Site Blocking Software and Internet Access in Public Libraries

Marc Marenco
Pacific University

Follow this and additional works at: http://commons.pacificu.edu/inter03

Recommended Citation
Site Blocking Software and Internet Access in Public Libraries

Rights
Terms of use for work posted in CommonKnowledge.

This article is available at CommonKnowledge: http://commons.pacificu.edu/inter03/22
Site Blocking Software and Internet Access in Public Libraries

Posted on April 1, 2003 by Editor

By Marc Marenco <marencom@pacificu.edu>

INDEX:

.01 Introduction
.02 The Internet in Public Libraries
.03 Legislative Attempts to Regulate the Internet
.04 Children’s Internet Protection Act (CIPA)
.05 The First Amendment
.06 Conceptualizing the Internet: Public Forum or Set of Non-conventional Acquisitions?
.07 Questions about ALA v. USA
.08 Questions about regulation of the Internet
.09 Forum for Sustaining the Conversation
.10 Footnotes

.01 Introduction (return to index)

It would be a gross understatement to say that public libraries have been in the news a good deal lately. The Patriot Act and more recently the Children’s Internet Protection Act (CIPA) have put public libraries in the lime light. The issues involved are two: 1) protection of patron privacy, in the case of the Patriot Act and 2) protection of unscreened patron access to Internet content in the case of CIPA. The American Library Association (ALA) [1] has been actively involved. Out of these two great public battles the figure of “Conan the Librarian” has emerged, protector of patron’s rights to privacy and access. The protection of patron privacy has always been a concern to public libraries but the Patriot Act has intensified the debate. [2] Unfiltered access to Internet resources in public libraries has been of concern for as long as libraries have provided online connections but has now come to a head with the pending Supreme Court case which is the subject of this article.
On May 31st 2002 a three judge panel in a district court in Philadelphia ruled in favor of the American Library Association, Multnomah County Library and other plaintiffs in a lawsuit (hereafter referred to as ALA v. USA) they brought to halt implementation of the Children’s Internet Protection Act (CIPA) which would have required public libraries to install and maintain website blocking software on their Internet connected computers if they wanted certain types of federal funding. The question is this: does the Internet in its current form belong (in whole or part) in the public library setting? If it does, should measures be taken to prevent patrons from accessing certain sites featuring hardcore pornography or illegal material such as child pornography, snuff films, etc.?

.02 The Internet in Public Libraries (return to index)

The first American public library opened its doors in Boston Massachusetts in 1854. The mission of that library was simple: “to promote equality of education opportunity, to advance scientific investigation, to save youth from the evils of an ill spent leisure, and to promote the vocational advancement of the workers.” Today we have over 9,000 public libraries all with modern mission statements reflecting the basic educational ideals reflected here though few, if any, make reference to the “evils of an ill spent leisure…”

Ninety-five percent of the 9,000 public libraries have installed computers with Internet access. Approximately 10% of the 143 million Internet users in America make some use of this service. A few public libraries, about 7%, have installed Internet filtering software for all patrons. A larger percentage have installed filtering software to be used when minors are online. [3] But many public libraries do not filter Internet content and rely on Internet use policies and other measures to regulate use of computers connected to the web. The 106th (?) Congress saw a problem with this situation. Children who use public libraries use these Internet connected computers. With the Internet being what it is there has been an ongoing concern that children will, intentionally or unintentionally, view content that may be harmful; material such as hardcore pornography, child pornography, extreme violence, snuff films, etc. [4] If we look at the indexable web [5] there are approximately 100,000 hardcore pornographic sites which can be viewed without cost and without verification of age. Anyone with minimal browsing skills can find these sites. There are also approximately 10,000 child pornography sites which are illegal. Again, this is on the indexable web. If we add this to the Deep Web [6], we can multiply these numbers many times.

