Technological limits of parental control over the Internet

Michele CRUDELE
Medical Informatics Laboratory
"Campus Bio-Medico" University of Rome
via Longoni 83 - 00155 ROMA
m.crudele@unicampus.it

Abstract

The need for an effective parental control over the Internet is a worldwide issue. Cases of paedophilia disclosed by news agencies have raised the warning level of the problem.

The Internet is a communication media out of the control of any national legislation; therefore it has been, since the very beginning of the World Wide Web, one of the best ways of diffusing pornography to a very wide audience.

Parents start now to realize that the danger from exposing their children to unlimited Internet access can be very high. Media often refer to paedophilia as the biggest risk, but actually it is necessary to protect minors from the wider set of immoral activity.

Parents can control Internet content by means of "blocking software" using different methodologies. The problem is that these systems are neither infallible nor bulletproof: children with a little software knowledge can easily disable most of them. They also raise ethical questions when they are used at school.

Government action seems to be ineffective, therefore parents have to take the lead in this defensive action.

1. Introduction

The diffusion of pornography and related material over the Internet is first analyzed in this paper. Means of controlling content are later illustrated, with various methodologies applied at home and at school. Limitations and flaws of parental control software are shown, with an ethical discussion on the availability of hacking tools. The topic of Internet filtering is mostly dealt in on line texts, therefore only URL references have been provided. All Internet sites have been checked on July 2nd, 1999.

2. The Scenario

The Internet started has a means of interchanging technical and scientific information among Universities. When the *http* protocol was introduced, with the capability of showing images in browsers, there was a very fast increase in the provision of any kind of material. Along with valuable information, a lot of useless texts and images were provided. In the graphical world of Internet, pornography found a new and promising way of diffusion. Now many firms offer free demo sites, charging when requested for more "exciting" material. In order to promote their business they are sending e-mails or advertising on frequently accessed sites. Newsgroups are also a means of diffusion, especially on the "alt" sections.

Pornography is sometimes referred as "the stimulation of sexual desire out of the natural sexual conjugal relation between a man and a woman". According to "The Oxford English Dictionary" it is a "description of the life, manner, etc of prostitutes and their patrons; hence, the expression or suggestion of obscene or unchaste subjects in literature or art".

These meanings are clearly negative, but in most countries there is a tendency in enhancing "freedom" of expression even when it uses explicit sexual manifestation. The background idea is that adults can choose what they like and only minors need to be protected. The problem is how to discriminate between a mature person and a child when the means of communication has no boundaries and does not differentiate according to the users' age. Selling porno-magazines in kiosks to "under 18" can be easily forbidden and relatively controlled. TV programs are more difficult to control. You can restrict adult programs only at late night or impose rating systems to broadcaster: before the beginning of a movie a code, like XXX or a red colour dot, is displayed to warn parents. These procedures have limited results and they always rely on proper family education and habits. For example, if in a family TV is always watched all together, or at least children are never left alone in front of the video, parents can have a full control of what they see.

This is not the case of Internet, which is an individual tool: for fun or for study. That's why, since the very beginning, it has been normal to have only one person for computer. Even though a parent can stay beside his or her child, the most common situation is having boys and girls navigate all alone. Therefore, boundaries are needed to avoid dangers, ranging from incorrect sexual education to getting in touch with paedophiles.

Now the necessity for an effective parental control over the Internet is a worldwide issue, after some cases of paedophilia originated through electronic communication were diffused by the news agencies. But the

Internet is out of the regulation of any national legislation, so control is left to the end user or to organizations for their members.

3. Controlling content

In order to control Internet content, specific software has been developed, mainly by USA companies. They are often referred as "blocking" or "parental control" software. We illustrate the main methods.

A list of unwanted sites, constantly updated by the providers, with different levels of blocking, according to the users' criteria: sex, violence, racism, etc. The sites' selection is the software company's choice, which may be questionable and it is always incomplete.

A list of forbidden words: every time one of these words appears in a site name or in its content, the page is not displayed. The drawback is that you are stopping also positive texts when they just contain an unwanted word. An example: XXX in USA means "only for adults" but it can mean 30 in roman numbers. You also need lists in many languages.

Text analysis is a more advanced version of word lists and it is able to evaluate how the words are used in order to rate the level of danger. This method has no complete guarantee but it works better than the previous ones. It also has the limit of plurality of languages. Almost all commercial software is English based, while at least the 25 languages searchable by Altavista (www.altavista.com) should be considered for a wide coverage.

Rating systems like RSACi (www.rsac.org) or SafeSurf (www.safesurf.com) are based on the W3C standard PICS (Platform for Internet Content Selection - www.w3.org/PICS). They rely on the behaviour of the site manager who is required to rate the content of his/her web site according to specific levels of decency or violence. Unfortunately very few sites are using PICS. Some content providers see PICS as a way of attracting more clients, because if they rate the site as "Very dangerous", they may expect people looking just for the most exciting offerings. But it is much more frequent to find unrated negative sites. A third party, which rates external sites and sells the results as a service, can also use PICS.

