:

(4) sex crimes
(4) explicit sexual acts
(3) non-explicit sexual acts
(2) non-explicit sexual touching
(2) clothed sexual touching
(1) passionate kissing
(0) innocent kissing or romance
(0) none of the above

Definitions for RSACi Sex Questions

PORTRAYAL
Any presentation including, but not limited to, pictures, no matter how crudely drawn or depicted, written descriptions, oral recitations, and or audio sounds.

HUMAN or HUMAN-LIKE BEINGS
Any sentient being, no matter how portrayed (photographed or drawn) or how crudely drawn (including stick figures) understood by any reasonable person as human or humanoids in form including alien sentient beings that have human-like form (head AND arms AND torso AND legs AND walking upright).

SEX CRIMES
Any portrayal of unwanted, unauthorized, or otherwise non-consensual sexual acts forced upon one sentient being by another sentient being (rape).
Any portrayal of explicit or non-explicit sexual acts, consensual or not, between a human or human-like being that a reasonable person would consider as being under the age of 18, and another human or human-like being that a reasonable person would consider over the age of 18. Any portrayal of sex, consensual or not, between an animal and a human or human-like being (bestiality).

EXPLICIT SEXUAL ACTS
Any portrayal of sexual activity that a reasonable person would consider as more than just non-explicit sexual activity because it shows genitalia. This includes any portrayal of sexual activity by one human or human-like being, or among multiple humans, including, but not limited to masturbation and sexual intercourse of any kind (oral, anal vaginal), that shows genitalia.

NON-EXPLICIT SEXUAL ACTS
Any portrayal of sexual activity that a reasonable person would consider as more than just clothed sexual touching or non-explicit sexual touching, either by one human or human-like being or among multiple humans, including, but not limited to masturbation and sexual intercourse of any kind (oral, anal, vaginal), that may show nudity, but does not show genitalia. Non-explicit sexual activity includes sound on an audio track, such as the kinds of groans, moans, and other sounds that to a reasonable person would imply sexual activity was taking place.

NON-EXPLICIT SEXUAL TOUCHING
Any portrayal of any touching between or among humans or human-like beings, that a reasonable person would consider more than just passionate

kissing, including but not limited to such things as groping, petting, licking, and rubbing, that falls short of intercourse (sexual, oral, or otherwise), and that does show bare buttocks or female breasts, but does NOT show genitalia. Non-explicit sexual touching does NOT include non-explicit or explicit sexual acts as defined above and does NOT include masturbation.

CLOTHED SEXUAL TOUCHING
Any portrayal of any activity or touching between or among humans or human-like beings, other than innocent kissing and passionate kissing, that falls short of intercourse (sexual, oral, or otherwise) or masturbation, and that does NOT show bare buttocks, female breasts, or genitalia, but that any reasonable adult would perceive as sexual in nature. This includes but is not limited to such things as groping, petting, licking, rubbing. Non-explicit sexual touching does NOT include non-explicit or explicit sexual acts as defined below and does NOT include masturbation.

PASSIONATE KISSING
Any portrayal of humans or human-like creatures kissing that a reasonable person would consider more than just innocent kissing. This includes any kissing during which tongues touch (or mouths are obviously open), and any kissing on, but not limited to, the neck, torso, breasts, buttocks, legs.

INNOCENT KISSING
Any portrayal of humans or human-like creatures which a reasonable person would consider as just kissing on lips (without touching of tongues), head, shoulder, hands or arms, but not any other areas including but not limited to neck, breasts, torso, or legs. Innocent kissing shows affection and/or love, but creates no reasonable perception of stronger sexual activity as defined in this methodology.

ROMANCE
Portrayals of activity showing love and affection with NO stronger sexual contact as defined in this methodology. This might include embraces, hugging, innocent kissing, holding hands, etc.

RSACi Rating Violence

In order to determine the level and type of violence, if any, in your content, you will be asked to go through a checklist of very specific terms about whether and how violence or its consequences are depicted. Definitions are provided for all terms which you need to understand in order to make the determinations necessary to answer the questions. The definitions are highly specific, and the objectivity of the system depends on using them carefully and correctly. You are urged to review the Definitions before submitting your answer.

Moving through the list below in order from top to bottom, please click the first button of the content descriptor that applies to your content. Does your content portray:

(4) wanton, gratuitous violence
(4) extreme blood and gore
(4) rape
(3) blood and gore

(3) intentional aggressive violence
(3) death to human beings
(2) the destruction of realistic objects with an implied social presence
(1) injury to human beings
(1) the death of non-human beings resulting from natural acts or accidents
(1) damage to or disappearance of realistic objects?
(0) sports violence
(0) none of the above

Definitions for RSACi Violence Questions

PORTRAYAL
Any presentation including, but not limited to pictures, no matter how crudely drawn or depicted, written descriptions, and/or oral recitations, and/or audio sounds.

THREATENING
The portrayal of the intention to inflict harm, injury, evil on another being. Something that a reasonable person would consider to be menacing to another's safety or well-being.

WANTON, GRATUITOUS VIOLENCE
The visual portrayal of the continuation of intentional aggressive violence that causes damage/harm/death to any sentient being once that being has been rendered helpless and/or non-threatening, such as physical torture, continued attacks on or damage to corpses, dismembering or eating a corpse.
EXTREME BLOOD/GORE:
The visual portrayal of living beings being torn apart or slaughtered, dismembered body parts.

RAPE
The portrayal (video, audio, or written) of any unwanted/unauthorized, non-consensual sexual intercourse, whether vaginal, anal, oral, or fondling, forced upon a sentient being by another sentient being(s). In any sexual or sexually suggestive interaction, "No" is assumed to mean "No."

BLOOD / GORE
The visual portrayal of blood splashing, pools of blood on the ground, objects or persons smeared or stained with blood.

INTENTIONAL AGGRESSIVE VIOLENCE
The existence of a threat or the actual carrying out of threatening actions that directly or indirectly cause, or if successful would cause, physical harm, damage,

destruction, or injury to a sentient being or realistic object. This includes the visual portrayal of the results of aggressive violence including,
but not limited to dead bodies, damage, audio distress, etc., even if the violent act itself is not shown. It does not include psychological attacks. but is limited to physical harm, damage, destruction, and injury. possible to have a credible threat which does not cause a change in behavior.

IMPLIED SOCIAL PRESENCE
The presumption, unless a reasonable person would clearly think otherwise, that a realistic object is inhabited, or carrying, or concealing humans, even though the humans have not been seen or heard.

SPORTS VIOLENCE
Competitive sports games such as football, basketball, car racing, sumo wrestling, etc. have may elements of violence but are not intentional aggressive violence. It is still sports violence if players or participants are shown carried off the field, conscious or unconscious, even though on a stretcher, unless there is death, dismemberment, or blood and gore involved.
Note: Sports violence does NOT include wrestling, boxing, street fighting, karate, etc. games if the intended goal is to hurt or render the opponent
unable to function. These actions are considered as intentional aggressive violence. A fight within a sports game, such as during a hockey game, would also be considered intentional aggressive violence. Definitions for Violence Rating: PORTRAYAL: Any presentation including, but not limited to pictures, no matter how crudely drawn or depicted, written descriptions, and/or oral recitations, and/or audio sounds.

Appendix 4: Filter Default Settings

CYBERsitter
Tested on 06-16-99 using 06-16-99 blocked site list
Default categories:

Adult/sexually oriented
PICS Ratings Adult/violence
Gay/Lesbian activities
Advocating illegal/radical activities
Advocating hate/intolerance
Cults/Occult
WWW Chat Rooms

Cyber Patrol
Tested on 06-17-99 using 04-29-99 blocked site list
Default categories:

Violence/profanity
Partial nudity
Full nudity
Sexual acts
Gross depictions
Intolerance
Satanic or cult
Drugs
Militant/extremist
Sex education
Questionable. illegal gambling
Alcohol and tobacco

Net Nanny
Tested on 06-17-99 using 05-29-99 blocked site list
Default categories:

Net Nanny has no blocking categories, only multiple lists of blocked sites which are by default turned on.

SurfWatch
Tested on 06-16-99 using 06-16-99 blocked site list
Default categories:

Sexually Explicit
Drugs/Alcohol,
Gambling,
Violence,
Hate Speech

Appendix 5: Web Sites Tested, RSACi Scores, and Blocking Decisions

Webcrawler Random Links

1. Explore Vietnam - Study Vietnam
http://www. explorevietnam. com/Learning/index. html

language = 0 CYBERsitter = not blocked
nudity = 0 Cyber Patrol = not blocked
sex = 0 Net Nanny = not blocked
violence = 0 SurfWatch = not blocked

2. Angle Tech
http://www.angle.qpg.com/

language = 0 CYBERsitter = not blocked
nudity = 0 Cyber Patrol = not blocked
sex = 0 Net Nanny = not blocked
violence = 0 SurfWatch = not blocked

3. XXXVirtualPorn
http://russian-porno.sammich.com/tours/index.html

language = 4 CYBERsitter = blocked
nudity = 4 Cyber Patrol = blocked
sex = 4 Net Nanny = not blocked
violence = 0 SurfWatch = blocked

4. Photo Image - Photofinishing, Digital Imaging, Judy's Gift's
http://www.photoimageinc.com/

language = 0 CYBERsitter = not blocked
nudity = 0 Cyber Patrol = not blocked
sex = 0 Net Nanny = not blocked
violence = 0 SurfWatch = not blocked

5. WebCastro "Hotlinks"
http://www.webcastro.com/hotlinks.htm

language = 0 CYBERsitter = not blocked
nudity = 1 Cyber Patrol = blocked
sex = 0 Net Nanny = not blocked
violence = 0 SurfWatch = not blocked

6. John Brown Limited, Inc.
http://www.jblnh.com/

language = 0 CYBERsitter = not blocked
nudity = 0 Cyber Patrol = not blocked
sex = 0 Net Nanny = not blocked
violence = 0 SurfWatch = not blocked

7. Maine Inspiration Charters - Shark and Tuna Fishing in Maine
http://www.charterme.com/

language = 0 CYBERsitter = not blocked
nudity = 0 Cyber Patrol = not blocked
sex = 0 Net Nanny = not blocked
violence = 0 SurfWatch = not blocked

8. Index
http://www.top10shop.freeserve.co.uk/

language = 0 CYBERsitter = not blocked
nudity = 0 Cyber Patrol = not blocked
sex = 0 Net Nanny = not blocked
violence = 0 SurfWatch = not blocked

9. Diablo's Games Page
http://members.tripod.com/~Ollassav/index.html

language = 0 CYBERsitter = not blocked
nudity = 0 Cyber Patrol = not blocked
sex = 0 Net Nanny = not blocked
violence = 0 SurfWatch = not blocked

10. Giraffes from How to Get a Head Without Hunting
http://www.animalhead.com/giraffes.html

language = 0 CYBERsitter = not blocked
nudity = 0 Cyber Patrol = not blocked
sex = 0 Net Nanny = not blocked
violence = 0 SurfWatch = not blocked

11. Owings Mills Network, Maryland
http://www.owingsmills.net/

language = 0 CYBERsitter = not blocked
nudity = 0 Cyber Patrol = not blocked
sex = 0 Net Nanny = not blocked
violence = 0 SurfWatch = not blocked

