Journal of Sexual Aggression
(July 2010), Vol. 16, No. 2, pp. 223–235

Routledge
Taylor & Francis Group

Internet service provider (ISP) filtering of child-abusive material: A critical reflection of its effectiveness

Marie Eneman
University of Gothenburg, Applied IT, Gothenburg, Sweden

Abstract *The availability of child-abusive material challenges traditional legal regulation. A response to this is internet service providers' (ISPs) recent implementation of filtering systems to regulate access of this material. This paper considers whether ISP-implemented filtering systems are effective in preventing and controlling access to child-abusive material. Evaluation of the effectiveness will be based upon empirical material collected through interviews with 15 offenders convicted of child pornography; in addition, a Detective Inspector with the Swedish National Criminal Police has been interviewed. The paper concludes that the filtering approach contains both effective and ineffective elements.*

Keywords *Child-abusive material; filtering technology; ISP; offender behaviour*

Introduction

The distribution of child abusive material through information and communication technologies (ICT) constitutes a serious and growing challenge for law enforcement agencies, due to technological innovations (Akdeniz, 2008; Eneman, Gillespie & Stahl, 2009; Gillespie, 2008). The impact and the role of ICT for the production, distribution and downloading of child-abusive material has been highlighted by a number of researchers in recent years (Davidson, 2008; Eneman, 2009; Sheldon & Howitt, 2007; Taylor & Quayle, 2003). Wall (2007) emphasizes the dualistic nature of technology, i.e. that the characteristics of ICT used for unwanted and criminal behaviour also can act as powerful "disciplinary tools" to regulate, police and prevent such behaviour. The use of technology to regulate unwanted and criminal behaviour is long-standing. Lessig (2006) emphasizes that structures and architectures can and do regulate individuals and uses Bentham's and Foucault's concept of Panopticon as an illustrative example.

One topical example where technology is used to control users behaviour involves internet service providers' (ISPs) implementation of filtering systems to prevent and block access to child-abusive material. In recent years in some countries law enforcement agencies have developed cooperation with the internet industry to tackle more effectively the distribution of child-abusive material by combining legal and technological regulation. The

*Corresponding author: E-mail: eneman@ituniv.se

ISSN 1355-2600 print/1742-6545 online
DOI: 10.1080/13552601003760014

COSPOL Internet Related Child Abusive Material Project (CIRCAMP) (available at: http://circamp.eu/), a European Commission-funded network of law enforcement agencies across Europe including Europol and Interpol, has formulated the following primary aims of ISPs' domain-based filtering of pre-identified websites containing child-abusive material to: (i) prevent the revictimization of children; (ii) prevent the illegal distribution of material and the files; (iii) prevent the illegal display of abuse material and reduce the harm to the general population while informing the public of the extent of the problem; and (iv) prevent access to child abuse material and thus limiting the "market", reducing the need for new production. The following countries are currently members of the CIRCAMP network: Norway, United Kingdom, Belgium, Denmark, Finland, France, Germany, Ireland, Italy, Malta, the Netherlands, Poland, Spain and Sweden. The filtering approaches differ somewhat, however, between the countries. In Sweden the model is based upon cooperation between the police and ISPs, where filtering technology is used to block access to blacklisted websites at domain level. The IT Crime Section at the Swedish National Criminal Police is responsible for and compiles the list used by the ISPs. The compiled list of domains is based on Swedish national legislation regarding child pornography. When a user is trying to access a website that has been blacklisted the user is directed automatically to a so-called "stop page". The displayed stop page contains information that the requested website is blocked due to illegal content and informs the user how to submit complaints about the specific websites blocked. All complaints are directed to the IT Crime Section at the Swedish National Criminal Police and will lead to the domain being reinvestigated (Sellström, 2009). The model used in the United Kingdom is based on cooperation between ISPs and the non-governmental organization, the Internet Watch Foundation (IWF). The IWF is responsible for and compiles the list used by ISPs that block access to URLs (Akdeniz, 2008). Both models are examples of filtering systems implemented at organizational level. The Australian government has launched a consultation process, called the Cyber Safety plan, proposing the implementation of internet filtering at a national level to control access to websites containing child-abusive material (Department of Broadband, Communications and the Digital Economy, 2008). The number of ISPs introducing filtering systems is growing (Akdeniz, 2008), and it is expected that this trend will grow even more in the near future. The issue has been placed on the political agenda in many countries, and the European Union (EU) has recently launched a proposal [Article 18 in Proposal for an EU Framework decision on combating the sexual abuse, sexual exploitation of children and child pornography] that suggests that "each member state shall take the necessary measures to enable the competent judicial or police authorities to order or similarly obtain the blocking of access by internet users to internet pages containing or disseminating child pornography", which means that states should be able to force ISPs to implement filtering mechanisms to block access to child-abusive material. Once this proposal is enacted the EU will require that the member states begin the work with adjusting their national legislations in accordance to the proposed framework.

