Filtering & Blocking Software

Filtering & Blocking Software in Education Settings

What is “filtering” or “blocking” software?

The two terms are sometimes used interchangeably but there are key differences between them. Internet filters are a common tool used to limit access to certain material and websites on the World Wide Web. These filters are a method schools systems use for internet security. Filtering software denies access to a website based on its content, while blocking software denies access based on the offending site’s URL (Faulkner, 1998).

Different types of filters and blocking software used in school settings

- Keyword blocking: software program looks for specific concepts based on a predetermined list of words, phrases, and word combinations that are not wanted by the program administrator. These filters scan pages and limit access to sites that contain the inappropriate and/or undesired words. Keyword blocking can be ineffective in schools because even if the website only uses one of the words from the list once, the whole site is completely blocked, assuming the entire site is about that specific keyword. This blocking method does not focus on the context of the word nor the context relevant on the site.
  For example: chicken breast, Anne _Sex_ ton. Because these words have a certain combination with an inappropriate keyword, the whole site would be blocked.

- Site blocking: predetermined list of specific websites that can or cannot be accessed and/or viewed. Site blocking can be effective because it can limit specific site to students. On the other hand, because the internet changes every day, the program and list of websites needs to be updated often. Site blocking software only blocks "known" websites and some of the programs only block domain level sites. Many filtering programs in school settings use site blocking for sites like Facebook, MySpace, or even YouTube. "Go lists" are commonly used with site blocking software which allows users to view specific pages. A teacher can give students the opportunity to view only specific websites with the "go list" strategy, therefore monitoring which selected websites students can use. Many people think this method limits students to in-depth research and discovery using the internet.

- Protocol blocking: software limiting access to a certain type of internet services. Domains such as Usenet and FTP are blocked because of their high concentration of sites unwanted in school. This method is used to block and kind of chat room or instant messaging service popular to students. For example: AOL Instant Messenger, SKYPE, etc.

- User blocking: when each user is given a username and/or password, then the access to sites is determined by the users criteria. User blocking is a widely used method in schools because of its tailored teacher versus student filter. Everyone in the school can use the same computers, but school administration can decide and apply different access levels based on the specific user. There is normally a less restricted access level for the teachers compared to the student users.

Why schools should or shouldn't use filters & blocking software controversy

In 1999, Congress passed the Children's Internet Protection Act (CIPA), requiring schools qualifying for federal E-rate funding to use filtering technology to block access to materials that are "obscene, child pornography, or harmful to minors" (Starr, 2003). This law generated a great deal of controversy on why schools should or should not use internet blocking and filtering strategies.

Schools have two main reasons for using filters and blocking software: student safety and school safety

Before the software was created, school administrations relied on close supervision of all online actions of students by teachers monitoring their activity (Huske, 1997). Protection of students is a main goal in every school in general and internet filters are another resource that help ensure the students will have a safer experience using the web. Schools are also concerned with protecting themselves from invasion of objectionable material and want to make sure the parents and community feel secure with their children using the web during class in the school. Filters give the appearance of a protected and secured environment.

Many people and sources of information believe filters should not be used in schools due to the fact that filters can limit student research resources and may not be effective at deterring sites that may be labeled “obscene” by authorities in a school setting. Some sources say these blocking software programs: may not work well or work too well, may violate family and/or community values, violate civil liberties, and define obscenity too narrowly. They back up these claims by reminding that there are better ways to protect children and that children can learn to filter for themselves.

Here are some interesting opinions from actual educators:

- "Is filtering software in schools necessary? Is it desirable? That is a very hard question to answer," Jayme Swinford told Education World. "As a parent, my first instinct is to say yes; I want my children protected from all of the evils of the world. As an educator, my instinct is to say no. I have a responsibility to produce active, media-literate members of society who are able to deal with any kind of information and who possess the ability to make sound decisions based on knowledge and understanding."

- "With filtering in place, a district can at least demonstrate that it is taking positive action toward protecting students from objectionable information."

- "I personally oppose filtering. Due to legal issues and concerns about parental reaction, however, filtering is a fact of life for most educators. Schools and districts cannot afford to face legal action brought by parents or city officials... I oppose filtering because filters prevent students from accessing information they need. For example, working at home, I have found some great Web sites for teaching students to use cognitive thinking and quicken their motor skills. When I tried to access the sites at school, however, they were blocked! It's very frustrating, both for me and for my students. Another problem I have with filtering software is that it is not foolproof. There are ways to bypass some filtering. Certain links also bypass filtering software." - Sith Nip
In my opinion, students are becoming more and more tech-savy in our classrooms today. While researching this topic, one website I came across within the first google search includes this information:
“Is your Internet access restricted? Is your School, University, Office or Government not allowing you to access famous web sites like Orkut, Hi5, Blogger, MySpace and other sites? Here are few tricks which you can play to access your favorite web sites by bypassing the ban...” This site continues on exposing different Proxy Server websites which allow you to browse the web anonymously and access sites that are blocked. This proves the filtering and blocking software a waste of time. In contrast, I do believe schools should do what they can to limit certain website access to not only protect the students, but the school. The CIPA law covers points that further explain this theory.

Sources Used:
http://www.educationworld.com/a_tech/tech155.shtml
http://students.ed.uiuc.edu/jwbrown3/EPS%20313/filter/intro%20paper.htm
http://www.webjunction.org/cipa/articles/content/445178
http://blog.techdreams.org/2007/06/access-blocked-web-sites-at-your-office.html