12. http://www.highway666.com/angel_witch.html

language = 1 CYBERsitter = not blocked
nudity = 0 Cyber Patrol = not blocked
sex = 0 Net Nanny = not blocked
violence = 3 SurfWatch = not blocked

13. MCW Home page
http://www.montanacomputers.com/

language = 0 CYBERsitter = not blocked
nudity = 0 Cyber Patrol = not blocked
sex = 0 Net Nanny = not blocked
violence = 0 SurfWatch = not blocked

14. CLN WWW Navigation Map
http://www.cln.org/map.html

language = 0 CYBERsitter = not blocked
nudity = 0 Cyber Patrol = not blocked
sex = 0 Net Nanny = not blocked
violence = 0 SurfWatch = not blocked

15. Alloy Ball and Seat Co. , Inc. : Ball and Seat Valves
http://www.alloyvalve.com/

language = 0 CYBERsitter = not blocked
nudity = 0 Cyber Patrol = not blocked
sex = 0 Net Nanny = not blocked
violence = 0 SurfWatch = not blocked

16. Malone College: A Christian College for the Arts, Sciences, and Professions
http://www.malone.edu/

language = 0 CYBERsitter = not blocked
nudity = 0 Cyber Patrol = not blocked
sex = 0 Net Nanny = not blocked
violence = 0 SurfWatch = not blocked
17. Welcome to our homepage
http://www.poliville.com/

language = 0 CYBERsitter = not blocked
nudity = 0 Cyber Patrol = not blocked
sex = 0 Net Nanny = not blocked

violence = 0 SurfWatch = not blocked

18. Excite Travel: Destinations: Australia: Queensland: Sunshine Coast
http://city.net/countries/australia/queensland/sunshine_coast/

language = 0 CYBERsitter = not blocked
nudity = 0 Cyber Patrol = not blocked
sex = 0 Net Nanny = not blocked
violence = 0 SurfWatch = not blocked

19. rates between served airports and common destinations in central Pa
http://members.bellatlantic.net/~propo/rates.html

language = 0 CYBERsitter = not blocked
nudity = 0 Cyber Patrol = not blocked
sex = 0 Net Nanny = not blocked
violence = 0 SurfWatch = not blocked

20. www. marksmodelcars. com
http://www.marksmodelcars.com/

language = 0 CYBERsitter = not blocked
nudity = 0 Cyber Patrol = not blocked
sex = 0 Net Nanny = not blocked
violence = 0 SurfWatch = not blocked

21. Sign Language Studies
http://www.vuw.ac.nz/~nzsldict/sls.html

language = 0 CYBERsitter = not blocked
nudity = 0 Cyber Patrol = not blocked
sex = 0 Net Nanny = not blocked
violence = 0 SurfWatch = not blocked

22. Tradepages Business Plaza
http://www.tradepages.co.kr/

language = 0 CYBERsitter = not blocked

nudity = 0 Cyber Patrol = not blocked
sex = 0 Net Nanny = not blocked
violence = 0 SurfWatch = not blocked

23. www. augustacc. com/
http://www.augustacc.com/

language = 0 CYBERsitter = not blocked
nudity = 0 Cyber Patrol = not blocked
sex = 0 Net Nanny = not blocked
violence = 0 SurfWatch = not blocked

24. I M A G E S U K
http://www.images-uk.com/

language = 0 CYBERsitter = not blocked
nudity = 0 Cyber Patrol = not blocked
sex = 0 Net Nanny = not blocked
violence = 0 SurfWatch = not blocked

25. Roadside America Pet Cemetery
http://www.roadsideamerica.com/pet/index.html

language = 0 CYBERsitter = not blocked
nudity = 0 Cyber Patrol = not blocked
sex = 0 Net Nanny = not blocked
violence = 0 SurfWatch = not blocked

26. Lamcon Group
http://www.lamconindia.com/

language = 0 CYBERsitter = not blocked
nudity = 0 Cyber Patrol = not blocked
sex = 0 Net Nanny = not blocked
violence = 0 SurfWatch = not blocked

27. Ratkobera's Page
http://ratkobera.youthofamerica.org/

language = 0 CYBERsitter = not blocked
nudity = 0 Cyber Patrol = not blocked
sex = 0 Net Nanny = not blocked
violence = 0 SurfWatch = not blocked

28. Consumer Reports | Search
http://www.consumerreports.org/Functions/Search/index.html

language = 0 CYBERsitter = not blocked
nudity = 0 Cyber Patrol = not blocked
sex = 0 Net Nanny = not blocked
violence = 0 SurfWatch = not blocked

29. Mallrats
http://www.viewaskew.com/mallrats/

language = 3 CYBERsitter = not blocked
nudity = 0 Cyber Patrol = not blocked
sex = 0 Net Nanny = not blocked
violence = 1 SurfWatch = not blocked

30. CAPCYBER - Capital Cyber Communications
http://www.capcyber.com/

language = 0 CYBERsitter = not blocked
nudity = 0 Cyber Patrol = not blocked
sex = 0 Net Nanny = not blocked
violence = 0 SurfWatch = not blocked

31. . . . Shtzville. . .
http://www.angelfire.com/md/shtzville/

language = 3 CYBERsitter = not blocked
nudity = 0 Cyber Patrol = not blocked
sex = 0 Net Nanny = not blocked
violence = 0 SurfWatch = not blocked

32. Saga magazine - Feature
http://www.saga.co.uk/publishing/specials/arthurc.html

language = 0 CYBERsitter = not blocked
nudity = 0 Cyber Patrol = not blocked
sex = 0 Net Nanny = not blocked
violence = 0 SurfWatch = not blocked

33. Keys For Kids - MAY 14
http://www1.gospelcom.net/cbh/kfk/kfk-05-14-95.html

language = 0 CYBERsitter = not blocked
nudity = 0 Cyber Patrol = not blocked
sex = 0 Net Nanny = not blocked
violence = 0 SurfWatch = not blocked

34. Webmaster 10 - Awards Page
http://www.webmaster10.com/award.htm

language = 0 CYBERsitter = not blocked
nudity = 0 Cyber Patrol = not blocked
sex = 0 Net Nanny = not blocked
violence = 0 SurfWatch = not blocked

35. Photos and Club Memorabilia
http://www.teleport.com/~pmadland/Flyaways/fun/photos.htm

language = 0 CYBERsitter = not blocked
nudity = 0 Cyber Patrol = not blocked
sex = 0 Net Nanny = not blocked
violence = 0 SurfWatch = not blocked

36. SpeedAssist Home Page
http://home2.swipnet.se/~w-20031/

language = 0 CYBERsitter = not blocked
nudity = 0 Cyber Patrol = not blocked
sex = 0 Net Nanny = not blocked
violence = 0 SurfWatch = not blocked

37. Health Informatin - Blindness to Dyslexia
http://www.radix.net/~mschelling/health2.html

language = 1 CYBERsitter = not blocked
nudity = 0 Cyber Patrol = not blocked
sex = 0 Net Nanny = not blocked
violence = 0 SurfWatch = not blocked

38. Available IP
http://www.teleport.com/~scd/avail_ip.htm

language = 0 CYBERsitter = not blocked
nudity = 0 Cyber Patrol = not blocked
sex = 0 Net Nanny = not blocked
violence = 0 SurfWatch = not blocked

39. Offset Pre-Press, Incorporated
http://www.offsetprepress.com/

language = 0 CYBERsitter = not blocked
nudity = 0 Cyber Patrol = not blocked
sex = 0 Net Nanny = not blocked
violence = 0 SurfWatch = not blocked

40. All Wired, Computer, Home Theater, Phone, Home Automation, Audio
http://allwiredinc.com/

language = 0 CYBERsitter = not blocked
nudity = 0 Cyber Patrol = not blocked
sex = 0 Net Nanny = not blocked
violence = 0 SurfWatch = not blocked

41. SHARKTAGGER. COM
http://www.sharktagger.com/

language = 0 CYBERsitter = blocked
nudity = 0 Cyber Patrol = not blocked
sex = 0 Net Nanny = not blocked
violence = 0 SurfWatch = not blocked

42. Some ted Nugent Stuff
http://www.iglou.com/sonic/nugent.html

language = 0 CYBERsitter = not blocked
nudity = 0 Cyber Patrol = not blocked
sex = 0 Net Nanny = not blocked
violence = 0 SurfWatch = not blocked

43. Enterprise Consultants Network
http://www.enterpriseconsultants.com/

language = 0 CYBERsitter = not blocked
nudity = 0 Cyber Patrol = not blocked
sex = 0 Net Nanny = not blocked
violence = 0 SurfWatch = not blocked

44. Decatur Jewelry & Pawn
http://www.decaturpawn.com/

language = 0 CYBERsitter = not blocked
nudity = 0 Cyber Patrol = not blocked
sex = 0 Net Nanny = not blocked
violence = 0 SurfWatch = not blocked

45. metsun1. sjsu. edu/

language = 0 CYBERsitter = not blocked
nudity = 0 Cyber Patrol = not blocked
sex = 0 Net Nanny = not blocked
violence = 0 SurfWatch = not blocked

46. metrotel paging beeper cellular motorola sales service
http://www.metrotel.com/

language = 0 CYBERsitter = not blocked
nudity = 0 Cyber Patrol = not blocked
sex = 0 Net Nanny = not blocked
violence = 0 SurfWatch = not blocked

47. Weather Underground: Laredo, Texas Forecast

http://www.wunderground.com/forecasts/LRD.html

language = 0 CYBERsitter = not blocked
nudity = 0 Cyber Patrol = not blocked
sex = 0 Net Nanny = not blocked
violence = 0 SurfWatch = not blocked

48. Bill Frakes, Photographer
http://www.billfrakes.com/

language = 0 CYBERsitter = not blocked
nudity = 0 Cyber Patrol = not blocked
sex = 0 Net Nanny = not blocked
violence = 0 SurfWatch = not blocked

49. Webbing Monthly - News, Views & Muse
http://www.jessanio.com/webbing_monthly/index.html

language = 0 CYBERsitter = not blocked
nudity = 0 Cyber Patrol = not blocked
sex = 0 Net Nanny = not blocked
violence = 0 SurfWatch = not blocked

50. Welcome to CableCo
http://www.cableco.co.uk/

language = 0 CYBERsitter = not blocked
nudity = 0 Cyber Patrol = not blocked
sex = 0 Net Nanny = not blocked
violence = 0 SurfWatch = not blocked

Yahoo Search Results

51. Yahoo! Movies
http://movies.yahoo.com/

language = 1 CYBERsitter = not blocked
nudity = 0 Cyber Patrol = not blocked
sex = 0 Net Nanny = not blocked
violence = 0 SurfWatch = not blocked

52. Yahoo! Yellow Pages
http://yp.yahoo.com/

language = 0 CYBERsitter = not blocked
nudity = 0 Cyber Patrol = not blocked
sex = 0 Net Nanny = not blocked
violence = 0 SurfWatch = not blocked

53. Yahoo! Shopping
http://shopping.yahoo.com/

language = 0 CYBERsitter = not blocked
nudity = 0 Cyber Patrol = not blocked
sex = 0 Net Nanny = not blocked
violence = 0 SurfWatch = not blocked

