Filtering Child Pornography on the Internet

An Investigation of National and International Techniques and Regulations

Summary

W.Ph. Stol
H.W.K. Kaspersen
J. Kerstens
E.R. Leukfeldt
A.R. Lodder

26 May 2008

Filtering Child Pornography on the Internet

An Investigation of National and International Techniques and Regulations

NHL University of Applied Sciences, Leeuwarden
Chair Safety and Security

Free University, Amsterdam
Computer Law Institute

W.Ph. Stol
H.W.K. Kaspersen
J. Kerstens
E.R. Leukfeldt
A.R. Lodder

CyREN – Cybersafety Research and Education Network

This study is conducted under the authority of the WODC (Research and Documentation Centre) of the Ministry of Justice

Summary

During the first half of 2006 the Lower House passed a motion in 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'. That motion was the reason for this research that offers an investigation of the technical and legal possibilities to filter and block child pornographic material on the internet.

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

1. Technical possibilities:
    a. Which technical possibilities (tools) are available for filtering and blocking child pornography on the internet?
    b. What experience has been acquired with those tools? What practical problems are connected to the application of those tools, such as the availability of those tools, ability to maintain, installation, effects on speed and capacity of internet traffic?
    c. Is the application of those tools effective, feasible and sustainable?

2. Legal context
    a. What legal possibilities are available for using filtering and blocking to prevent child pornography on the internet?
    b. Are there any legal impediments and/or bottlenecks and how can a solution to these be found?

3. Self-regulation:
    a. How can self-regulation (i.e. regulation of behaviour without legal duress) by internet providers be an effective and long-term way to filter and block child pornographic material on the internet?
    b. Which possibilities are available for the government for 'controlled self-regulation'?
    c. In relation to the internet what has the experience of 'self-regulation' been?

4. Abroad:
    a. In other countries, how have they attempted to filter and block child pornographic material on the internet?
    b. What are the technical means that are being used?
    c. How are the filtering and blocking legally embedded?
    d. What is the practical experience that has been acquired with filtering and blocking (with respect to effectiveness, feasibility and sustainability?
    e. Can the foreign experience be translated to the Dutch situation?

5. Further technical developments
    a. Does it make sense to expand the existing possibilities?
    b. If yes, what type of applications should be built?
    c. If yes, who should be building those applications?
    d. Is there a role for the government in the development of such applications?

The two main methods of research are: desk research (literature, documents, media websites) and semi-structured interviews with experts and those involved. Because in the Netherlands there is still little experience with filtering information from internet, experience from abroad is involved in the research. Furthermore the research team on the scene has formed an opinion about the procedures being used by the *KLPD* (*Korps Landelijke Politiediensten* / National Police Services Agency) putting together and maintaining the so-called blacklist.

In this research the technical investigation of the maintenance strategy and the legal knowledge about the prevention of child pornography on internet are linked together.

We did not save putting together the connections between the information acquired during the research for the phase of analysis at the end of the research but it has been part of the research process right from the beginning.

In that way jurists, for instance, were able to react to technical possibilities and shortcomings proposed by technicians and investigation specialists were able to react to ISP's standpoints.

Filter techniques

In order to be able to filter and block child pornography on internet there should be an understanding exactly how this material is being spread. Exact figures about the size and the routes along which the distribution takes, however are unknown. From other research and statistical material can be deducted through which kinds of internet traffic child pornography is being spread: Websites, P2P networks, virtual hard disks, newsgroups and chat boxes. It is known that P2P networks substantially contribute to the spread of child pornography and it is suspected that this way of spreading child pornography around will play the biggest role in the future. Because it is unknown how much child pornography is being spread through which internet facilities, this research is unable to judge the effects of filtering and blocking certain parts of internet on the total spread of child pornography.

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). Dynamic filtering leads relatively to a lot of *overblocking.* As far as it is known in Europe only use is being made of block lists put together by people for filtering child pornography.

Blocking on the basis of a blacklist can be done with IP addresses, domain names, URLs or hash codes. Blocking on the basis of an IP address is not suitable because it is not precise enough. In the Netherlands blocking on the basis of domain names is being done at this time. This is relatively easy and cheap but not as precise and quite easy to get around. The opposite applies to blocking on the basis of the URL or the hash code. However this method requires substantial technical investments because all internet traffic has to be controlled with respect to content. A technical solution for the latter problem is a two-stage filter method in which from all traffica suspected data flow is filtered first (for example on the basis of IP addresses), after which just this traffic (for example on the basis of the URLs) is checked for content.