The Internet has become a vast largely unregulated global public forum. What makes the Internet so powerful is its highly sophisticated capacity for interaction. It is not “Information Technology” (IT) but “Information and Communication Technology” (ICT). It is not just the instantaneous global distribution of text, data, audio, and visual files but the global interactive exchange of these things that define the Internet. 400 million people world-wide have access to Internet based ICT. 1.5 million web pages are added every day. Another important feature of the Internet is anonymity. Because of the use of proxy servers and anonymizers [7] it is difficult to track down the actual content owners of material on the web.
Legislative Attempts to Regulate the Internet

Not surprisingly there have been various attempts to regulate the Internet and to protect children and unwary adults from unwanted, harmful or illegal content. There have been two major pieces of legislation coming out of Congress attempting to do this. One was the Communications Decency Act (CDA) \[8\]. The other was the Children’s Online Protection Act (COPA) \[9\]. Neither of these laws has fared well in the courts. Both of them have been more or less ruled unconstitutional; violating provisions for freedom of expression guaranteed by the 1st Amendment. CIPA \[10\] was the third attempt at crafting a piece of legislation regulating the Internet that would pass constitutional scrutiny. It was passed in December of 2000 and was to be implemented July 2002. Then in May a district court in Philadelphia declared it unconstitutional stating that CIPA would force states to engage in activity in violation of the 1st Amendment if they were required to install Internet filters. A provision in CIPA made it mandatory that any successful challenge in a lower court would be automatically brought to the Supreme Court for consideration. It is now on the Supreme Court docket for early spring 2003.

Children's Internet Protection Act (CIPA)

What is CIPA? CIPA requires all who wish to receive e-rate discounts \[11\] and/or LSTA (Library Services and Technology Act) funding to install and maintain filtering software in order to prevent patrons from accessing material on the Internet which is obscene or child pornography or, in the case of minors, visual depictions that are harmful to minors. Any adult patron can request that the filtering be disabled “to enable access for bona fide research or other lawful purposes.” \[12\]

The plaintiffs in American Library Association, et.al. v. United States of America, et al. and Multnomah County Library, et al. v. United States of America, et. al. did not argue that all content on the Internet is constitutionally protected. They were well aware that the Internet contains all sorts of speech not protected by the 1st Amendment. Instead they argued that all Internet filtering software under-blocks material that is not protected and over-blocks material that is protected. The claim was that programs like Cyber Patrol, N2H2 and SmartFilter just don’t work well enough to fulfill the provisions of CIPA. They block many sites that are not forbidden by CIPA and they do not block many sites which are forbidden by CIPA.

The First Amendment

A note on the first amendment aspect of this case. It may come as a surprise to some, but there is a good deal of speech that this NOT protected by the first amendment. \[13\] Some of this unprotected speech is fairly uncontroversial. To use a simple example, few people would defend the right of someone to yell “fire” in a crowded theater where there is no fire. This speech is not protected by the first amendment. Speech which a reasonable person would see likely to lead to imminent danger without justification is not protected by the first amendment. Speech which is likely to lead directly to the commission of a crime or a violence is also not protected. Speech which is defamatory is also not protected. More controversially, speech which is obscene is not.
protected by the first amendment. States vary in the way they regulate obscenity. Some states, like Oregon, do very little regulation. For example, in Oregon, it is permissible for people to take off all of their clothes in strip clubs whereas in most other states the person must keep genitalia covered if only superficially. [14] Pornographic images are also regulated differently from state to state. A photograph which is legal in Oregon may not be legal in Kentucky.