There are also secure and evaluated Internet environments built by associations, but unless you use the software they provide, you can normally jump out of it. As there is always a standard browser in every PC, you cannot be sure that the child is only using the safe tools.

3.1 Parental control using a browser

Both leading browsers have an embedded system for enabling PICS analysis using RSACi or SafeSurf. You can also set them for browsing only rated sites, at the level you want. Beside the mentioned rating system's

limitation, it is also easy to bypass the password-based protection.

Netscape Navigator, at least up to version 4.61, writes all ratings specifications of what they call NetWatch, in a javascript text file, *prefs.j*. Unfortunately in the string *user_pref("browser.PICS.ratings_enabled", true);* you can manually change the word "true" with "false" and the protection is disabled after restarting the program. You can restore the protection by replacing the "true" parameter and the password owner will not even realize that there has been a violation.

Also Microsoft Interner Explorer, even in its most recent version 5, has a protection which can be disabled by joining to the registry the following .reg file and restarting the program.

REGEDIT4
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies]
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Ratings\.Default]
"Enabled"=dword:00000000

You can restore the protection, and nobody will know about the violation, by simply joining the same .reg file again but with *dword:00000001*

According to Microsoft's technical support, this is a feature required in order to have a way of recovering when the user forgets the password.

3.2 Filtering on a proxy

A proxy server is a machine through which all communication transits before reaching the end user. It may be the only computer directly connected to the Internet, while all the others are in an internal network. It is a sort of a bottleneck. Therefore it is the best place where to install filtering software. The filter controls all connections and there is no special client filtering software on the user's PC. The user cannot disable the filtering, unless there is an option for bypassing it using a password.

From the technical point of view, filters on a proxy are the most secure solutions, especially if there is no way of bypassing it. But in this case there is no way of de-blocking a site if the content is erroneously blocked. You need to contact the proxy administrator for such an operation.

3.3 Parental control software

As an overview of parental control software, here are two examples. Cyber Patrol (www.cyberpatrol.com) won PCMagazine Editors' 1999 choice (www.zdnet.com/pcmag/features/utilities99/parfilt02.html) and Edunet (www.edunet.es) which provides the most effective multilanguage filter.

Cyber Patrol

It works on Windows and Mac and with any browser, costing only 30 US$ plus other 30$ for yearly lists update. It filters http, chat, ftp and newsgroups. You can set the time limits for Internet access: day and hour

and total daily and weekly hours, which means giving additional control to parents, also for money saving (Internet is still costly, either for telephone charge or for ISP service or for both). A good practise would be allowing access only at times when parents are present near the child.

There are users' profiles, so settings can be different for family members. Protection is password based. There is a version for proxy servers.

Edunet

A Spanish firm builds the best commercial European filtering system. The end user system relies on their Spain based proxy server. After installing a client software, so far available only for Windows PC's, using winsock2, you have to set up the browser to use Edunet proxy, otherwise you cannot navigate at all. The filter works with Spanish, English, French, Italian, German and Portuguese. It is quite smart in detecting what is really worth discarding and what is inoffensive. If you find a positive site blocked you can ask them via e-mail to release it: they do it in 10 minutes. Passing through a proxy in Spain may mean longer waiting times for non-Spanish users. Tests show that from UK and Italy the additional delay is not noticeable on modem connections. They are planning to replicate the proxy servers in other countries. Edunet has a version for proxy servers.

4. Parental control implementation at school

The diffusion of Internet terminals in schools makes the risk of accessing dangerous content higher for young students. If each one has his/her own computer, one teacher cannot control all of them at the same time. A filtering system must be enabled. One the most famous wide initiatives of school protection is in USA, in Utah. Schools and libraries have Internet access through the Utah Education Network (www.uen.org), a state agency, which uses a commercial software package, called SmartFilter to censor sites. Some people have objected that this policy prevents children from reading important sources, which are erroneously blocked. The list of "mistakes" includes the Bible, the adventures of Sherlock Holmes and all Shakespeare's plays. There is a detailed analysis of this system, produced by the Censorware project (www.censorware.org/reports/utah/main.shtml).

On the other side, it is unquestionable that a form of protection from dangerous sites, such as paedophiles' ones, is given.

The ethical issue is a general one: how far can protection go when there is a child involved? In family life parents' decision cannot be opposed: they have all the rights of deciding how to breed their children. But in schools you have to cope with many children and many families. If parents can freely choose the school, state or private, without any additional charge (which is

not the case in Italy, where non-State education is not economically supported by the State), they just adhere to the educational institution policy and they can even influence it. When parents have no real alternative to State school and they cannot choose any educational policy, it is the Government's task to decide it. Therefore the Government has the duty of providing a form of defence from negative Internet content in the same way it does it when protecting children from traffic dangers just out of school.

Any kind of filtering is based on some rules, which cannot be universally accepted. But it is better to be more restrictive (which means prudent) than liberal. The Internet is not the only way of gaining knowledge, so you cannot think that students can't live without it.