Filtering can be done in different places: on the computer of the person using the internet, in search engines, in the central server of an organisation, in the server(s) of the ISPs or on a national level. The latter is not under discussion in Europe. Filtering on the level of individual users and organisations does not meet technical or legal difficulties. Filtering on the ISP level of chat channels, P2P networks, MMS and webcam traffic is much more difficult to filter than websites on internet. Moreover it cannot always be done on the basis of block lists since such connections usually run through less structured channels.

Technically it is impossible to manufacture a filter that stops child pornography 100 percent and at the same time lets all legal information through. On top of which the

information that is being put on the internet is changing continually. What rightfully is being filtered now in a few moments could be wrongful. Whoever wants to put up a serious barrier against child pornography, realistically spoken[1] has to accept a certain amount of structural *overblocking.*

Legal context

The penalization of child pornography in art. 240 Sr was first aimed at abuse of youngsters. Also in the Netherlands under the influence of international developments, the realisation has gotten through that it is at least as important that youngsters are being protected from behaviour that can be used to encourage or tempt them to participate in sexual intercourse or against behaviour that can become a part of a subculture that encourages sexual abuse of youngsters.

Internationally considered there have been efforts to harmonize legislation on child pornography. Although these efforts have not been without results major differences between countries continue to exist. Virtual child pornography for example is not punishable in all countries. Also the age limit of 18 years old does not apply everywhere. Because of this a situation can exist where even with countries that the Netherlands has a treaty with for legal cooperation it is not possible to act against all the manifestations of child pornography. The Netherlands has the authority to block child pornography when the consequences of the criminal offence manifest themselves within the Dutch rule of law. That also applies to other countries as well. Because of this the situation can arise that visual material that is being put on (internet) traffic lawfully here will be stopped by other countries as liable to punishment. The opposite can also be the case.

The application of filtering or blocking of internet traffic means that the content of certain flows of traffic will become known. The confidentiality of this traffic is guaranteed by art. 8 EVRM and the corresponding provisions of the Dutch Constitution. That means that blocking should be done by or in name of the government on the basis of a formal statutory authority. Blocking child pornography through ISPs needs the approval of the subscribers.

Based on European rules, internet providers are not responsible for the traffic of data that they did not initiate or influence with respect to content. They do not have to verify whether or not they host punishable information or information that violates the law, but they are supposed to act in case they have knowledge of the punishable or unlawful character of the information.

In art 125o Sv the present law provides the legal authorities with the power to make stored data inaccessible. For art. 54a Sr (another article with respect to removing data from a suspected persons computer) holds that it is not clear to where the jurisdiction exactly extends and in which cases that jurisdiction can apply. In a continuation of this an addition and a revision of art. 125o Sv as well as 54a Sr for a mutual cohesion is desired. The starting point after all should be that the law gives the permission to remove or to have removed certain information from the systems of internet providers and individual users of internet. This should also extend to the blocking of the flow of information by which child pornography has been offered.

Limitations of the basic law of freedom of speech need to be set by formal law. All the rules enabling filtering and blocking are coupled to a certain amount of overblocking. Blocking by or on behalf of the government, provided the law would give authority to that, binds one to a careful choice of the instruments to be used and a continuous verification whether the measure serves its purpose. This is to prevent that application of the rule is in violation with art. 10 EVRM and art. 7 GW.

[1] Theoretical but not realistic is the option that people have all the items on the block list checked for their correctness by experts all the time.

International developments

Blocking of the supply of information on the internet happens in at least forty countries. How filtering and blocking have been dealt with in a number of western and non-western countries has been investigated.

During this research the situation in Norway, Sweden and England has been looked at in particular. The situation in Norway has been extra emphasized because the Norwegian initiative to block websites with child pornographic content has been brought through UPC to the Netherlands. Furthermore the United States is briefly discussed and as far as the non-western countries is concerned – more as an illustration – Saudi-Arabia, Iran and China have also been looked at.

In Europe two filter models are used: the Scandinavian (Norway and Sweden) and the English model. The Scandinavian one is organisationally spoken in the first instance based on a voluntary public-private cooperation between the police and the ISPs in particular and technologically spoken on the blocking of domains. The English model organisationally spoken is based on self-regulation by commercial ISPs supported by the NGO IWF and technically spoken is based on the blocking of URLs.

The English model compared to the Scandinavian model is more complicated and more expensive but in addition it is also of a more intricate structure. In Norway and Sweden the ultimate goal of filtering is ambitiously formulated: reduce the number of abused children. In England the chief purpose is: to prevent innocent users of internet unintentionally from getting in contact with child pornography. If there are any internet users that are unwillingly getting in contact with web pages (the filters are aimed at those) with child pornographic material however is a very well kept secret.

The United States take a special position. The prevailing First Amendment doctrine offers the American government few possibilities for filtering and blocking of child pornographic material on the internet. This doctrine does not play a role with respect to filtering and blocking by private citizens. There are a number of companies that manufacture and offer filters. Research however shows that the performance of these filters is mediocre.