54. Yahoo! Local Events
http://localevents.yahoo.com/

language = 0 CYBERsitter = blocked
nudity = 0 Cyber Patrol = not blocked
sex = 0 Net Nanny = not blocked
violence = 0 SurfWatch = not blocked

55. Yahoo Weather Forecast
http://weather.yahoo.com/

language = 0 CYBERsitter = not blocked
nudity = 0 Cyber Patrol = not blocked
sex = 0 Net Nanny = not blocked
violence = 0 SurfWatch = not blocked

56. Yahoo! Travel
http://travel.yahoo.com/

language = 0 CYBERsitter = not blocked
nudity = 0 Cyber Patrol = not blocked
sex = 0 Net Nanny = not blocked
violence = 0 SurfWatch = not blocked

57. Yahoo! Games
http://games.yahoo.com/

language = 0 CYBERsitter = not blocked

nudity = 0 Cyber Patrol = not blocked
sex = 0 Net Nanny = not blocked
violence = 1 SurfWatch = not blocked

58. Yahoo! The Motley Fool
http://fnews.yahoo.com/fool/

language = 0 CYBERsitter = not blocked
nudity = 0 Cyber Patrol = not blocked
sex = 0 Net Nanny = not blocked
violence = 0 SurfWatch = not blocked

59. Yahoo! Real Estate
http://realestate.yahoo.com/

language = 0 CYBERsitter = not blocked
nudity = 0 Cyber Patrol = not blocked
sex = 0 Net Nanny = not blocked
violence = 0 SurfWatch = not blocked

60. Yahoo! Lodging
http://lodging.yahoo.com/

language = 0 CYBERsitter = not blocked
nudity = 0 Cyber Patrol = not blocked
sex = 0 Net Nanny = not blocked
violence = 0 SurfWatch = not blocked

Warez Search Results

61. pages. prodigy. . . erswarez. html
http://pages.prodigy.com/OH/hackershell/hackerswarez.html

language = 1 CYBERsitter = not blocked
nudity = 0 Cyber Patrol = blocked
sex = 0 Net Nanny = not blocked
violence = 1 SurfWatch = not blocked

62. Pennywise's Warez Page
http://www.pemmy.demon.co.uk/index.htm

language = 1 CYBERsitter = not blocked
nudity = 0 Cyber Patrol = blocked
sex = 0 Net Nanny = not blocked
violence = 3 SurfWatch = not blocked

63. Warez Mp3 Dimension !
http://mp3.warezdimension.com/

language = 4 CYBERsitter = blocked
nudity = 2 Cyber Patrol = blocked
sex = 3 Net Nanny = not blocked
violence = 0 SurfWatch = blocked

64. 50 Best Warez Sites
http://w50.village21.com/w50/all66.htm

language = 3 CYBERsitter = blocked
nudity = 0 Cyber Patrol = not blocked
sex = 0 Net Nanny = not blocked
violence = 0 SurfWatch = not blocked

65. Dominating Minds International Warez
http://www.dominating.net/main.html

language = 4 CYBERsitter = blocked
nudity = 0 Cyber Patrol = blocked
sex = 0 Net Nanny = not blocked
violence = 0 SurfWatch = not blocked

66. Warez _4 _Free
http://warez-4-free.particles.org/

language = 0 CYBERsitter = not blocked
nudity = 0 Cyber Patrol = not blocked
sex = 0 Net Nanny = not blocked
violence = 0 SurfWatch = not blocked

67. The Toplist of Mp3/warez Sites
http://members.spree.com/sip/toplist/toplist.html

language = 0 CYBERsitter = not blocked
nudity = 0 Cyber Patrol = not blocked
sex = 0 Net Nanny = not blocked
violence = 0 SurfWatch = not blocked

68. main. html
http://members.tripod.com/~masters1998/main.html

language = 3 CYBERsitter = not blocked
nudity = 0 Cyber Patrol = not blocked
sex = 0 Net Nanny = not blocked
violence = 0 SurfWatch = not blocked

69. index. html
http://homepages.paradise.net.nz/~fishboy/index.html

language = 0 CYBERsitter = not blocked
nudity = 0 Cyber Patrol = not blocked
sex = 0 Net Nanny = not blocked
violence = 0 SurfWatch = not blocked

70. The Warez Fix0r
http://www.wirm.net/main.html

language = 0 CYBERsitter = not blocked
nudity = 0 Cyber Patrol = not blocked
sex = 0 Net Nanny = not blocked
violence = 0 SurfWatch = not blocked

Hotmail Search Results

71. CNET News. com - Microsoft buys Hotmail
http://www.news.com/News/Item/0,4,17725,00.html

language = 0 CYBERsitter = not blocked
nudity = 0 Cyber Patrol = not blocked
sex = 0 Net Nanny = not blocked
violence = 0 SurfWatch = not blocked

72. HOTMAIL MOST VULNERABLE E-MAIL ACCOUNT
http://www.geocities.com/ResearchTriangle/Lab/6601/shailesh/hotmail.html

language = 0 CYBERsitter = not blocked
nudity = 0 Cyber Patrol = not blocked
sex = 0 Net Nanny = not blocked
violence = 0 SurfWatch = not blocked

73. Hotmail exploit
http://rubicon.cx.net/~munkean/hotmail.html

language = 0 CYBERsitter = not blocked
nudity = 0 Cyber Patrol = not blocked
sex = 0 Net Nanny = not blocked
violence = 0 SurfWatch = not blocked

74. Hotmail Accounts Easily Accessed by Hackers - Nus - Email
http://email.miningco.com/library/nus/bl120898-1.htm

language = 0 CYBERsitter = not blocked
nudity = 0 Cyber Patrol = not blocked
sex = 0 Net Nanny = not blocked
violence = 0 SurfWatch = not blocked

75. Hotmail posts fix to password flaw
http://www.zdnet.com/zdnn/stories/zdnn_smgraph_display/0,3441,2131377,00.html

language = 0 CYBERsitter = not blocked
nudity = 0 Cyber Patrol = not blocked
sex = 0 Net Nanny = not blocked
violence = 0 SurfWatch = not blocked

76. CNET News. com - Hotmail bug fix not a cure-all
http://www.news.com/News/Item/0,4,25662,00.html

language = 0 CYBERsitter = not blocked

nudity = 0 Cyber Patrol = not blocked
sex = 0 Net Nanny = not blocked
violence = 0 SurfWatch = not blocked

77. CNET News. com - New security glitch for Hotmail
http://www.news.com/News/Item/0,4,25887,00.html

language = 0 CYBERsitter = not blocked
nudity = 0 Cyber Patrol = not blocked
sex = 0 Net Nanny = not blocked
violence = 0 SurfWatch = not blocked

78. Hotmail - The World's FREE Web-Based Email
http://www.hotmailpop3.8m.com/

language = 0 CYBERsitter = not blocked
nudity = 0 Cyber Patrol = not blocked
sex = 0 Net Nanny = not blocked
violence = 0 SurfWatch = not blocked

79. crazybytes domain supplied by RM meinenr@hotmail. com
http://www.crazybytes-cd.com/

language = 0 CYBERsitter = not blocked
nudity = 0 Cyber Patrol = blocked
sex = 0 Net Nanny = not blocked
violence = 0 SurfWatch = blocked

80. Hotmail glitch tricks users into revealing passwords
http://www.zdnet.com/zdnn/stories/zdnn_smgraph_display/0,3441,2131228,00.html

language = 0 CYBERsitter = not blocked
nudity = 0 Cyber Patrol = not blocked
sex = 0 Net Nanny = not blocked
violence = 0 SurfWatch = not blocked

Sex Search Results

81. Free Sex Pics Nude Girls Fucking Hardcore Sex Pics
http://www.xxxhardcore.net/main.htm

language = 4 CYBERsitter = blocked
nudity = 4 Cyber Patrol = blocked
sex = 4 Net Nanny = blocked
violence = 1 SurfWatch = blocked

82. UltraVixen
http://www.ultravixen.com/

language = 4 CYBERsitter = blocked
nudity = 3 Cyber Patrol = blocked
sex = 4 Net Nanny = not blocked
violence = 0 SurfWatch = blocked

83. Videoconferencing, live sex, video sex, phone sex, xxx
http://www.xtacy.com/

language = 4 CYBERsitter = blocked
nudity = 4 Cyber Patrol = not blocked
sex = 4 Net Nanny = not blocked
violence = 0 SurfWatch = blocked

84. Your Trial Membership for 3sex. com is FREE
http://w-w.3sex.com/guests/

language = 4 CYBERsitter = blocked
nudity = 4 Cyber Patrol = blocked
sex = 4 Net Nanny = not blocked
violence = 0 SurfWatch = blocked

85. HappyNight - Nr. 1 in Europa, der Sex- und Erotikführer
http://www.weekend.de/Home/HappyNightE.htm

language = 4 CYBERsitter = blocked
nudity = 4 Cyber Patrol = not blocked
sex = 4 Net Nanny = not blocked
violence = 0 SurfWatch = blocked

86. 411 for Sex
http://www.411forsex.com/411.html

language = 4 CYBERsitter = blocked
nudity = 3 Cyber Patrol = blocked
sex = 4 Net Nanny = blocked
violence = 0 SurfWatch = blocked

87. Gossips !
http://www.gossips.com/

language = 4 CYBERsitter = blocked
nudity = 4 Cyber Patrol = not blocked
sex = 4 Net Nanny = not blocked
violence = 0 SurfWatch = blocked

88. Trailer Park Trash!
http://www.trailerparktrash.com/

language = 4 CYBERsitter = blocked
nudity = 4 Cyber Patrol = blocked
sex = 4 Net Nanny = not blocked
violence = 0 SurfWatch = blocked

89. info. htm
http://www.sexis.com/russia/info.htm

language = 0 CYBERsitter = blocked
nudity = 3 Cyber Patrol = not blocked
sex = 0 Net Nanny = not blocked
violence = 0 SurfWatch = blocked

90. Animal Instincts- xxx adult free nude sex pics
http://www.animal-instincts.com/pix1.htm

language = 4 CYBERsitter = blocked
nudity = 4 Cyber Patrol = blocked
sex = 4 Net Nanny = blocked

violence = 0 SurfWatch = blocked

MP3 Search Results

91. actions. php3
http://www.radiomoi.com/radio-moi/actions.php3?

language = 0 CYBERsitter = not blocked
nudity = 0 Cyber Patrol = not blocked
sex = 0 Net Nanny = not blocked
violence = 0 SurfWatch = not blocked

92. right2. htm
http://doboy.digitaljams.com/right2.htm

language = 1 CYBERsitter = not blocked
nudity = 0 Cyber Patrol = not blocked
sex = 0 Net Nanny = not blocked
violence = 0 SurfWatch = not blocked

93. Crowes MP3 Page
http://crowe.lightspeed.net/bands.html

language = 0 CYBERsitter = not blocked
nudity = 0 Cyber Patrol = not blocked
sex = 0 Net Nanny = not blocked
violence = 0 SurfWatch = not blocked

94. MP3 Downloads
http://www.mp3now.com/html/downloads.html

language = 0 CYBERsitter = not blocked
nudity = 0 Cyber Patrol = not blocked
sex = 0 Net Nanny = not blocked
violence = 0 SurfWatch = not blocked