5. Parental control implementation at home

Freedom of choice of the best tool is total at home, but lack of technical knowledge can prevent parents from effective protection. The above mentioned software solutions can constitute a barrier to negative content, but the general advice of not letting children stay alone too long in front of an Internet connected computer is always the best practise.

A secure approach for a parent is to give their children access only to some pre-evaluated and trusted sites. Some parental control software calls these the YES-lists, as opposed to the NO-lists. While this policy somehow limits the intrinsic value of the Internet as a system without boundaries, it can be a positive solution. It is like not giving free access to the pharmacy store: it means restricting the self-curing capabilities of children, but it avoids the risk of getting very dangerous drugs. They can't get a tablet by themselves if they have a headache, but this limitation is really worth while.

Proxy solutions are not applicable to home Internet access, unless they are provided by the ISP. AOL in USA gives this choice to its clients: setting up the protection is password based, in order to disable it when needed. There are at least two ways of cheating this protection: a child may discover this password as explained later or may connect to a free Internet provider like Freenet in UK or Tiscali in Italy using a browser other than AOL's, with uncensored access.

6. E-mail control

Spamming, which means mass unsolicited electronic mailing, is related to pornography because it is one of the most used ways of contacting new clients. By mailing millions of users, sending them a link to images, there is a high chance of convincing some of them to buy related "services" with more erotic material. E-mail's do not discriminate between children and adults,

therefore it is very likely that minors can get this unwanted mail. Even though they may not reach the link, because of parental control software, the text inside the mail and maybe an attached image is by itself dangerous. There are forms of defence, called antispamming, but teaching children not give his/her e-mail to anyone but his/her very friends is the most effective defence.

7. Hacking information: ethical issues

You can get all the "hacking" information provided above, from a number of sites, simply by choosing the proper words in any major search engine. There is also a site against Internet censorship (www.peacefire.org), full of information about disabling all kind of parental control software. We can check that almost all parental control commercial software packages are quite easy to cheat.

The filters normally block all these sites, but for a child it is relatively easy to ask a friend to provide him or her the required information.

Let's analyze Microsoft's policy for Internet Explorer, as explained above. They have a means of disabling parental control for emergency reasons. But this information is easily available, therefore it works like a safe locked with a number combination published on a worldwide magazine. Is this ethical? They are not telling parents beforehand this backdoor, so that many people trust it. But children are much more skilled than mothers and fathers in discovering this sort of tricks. It would be much fairer to have at least a blocking system that shows up clearly if it has been forced.

Netscape's policy is probably the result of being a cross platform browser which must work with javascript and not with specific dll's. But it is not acceptable at all.

If you try to bypass Cyber Patrol 4.0 protection using the latest suggested tool by peacefire.org, you do not succeed. It seems that Cyber Patrol is always updating the password encryption system to cope with deciphering by that organization. The company says there is a procedure for recovering the administrator's password. but there are no traces of this procedure on the web and on newsgroups. However, any system based on a password is secure as long as the password is not known. Trojan horses are software programs that capture anything that is written on a keyboard: they can be a simple way of discovering a password. On a Windows 95 PC a Trojan horse can be installed and run unnoticed. On Windows NT workstations only the administrator can install a Trojan horse.

Edunet's local filter can be bypassed only reinstalling the TCP/IP, which makes it quite visible. There is no password for temporarily disabling it,

which means it is a secure system at home.

8. Conclusions

Quite a few organizations are publishing information on the web regarding safe use of Internet (www.safekids.com or www.netparents.org) or more specifically to filtering software (www.filteringfacts.org). A lot of discussion is running about the opportunity of censorship. Government intervention is different all over the world, but in most of the cases it is not sufficient for parental control. The problem of content protection over the Internet for preserving children from unwanted exposure is two-sided: technical and human.

Blocking software for both organizations and end users is available but it has limited power. More research is needed in the field. The European Commission has recently started an "Action plan on promoting safer use of the Internet" (www.echo.lu/iap) following the Decision No 276/1999/EC (www.echo.lu/iap/decision/en.html) of the European Parliament and of the Council of 25 January 1999 adopting a multiannual Community action plan on promoting safer use of the Internet by combating illegal and harmful content on global networks. Funding will be given in 1999 to proposals to demonstrate content filtering and rating systems and to prepare awareness actions. This will boost European research on the field, while now we see an almost completely USA driven production.

In general terms it seems that pornography for adults is not considered a subject to be regulated at all. In the USA many say that it is a violation of the First and Fourteenth Amendments to restrict adults from reading playboy.com on a terminal in a public library. In the above mentioned decision of the European Parliament, article 3 says: "for example, dealing with content such as child pornography or content which incites hatred on grounds of race, sex, religion, nationality or ethnic group" which means that blocking pornography for adults is not considered at all.

Hence, each family is compelled to defend its own moral criteria by personal means. A really effective procedure is to be present while children navigate through Internet resources. List of suggested behaviours for parents and children are published, but it's clear that family education is not only based on a set of rules. Parents' behaviour is what most influences children, therefore their own habit of not browsing questionable pages is the best teaching.