The Internet has made it difficult, if not impossible, for states to regulate obscenity. If we add to the mix the fact that images and video can easily be sent from servers from anywhere in the world the reader can grasp the scope of the problem. One of the problems with obscenity statutes is that they require fairly subjective judgments on the part of viewers. Images also depend on context for their meaning. For example there is a photograph of a young girl without underwear holding up her dress in the now infamous Robert Maplethorpe exhibit. This image sat between two images depicting adult sexual acts. As it turns out this same photograph sits proudly on the wall in the living room of the parents of the child. To them it reflects a beautiful free spirit in their daughter. In the other context it becomes pornographic because of the sexualized context. There is a famous phrase in philosophy: “meaning is in use.” This roughly means that meaning is a function of human attribution not intrinsic quality. The meaning is not in the thing but in the human use of some thing. For the most part we have fairly broad agreement about certain images, say hardcore child pornography. But think through the logic of this. The reason child pornography is illegal is because it involves actual criminal acts with children. It is not because the image itself, by virtue of depicting a certain content, is illegal. Computer technology has produced a new dilemma for us in that it is now possible to morph adult pornography in such a way so as to appear to be child pornography. It is also possible to create what appears to be photographs graphically from scratch without any actual photo content at all. These are increasingly difficult to distinguish from the real thing. For the first time, the Supreme Court ruled in Reno v. ACLU that it is not illegal to posses these realistic depictions since no children were actually harmed in their production. This ruling is likely to produce a good deal of chaos in the courts since anyone with child pornography can always say that they sincerely believed that the childlike pornographic images they possessed were computer generated or computer morphed, not the real thing.

In the ALA v. USA case these first amendment issues do not figure as prominently as one might think. The government recognizes that nothing should be forbidden to the adult library patron doing bona fide research unless the material being sought is illegal. CIPA provides for adults requesting that filtering software be disabled. The ALA’s argument was simply that website blocking software mistakenly blocks a significant amount of constitutionally protected speech and thus the federal government would be forcing states to break the law by imposing the filtering requirement on public libraries.

.06 Conceptualizing the Internet: Public Forum or Set of Non-conventional Acquisitions? (return to index)

An interesting and important twist in this case is the detailed legal analysis of the Internet itself. I
have included all of the relevant primary sources in this case and encourage the reader to take the time to read them. They are important documents for cyber culture analysis. According to the government the Internet should be viewed like any other acquisition in the library setting. There is nothing special about the Internet that would require special treatment. Libraries have always been given wide latitude in deciding what they will include in their collections and make available to patrons. Everything that is recommended for acquisition goes under review and based on criteria such as community interest, authority of the source, reviews in professional journals and so on, a book or tape or video will be accepted or rejected as part of a libraries holdings. According to the government there is nothing unconstitutional in libraries deciding what Internet content they want to include or exclude from their collection. Therefore, argues the government, CIPA is not asking libraries to do anything unconstitutional by attempting to exclude unprotected speech using filtering software.

However, according to the plaintiffs, the Internet is not like anything else in the library. In fact, the moment a library turns on the computer and connects to the Internet they have done something they have never done before, namely created a bona fide legal public forum within their walls, albeit an untraditional one. Anyone with Internet access can write a few words on any subject they wish and publish it for worldwide distribution with a few keystrokes. The analogy is Hyde Park where a person goes expecting to hear anything and everything. Whenever a public forum is created the courts must use something called “strict scrutiny” when evaluating regulations which remove material based on content. In the case of all other acquisitions in the library only “rational review” is required. The plaintiffs have no problem with the decisions which exclude material from the shelves of any given library. But when it comes to the Internet “strict scrutiny” must be used in excluding anything and filtering software blocks a substantial amount of material that would not pass strict scrutiny in other contexts. Therefore CIPA would be forcing libraries to engage in unlawful activity by blocking constitutionally protected speech found on the Internet, conceived here as a public forum.

The plaintiffs won. Will they win in the Supreme Court? Bets are they will. But the conceptual dispute over the nature of the Internet is significant and has implications far beyond the public library context. It reveals, once again, that we are still groping for the right way to understand the phenomenon of the Internet. Could the 2 billion plus web pages on the Internet be construed as artifacts that could be acquired by libraries? Doesn’t it seem reasonable that libraries should be able to be selective about the Internet content they provide to patrons? Let’s think this through for a moment.