95. MP3 Contest Battle of the Web Bands Alternative Music
http://musicglobalnetwork.com/alternative.html

language = 0 CYBERsitter = not blocked

nudity = 0 Cyber Patrol = not blocked
sex = 0 Net Nanny = not blocked
violence = 0 SurfWatch = not blocked

96. MP3 News - MP3 News Daily. . .
http://www.mp3.com/news/daily.html

language = 0 CYBERsitter = not blocked
nudity = 0 Cyber Patrol = not blocked
sex = 0 Net Nanny = not blocked
violence = 0 SurfWatch = not blocked

97. Digital-Death METAL Online Ordering
http://www.digital-death.org/

language = 1 CYBERsitter = not blocked
nudity = 0 Cyber Patrol = not blocked
sex = 0 Net Nanny = not blocked
violence = 0 SurfWatch = not blocked

98. Empeg Ltd's Empeg MP3 Car Audio Player
http://www.empeg.com/main.html

language = 0 CYBERsitter = not blocked
nudity = 0 Cyber Patrol = not blocked
sex = 0 Net Nanny = not blocked
violence = 0 SurfWatch = not blocked

99. MP3Bench. com - Site re-opening in a few weeks.
http://mp3bench.com/

language = 0 CYBERsitter = not blocked
nudity = 0 Cyber Patrol = not blocked
sex = 0 Net Nanny = not blocked
violence = 0 SurfWatch = not blocked

100. Rio Pmp300 Par Port 32Mb Mp3 Player W/ Headphones
http://www.netsales.net/pk.wcgi/wxusa/prod/1216674-1

language = 0 CYBERsitter = not blocked
nudity = 0 Cyber Patrol = not blocked
sex = 0 Net Nanny = not blocked
violence = 0 SurfWatch = not blocked

COPA litigants

101. Welcome to UPSIDE TODAY
http://www.upsidetoday.com/

language = 0 CYBERsitter = not blocked
nudity = 0 Cyber Patrol = not blocked
sex = 0 Net Nanny = not blocked
violence = 0 SurfWatch = not blocked

102. Welcome to City Lights Booksellers and Publishers
http://www.citylights.com/

language = 0 CYBERsitter = not blocked
nudity = 0 Cyber Patrol = not blocked
sex = 0 Net Nanny = not blocked
violence = 0 SurfWatch = not blocked

103. Sexual Health Network - Sexuality and Disability or Illness
http://www.sexualhealth.com/

language = 4 CYBERsitter = blocked
nudity = 3 Cyber Patrol = blocked
sex = 1 Net Nanny = not blocked
violence = 0 SurfWatch = not blocked

104. A Different Light Bookstore: Gay and Lesbian Literature
http://www.adlbooks.com/

language = 0 CYBERsitter = blocked
nudity = 0 Cyber Patrol = not blocked
sex = 0 Net Nanny = not blocked
violence = 0 SurfWatch = not blocked

105. BookWeb: BookWeb Home Page
http://www.bookweb.org/

language = 0 CYBERsitter = not blocked
nudity = 0 Cyber Patrol = not blocked
sex = 0 Net Nanny = not blocked
violence = 0 SurfWatch = not blocked

106. artnet. com home page
http://www.artnet.com/

language = 0 CYBERsitter = not blocked
nudity = 0 Cyber Patrol = not blocked
sex = 0 Net Nanny = not blocked
violence = 0 SurfWatch = not blocked

107. The BlackStripe
http://www.blackstripe.com/

language = 4 CYBERsitter = blocked
nudity = 0 Cyber Patrol = not blocked
sex = 4 Net Nanny = not blocked
violence = 0 SurfWatch = not blocked

108. Condoms @ Condomania | Condomania's World of Safer Sex
http://www.condomania.com/

language = 4 CYBERsitter = blocked
nudity = 1 Cyber Patrol = blocked
sex = 0 Net Nanny = not blocked
violence = 0 SurfWatch = blocked

109. Free Speech Internet Television
http://www.freespeech.org/

language = 0 CYBERsitter = not blocked
nudity = 0 Cyber Patrol = not blocked
sex = 0 Net Nanny = not blocked

violence = 1 SurfWatch = blocked

110. Internet Content Coalition
http://www.netcontent.org/

language = 0 CYBERsitter = not blocked
nudity = 0 Cyber Patrol = not blocked
sex = 0 Net Nanny = not blocked
violence = 0 SurfWatch = not blocked

111. OBGYN. net - The Obstetrics & Gynecology Network
http://www.obgyn.net/

language = 0 CYBERsitter = not blocked
nudity = 0 Cyber Patrol = not blocked
sex = 0 Net Nanny = not blocked
violence = 0 SurfWatch = not blocked

112. PGN Philadelphia Gay News
http://www.epgn.com/

language = 0 CYBERsitter = not blocked
nudity = 0 Cyber Patrol = not blocked
sex = 0 Net Nanny = not blocked
violence = 0 SurfWatch = not blocked

113. PlanetOut: Land On It!
http://www.planetout.com/

language = 1 CYBERsitter = blocked
nudity = 0 Cyber Patrol = not blocked
sex = 0 Net Nanny = not blocked
violence = 0 SurfWatch = not blocked

114. Powell's Books - New, Used, and Out of Print
http://www.powells.com/

language = 0 CYBERsitter = not blocked

nudity = 0 Cyber Patrol = not blocked
sex = 0 Net Nanny = not blocked
violence = 0 SurfWatch = not blocked

115. www. riotgrrl. com/
http://www.riotgrrl.com/

language = 0 CYBERsitter = blocked
nudity = 1 Cyber Patrol = blocked
sex = 0 Net Nanny = not blocked
violence = 0 SurfWatch = blocked

116. Salon. com
http://www.salon.com/

language = 1 CYBERsitter = not blocked
nudity = 0 Cyber Patrol = not blocked
sex = 0 Net Nanny = not blocked
violence = 0 SurfWatch = not blocked

117. West Stock digital stock photography
http://www.weststock.com/

language = 0 CYBERsitter = not blocked
nudity = 0 Cyber Patrol = not blocked
sex = 0 Net Nanny = not blocked
violence = 0 SurfWatch = not blocked

CDA Litigants

118. ACLU: American Civil Liberties Union
http://www.aclu.org/

language = 0 CYBERsitter = not blocked
nudity = 0 Cyber Patrol = not blocked
sex = 0 Net Nanny = not blocked
violence = 0 SurfWatch = not blocked

119. AIDS HIV AEGIS
http://www.aegis.com/

language = 0 CYBERsitter = not blocked
nudity = 0 Cyber Patrol = not blocked
sex = 0 Net Nanny = not blocked
violence = 0 SurfWatch = not blocked

120. BiblioBytes
http://www.bb.com/

language = 0 CYBERsitter = not blocked
nudity = 0 Cyber Patrol = not blocked
sex = 0 Net Nanny = not blocked
violence = 0 SurfWatch = not blocked

121. Clarinet Communications Corp. Home Page
http://www.clari.net/

language = 0 CYBERsitter = not blocked
nudity = 0 Cyber Patrol = not blocked
sex = 0 Net Nanny = not blocked
violence = 1 SurfWatch = not blocked

122. Critical Path AIDS Project
http://www.critpath.org/

language = 0 CYBERsitter = not blocked
nudity = 0 Cyber Patrol = not blocked
sex = 0 Net Nanny = not blocked
violence = 0 SurfWatch = not blocked

123. Computer Professionals for Social Responsibility
http://www.cpsr.org/

language = 0 CYBERsitter = not blocked
nudity = 0 Cyber Patrol = not blocked
sex = 0 Net Nanny = not blocked
violence = 0 SurfWatch = not blocked

124. EFFweb - The Electronic Frontier Foundation
http://www.eff.org/

language = 0 CYBERsitter = not blocked
nudity = 0 Cyber Patrol = not blocked
sex = 0 Net Nanny = not blocked
violence = 0 SurfWatch = not blocked

125. Electronic Privacy Information Center
http://www.epic.org/

language = 0 CYBERsitter = not blocked
nudity = 0 Cyber Patrol = not blocked
sex = 0 Net Nanny = not blocked
violence = 0 SurfWatch = not blocked

126. The Ethical Spectacle
http://www.spectacle.org/

language = 0 CYBERsitter = not blocked
nudity = 0 Cyber Patrol = not blocked
sex = 0 Net Nanny = not blocked
violence = 0 SurfWatch = not blocked

127. Human Rights Watch - Home Page
http://www.hrw.org/

language = 0 CYBERsitter = not blocked
nudity = 0 Cyber Patrol = not blocked
sex = 0 Net Nanny = not blocked
violence = 0 SurfWatch = not blocked

128. Journalism Education Association
http://www.jea.org/

language = 0 CYBERsitter = not blocked
nudity = 0 Cyber Patrol = not blocked
sex = 0 Net Nanny = not blocked

violence = 0 SurfWatch = not blocked

129. The Justice on Campus Project
http://joc.mit.edu/

language = 0 CYBERsitter = not blocked
nudity = 0 Cyber Patrol = not blocked
sex = 0 Net Nanny = not blocked
violence = 0 SurfWatch = not blocked

130. CyberWire Dispatch, by Brock N. Meeks
http://www.cyberwerks.com/cyberwire/

language = 0 CYBERsitter = not blocked
nudity = 0 Cyber Patrol = not blocked
sex = 0 Net Nanny = not blocked
violence = 0 SurfWatch = not blocked

131. National Writers Union Home Page
http://www.nwu.org//

language = 0 CYBERsitter = not blocked
nudity = 0 Cyber Patrol = not blocked
sex = 0 Net Nanny = not blocked
violence = 0 SurfWatch = not blocked

132. Planned Parenthood
http://www.plannedparenthood.org/

language = 0 CYBERsitter = blocked
nudity = 0 Cyber Patrol = not blocked
sex = 0 Net Nanny = not blocked
violence = 0 SurfWatch = not blocked

133. Queer Resources Directory
http://www.qrd.org/qrd/

language = 1 CYBERsitter = blocked

nudity = 0 Cyber Patrol = not blocked
sex = 0 Net Nanny = blocked
violence = 0 SurfWatch = not blocked

134. Stop Prisoner Rape, Inc.
http://www.igc.apc.org/spr/

language = 0 CYBERsitter = blocked
nudity = 0 Cyber Patrol = blocked
sex = 0 Net Nanny = not blocked
violence = 0 SurfWatch = not blocked

135. s a f e r s e x . o r g | an online journal of safe sexuality
http://www.safersex.org/

language = 0 CYBERsitter = blocked
nudity = 4 Cyber Patrol = blocked
sex = 0 Net Nanny = not blocked
violence = 0 SurfWatch = not blocked

136. Gay Wired Presents Wildcat Press
http://www.gaywired.com/wildcat/index.html

language = 0 CYBERsitter = blocked
nudity = 0 Cyber Patrol = blocked
sex = 0 Net Nanny = not blocked
violence = 0 SurfWatch = not blocked