Designing regulation is a complex issue, not without certain problems and critics (Murray, 2007). Although most people would agree that child-abusive material should be regulated through legislation, critical voices have been raised about technological regulation attempts such as ISP filtering systems. One of the main arguments in the debate regarding this controversial issue is that internet filtering is a form of censorship associated primarily with oppressive regimes, for example Saudi Arabia and Iran, and constitutes a threat to important civil liberties such as freedom of expression and privacy (Deibert & Villeneuve, 2005; Hamilton, 2004). Freedom of expression and privacy have been in the focus of the civil liberties and technology debate for more than a century (Eneman, 2005; Wong, 2005). One could, however, argue that they should not be considered as absolute rights and that an

acceptable balance has to be found between different rights, such as the right of the child not to be sexually exploited or abused (Eneman, 2005; Wall, 2007).

Even though a number of academic studies are available about internet filtering (Deibert, Palfrey, Rohozinski & Zittrain, 2008; Hamilton, 2004), little academic research exists in relation to ISP filtering of websites containing child-abusive material (Akdeniz, 2008). One of the most recent and comprehensive studies of internet filtering has, due to ethical reasons, deliberately excluded the issue of internet filtering and child-abusive material (Deibert et al., 2008).

This paper therefore addresses the important and topical question of whether ISP-implemented filtering systems are effective in preventing and controlling access to child-abusive material. Empirical material, collected through qualitative semi-structured interviews with 15 offenders convicted of child pornography, will be presented and used in the analysis. In addition, the head of the IT Crime Section with the Swedish National Criminal Police has been interviewed. The empirical material provides valuable information about the offenders' view and behaviour towards ISP filtering of websites containing child-abusive material and also a law-enforcement perspective on the same phenomenon. This paper contributes to the debate of this topical issue, and thereby aims to support policy developments in relation to technological regulation of child-abusive material.

Child pornography versus child-abusive material

The term "child pornography" has been used widely to refer to sexually explicit material of children. Gillespie (2008) notes that experts view "child pornography" as "an extremely controversial label", as it reduces the gravity of what the material portrays and invites comparisons with adult pornography. Furthermore, there is no single definition of the term "child pornography", which can be problematic. Interpol defines child pornography thus: "Child pornography is created as a consequence of the sexual exploitation or abuse of a child. It can be defined as any means of depicting or promoting the sexual exploitation of a child, including written or audio material, which focuses on the child's sexual behaviour or genitals" (Sheldon & Howitt, 2007). This useful definition highlights the fact that child pornography can exist in different forms: for example, visual, audio and textual depictions (Gillespie, 2008).

Quayle, Lööf and Palmer (2008) recognize that there has been a significant change in the discourse when referring to sexually explicit material of children. They note that the terms "abusive images" and "abusive material" are now used frequently by professionals. As shown above, with Interpol's definition, not all sexual depictions of children are visual, therefore the latter term "abusive material" is more appropriate to use as it also captures non-visual material such as audio and text (Sheldon & Howitt, 2007).

This paper will primarily use the term "child-abusive material", but the term "child pornography" will also be used due to the fact that most international and national instruments still use the term "child pornography" (Akdeniz, 2008). The author does, however, agree with Gillespie (2008) and Quayle et al. (2008) that the term "child pornography" is inadequate. The current Swedish legal position criminalizes the production, distribution and possession of child pornography. Swedish legislation has been proved to be inadequate in parts (Eneman, 2005), and has not been adjusted to tackle contemporary technological challenges (Akdeniz, 2008; O'Donnell & Milner, 2007). The limitations refer to the lack of legal regulation of viewing child pornography without downloading the files and the current classification of child pornography as a "crime against public order", and not as a

sexual crime. [Sweden has recently (November 2009) delivered a law proposal for circulation regarding viewing child pornography online.] The jurisdiction of England and Wales has solved the issue of deliberately viewing child pornography online by inserting the verb "to make" into the legislation to adjust it more effectively to modern advanced technology (Gillespie, 2005, 2008).