Imagine yourself in the entryway of your local public library. As you enter you read the following sign: “some of the books in these stacks contain illegal content. We do not know which ones they are and it is not always clear from either the classification or title what the actual content of a book will be. Also, there is no necessary connection between what you find in our card catalogue and what you find in the actual book. Books in this library appear and disappear regularly. They also change content, titles and whereabouts on the shelf. The average life for any book in this library is about 90 days. If you happen to find a book which is illegal to posses you
could be arrested and prosecuted. Use this library at your own risk and have a nice day.” This is the Internet conceived as a set of library acquisitions.

Case. A recent incident at the Forest Grove Public Library. Someone had accessed what appeared to be illegal child pornography. They left the images in full view of patrons and staff and left the building. When someone pointed the images out to the library staff the local police were called since the images were not just offensive but possibly illegal. The police came and took away the computer for analysis in an attempt to catch and prosecute the perpetrator. Now… who was the perpetrator? Where did this patron find the illegal child pornography? On the digital shelves of Forest Grove Public Library… Who put them there? Were they smuggled in from the outside? No. Forest Grove Public Library paid a provider to have access to them. Who is in possession of these illegal images? Well, when the police arrived they were sitting on the table in the Forest Grove Public Library.

I do not believe the government understood the full meaning of its own arguments in the ALA v. USA case. If the government wins in the Supreme Court this spring wouldn’t it follow that every library must then take responsibility for every individual web page it makes available to patrons on the Internet? The implication of installing filtering software is that libraries are responsible for Internet content which they provide. Once they do that they are open to criticism from both sides; for letting through and thus making available illegal images on the one hand, and blocking sites that are constitutionally protected on the other hand. I do not know if libraries realize that the principle they are using in the decision to install filters is the rope that will be used to hang them.

But if the plaintiffs win, what then? Do we really want a protected public forum in our libraries? Is that the place for such things? Does this serve the mission of libraries? Public libraries, even modern ones, have more or less well defined mission statements. In the Internet policy of public library in Astoria Oregon we find, “computers are provided primarily for research and education. Use of chat rooms and email is strongly discouraged.” [15] Here we have a clear statement of what library resources are for, “research and education.” Here we also have a judgment of what will and what will not count as bona fide research and education. Email and chat rooms are viewed as outside the mission of a public library. Yet during my brief stay there I observed a total of 8 people using the Internet, all of whom were reading or writing email (including me.) When I went to breakfast I noticed a computer with high speed access being used by a customer. She too was doing email, $2.50 for 15 minutes. If the Internet really is completely different from any other kind of acquisition libraries have had in the past then what is it doing there in the first place? This mingling of two quite different pictures of what a library is, what its function and purpose is is at the heart of the problem in this case. In the legitimate attempt to provide patrons with the latest ICT public libraries have not sufficiently taken into account the consequences of the radical disjunct between this new technology and anything else libraries have provided to patrons in the past. [16] It would be interesting to do research on Internet use logs in public libraries to see how they in fact are being used. I am not aware of any such studies. Is expanding Internet access in public libraries changing their basic self-understanding? If so, how? Is this a good thing?
What does it mean to provide access to everything that is on the Internet? If we think of web pages as an expansion of holdings then we have a rather bizarre situation given the nature of these holdings. They change regularly, are unreliably taxonomized and contain, in some cases, illegal content. If I do a google search in a public library and then call up a website which turns out to contain illegal child pornography, how would this be different from going into the stacks, pulling out a book, opening and discovering it was illegal child pornography? WHERE did I find this material? In both cases I found it in the public library... The moment a library turns on an Internet connected computer they have instantly put over 2 billion new items on their shelves, much of it material that would never pass muster in even the most rudimentary of screening processes which every one of the more than 9,000 public libraries do on all other acquisitions.