Portals

137. Yahoo!
http://www.yahoo.com/

language = 0 CYBERsitter = not blocked
nudity = 0 Cyber Patrol = not blocked
sex = 0 Net Nanny = not blocked
violence = 0 SurfWatch = not blocked

138. GO Network
http://www.go.com/

language = 0 CYBERsitter = not blocked
nudity = 0 Cyber Patrol = not blocked
sex = 0 Net Nanny = not blocked
violence = 0 SurfWatch = not blocked

139. Excite
http://www.excite.com/

language = 0 CYBERsitter = not blocked
nudity = 0 Cyber Patrol = not blocked
sex = 0 Net Nanny = not blocked
violence = 0 SurfWatch = not blocked

140. AltaVista
http://www.altavista.com/

language = 0 CYBERsitter = not blocked
nudity = 0 Cyber Patrol = not blocked
sex = 0 Net Nanny = not blocked
violence = 0 SurfWatch = not blocked

141. Snap
http://www.snap.com/

language = 0 CYBERsitter = not blocked
nudity = 0 Cyber Patrol = not blocked
sex = 0 Net Nanny = not blocked
violence = 0 SurfWatch = not blocked

Political Sites

142. Welcome To The White House
http://www.whitehouse.gov/WH/Welcome.html

language = 0 CYBERsitter = not blocked
nudity = 0 Cyber Patrol = not blocked
sex = 0 Net Nanny = blocked
violence = 0 SurfWatch = not blocked

143. United States House of Representatives - 106th Congress
http://www.house.gov/

language = 0 CYBERsitter = not blocked
nudity = 0 Cyber Patrol = not blocked
sex = 0 Net Nanny = not blocked
violence = 0 SurfWatch = not blocked

144. Republican National Committee
http://www.rnc.org/

language = 0 CYBERsitter = not blocked
nudity = 0 Cyber Patrol = not blocked
sex = 0 Net Nanny = not blocked
violence = 0 SurfWatch = not blocked

145. DNC Homepage
http://www.democrats.org/index.html

language = 0 CYBERsitter = not blocked
nudity = 0 Cyber Patrol = not blocked
sex = 0 Net Nanny = not blocked
violence = 0 SurfWatch = not blocked

146. Welcome to the Gore 2000 web site
http://www.algore2000.com/

language = 0 CYBERsitter = not blocked
nudity = 0 Cyber Patrol = not blocked
sex = 0 Net Nanny = not blocked
violence = 0 SurfWatch = not blocked

Feminist Sites

147. National Organization for Women (NOW) Home Page
http://www.now.org/

language = 0 CYBERsitter = blocked
nudity = 0 Cyber Patrol = not blocked
sex = 0 Net Nanny = not blocked
violence = 0 SurfWatch = not blocked

148. FEMINIST MAJORITY FOUNDATION
http://www.feminist.org/

language = 0 CYBERsitter = not blocked
nudity = 0 Cyber Patrol = not blocked
sex = 0 Net Nanny = not blocked
violence = 0 SurfWatch = not blocked

149. Women Leaders Online & Women Organizing for Change
http://wlo.org/

language = 0 CYBERsitter = not blocked
nudity = 0 Cyber Patrol = not blocked
sex = 0 Net Nanny = not blocked
violence = 0 SurfWatch = not blocked

150. Guerrilla Girls: Facts, Humor and Fake Fur
http://www.guerrillagirls.com/

language = 0 CYBERsitter = blocked
nudity = 1 Cyber Patrol = not blocked
sex = 0 Net Nanny = not blocked
violence = 0 SurfWatch = not blocked

151. Feminism at Feminist Utopia
http://www.FeministUtopia.com/

language = 1 CYBERsitter = not blocked
nudity = 1 Cyber Patrol = not blocked
sex = 0 Net Nanny = not blocked
violence = 0 SurfWatch = not blocked

Hate Sites

152. KKK. COM Homepage
http://www.kkk.com/

language = 4 CYBERsitter = blocked
nudity = 0 Cyber Patrol = blocked
sex = 0 Net Nanny = blocked
violence = 1 SurfWatch = not blocked

153. www. resist. com/

language = 4 CYBERsitter = not blocked
nudity = 0 Cyber Patrol = blocked
sex = 0 Net Nanny = blocked
violence = 1 SurfWatch = blocked

154. Stormfront White Nationalist / White Pride Resource
http://www.stormfront.org/

language = 4 CYBERsitter = blocked
nudity = 0 Cyber Patrol = blocked
sex = 0 Net Nanny = blocked
violence = 0 SurfWatch = blocked

155. Home Web page of Arthur R. Butz
http://pubweb.acns.nwu.edu/~abutz/

language = 0 CYBERsitter = not blocked
nudity = 0 Cyber Patrol = not blocked
sex = 0 Net Nanny = blocked
violence = 0 SurfWatch = blocked

156. Adelaide Institute - The final Intellectual adventure of the 20th century
http://www.adam.com.au/fredadin/adins.html

language = 0 CYBERsitter = not blocked
nudity = 0 Cyber Patrol = not blocked
sex = 0 Net Nanny = blocked
violence = 0 SurfWatch = blocked

Gambling Sites

157. Atlantis Gaming
http://www.atlantis-gaming.com/

language = 0 CYBERsitter = not blocked
nudity = 0 Cyber Patrol = blocked
sex = 0 Net Nanny = not blocked

violence = 0 SurfWatch = blocked

158. All Sports Casino - Online Offshore Internet Sports Book and Casino
http://www.allsportscasino.com/

language = 0 CYBERsitter = blocked
nudity = 0 Cyber Patrol = blocked
sex = 0 Net Nanny = not blocked
violence = 0 SurfWatch = blocked

159. Sportxction
http://www.sportxction.com/

language = 0 CYBERsitter = not blocked
nudity = 0 Cyber Patrol = not blocked
sex = 0 Net Nanny = not blocked
violence = 0 SurfWatch = not blocked

160. Casino/Sportsbook at Superbet. com Casino and Sportsbook!
http://www.superbet.com/

language = 0 CYBERsitter = not blocked
nudity = 0 Cyber Patrol = blocked
sex = 0 Net Nanny = blocked
violence = 0 SurfWatch = not blocked

161. online casinos, internet casino, internet gambling, online casino
http://www.platinumcasino.com/

language = 0 CYBERsitter = blocked
nudity = 0 Cyber Patrol = not blocked
sex = 0 Net Nanny = not blocked
violence = 0 SurfWatch = blocked

Religous Sites

162. The Holy See
http://www.vatican.va/

language = 0 CYBERsitter = not blocked
nudity = 0 Cyber Patrol = not blocked
sex = 0 Net Nanny = not blocked
violence = 0 SurfWatch = not blocked

163. Muslims Online - The Muslim Community Online
http://www.muslimsonline.com/

language = 0 CYBERsitter = not blocked
nudity = 0 Cyber Patrol = not blocked
sex = 0 Net Nanny = not blocked
violence = 0 SurfWatch = not blocked

164. Project Genesis: Torah on the Information Superhighway
http://www.torah.org/

language = 0 CYBERsitter = not blocked
nudity = 0 Cyber Patrol = not blocked
sex = 0 Net Nanny = not blocked
violence = 0 SurfWatch = not blocked

165. http://www. hinduism. co. za
http://www.hinduism.co.za/

language = 0 CYBERsitter = not blocked
nudity = 0 Cyber Patrol = not blocked
sex = 0 Net Nanny = not blocked
violence = 0 SurfWatch = not blocked

166. Scientology: SCIENTOLOGY HOME PAGE
http://www.scientology.org/

language = 0 CYBERsitter = blocked
nudity = 0 Cyber Patrol = not blocked
sex = 0 Net Nanny = not blocked
violence = 0 SurfWatch = not blocked

Gay Sites

167. QWorld Contents Page

http://www.qworld.org/TOC.html

language = 0 CYBERsitter = blocked
nudity = 0 Cyber Patrol = blocked
sex = 0 Net Nanny = not blocked
violence = 0 SurfWatch = not blocked

168. Pride Net
http://www.pridenet.com/

language = 0 CYBERsitter = blocked
nudity = 0 Cyber Patrol = not blocked
sex = 0 Net Nanny = not blocked
violence = 0 SurfWatch = not blocked

169. Welcome to The QueerZone!
http://www.queerzone.com/

language = 0 CYBERsitter = blocked
nudity = 0 Cyber Patrol = not blocked
sex = 0 Net Nanny = not blocked
violence = 0 SurfWatch = not blocked

170. Out on the Web
http://www.outontheweb.com/ootw/home/home.html

language = 0 CYBERsitter = not blocked
nudity = 0 Cyber Patrol = not blocked
sex = 0 Net Nanny = not blocked
violence = 0 SurfWatch = not blocked

171. Queer Living - "Promoting With Pride"
http://www.qmondo.com/queerliving/

language = 0 CYBERsitter = blocked
nudity = 0 Cyber Patrol = blocked
sex = 0 Net Nanny = not blocked
violence = 0 SurfWatch = not blocked

Alcohol, Tobacco, Drugs

172. Budweiser. com
http://www.budweiser.com/homepage/default.html

language = 0 CYBERsitter = not blocked
nudity = 0 Cyber Patrol = blocked
sex = 0 Net Nanny = not blocked
violence = 0 SurfWatch = blocked

173. Absolut Vodka
http://www.absolutvodka.com/

language = 0 CYBERsitter = blocked
nudity = 0 Cyber Patrol = blocked
sex = 0 Net Nanny = not blocked
violence = 0 SurfWatch = blocked

174. RJ Reynolds Tobacco Company Home Page
http://www.rjrt.com/

language = 0 CYBERsitter = not blocked
nudity = 0 Cyber Patrol = not blocked
sex = 0 Net Nanny = not blocked
violence = 0 SurfWatch = blocked

175. Welcome to UST
http://www.ustshareholder.com/

language = 0 CYBERsitter = not blocked
nudity = 0 Cyber Patrol = not blocked
sex = 0 Net Nanny = not blocked
violence = 0 SurfWatch = not blocked

176. Welcome to NORML
http://www.natlnorml.org/

language = 0 CYBERsitter = not blocked
nudity = 0 Cyber Patrol = not blocked
sex = 0 Net Nanny = not blocked
violence = 0 SurfWatch = not blocked

Porn Sites

177. www. 18Only. com
http://www.18only.com/

language = 4 CYBERsitter = blocked
nudity = 4 Cyber Patrol = not blocked
sex = 4 Net Nanny = not blocked
violence = 0 SurfWatch = not blocked

178. 4 AMATUER LOVERS
http://www.4amateurlovers.com/

language = 4 CYBERsitter = blocked
nudity = 4 Cyber Patrol = blocked
sex = 4 Net Nanny = not blocked
violence = 0 SurfWatch = not blocked

179. BIG NIPPLE : tits,tinytits,nipples
http://www.bignipple.com/

language = 4 CYBERsitter = blocked
nudity = 4 Cyber Patrol = blocked
sex = 4 Net Nanny = not blocked
violence = 0 SurfWatch = not blocked

180. MoneyGirls. Com!!
http://www.moneygirls.com/

language = 4 CYBERsitter = blocked
nudity = 4 Cyber Patrol = blocked
sex = 4 Net Nanny = not blocked
violence = 0 SurfWatch = not blocked