Internet filtering

The term "internet filtering" refers to a variety of techniques and products that can be used to block access to certain content. The idea of censorship and control of information is long established and is the main method used by states and organizations attempting to regulate information access (Murray, 2007). The development and use of modern technology has made the regulation mechanisms more sophisticated, systematic and less obvious (Zittrain & Palfrey, 2008). The purpose of implementing internet filtering is to regulate access of certain information that for some reason is regarded inappropriate for users. Internet filtering is used currently to control access of varying content, for example political, religious, illegal and harmful content (Faris &Villeneuve, 2008; Rosenberg, 2001). Furthermore, internet filtering can be implemented on different levels, such as national, organizational or individual (Hamilton, 2004). An illustrative example of a national filtering system attempting to control access to political content is the "Great Firewall of China"; from many aspects, this is a complex and sophisticated system. It includes a matrix of control mechanisms and uses a combination of different filtering technologies to prevent access to certain IP addresses through a standard firewall and proxy servers at the internet gateways (Deibert & Villeneuve, 2005; Murray, 2007). Although this system is considered relatively sophisticated, it is possible to circumvent it by using "circumvention tools" (Murray, 2007).

This paper focuses upon ISP so-called "voluntary" internet filtering of child-abusive material, which constitutes an interesting example of organizational use of internet filtering of harmful and illegal material. The main function of ISPs, although they cover different characteristics and services, is the commercial provision of internet access services to users (Sutter, 2005). The services of an ISP are a prerequisite to being able to access the internet, especially for home users, and therefore the role of ISPs is crucial. The ISP key role in enabling access to material provided by a third party has given rise to the question of whether they have, or should have, any liability in relation to the material they provide access to (Akdeniz, 2008). This issue has been highlighted specifically in relation to the availability of illegal material such as child-abusive material (Akdeniz, 2008; Murray, 2007). Many states and national law-enforcement agencies consider ISPs to be part of the distribution chain of child-abusive material (O'Donnell & Milner, 2007; Taylor & Quayle, 2003). The question of what constitutes the appropriate level of liability to be placed upon ISPs in relation to the content to which they provide access is beyond the scope of this paper.

Different types of internet filtering

The most-used approaches for internet filtering are: (i) inclusion filtering, (ii) exclusion filtering and (iii) content analysis (Hamilton, 2004). These different approaches can be used in combination to achieve desired effect. The first approach, inclusion filtering, is referred to commonly as "whitelisting", which allows users to access websites that have been checked and approved in advance. Instead of compiling lists of unacceptable information, this approach entails the creation of "white lists" containing approved and acceptable information. The

inclusion filtering approach is very limited, as it allows access only to pre-approved websites and blocks all other content, and is therefore not used widely (Deibert & Villeneuve, 2005). The second approach, exclusion filtering, is often labelled "blacklisting", and can be seen as the opposite of whitelisting. Blacklisting refers to the process of compiling lists of unacceptable websites. When using this approach, all requests of content that occur on a "blacklist" are blocked and the user is often directed to a so-called stop page that informs the user that the requested website is blocked because it contains illegal material. All other information, not found on a blacklist, is accessible. Blacklisting is considered to be the most efficient and commonly used filtering approach (Hamilton, 2004; Rosenberg, 2001). The third approach is content analysis, and this is a growing filtering technique (Hamilton, 2004). The concept is to avoid precompiled lists and to focus upon analysis of the requested content. This approach uses certain predefined criteria to scan requested content before delivering it to the user, i.e. allowing user access (Deibert & Villeneuve 2005). One of the advantages with content analysis is that this approach distinguishes between different types of content, as opposed to filtering entire websites.

Arguments for and against internet filtering

Zittrain and Palfrey (2008) argue that although internet filtering is a controversial topic, it is possible to discern a certain degree of acceptance by society. Such acceptance is necessary to allow states and organizations to carry out some measure of regulation of harmful content. A number of arguments are used in the debate about internet filtering; the main argument used to support the implementation of internet filtering is that certain content is harmful and that citizens should be protected from such content (Hamilton, 2008; Wall, 2007). There is a variety of harmful content that already is, or is suggested to be, subject to filtering systems. Child pornography is considered commonly to be the most harmful content (Murray, 2007) and in many states is currently subject to organizational internet filtering (Akdeniz, 2008). Besides being harmful, in most jurisdictions many actions surrounding child pornography are also criminal offences (Gillespie, 2008). Another area of concern, used frequently in the debate to justify internet filtering, is the issue of international terrorism (Hamilton, 2004). After 11 September, there has been an increased implementation of filtering and surveillance systems as a tool to counteract international terrorism (Lyon, 2003). Examples of other areas of concern within this context are: instructions for how bombs and weapons are made, instructions for how to commit suicide, violent content such as extreme pornography, images of violence, hate speech, racism, copyrighted material (music, films, etc.) and gambling.