The implications of the successful ALA challenge to CIPA may not be that libraries should be allowed to offer unfiltered access to the Internet. The implication may be that any library offering Internet access must, as a matter of law, offer unfiltered access. Note that many libraries have instituted measures without filtering to control the sites patrons may view. If the ALA v. USA case is upheld in the Supreme Court surely there will be lawsuits by patrons to remove any filtering software in libraries which want to filter content since the Internet is viewed by the court as a public forum and as such cannot be restricted on the basis of content. Libraries will be forced to install privacy screens or recessed monitors so that first amendment rights to free expression don't come into conflict with 14th amendment rights to privacy. If other patrons are offended by sexually explicit conduct and complain then I might be compelled to refrain from viewing such sites even though I have a right to do so.

I would like to end with two sets of questions that ALA v. USA raises. The first set deals with the specific question of Internet access in libraries. The second set deals with questions this case raises more generally about regulation of the Internet.

Questions about ALA v. USA (return to index)

1. What is a public library? Knowing what a public library is will help us know what activities should be going on in there and what materials should be provided to help patrons engage in those activities. Most public library mission statements are rough variants of the Boston Public Library established in 1854. When that first public library plugged in its first Internet connection and made it available to that first patron something very dramatic happened even though it probably seemed totally benign and obviously beneficial at the time. If the Supreme Court decisions against CDA, COPA and the district court decision against CIPA hold then the Internet will remain unregulated for the foreseeable future. This is unlike anything else that has ever come into the public library setting. We may approve of the change. But like so much technology before, the technology itself seems to drive the discourse rather than human vision and purpose driving decisions about the technology.

When the Astoria Library discourages use of email and chat rooms they reveal the concept of a library as serving a specific purpose which email and chatrooms are not a part of. In discouraging...
rather than regulating email and chatrooms Astoria Library is saying that it is very difficult to
regulate patron activities. (fn. The head librarian informed me that decisions about filtering
software and regulating email and chatrooms through software were purely economic decisions.
They cannot afford the software and do not have the technical knowledge to implement changes
in the machines themselves. It is interesting that in the $20,000 Gates grant that allowed the
purchase of the new machines in Astoria Library that provision was not made for library
appropriate alterations if indeed the library does not want patrons to use the computers for email
and chatrooms.) We either need to change or expand what we mean by a public library to
include what the Internet does (in whole or part) or remove it from public libraries and think
through a policy for acquiring content on the net which is not otherwise available when creating a
public forum.

2. What is the Internet? Knowing what the Internet is would be useful in deciding whether it
belongs (in whole or part) in a public library. Is the Internet simply a collection of resources like
books on a shelf that one can pick and choose from, or is it a public forum which must, by its
very nature, remain unregulated and unfiltered except insofar as it is used for illegal purposes? So
far, the Supreme Court has said that either libraries must let it all in or let in ONLY what they
want to acquire using the traditional methods of rational review which they can then make
available to patrons on what would amount to an inter-library intranet.

3. How has Internet access been used in public libraries so far? There are lots of Internet use
logs out there which could be used in anonymous research to get an idea of the amount of time
the connections are actually being used for library relevant purposes. One could also get an idea
of how much of the information sought on the Internet could just as well be sought using a
libraries non-Internet resources. If, for example, 90% of Internet usage is for email, chatrooms,
and video games and 5% used for research that could just as easily be done without the
Internet, would the expenditure for the software, hardware, and access be worth the remaining
5%? Or would it be easier and cheaper to find a way to acquire that 5% and provide access to it
some other way?

4. Are there ways of responding to CIPA type concerns (which if the Fort Vancouver case is
indicative are also public concerns) without install filtering software which grossly under and over
blocks Internet content? Why not use the electronic materials acquisition process already
established in libraries to select out from the Internet resources that would pass minimal rational
basis review and offer them on what amounts to an educational inter-library intranet?