181. Vegas Virgins - sex, xxx XXX, SEX, Sex, nudity, porn, cumshots
http://www.vegasvirgins.com/

language = 4 CYBERsitter = blocked
nudity = 4 Cyber Patrol = blocked
sex = 4 Net Nanny = not blocked

violence = 0 SurfWatch = blocked

News Sites

182. ABCNEWS. com

language = 0 CYBERsitter = not blocked
nudity = 0 Cyber Patrol = not blocked
sex = 0 Net Nanny = not blocked
violence = 0 SurfWatch = not blocked

183. CNN Interactive
http://www.cnn.com/

language = 0 CYBERsitter = not blocked
nudity = 0 Cyber Patrol = not blocked
sex = 0 Net Nanny = not blocked
violence = 0 SurfWatch = not blocked

184. MSNBC Cover Page
http://www.msnbc.com/news/default.asp

language = 0 CYBERsitter = not blocked
nudity = 0 Cyber Patrol = not blocked
sex = 0 Net Nanny = not blocked
violence = 0 SurfWatch = not blocked

185. The New York Times on the Web
http://www.nytimes.com/

language = 0 CYBERsitter = not blocked
nudity = 0 Cyber Patrol = not blocked
sex = 0 Net Nanny = not blocked
violence = 0 SurfWatch = not blocked

186. USA TODAY
http://www.usatoday.com/

language = 0 CYBERsitter = not blocked

nudity = 0 Cyber Patrol = not blocked
sex = 0 Net Nanny = not blocked
violence = 0 SurfWatch = not blocked

Violent Games

187. id Software
http://www.idsoftware.com/

language = 0 CYBERsitter = not blocked
nudity = 0 Cyber Patrol = not blocked
sex = 0 Net Nanny = not blocked
violence = 3 SurfWatch = not blocked

188. Welcome to PlanetQuake!
http://www.planetquake.com/

language = 0 CYBERsitter = not blocked
nudity = 0 Cyber Patrol = not blocked
sex = 0 Net Nanny = not blocked
violence = 3 SurfWatch = not blocked

189. Doom World
http://frag.com/doomworld/

language = 0 CYBERsitter = not blocked
nudity = 0 Cyber Patrol = not blocked
sex = 0 Net Nanny = not blocked
violence = 4 SurfWatch = not blocked

190. DUKE NUKEM
http://www.Duke-Nukem.com/duke4/index_n4.html

language = 1 CYBERsitter = not blocked
nudity = 0 Cyber Patrol = not blocked
sex = 0 Net Nanny = not blocked
violence = 3 SurfWatch = not blocked

191. P l a n e t U n r e a l
http://planetunreal.com/

language = 1 CYBERsitter = not blocked
nudity = 0 Cyber Patrol = not blocked
sex = 0 Net Nanny = not blocked
violence = 3 SurfWatch = not blocked

Safe Sex/Aids Prevention Sites

192. The Body: An AIDS and HIV Information Resource
http://www.thebody.com/index.shtml

language = 0 CYBERsitter = blocked
nudity = 0 Cyber Patrol = not blocked
sex = 0 Net Nanny = not blocked
violence = 0 SurfWatch = not blocked

193. ENJOYING SAFER SEX
http://wso.williams.edu/orgs/peerh/sex/safesex/

language = 1 CYBERsitter = blocked
nudity = 0 Cyber Patrol = not blocked
sex = 0 Net Nanny = not blocked
violence = 0 SurfWatch = not blocked

194. FPQ - Contraception
http://www.powerup.com.au/~fpq/contraception.html

language = 1 CYBERsitter = not blocked
nudity = 0 Cyber Patrol = not blocked
sex = 0 Net Nanny = not blocked
violence = 0 SurfWatch = not blocked

195. CPS Home
http://www.positive.org/Home/index.html

language = 1 CYBERsitter = blocked
nudity = 0 Cyber Patrol = blocked
sex = 0 Net Nanny = blocked
violence = 0 SurfWatch = not blocked

196. SIECUS Home Page
http://www.siecus.org/

language = 1 CYBERsitter = blocked
nudity = 0 Cyber Patrol = blocked
sex = 0 Net Nanny = not blocked
violence = 0 SurfWatch = not blocked

Abortion Sites

197. Pro-Life America
http://www.prolife.com/

language = 1 CYBERsitter = blocked
nudity = 0 Cyber Patrol = not blocked
sex = 0 Net Nanny = not blocked
violence = 0 SurfWatch = not blocked

198. National Right to Life
http://www.nrlc.org/main.htm

language = 0 CYBERsitter = not blocked
nudity = 0 Cyber Patrol = not blocked
sex = 0 Net Nanny = not blocked
violence = 0 SurfWatch = not blocked

199. ProChoice Resource Center
http://www.prochoiceresource.org/

language = 0 CYBERsitter = not blocked
nudity = 0 Cyber Patrol = not blocked
sex = 0 Net Nanny = not blocked
violence = 0 SurfWatch = not blocked

200. NARAL Choice for America
http://www.naral.org/choice/index.html

language = 0 CYBERsitter = not blocked
nudity = 0 Cyber Patrol = not blocked
sex = 0 Net Nanny = not blocked

violence = 0 SurfWatch = not blocked

Appendix 6: The Childrens' Internet Protection Act

106th CONGRESS

1st Session

S. 97

To require the installation and use by schools and libraries of a technology for filtering or blocking material on the Internet on computers with Internet access to be eligible to receive or retain universal service assistance.

IN THE SENATE OF THE UNITED STATES

January 19, 1999

Mr. MCCAIN (for himself and Mr. HOLLINGS) introduced the following bill; which was read twice and referred to the Committee on Commerce, Science, and Transportation

A BILL

To require the installation and use by schools and libraries of a technology for filtering or blocking material on the Internet on computers with Internet access to be eligible to receive or retain universal service assistance.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the `Childrens' Internet Protection Act'.

SEC. 2. NO UNIVERSAL SERVICE FOR SCHOOLS OR LIBRARIES THAT FAIL TO IMPLEMENT A FILTERING OR BLOCKING TECHNOLOGY FOR COMPUTERS WITH INTERNET ACCESS.

(a) IN GENERAL- Section 254 of the Communications Act of 1934 (47 U.S.C. 254) is amended by adding at the end thereof the following:

`(l) IMPLEMENTATION OF AN INTERNET FILTERING OR BLOCKING TECHNOLOGY-

`(1) IN GENERAL- An elementary school, secondary school, or library that fails to provide the certification required by paragraph (2) or (3), respectively, is not eligible to receive or retain universal service assistance provided under subsection (h)(1)(B).

`(2) CERTIFICATION FOR SCHOOLS- To be eligible to receive universal service assistance under subsection (h)(1)(B), an elementary or secondary school (or the school board or other authority with responsibility for administration of that school) shall certify to the Commission that it has--

`(A) selected a technology for computers with Internet access to filter or block material deemed to be harmful to minors; and

`(B) installed, or will install, and uses or will use, as soon as it obtains computers with Internet access, a technology to filter or block such material.

`(3) Certification for libraries-

`(A) LIBRARIES WITH MORE THAN 1 INTERNET-ACCESSING COMPUTER- To be eligible to receive universal service assistance under subsection (h)(1)(B), a library that has more than 1 computer with Internet access intended for use by the public (including minors) shall certify to the Commission that it has installed and uses a technology to filter or block material deemed to be harmful to minors on one or more of its computers with Internet access.

`(B) LIBRARIES WITH ONLY 1 INTERNET-ACCESSING COMPUTER- A library that has only 1 computer with Internet access intended for use by the public (including minors) is eligible to receive universal service assistance under subsection (h)(1)(B) even if it does not use a technology to filter or block material deemed to be harmful to minors on that computer if it certifies to the Commission that it employs a reasonably effective alternative means to keep minors from accessing material on the Internet that is deemed to be harmful to minors.

`(4) TIME FOR CERTIFICATION- The certification required by paragraph (2) or (3) shall be made within 30 days of the date of enactment of the Childrens' Internet Protection Act, or, if later, within 10 days of the date on which any computer with access to the Internet is first made available in the school or library for its intended use.

`(5) Notification of cessation; additional internet-accessing computer-

`(A) CESSATION- A library that has filed the certification required by paragraph (3)(A) shall notify the Commission within 10 days after the date on which it ceases to use the filtering or blocking technology to which the certification related.

`(B) ADDITIONAL INTERNET-ACCESSING COMPUTER- A library that has filed the certification required by paragraph (3)(B) that adds another computer with Internet access intended for use by the public (including minors) shall make the certification required by paragraph (3)(A) within 10 days after that computer is made available for use by the public.

`(6) PENALTY FOR FAILURE TO COMPLY- A school or library that fails to meet the requirements of this subsection is liable to repay immediately the full amount of all universal service assistance it received under subsection (h)(1)(B).

`(7) LOCAL DETERMINATION OF MATERIAL TO BE FILTERED- For purposes of paragraphs (2) and (3), the determination of what material is to be deemed harmful to minors shall be made by the school, school board, library or other authority responsible for making the required certification. No agency or instrumentality of the United States Government may--

`(A) establish criteria for making that determination;

`(B) review the determination made by the certifying school, school board, library, or other authority; or

`(C) consider the criteria employed by the certifying school, school board, library, or other authority in the administration of subsection (h)(1)(B).'.

(b) CONFORMING CHANGE- Section 254(h)(1)(B) of the Communications Act of 1934 (47 U.S.C. 254(h)(1)(B)) is amended by striking `All telecommunications' and inserting `Except as provided by subsection (l), all telecommunications'.

SEC. 3. FCC TO ADOPT RULES WITHIN 4 MONTHS.

The Federal Communications Commission shall adopt rules implementing section 254(l) of the Communications Act of 1934 within 120 days after the date of enactment of this Act.

BIBLIOGRAPHY

AltaVista (1999). About AltaVista. Available via the World Wide Web at http://www.altavista.com/av/content/about_our_technology.htm .

AltaVista. (1997, 21 May). Net Shepherd and AltaVista to offer "filtered" web search service. Available via the World Wide Web at http://www.altavista.com/av/content/pr100197.htm .

Alter, A. I. (1984). An introduction to the exhibit. in Censorship: 500 years of conflict. New York: New York Public Library.

American Civil Liberties Union. (1998). Censorship in a box: Why blocking software is wrong for public libraries. Available via the World Wide Web at http://www.aclu.org/issues/cyber/box.html .

American Civil Liberties Union. (1997, 16 July). ACLU wary of White House goals on "voluntary" internet censorship. Available via the World Wide Web at http://www.aclu.org/news/n071697a.html .

American Library Association. (1997, 1 July). Statement on library use of filtering software. Available via the World Wide Web at http://www.ala.org/alaorg/oif/filt_stm.html .

Anderson, B. (1991). Imagined communities. New York: Verso.

Arthur, C. (1997, 25 February). No censor humor. The Independent (London). N5.

Arthur, C. (1996). Real ale is too strong for American moralists. The Independent (London). 11.

Baker, C.E. (1989). Human liberty and freedom of speech. New York: Oxford.

Balkin, J. (1996). Media filters, the v-chip, and the foundations of broadcast regulation. Duke Law Journal, 45, 1131.