The main argument against internet filtering is that it is a form of censorship that constitutes a threat to important civil liberties, particularly freedom of expression and privacy, which are considered to be important foundations of democracies (Hamilton, 2004; Rundle & Birdling, 2008). A related argument to this is that illegal content should be regulated by international law or national legal systems (Akdeniz, 2008; Gillespie, 2008). There are also concerns raised that internet filtering threatens the end-to-end principle, which is considered to be the basic principle of network design (Lessig, 2006; Murray, 2007). The end-to-end principle refers to the idea that information should be able to flow between endpoints without disruption. Another argument is that no state or organization has managed to implement a perfect system (Zittrain & Palfrey, 2008). To date, there is no example of implemented filtering systems that neither underblocks nor overblocks content; every system suffers from either (Hamilton, 2004). Overblocking occurs when content not meant to be blocked is blocked and underblocking occurs when not all content meant to be blocked is blocked (Rosenberg, 2001). Furthermore, it is possible to circumvent existing filtering systems. As

mentioned earlier, strategies and circumvention tools have been developed and used to circumvent even the expensive and sophisticated system called "Great Firewall of China" (Murray, 2007). The legitimatization of internet filtering could also be questioned, as any filtering system that classifies or describes content (for example, compiling "blacklists") is affected on the subjective judgement of involved actors (Rosenberg, 2001). The main arguments used in the debate of internet filtering have now been highlighted.

Research approach

Researching the "world of child pornography" (Taylor & Quayle, 2003) involves both certain practical and ethical considerations. This includes, for example, how to gain access to people who have experience from this world, as they can be characterized as a "hard-to-reach" group for people outside this world (Taylor & Quayle, 2003; Wilson & Jones, 2008). Due to the fact that the production, distribution and possession of child pornography is a criminal offence in most western countries, it is unlikely that people involved in this world would be willing to discuss their activities prior to conviction. It would also be an extremely difficult and complex issue, practically, ethically and legally, for a researcher to try to gain access to non-convicted people who have experience of producing and/or downloading and/or distributing child-abusive material.

The approach used within this study has been to interview offenders convicted of child pornography. It could be argued that offenders who have been involved in activities related to the child pornography world are "key experts", and can thus provide information about their activities and behaviour within this world (Taylor & Quayle, 2003; Wilson & Jones, 2008). The reason for interviewing convicted offenders was to obtain information to increase understanding about the individual offender's (1) attitude and (2) behaviour towards ISP filtering of websites containing child-abusive material. In addition, the head of the Child Protection Team at the IT crime section within the Swedish National Criminal Police, i.e. Detective Inspector Sellström, has been interviewed to obtain his view regarding this issue.

Data collection

The data were collected through semi-structured interviews with 15 male offenders, aged between 19 and 55 years. They have all been convicted of production and/or distribution and/or possession of child pornography in Sweden. All the 15 offenders have used ICT for the child pornography crimes. Among these 15 offenders, 11 were also convicted for other sexual offences, mainly sexual abuse against children. The offenders came from a variety of demographic backgrounds and their engagement with treatment programmes also varied. Twelve offenders could be described as very experienced technology users; some of them could even be classed as advanced. A common factor among these 12 offenders is that they have either higher education in computer science (or related subject) and/or worked with computers and use computers every day both for work and leisure. The other three offenders did not have any formal education related to computers or experience of working with computers. The researcher gained access to the offenders through prison psychologists at the prison and through probation services. Noaks and Wincup (2004) emphasize that it is important that researchers address the responsibilities they have to their respondents. This includes ensuring that the relationship between the researcher, who collects the data, and the respondent, who provides the data, is clear and professional. This was achieved by providing all the respondents, prior to the interviews, with an information letter about the study and

seeking informed consent (Noaks & Wincup, 2004). The letter contained information about (1) the purpose of the study and the interviews; (2) how the data would be used and stored; (3) the issue of confidentiality; (4) that participation was voluntary and that respondents could withdraw at any time and if so none of the data would be used; and finally (5) information on how to contact the researcher at a later stage if the respondent widhed to comment and/or ask anything in relation to the study.

