available at www.sciencedirect.com

ScienceDirect

www.compseconline.com/publications/prodclaw.htm

Computer Law & Security Review

Governmental filtering of websites: The Dutch case

W.Ph. Stol[a,c], H.K.W. Kaspersen[b,c], J. Kerstens[a,c], E.R. Leukfeldt[a,c], A.R. Lodder[b,c]

[a]NHL-University of Applied Sciences Leeuwarden, Chair Cybersafety, The Netherlands
[b]Free University Amsterdam, Computer Law Institute, The Netherlands
[c]Cybersafety Research and Education Network (CyREN)

Keywords:
Internet
Police
Cybercrime
Privacy
Child pornography
Child abuse

ABSTRACT

Following the example of Norway and other European Countries, such as Sweden and Denmark, in April 2007 the Dutch government started filtering and blocking web pages with child pornographic content. In this paper we present a research into the technological, legal and practical possibilities of this measure. Our study leads us to the conclusion that the deployment of filters by or on behalf of the Dutch government is not based on any founded knowledge concerning the effectiveness of the approach. Furthermore, the actions of the Dutch law enforcement authorities do not avail over legal powers to filter and block internet traffic. Consequently the Dutch filtering practice was found to be unlawful. The government could enact a law that provides the police with the relevant powers. However, child porn filters always cause a certain amount of structural overblocking, which means that the government is then engaged in structural blocking of information that is not against the law. This would be in conflict with basic rights as laid down in the European Convention on Human Rights and Fundamental Freedoms and in national legislation. Maintaining a blacklist that is serious in size (a necessary condition for being effective), and at the same time is up-to-date and error-free (which is needed to prevent overblocking), is very labour-intensive, if not impossible to maintain. From the Dutch national police policy perspective it follows that putting so much labour in maintaining a blacklist cannot be considered as a police task. Why then did the Dutch police start filtering? In a society where child pornography is judged with abhorrence, in which safety is rated higher then privacy, and in which managers and politicians frequently have a naive faith in technology, the advocates of internet filters against child pornography quickly find wide-spread support. Although this paper refers to the situation in The Netherlands, it includes a number of elements and issues that are relevant to other European States as well.

1. Introduction

At present, governments of at least forty countries are filtering the supply of information on the internet (Deibert et al., 2008). Not only do non-Western governments (try to) regulate the flows of information on the internet, also in several Western communities governmental bodies are active in filtering and blocking websites, for example in Norway (starting 2004), Sweden (2005), Denmark (2005) and, since April 2007, in The Netherlands (Stol et al., 2008). Yet, the first European country where ISPs started to filter the internet was the UK, in 2004, some months before Norway. In the British situation however, it is not the government but the Internet Watch Foundation (IWF) that maintains a so-called blacklist. Consequently, we

0267-3649/$ – see front matter
doi:10.1016/j.clsr.2009.03.002

do not call this filtering system a form of *governmental* filtering. We will come back to the British approach later.

All the above-mentioned filtering activities in European countries are part of the fight against child pornography on the internet. A central problem in connection with this development is how governmental filtering of the internet relates to freedom of speech and other constitutional rights.

During the first half of 2006, when some European countries had already started filtering websites but when there was no filtering practice in The Netherlands yet, the Dutch Lower House passed a motion by which it requested the Minister of Justice 'to promote the further development and use of the technical possibilities to block, filter and to cut off child pornographic material from the internet and other media and to further inform the House about this'. Before responding to this resolution, the Minister of Justice commissioned a scientific report about the technical and legal possibilities of filtering and blocking child pornographic material on the internet. This paper provides an overview of that report.

In the mean time, the Dutch police had adopted the Norwegian approach in filtering the world-wide web and had obtained the collaboration of three ISPs (UCP, Scarlet and Kliksafe). Our research started in December 2007, more than half a year after the police had started this filtering project; we finished gathering research material on the 1st of May, 2008. In this paper we present the findings of our investigation into the Dutch state of affairs as of May 2008. In the concluding paragraph we pay attention to the quality of the Dutch policy concerning internet filtering and to the Minister of Justice's reaction to our findings.

2. Research questions, methods and material

The main question of this research is: What are the technical possibilities of filtering and blocking information on the world-wide web and on what grounds can these possibilities be legitimized? This main question has been worked out in five research questions:

1. Which technical possibilities (tools) are available for filtering and blocking child pornography on the internet, particularly on web pages?
2. What experience has been acquired with those tools in terms of effectiveness?
3. What legal possibilities are available for the use of filtering and blocking to prevent child pornography on the internet?
4. How does the Dutch filtering system work out in everyday practice?
5. What is the relation between technical possibilities and the actual filtering practice on the one hand and legal possibilities on the other?

The three main methods of research are: desk research, semi-structured interviews with experts and those involved in filtering practice, and an on-site review of the filtering practice, including a check of the blacklist and the corresponding websites. Because there is still little experience with filtering information from internet in The Netherlands, experience from abroad is involved in the research.

The technical investigation of filtering possibilities and the legal knowledge about the prevention of child pornography on internet are linked together in this research. Putting together the connections between the (technical and legal) information acquired during the research was not kept until the phase of analysis at the end of the research, but it has been part of the research process right from the beginning. In this way lawyers, for instance, were able to react to technical possibilities and shortcomings proposed by technicians and investigation specialists were able to react to ISPs standpoints, et cetera.

Besides a regular study of literature with the use of databases such as ScienceDirect, our desk research included 80 digitally published news articles about developments abroad, about 60 newspaper articles about the situation in The Netherlands (using the LexisNexis news portal), as well as some 140 postings from Norwegian internet forums. In addition, we studied several (governmental) policy documents and texts of law concerning the situation in The Netherlands, Norway, Sweden, Denmark, UK and the US. We were able to study the original versions from the Scandinavian countries, since one of the researchers reads these languages. In total, we interviewed 25 Dutch persons, mainly from ISPs and law enforcement agencies. Furthermore, we discussed our research with several experts in the field of internet filtering and/or child safety when we met representatives from the International Centre for Missing and Exploited Children in Brussels, and when we visited the Dutch national meeting concerning 'Notice and take Down' in Amsterdam in December 2007, the Egyptian Internet Safety Conference in Cairo in March 2008 and the so-called Octopus Conference in Strasbourg in April 2008. Our on-site review included 70 internet domains that were on the Dutch blacklist. This review we also used to get a picture of the procedures used by the police in putting together and maintaining the blacklist.

3. Technical possibilities

Our research focuses on the possibilities to filter web pages (and not e-mail messages or news group postings for example) since the actual filtering practices in The Netherlands and in the other above-mentioned European countries are oriented towards web pages.

In general, filters work on the basis of lists with addresses and/or codes that have to be blocked (blacklist filtering) or on the basis of general criteria by which the filter program determines if certain information can or cannot be allowed to pass through (dynamic filtering) (Haselton, 2007). As far as we know in Europe only manually composed blacklists are used for filtering child pornography. This means that all web pages that are on the list have been judged on the basis of human intelligence (*human review*). A disadvantage of this kind of system is that new information appearing on the internet is untouched by the filter. The editors first will have to notice the new information, judge it, and then put it on the list. That brings us to the second disadvantage: composing a blacklist on the basis of human review is labour-intensive, because the