Bastian, J. (1997). Filtering the internet in American public libraries: Sliding down the slippery slope. First Monday, Available via the World Wide Web at http://www.firstmonday.dk/issues/issue2_10/bastian/ .

Baudrillard, J. (1983). In the shadow of the silent majorities, or, the end of the social and other essays. New York: Semiotext(e).

Bell, D. (1973). The Coming of post-industrial society: A venture in social forecasting. Harmondsworth: Penguin, Pergrine Books.

Berger, F.R. (1980). Freedom of expression. Belmont, CA: Wadsworth.

Berger, J. (1996). Zoning adult establishments in New York. Fordham Urban Journal, 24, 105.

Bertot, J.C. and McClure, C.R. (1998, October). The 1998 National Survey of Public Library Outlet Internet Connectivity. Survey prepared or the American Library Association Office for Information Technology Policy and the U.S. National Commission on Libraries and Information Science.

Bloomberg News. (1999, 13 May). Senate unanimously passes filtering bill. Bloomberg News. Available via the World Wide Web at http://www.news.com/News/Item/0,4,36540,00.html .

Board of Education v. Pico (1982). 457 U.S. 853.

Bosmajian, H. A. (1976). Obscenity and freedom of expression. New York: Burt Franklin.

Brin, D. (1998). The Transparent society. Reading, MA: Addison-Wesley.

Carey, J. (1995). The press, public opinion, and public discourse. in T. Glasser and C. Salmon (Eds.) Public opinion and the communication of consent. New York: Guilford. 373-403.

Cate, F.H. (1998). The Internet and the First Amendment: Schools and sexually explicit expression. Bloomington, IN: Phi Delta Kappa.

Censorware. (1999). Censored internet access in Utah public schools and libraries. The Censorware Project. Available via the World Wide Web at http://censorware.org/reports/utah/main.shtml .

Censorware. (1998). Cyber Patrol and Deja News. The Censorware Project. Available via the World Wide Web at http://www.censorware.org/reports/dejanews.html .

Censorware. (1998). The X-Stop files: Deja voodo. The Censorware Project. Available via the World Wide Web at http://www.censorware.org/reports/x-stop.html .

Censorware. (1997). Blacklisted by Cyber Patrol: From Ada to Yoyo. The Censorware Project. Available via the World Wide Web at http://www.censorware.org/reports/ada-yoyo.html .

City of Euclid v. Ambler Realty Co. (1926). 272 U.S. 365.

Cleaver, C. (1996, 9 September). Cyberchaos: Not First Amendment's promise. Family Research Council. Available via the World Wide Web at http://www-swiss.ai.mit.edu/6805/articles/cda/cleaver-cyberchaos.html .

Clinton, B. (1997, 16 July). Remarks by the President at event on the e-chip for the internet. The White House Office of the Press Secretary. Available via the World Wide Web at http://www.whitehouse.gov/WH/News/Ratings/remarks.html .

Clinton, B. (1997, 26 June). CDA decision statement by the President. The White House Office of the Press Secretary. Available via the World Wide at http://www.epic.org/cda/clinton_cda_decision.html .

Cornog, M. (1991). A case study of censorship? The Library of Congress and the brailling of Playboy. In Libraries, Erotica, Pornography, Martha Cornog (Ed.). Phoenix, AZ: Oryx Press.

Cornog, M. & Perper, T. (1991). For sex, see librarian. In Libraries, Erotica, Pornography, Martha Cornog (Ed.). Phoenix, AZ: Oryx Press.

Coulter, A. (1987, June). Restricting adult access to material obscene as to juveniles. Michigan Law Review, 85, 1681.

Cyber Patrol. (1999). Product literature. Available via the World Wide Web at http://www.cyberpatrol.com/ .

Davison, W.P. (1983). The third-person effect in communication. Public Opinion Quarterly, 47.

DejaNews. (1999, June) DejaNews indexed usenet newsgroups. Available via the World Wide Web at http://www.deja.com/ .

Department of Justice. (1996, 14 February). Defendant's opposition to plaintiffs' motion for a temporary restraining order. Available via the World Wide Web at http://www.epic.org/free_speech/cda/lawsuit/DOJ_brief.html .

Einstein, D. (1996, 7 March). SurfWatch strikes gold as Internet guardian. The San Francisco Chronicle. D1.

Eisenstein, E. (1980). The Printing press ss an agent of change : Communications and cultural transformations in early-modern Europe. Cambridge: Cambridge University Press.

Electronic Privacy Information Center. (1997, December). Faulty filters: How content filters block access to kid-friendly information on the internet. Available via the World Wide Web at http://www.epic.org/reports/filter-report.html .

Elmer-Dewitt, P. (1995, 3 July). On a screen near you: cyberporn. Time Magazine.

Encyclopedia Britannica Online. (1999). Europe, history of. Available via the World Wide Web at http://www.eb.com:180/bol/topic?eu=108605&sctn=1&pm=1 .

Erznoznik v. City of Jacksonville. (1975). 422 U.S. 205 .

European Commission. (1996). Green paper on the protection of minors and human dignity in audiovisual and information services. Available via the World Wide Web at http://www2.echo.lu/legal/en/internet/gpen-toc.html .

Felsenthal, E. & Sandberg, J. (1997, 27 June). High court strikes down internet smut law, Wall Street Journal, B1.

Findland, P. (1993). Humanism, politics and pornography in Renaissance Italy. in The Invention of pornography : obscenity and the origins of modernity, 1500-1800. L. Hunt (Ed.), New York: Zone Books.

Garfinkel, S. (1998, November/December). The Web's unelected government. Technology Review. Available via the World Wide Web at http://www.techreview.com/articles/nov98/garfinkel .

Garfinkel, S. (1997, May). Good clean PICS. Hotwired. Available via the World Wide Web at http://www.hotwired.com/packet/garfinkel/97/05/index2a.html .

Garry, P. (1993). An American paradox: Censorship in a nation of free speech. Westport, CN: Praeger.

Gates, B. (1999). Business @ the speed of thought : Using a digital nervous system. New York: Warner.

Gates, B. (1996). The Road ahead. New York: Penguin.

Gay and Lesbian Alliance Against Defamation. (1998). Access denied: An impact of Internet filtering software on the gay and lesbian community. Gay and Lesbian Alliance Against Defamation. Available via the World Wide Web at http://www.glaad.org/ .

Ginsberg v. New York. (1968). 390 U.S. 629.

Goldstein, R. J. (1989). Political censorship of the arts and the press in nineteenth-century Europe. New York: St. Martin's.

Goodwin, M. (1998). Cyber Rights. New York: Random House.

Gore, A. (1999, 5 May). Remarks on the Internet. White House Office of the Press Secretary. Available via the World Wide Web at http://www.whitehouse.gov/WH/New/html/19990505-4219.html .

Grassley, C. (1995, 26 June). Senate testimony. Congressional Record. S9017-S9023.

Greenwalt, K. (1989). Free Speech Justifications. Columbia Law Review, 89, 119.

Grendler, P. E. (1984). The Advent of printing. in Censorship: 500 years of conflict. New York: New York Public Library.

Guernsey, L. (1999, 8 April). Sticks and stones can hurt, but bad words pay. The New York Times.

Hoffman, D. and Novak, T. (1995). Rimm commentary. Project 2000. Available via the World Wide Web at http://www2000.ogsm.vanderbilt.edu .

Hoyt, O. G. & Hoyt, E. P. (1970). Censorship in America. New York: Seabury.

Hudson, D. (1998, 3 May). Pornography and the Internet: Tackling an old issue in a new medium. Free!. The Freedom Forum Online. Available via the World Wide Web at http://www.freedomforum.org/ .

James v. Board of Education. (1972). 461 F.2d 566, 573, 2d Cir.

Jansen, S. C. (1988). Censorship: The Knot that binds power and knowledge. New York: Oxford.

Johnson, P. (1996, November). Pornography drives technology: Why not censor the Internet. Federal Communications Law Journal, 49, 217.

Kahle, B. (1997, March). Preserving the Internet. Scientific American. Available via the World Wide Web at http://www.sciam.com/0397issue/0397kahle.html .

K.I.D.S. (1998, 26 February). Position Paper. Available via the World Wide Web at http://www.garlic.com/~robthrr/KIDS/report.html .

Kendrick, W. (1987). The Secret museum: Pornography in modern culture. New York: Viking.

Kennard, W. (1999, May 4). Remarks of William Kennard at the Annenberg Public Policy Center conference on Internet and the family. Available

via the World Wide Web at
http://www.fcc.gov/Speeches/Kennard/spwek916.html .

Kruger, C. (1998). Censoring the Internet with PICS: An Australian stakeholder analysis. Research Report No. 5. LaTrobe University Online Media Program. Available via the World Wide Web at http://teloz.latrobe.edu.au/reports/kruger.pdf .

Kubota, G. (1997). Public school usage of internet filtering software: Book banning reincarnated? Loyola of Los Angeles Entertainment Law Journal, 17.

Lasica, J. (1997, October). X-rated ratings? American Journalism Review NewsLink. Available via the World Wide Web at http://ajr.newslink.org/ajrjdl21.html .

Lasica, J. (1997, 31 July). Ratings today, censorship tomorrow. Salon. Available via the World Wide Web at http://www.salonmagazine.com/july97/21st/ratings970731.html .

Lawrence, D.H. (1936). Pornography and so on. London: Faber and Faber.

Lessig, L. & Resnick, P. (1998, September). The Architectures of mandated access controls. Unpublished draft. Presented at the Telecommunications Policy Research Conference.

Lessig, L. (1998, September). The law of the horse: What cyberlaw might teach. Unpublished draft. Available via the World Wide Web at http://cyber.harvard.edu/works/lessig/LNC_Q_D2.PDF .

Lessig, L. (1998, May). What things regulate speech: CDA 2.0 vs. filtering. Unpublished draft. Available via the World Wide Web at http://cyber.harvard.edu/works/lessig/what_things.pdf .

Lessig, L. (1998, March). The Laws of cyberspace. Paper presented at Taiwan Net '98, Taipei, Taiwan. Available via the World Wide Web at http://cyber.harvard.edu/works/lessig/laws_cyberspace.pdf .

Lessig, L. (1996). Reading the constitution in cyberspace. Emory Law Journal, 45 (3).

Lessig, L. (1996). The Zones of cyberspace. Stanford Law Review, 48, 1403.

Liszt directory (1999, June). Mailing lists, newsgroups, and IRC channels indexed by Liszt. Available via the World Wide Web at http://www.liszt.com/ .

Macavinta, C. (1999, 16 March). ICQ filter ensnarled in free speech debate. News.com. Available via the World Wide Web at http://www.news.com/ .

Macavinta, C. (1999, 3 February). Net filters foiled again. News.com. Available via the World Wide Web at http://www.news.com/ .

Macavinta, C. (1998, 6 February). ACLU takes filtering to court. News.com. Available via the World Wide Web at http://www.news.com/ .

Macavinta, C. (1997, 16 July). Clinton: Technology is the answer. News.com. Available via the World Wide Web at http://www.news.com/ .

Macavinta, C. (1997, 26 June). Next decency fight: Libraries. News.com. Available via the World Wide Web at http://www.news.com/ .