All the interviews with the offenders took place in the prison, either in the visiting room or in the prison psychologist's office. The interviews, each lasting between one-and-a-half and two hours, were tape-recorded in 11 cases and transcribed later. In four cases, where the respondents did not want the interview to be tape-recorded, fieldnotes were taken and written out carefully immediately after the interview (Noaks & Wincup, 2004; Silverman, 2005). The same researcher interviewed the respondents and transcribed the data. As mentioned earlier, the purpose of the interviews was to obtain a deeper understanding of the individual offender's (1) attitude and (2) behaviour towards ISP filtering of websites containing child-abusive material. To avoid "one-word answers" (Hollway & Jefferson, 2004) open-ended questions were designed, such as "tell me about your experiences of filtering systems when trying to download child abusive material". Follow-up questions were used to develop further the respondents' stories (Silverman, 2005). Because this study is part of a wider ongoing research project exploring offenders' use of ICT for child-abusive material, the interviews covered more issues than those related to ISP filtering techniques.

The semi-structured interview with Detective Inspector Sellström was focused upon issues related to filtering; for example, the creation and management of the list, collaboration with the ISP and the effects of using filtering systems. This interview lasted between one-and-a-half and two hours and was recorded and transcribed.

Data analysis

Once the data were transcribed, the material was first read and re-read and notes were made. In the next stage the material was structured and coded in relation to the research question and the data sorted into emerging categories based upon attitudes and behaviour (Noaks & Wincup, 2004; Taylor & Quayle, 2003). During the last stage subjective meanings, differences and similarities were searched (Hollway & Jefferson, 2000).

Critical and ethical reflections

The limitations of this material should be noted. The child pornographers interviewed in this study have all been arrested and convicted of child pornography and in many cases, as mentioned above, also for other sexual offences. It should be acknowledged that arrested and convicted offenders represent only a fraction of all child pornographers, and that child pornography and other sexual crimes have a very low reporting rate (Noaks & Wincup 2004; Quayle, Erooga, Wright, Taylor & Harbinson, 2006).

This study follows the ethical rules and guidelines for research formulated by the Swedish Research Council. As described above, prior to their involvement in the study all the respondents were provided with information about the purpose of the study and how the material would be used and stored. Furthermore, the respondents gave their consent to participate in the study. Another important consideration for this study has been to ensure confidentiality for the respondents. All identifying information has been removed or changed to ensure this. It should be noted that Detective Inspector Sellström has given his consent to

use his name in the paper. As described above, this paper is part of a wider ongoing project, approved by the Ethical Committee at the University of Gothenburg.

Evaluating the effectiveness of ISP filtering of child-abusive material

This section presents the empirical findings about the offenders' views and behaviour regarding ISP filtering approaches; the implications are then discussed in relation to the views of the Swedish National Criminal Police.

The offender's view of filtering systems

The findings show that all the offenders are aware that most ISPs in Sweden have implemented filtering systems. Furthermore, they seem to be well informed about the technological characteristics of the filtering mechanism, i.e. that it is based upon blacklisting on domain-level and that not all ISPs in Sweden have introduced it.

All the respondents were unanimous in their attitude that current filtering systems do not hinder child pornographers, whose intent is to access child-abusive material. One respondent expressed it like this:

> This type of filtering is completely pointless... it will not make any difference at all. (1L)

Several times during the interviews the respondents expressed that ISP filtering would have no effect on people with a sexual interest in children from accessing this type of material. Some of the respondents argued, however, that a positive aspect of the filtering approach is that it may prevent the public from accessing child-abusive material.

> Well it is good since it probably will hinder innocent people to get in contact with child porn. I wouldn't want my kids to end up looking at it when they are out there... and not my mum either so I suppose it could do some use after all... for the public so to speak. (1A)

They expressed concern that the public, and specifically children, could access such content unintentionally. This is an interesting paradox, and illustrates further the complexity involved within the area of sexual abuse of children.

Another recurrent theme when discussing the effectiveness of ISP filtering was that law-enforcement agencies seem to lack technological skills and adequate knowledge of child pornographers' behaviour when downloading child-abusive material. None of the respondents in this study considered ISP filtering to be a serious approach to regulating the behaviour of users who wish to access this particular content, although once again some expressed the potential of preventing the public from accessing child-abusive material unintentionally.

> It is like a bad joke, what do they think? It only shows how stupid they are if they really think that this will solve anything. They don't have the faintest idea how people that want to access child porn behave. It is actually quite laughable because it sort of makes it more fun since we trick the police. (1G)

All the respondents claim that they know how to bypass current ISP filtering mechanisms. Additionally, it is interesting to note that many of the respondents described different possible ways of bypassing the system. As argued elsewhere by the author, regulation mechanisms can, and do, evoke active resistance among the users where they develop and implement different

social and technological strategies to circumvent the regulation (Eneman, 2009). The quotation below also reveals offenders' attitudes towards the police, i.e. that the police do not seem to have enough resources to be able to detect child pornographers.