.08 Questions about regulation of the Internet (return to index)

1. Should the Internet be regulated? I expect most people would say yes, but only using what
legal analysts call ‘strict scrutiny’, that is forbidding censorship based on content or viewpoint.
Using strict scrutiny there is still much that can and perhaps should be restricted based on the
taxonomy of speech categories not protected by the first amendment. For example a number of
states have initiated anti-spam legislation. Speech which is otherwise unprotected by the first
amendment should not become protected simply by being expressed through the Internet environment. There are also security issues to be considered. Many people who consider themselves civil libertarians have been challenged by 9.11 and subsequent war on terrorism. Confidentiality and anonymity are not synonymous concepts and some argue that we should give up anonymity as the guiding concept of privacy and beef up the concept of confidentiality as a way of reducing illegal uses of ICT. A right to privacy does not entail a right to anonymity. The American Library Association’s “Principles for the Networked World” confuses these concepts in their five principles on privacy. [17]

There is also the problem of pornography. Obscene speech is not protected speech. Unlike the other forms of unprotected speech obscene speech is highly controversial. It may not be useful to ask the question, “is pornography harmful?” Why? Because research on this subject tends to be limited to the question of whether or not exposure to pornography leads to criminal acts and on that score the results are decidedly inconclusive. Research that does more than this tends to assume certain moral attitudes toward sexual activity which are not shared by all. In other words, if research showed that early exposure to pornography leads to early experimentation with sex you would still have arguments about whether this outcome should be considered a harm. The boundary between social harm and moral beliefs is quite thin in this case. This is why CIPA uses the language “… material that may be harmful to minors” (emphasis mine) rather than is harmful to minors.

2. How should the Internet be regulated? If the answer to question one is yes, then the question remains HOW should we regulate the Internet. What would it take? Is it possible? Would such attempts be effective enough to warrant the effort? How can we insure that access to content protected by the first amendment will remain available? The focus on Internet regulation seems to be moving to two important groups of people, Internet content providers and Internet service providers (ISP’s). Some have argued that a virtual store on the Internet must comply with all federal, state and local laws that it provides content to. If Portland Oregon allows adult video stores but does not allow store owners to install billboards with hardcore content outside then anyone providing hardcore pornography to people in Oregon must not use hardcore images on their opening screen in their virtual store. This is, to say the least, a difficult thing to enforce. It is difficult for the owner of the virtual store to know who is digitally knocking on their door and it is difficult for the patron to know on whose door they are knocking. We also have the conceptual problem of cyber geography. WHERE is this store located? Have I gone out of state into a store in New York or has the content provider in New York effectively opened a store in Oregon? I never leave Oregon and the content provider never leaves New York. The “community standards” relevant to the Internet seem to be nothing less than the global neighborhood encompassing every country, state, county, city and neighborhood block. How do you establish and enforce standards on that scale?

ISP providers have also been the focus of intense scrutiny, especially since 9.11. They provide a gateway for people to get onto the Internet. Getting an account with an ISP amounts to a license to surf. There is usually a name, a billable address, and other identifiable information given
to ISP’s. They also keep or are capable of keeping logs of client Internet usage. With this information plus information about Internet content providers and local, state and federal laws (so it is argued) some regulation could be developed without restricting protected speech. Among the technical issues that are crucial here are proxy servers, anonymizers, and the use of encryption software. Among the non-technical issues that are crucial to the question of regulation are accountability, anonymity, and the concept of a right to access.

3. Jeff Barlow has been making many excellent points in his series on the Internet and globalization. In his last article Dr. Barlow makes a distinction between filtering and censorship. He asks the question whether or not states have the right to shape Internet access in keeping with the cultural values of a specific historical tradition. The point, I think, is that given the nature of ICT there is a kind of default de facto hegemony of Western beliefs and values that permeate what the rest of the world is exposed to through ICT, mostly television and the Internet. In a chapter entitled, “Televison: Satellites and the Cloning of Cultures” Jerry Mander makes this point using the Dene Indians in the Northwest Territories of Canada as a case study. [18] Does freedom of access imply a kind of de facto cultural hegemony? Given the huge gap between the capacities of wealthy corporate Western content providers and everyone else won’t the Internet evolve in keeping with those interests? Should we accept and respect the attempt in France to preserve French culture by limiting the exposure of American films and television programs? In promoting unrestrained freedom of access are we not in fact simply promoting (perhaps inexorably) global cultural evolution in one direction, namely the West? Without the benefit of something like “cultural affirmative action” doesn’t globalization mean westernization? Dr. Barlow does not go this far, but he rightly asks the question of the limits of freedom of expression in the global context.