Mainstream Loudoun, et. al. v. Board of Trustees of the Loudoun County Library. (1998). Civil Action No. 97-2049-A. Available via the World Wide Web at http://www.aclu.org/court/loudounvboard_dec.html .

Marshall, J. (1998, January). ILPN talks with professor Lawrence Lessig about PICS. ILPN. Available via the World Wide Web at http://www.collegehill.com/ilp-news/lessig.html .

McCain, J. (1999, 4 March). Senate testimony regarding S.97. Available via the World Wide Web at http://www.senate.gov/~commerce/hearings/0304jsm.pdf

McCain, J. (1999). Childrens' Internet protection act. Senate Bill 97. Available via the World Wide Web at http://www.thomas.loc.gov/ .

McCullagh, D. (1999, 28 June). Liddy: Put a lid on libraries. Wired News. Available via the World Wide Web at http://www.wired.com/ .

McCullagh, D. (1999, 23 April). Looking for something to blame. Wired News. Available via the World Wide Web at http://www.wired.com/.

McKenzie, J. (1999, May). Since when is adult a dirty word? From Now On, Vol. 8 (8). Available via the World Wide Web at http://www.fno.org/may99/adult.html .

Meiklejohn, A. (1965). Political Freedom. New York: Oxford.

Miller v. California. (1973). 413 U.S. 15, 24 .

Mincberg, E.M. (1999, 4 March). Senate testimony regarding S.97. Available via the World Wide Web at http://www.senate.gov/~commerce/hearings/0304min.pdf .

Modern History Sourcebook. (1999). Rules on prohibited books. Available via the World Wide Web at http://www.fordham.edu/halsall/mod/trent-booksrules.html .

Morais, R.C. (1999, 14 June). Porn goes public. Forbes.

Morgan, C. (1999, 4 March). Senate testimony regarding S.97. Available via the World Wide Web at http://www.senate.gov/~commerce/hearings/0304mor.pdf .

Mosquera, M. (1998, 23 March). White House backs Internet filtering legislation. TechWeb. Available via the World Wide Web at http://www.techweb.com/wire/story/TWB19980323S001 .

National Center for Education Statistics. (1999). Internet access in public schools and classrooms: 1994-98. Available via the World Wide Web at http://nces.ed.gov/pubs99/1999017.html .

National Commission on Libraries and Information Science. (1998). Moving toward more effective public internet access: The 1998 National survey of public library outlet internet connectivity. Available via the World Wide Web at http://www.nclis.gov/what/1998plo.pdf .

Negroponte, N. (1995). Being digital. New York: Vinatage.

Nessinger, T. (1997). The Third-person effect and parental perceptions of media effects on children. Unpublished thesis in Communication. Annenberg School for Communication, University of Pennsylvania.

Netcraft. (1999, June). Netcraft Web Server Survey. Available via the World Wide Web at http://www.netcraft.com/survey/ .

Net Nanny. (1999). Product literature. Available via the World Wide Web at http://www.netnanny.com/netnanny/netnanny.htm .

Neuman, W.R. (1991). The Future of the mass audience. New York: Cambridge University Press.

O'Brien, J. (1996, January). Teach your children and save money. Computer Shopper. Vol. 16 (1), 667.

Plato. (1977). The Republic. S. Buchanan Ed., New York: Penguin.

Peters, R. (1998). Cyber Patrol intolerance standard: Political correctness or bigotry? Morality in Media. Available via the World Wide Web at http://pw2.netcom.com/~mimnyc/cyberpat.htm .

Postman, N. (1992). Technopoly. New York: Vintage.

Quality Education Data. (1998). Internet usage in public schools, 1998.

Reagle, J. & Weitzner, D. (1998, 1 June). Statement on the intent and use of PICS: Using PICS well. World Wide Web Consortium. Available via the World Wide Web at http://www.w3.org/TR/NOTE-PICS-Statement/ .

Reidenberg, J. (1998, February). Lex informatica: The Foundations of information policy through technology. Texas Law Review, 76.

Reno v. ACLU. (1997). 117 S.Ct. 2329.

Renton v. Playtime Theaters. (1986). 106 S. Ct. 925.

Resnick, P. (1998, 26 January). PICS, censorship, & intellectual freedom faq. World Wide Web Consortium. Available via the World Wide Web at http://www.w3.org/PICS/PICS-FAQ-980126 .

Resnick, P., and Miller, J. (1996). PICS: Internet access controls without censorship. Communications of the ACM. Vol. 39 (10). 87-93.

Rheingold, H. (1993). The Virtual community : Homesteading on the electronic frontier. New York: HarperPerennial.

Riley, G. B. (1998). Censorship. New York: Facts on File.

Roberts, D. (1997). The jurisprudence of ratings symposium part I: On the plurality of ratings. Cardozo Arts & Entertainment Law Journal, 15, 105.

Roberts, D. (1996, 28 August). Media content rating systems. The Wally Langenschmidt Memorial Lecture. Available via the World Wide Web at http://www.rsac.org/ .

Roberts-Witt, S.L. (1998, 10 August). Smut surfers: A look at net filtering. Internet World News.

Rojas, H., Shah, D.V. and Faber, R.J. (1996). For the good of others: Censorship and the third-person effect. International Journal of Public Opinion Research, Vol. 8 (2).

Sacramento Bee. (1997, 5 December). Editorial: Tangled web. Sacramento Bee. B8.

Salamonsen, W.B., and Yeo, R. (1996). PICS-Aware proxy systems vs. proxy server filters. Available via the World Wide Web at http://power2.nsysu.edu.tw/INET98/inet97/a7/a7_3.htm .

Schad v. Borough of Mt. Ephraim. (1981). 452 U.S. 61.

Schiller, H. (1976). Communication and cultural domination. White Plains, New York: Pantheon Books.

Schwartz, J. & Biskupic, J. (1997, 27 June). 1st Amendment applies to internet, justices say. Washington Post, A1.

Seif, M. (1997). Symposium comments cited in B.U. Journal of Science and Technology Law, Vol 3.

Shenk, D. (1997). Data smog. San Francisco: Harper Collins.

Sims, M. (1998, 6 April). Why censorware can't work. The Censorware Project. Available via the World Wide Web at http://www.censorware.org/essays/whycant_2_ms.html .

Smith, K. (1991). Zoning adult entertainment: A reassessment of Renton. California Law Review, 79, 119.

Smolla, R. (1997, Summer). The Culture of regulation. CommLaw Conspectus, 193.

Smolla, R. (1992). Free speech in an open society. New York: Vintage.

Smythe, D.W. (1981). Dependency road: Communications, capitalism, consciousness, and Canada. Norwood, NJ: Ablex.

Solid Oak. (1999). Product literature. Available via the World Wide Web at http://www.cybersitter.com/ .

Starker, S. (1989). Evil Influences. New Brunswick, NJ: Transaction Publishers.

St. John-Stevas, N. (1962). The Church and censorship. in J. Chandos (Ed.). To deprave and corrupt. New York: Associated Press.

Stone, I. F. (1987). The Trial of Socrates. Boston: Little, Brown.

Stutz, M. (1997, 15 December). PICS walks fine line on net filtering. Wired News. Available via the World Wide Web at http://www.wired.com/news/ .

SurfWatch. (1999). Product literature. Available via the World Wide Web at http://www.surfwatch.com/ .

Symons, A.K. (1999, 4 May). Keynote address at the Annenberg national conference on the Internet and the family. Available via the World Wide Web at http://www.ala.org/pio/speeches/annenberg.html/ .

Taggart, S. (1999, 30 June). Turning the screws on content. Wired News. Available via the World Wide Web at http://www.wired.com/news/ .

Tarde, G. (1898/Unpublished translation). Opinion and Conversation. in L'opinion et la Foule. Paris: Alcan.

Taylor, B. (1999, 4 March). Senate testimony regarding S.97. Available via the World Wide Web at http://www.senate.gov/~commerce/hearings/0304tay.pdf

Taylor, P. (1998). Lawmakers, citizens groups step up efforts to monitor entertainment industry. Free!. Available via the World Wide Web at http://www.freedomforum.org/ .

Teford, T. L. (1993). Freedom of speech in the United States. Second Edition. New York: McGraw Hill.

Toffler, A. (1980). The Third wave. New York: Bantam.

Tucker, D. (1997). Preventing the secondary effects of adult entertainment establishments: Is zoning the solution? Journal of Land Use & Environmental Law, 12, 383.

Turchi, K. (1983). Municipal zoning restrictions on adult entertainment. Indiana Law Journal, 58, 505.

Turkle, S. (1997). Life on the screen. New York: Simon & Schuster.

Turow, J. (1999, May). The Internet and the family: The View from parents the view from the press. Annenberg Public Policy Center of the University of Pennsylvania, Report No. 27.

Turow, J. (1997). Breaking Up America. Chicago: University of Chicago Press.

Vesely, R. (1997, 16 July). Clinton-Gore porn filtering "toolbox". Wired News. Available via the World Wide Web at http://www.wired.com/news/ .

Volokh, E. (1997). Freedom of speech, shielding children, and transcending balancing. Supreme Court Review, 31.

Wallace, J. (1997). Why I will not rate my site. The Ethical Spectacle. Available via the World Wide Web at http://www.spectacle.org/cda/rate.html .

Wallace, J. (1997). The X-Stop Files. Available via the World Wide at http://censorware.org/essays/xstop_files_jw.html .

Wallace, J. and Mangan, M. (1996). Sex, Laws, and Cyberspace. New York, NY: Henry Holt & Company.

Wallack, T. (1999, 5 February). Program cracks Cyber Patrol. The Boston Herald. 037.

Webster, F. (1995). Theories of the information society. New York: Routledge.

Weinberg, J. (1997). Rating the net. Hastings Communication & Entertainment Law Journal, 19, 453.

Wilkins, J. (1997, 17 September). Protecting our children from Internet smut: moral duty or moral panic? The Humanist, 57, (5), 4.

Wilson (1975). Belief in freedom of speech and press. Journal of Social Issues, Vol. 31 (2).

Wolfson, N. (1997). Hate speech, sex speech, free speech. Westport, CN: Praeger.

World Wide Web Consortium. (1998). PICS signed labels (DSig). 1.0 Specification. P. DesAutels (Ed.). Available via the World Wide Web at http://www.w3.org/pics/ .

World Wide Web Consortium. (1997). PICSRules 1.1. M. Presler-Marshall (Ed.). Available via the World Wide Web at http://www.w3.org/pics/ .

World Wide Web Consortium. (1996). PICS Label distribution label syntax and communication protocols. Version 1.1. J. Miller (Ed.). Available via the World Wide Web at http://www.w3.org/pics/ .

World Wide Web Consortium. (1996). Rating services and rating systems (and their machine readable descriptions). Version 1.1. J. Miller (Ed.). Available via the World Wide Web at http://www.w3.org/pics/ .

World Wide Web Consortium. (1996, 4 December). W3C issues PICS as a recommendation. Available via the World Wide Web at http://www.inria.fr/Nedit/pre25-eng.html .

Young v. American Mini Theaters. (1976). 427 U.S. 50.

47 U.S.C. 223(a)(1)(A) (1996).

47 U.S.C. 223(d)(1) (1996).