> Firstly, it is very easy to bypass it, there are many ways to do that, the police is always far behind. Secondly, it blocks much more than just child pornography. (1E)

All the respondents think that the ISPs currently block more than child-abusive material and refer to websites with "totally innocent adult porn" and "extreme but legal pornography". This statement indicates further that some of the respondents in this study seem to have accessed both "adult pornography" and child-abusive material.

The offender's behaviour in relation to filtering systems

As shown above, the offenders consider it easy to circumvent the filtering system and are informed about different techniques. The quotation below illustrates that people are helping each other with information on how to circumvent ISP filtering:

> You quickly learn how to bypass filtering... people want to help each other and when I was a new-beginner I got tip-off from another person, more experienced than me about how to bypass the filtering. (IB)

In most jurisdictions, many actions surrounding child pornography are criminal offences (Gillespie, 2008) and therefore the issue of security is considered very important. Child pornographers use a variety of technologies in order to be anonymous when downloading and distributing child-abusive material and when interacting with like-minded individuals. Certain types of anonymous technologies are also used to circumvent filtering systems.

> I can't say that it was a problem, more something that annoyed me. I used proxy servers, so there were never any problems for me and I think most of the others I knew also used proxy. (1H)

Proxy servers seem to be used commonly among the respondents in this study: by using proxy servers the users can be anonymous and circumvent filtering systems. A majority of the respondents have used this type of technology. It should be emphasized that child pornographers use different types of technology which can be used as circumvention tools and to provide anonymity (Eneman, 2009; Gillespie, 2008).

A majority of the respondents have been members of networks with like-minded people sharing sexual interest in children. Within these networks they can access and exchange child-abusive material, but another function regarded important is the availability of technical support.

> It was not difficult at all, all you have to do was to swap to another ISP or manipulate your DNS, it was a bit tricky in the beginning but we had manuals and admins that helped us to adjust our DNS. (1J)

This quotation shows that the respondent received technical support from the network to learn how to manipulate the domain name server (DNS). The strategy of DNS manipulation seems to be used commonly among the individuals within this study. Furthermore, the quotation illustrates awareness of changing to another ISP that has yet not implemented such a system.

Research (Eneman, 2009; Taylor & Quayle, 2003) has shown that membership of networks is considered important by child pornographers and that they can have a hierarchical

and well-organized structure with individuals responsible for certain areas. Within certain networks the members are forced to use particular technology that is considered secure, in order to increase protection for all the network members (Eneman, 2009). Some of the members put a great deal of time and effort into the management of the organization within the network. Within some networks, work schedules are used to ensure that an administrator is always available within the environment to monitor the activities taking place and answer questions.

> Within my group we had a special tech board with a FAQ for questions of technical character, where we could put questions to our admins. Admins are very skilled at computers and are willing to help others how to surf anonymously, how to bypass filtering... they want to help others to access material so more and new material is distributed in our group. (1F)

What is shown here is that within this network they have a special technical board with a frequently asked questions (FAQ) function, where members can post questions of a technical character. It is also possible to read previous questions and answers, just as with an ordinary FAQ. The questions were concerned mainly with issues of anonymity and circumventing filtering systems.

Implications

As described in the Introduction, the main purpose of the ISP filtering approach is to prevent and control access to child-abusive material. Based on the findings, it is possible to identify both certain advantages and disadvantages with the ISP current filtering approach.

In a number of cases, child-abusive material remains available on the website despite the specific access point having been blocked. This means that the website can still be accessed using a different type of ICT or ISP, etc. The findings show that the offenders know how to circumvent the filtering mechanism by using different technological and social strategies. This means that the current filtering approach cannot be seen as an effective measure to prevent and control the behaviour of child pornographers who are intent upon accessing child-abusive material. The findings indicate, however, that the filtering approach seems to act as a preventive measure to protect the public from accessing child-abusive material. This is also confirmed by Sellström (2009), who states that this mechanism can be seen as a "general prevention" in society. Although the filter mechanisms do not seem to hinder child pornographers who are intent upon accessing child-abusive material, one could argue that the systems may have the effect of preventing potential offenders from starting to access such material. Regulation models that require extra steps for the users to gain access to child-abusive material may prevent people who may try to access this type of content based on curiosity. Such regulation could have a positive effect by limiting the market of child-abusive material. Sellström (2009) argues that ISP filtering of child-abusive material is an important statement in our society, showing that it is considered unacceptable and that different strategies are used to reduce distribution of the material.