Whatever decision the Supreme Court makes this spring we should all carefully read the full text of the court’s opinion. It is bound to be full of conceptual distinctions that are simultaneously illusive and yet crucial to public discussion of the Internet. There are no short cuts to understanding and we need many people who are familiar with the details of the arguments if we have any hope of shaping public policy.

The goal, as always, is to strike a balance between adaptation to emerging ICT and creating an environment where there is robust critique of ICT. We need to be vigilant in maintaining our autonomy in relation to technology through an honest assessment of its impact on us and whether or not a particular use of ICT truly furthers our authentically human goals and commitments.

.09 Forum for Sustaining the Conversation (return to index)

We have established a moderated forum for discussion of the question of Internet access in public libraries. Criteria for posting to the forum are simple. They must be relevant to the public policy question of Internet access in public libraries and they must conform to minimal standards of civility and respect for differences of opinion.
Footnotes


[2] With the establishment of the Department of Homeland Security the tension between privacy and security is only going to intensify. On September 13th the Pacific Institute for Ethics and Social Policy, together with the Department of Justice and Oregon Association of Chiefs of Police, held a symposium on Security, Freedom and Justice. Hardy Myers (Oregon State Attorney General) and Charlie Mathews (Chief field agent in Oregon for the FBI) were among the participants. The morning session was devoted to the controversial provision of the Patriot Act which gives the FBI the power to search computers in public libraries to see what books patrons have been reading and what websites they have browsed in the course of anti-terrorist intelligence operations. Here are the materials, including a case study, used at this symposium:

http://pacinst.pacificu.edu/9132002/index.html

[3] Fort Vancouver Public Library, one of the plaintiffs in the case soon to be heard in Supreme Court has just installed filtering software to be used by children under the age of 13 with 13 to 17 year olds requiring permission from a parent for unrestricted access. The board vote to institute this policy was close: 3 to 4.

[4] According to testimony given at the circuit court trial 41% of the blocks at Tacoma Public Library where filtering software is installed were triggered by 11 to 15 year olds.

[5] The indexable web is the sum total websites which can be found, in theory, using a web search engine. For a site to be indexable it must have a reference to it on some other site. Search engines find websites by using “spidering” technology which goes through the first few levels of a website to find links. 50% at most of indexable content is found by all search engines.

[6] The Deep Web comprises all non-indexable web pages. Testimony used in the ALA and Multnomah County Library v. United States of America cases set the total number of pages to be between 2 and 10 times the 2 billion indexable pages. Child pornography is often distributed through the Deep Web by sending a URL through email. The site never appears in a search engine.

[7] A proxy server is a server which provides access to websites without disclosing their IP address. Your browser may show 12.44.33.66 but you are actually viewing content at 44.33.66.77. Sometimes proxy servers are used to translate sites from one language to another. They are also used as loopholes to circumvent filtering software and provide content which is controversial or illegal.


[11] E-rate discounts reduce the cost of Internet access by between 20% and 90% depending on the extent of economic disadvantage in a region.


[13] Here is a link to a site with an overview of unprotected speech: http://www.csulb.edu/~jvancamp/freedom1.html#C

[14] Late breaking story. On January 8th 2003 the Oregon Appeals Court ruled for the first time that nude dancing is not “protected speech.”


[16] The analogy of expansion of holdings through inter-library loans and electronic subscriptions does not work here since everything made available through inter-library loans and electronic subscriptions has been vetted by a library within the system. Though procedures differ from library to library they do not differ substantially and no library acquires content without judging its suitability, which is not the case with the Internet.


This entry was posted in Uncategorized by Editor. Bookmark the permalink [http://bcis.pacificu.edu/interface/?p=2742].