According to Sellström (2009), the police always investigate the possibility of removing content from an identified website but in many cases this is not possible, due to juridical issues. Difficulties arise, for example, when a Swedish ISP blocks access to a website containing child-abusive material and the server hosting this content is placed in another jurisdiction with different legislation regarding child-abusive material (Sellström, 2009). This highlights further the need for national and international coordination to achieve desired effectiveness with internet filtering as a measure to prevent and control access to illegal

content. The currently used approach (blacklisting) requires pre-identification of the material so that it is known to the system. This means that users can access "new" material that has not yet been detected and blacklisted by the police. Sellström (2009) emphasizes the importance of the public always reporting to the police if they contact child-abusive material through ICT, because the police can then investigate further.

One of the critiques often used in the debate about internet filtering is that filtering mechanisms suffer from overblocking, i.e. they block access to more content than they should. This argument is used commonly in the debate about ISP filtering of child-abusive material and, as the findings show, offenders think that the current filtering approach overblocks. Sellström (2009) claims, however, that the current approach suffers from underblocking. The list used at present contains approximately 380 links, and the links are rechecked every month by the police responsible for the list. The transparency of the Swedish list is seriously flawed, as it has not been evaluated by a third party. This list will soon be evaluated by the author, as the IT Crime Section of the Swedish National Police has approved the new research project and welcomes such evaluation. This means that the author will analyse all the links on the list and use the Swedish legal definition of child pornography to evaluate whether the list suffers from either underblocking and/or overblocking.

The Swedish model is based upon a voluntary partnership between law enforcement and the internet industry. Sellström (2009) believes that this collaboration benefits from its voluntary nature, i.e. that each ISP can choose to take part actively in the regulation of child-abusive material.

Finally, it could be argued that ISPs filtering of child-abusive material serves an important purpose because it reduces the display of the material and consequently reduces the revictimization of the abused child.

Conclusion

As this paper has shown, the current ISP filtering system used to prevent and control access of child-abusive material contains both effective and ineffective elements.

The ineffectiveness of the system can be explained mainly by the ease of circumventing the current approach. To achieve a higher degree of effectiveness, the system should cover several types of ICT. The current approach blocks websites, which is the only possible solution with the filtering techniques available. However, this is not an effective solution, as child pornographers use different types of ICT to distribute and access child-abusive material. Child pornographers' use of, for example, peer-to-peer file sharing programmes in combination with encryption and anonymizing services constitutes a complex and serious challenge for law enforcement and highlights the need for new technological innovations that can be used to reduce the distribution of and access to child-abusive material.

In order to regulate effectively the distribution of child-abusive material, international coordination is required based upon collaboration between the significant actors, such as law enforcement, the internet industry, non-governmental organizations and the banking sector (for example, the Swedish Financial Coalition, the American Financial Coalition against Child Pornography).

The effectiveness of the ISP current filtering system refers to its ability to act as a preventive measure for the public, i.e. to prevent the public from gaining access to child-abusive material unconsciously. Furthermore, the filtering mechanism requires extra steps from users to access the blocked content, and consequently may act as either a hindrance or a

disturbance factor that makes access more difficult. Finally, it reduces the display of child-abusive material and consequently reduces revictimization of the abused child.

In the debate of internet filtering a significant amount of attention has been placed upon the issues of freedom of expression and privacy. Filtering is considered a serious threat to these civil liberties. Although they are important rights that should be protected, they need to be better balanced with other important liberties, such as the right of the child not to be sexually exploited or abused. Child-abusive material is documented evidence of the sexual exploitation of a child, and once the material is available on the internet it constitutes permanent revictimization.

Acknowledgements

The author would like to thank the Swedish Crime Victim Compensation and Support Authority, who funded this research.

References

Akdeniz, Y. (2008). *Internet Child Pornography and the Law: National and International Responses*. Farnham, UK: Ashgate Publishing Company.

Davidson, J. (2008). *Child Sexual Abuse: Media Representation and Government Reactions*. Abingdon, UK: Routledge Cavendish.

Deibert, R., Palfrey, J., Rohozinski, R., & Zittrain, J. (Eds). (2008) *Access Denied: The Practice and Policy of Global Internet Filtering*. Cambridge, MA: MIT Press.

Deibert, R. J., & Villeneuve, N. (2005). Firewalls and power: An overview of global state censorship of the internet. In M. Klang & A. Murray (Eds), *Human Rights in the Digital Age* (pp. 111–124). London, UK: Cavendish Publishing.

Department of Broadband, Communications and the Digital Economy (2008). *Internet Service Provider (ISP) filtering*. Melbourne, Australia: Australian Government.

Eneman, M., Gillespie, A. A., & Stahl, B. C. (2009). Criminalising fantasies: The regulation of virtual child pornography. *Proceedings of the 17th European Conference on Information Systems*, 8–10 June 2009, Verona, Italy.

Eneman, M. (2005). The new face of child pornography. In M. Klang & A. Murray (Eds), *Human Rights in the Digital Age* (pp. 27–39). London, UK: Cavendish Publishing.

Faris, R., & Villeneuve, N. (2008). Measuring global internet filtering. In R. Deibert, J. Palfrey, R. Rohozinski & J. Zittrain (Eds), *Access Denied: The Practice and Policy of Global Internet Filtering* (pp. 5–27). Cambridge, MA: MIT Press.

Gillespie, A. A. (2008). *Child Exploitation and Communication Technologies*. Lyme Regis, UK: Russell House Publishing.

Gillespie, A. A. (2005). Indecent images of children: The ever-changing law. *Child Abuse Review, 14*, 430–443.

Hamilton, S. (2004). *To what extent can libraries ensure free, equal and unhampered access to internet-accessible information resources from a global perspective?* Doctoral Dissertation, Royal School of Library and Information Science, Copenhagen, Denmark.

Hollway, W., & Jefferson, T. (2004). *Doing Qualitative Research Differently: Free Association, Narrative and the Interview Method*. London, UK: Sage Publications.

Lessig, L. (2006). *Code and Other Laws of Cyberspace: Version 2.0*. New York, NY: Basic Books.

Lyon, D. (2003) *Surveillance after September 11*. Cambridge: Polity Press.

Murray, A. D. (2007). *The Regulation of Cyberspace: Control in the Online Environment*. Abingdon, UK: Routledge-Cavendish.

Noaks, L., & Wincup, E. (2004). *Criminological Research: Understanding Qualitative Methods*. London: Sage Publications.

O'Donnell, I., & Milner, C. (2007). *Child Pornography: Crime, Computers and Society*. Devon, UK: Willan Publishing.

Quayle, E., Lööf, L., & Palmer, T. (2008). *Child Pornography and Sexual Exploitation of Children Online*. Thematic paper to the World Congress III against Sexual Exploitation of Children and Adolescents. Rio de Janeiro, Brazil.

Quayle, E., Erooga, M., Wright, L., Taylor, M., & Harbinson, D. (2006). *Only Pictures? Therapeutic Work with Internet Sex Offenders*. Lyme Regis: Russell House Publishing.

Rosenberg, R. S. (2001). Controlling access to the internet: The role of filtering. *Journal of Ethics and Information Technology, 3*, 35–54.

Rundle, M., & Birdling, M. (2008). Filtering and the international system. In R. Deibert, J. Palfrey, R. Rohozinski & J. Zittrain (Eds), *Access Denied: The Practice and Policy of Global Internet Filtering* (pp. 73–101). Cambridge, MA: MIT Press.

Sheldon, K., & Howitt, D. (2007). *Sex Offenders and the Internet*. Chichester, UK: John Wiley & Sons.

Silverman, D. (2005). *Doing Qualitative Research*. London: Sage Publications.

Sutter, G. (2005). Internet service providers and liability. In M. Klang & A. Murray (Eds), *Human Rights in the Digital Age*. London, UK: Cavendish Publishing.

Taylor, M., & Quayle, E. (2003). *Child Pornography: An Internet Crime*. Hove, UK: Brunner-Routledge.

Wall, D. S. (2007). *Cybercrime: The Transformation of Crime in the Information Age*. Polity Press.

Wilson, D., & Jones, T. (2008). In my own world: A case study of a paedophile's thinking and doing and his use of the internet. *Howard Journal of Criminal Justice*, *47*, 107–120.

Wong, R. (2005). Privacy: Charting its Developments and Prospects. In M. Klang & A. Murray (Eds.), *Human Rights in the Digital Age* (pp. 147–161). London: Cavendish Publishing.

Zittrain, J., & Palfrey, J. (2008). Internet filtering: The politics and mechanisms of control. In R. Deibert, J. Palfrey, R. Rohozinski & J. Zittrain (Eds), *Access Denied: The Practice and Policy of Global Internet Filtering* (pp. 103–122). Cambridge, MA: MIT Press.