Saudi-Arabia, Iran and China show that it is possible to filter on a national level. A national filter structure includes technology, law and monitoring organisations.

China seems to be the most effective, but this country accepts a high degree of overblocking. A worldwide survey of internet filtering shows that filtering governments are not able to get those systems watertight, because governments cannot keep up with the strategies that are being developed by users to avoid these filters.

Concrete, measurable aims in order to filter and block child pornography are often lacking. The aims frequently mentioned are: preventing sexual abuse of children, making the sale of child pornography unattractive and protecting unsuspecting internet users from child pornography. No studies have been done about the social effectiveness of filtering and blocking child pornographic material on the internet. Who, whatever the circumstances, encounters a filter and what that results in is unknown. The argument for using filters and blocking child pornographic material would then also be based mainly on the expectation that the measure is effective.

In Western countries self-regulation is a reoccurring and essential part of filtering and blocking child pornography on the internet. Mostly we then see government intervention in the background, not infrequently threatening ISPs with legislation. In Norway and Sweden the authorities keep up the blacklist and the ISPs carry out the filtering. In England the upkeep of the blacklist is done by a private business (IWF – Internet Watch Foundation). In addition we also see self-regulation by internet users (parents) and LAN administrators. They use filters that again are developed by other private parties: commercial businesses that see a market in

this. In the US the legislature has charged the public schools and libraries with the duty to take measures against child pornography on the internet; in Norway employers and management are legally obliged to take measures to prevent employees from downloading child pornography. Altogether it seems that filtering of child pornography can be regulated by means of self-regulation, provided the observations made earlier about the effectiveness of filtering are then also applicable.

The situation in the Netherlands

In the Netherlands a lively political-social discussion has taken place concerning the manner in which the spread of child pornography on the internet can be prevented. The discussion moves between two polarities, by which on one hand the dangers of internet censure is emphasised and on the other side the need for a clamp down in which every measure seems to be justified. Also the present government wants to act to combat child pornography and with that answer the moral indignation of society. Since there is, as already stated, no research available about the effectiveness of filtering and blocking, the present application of filters by or on behalve of the Dutch government is not based upon well-founded knowledge about the effectiveness of this measure.

At this moment websites containing pornographic material that are hosted in the Netherlands are physically removed by the hosting provider. Websites with child pornography that are hosted in countries with which the Netherlands has a legal cooperation treaty can under the terms of a legal cooperation be removed by the appropriate authorities. For websites that are hosted in countries with which the Netherlands has no legal cooperation treaty this is not possible. The one option that remains is to block the sites. The *KLPD* has taken the first step for this purpose following and analogous to Norway's way of blocking.

From this study has been found that the contents and the manner of compilation of the *KLPD*'s blacklist on the basis with which the ISP's block child pornography sites contain a number of inadequacies. The list has connection with about 100 websites, while the total number of child porno sites that fall within the range of art. 240b Sr probably is a multiple of this. Moreover the list contains websites that (by now) do not exist anymore or that (by now) do not contain child pornography anymore. Also sites appear on the list that are hosted in the Netherlands and an important portion of the stated sites are hosted in countries with which the Netherlands has a legal cooperation treaty (especially the US). No procedures have been established for the management of the list by the *KLPD* and no verifiable criteria have been formulated on the basis from which additions to the list are decided. The upkeep of the list is not frequent enough.

The required time investment for the realisation of the blacklist forms, considering the (investigation) task of the *KLPD*, a disproportionately large demand on the detectives' available time. Also in the framework of the debate about the core responsibilities of the police is it then also the question whether or not the set up and the upkeep of a blacklist should be left to other parties.

Legal analysis of the practise of filtering in the Netherlands

The *KLPD* makes agreements with internet providers to the extent that an ISP blocks domains that the *KLPD* considers child pornographic and therefore are placed on a blocking list by the *KLPD*. The ISP is obliged to use the *KLPD*'s list and does not direct the internet user to the requested domain but to a so-called stop page. The *KLPD* protects the ISP from third-party claims because of the instruction of the applied blocking by the *KLPD*.

The *KLPD* implements convents with private parties of a presupposed public duty, namely the actual maintenance of the rule of law. Since the filtering and blocking of internet traffic infringe on the constitutional right of confidential information, as regulated in art. 13

GW and art. 8 EVRM, these require a similar measure for a formal legal basis. So if the law in a similar competence would provide this – article 54a Sr and art. 125o Sv are not geared to this – this does not depend on the police or the *KLPD* as a part of that. Art. 2 Polw provides just as little basis for filtering and blocking internet traffic. These agreements form therefore an unacceptable thwarting of public law authority and with this public safeguards. These agreements are therefore not legally valid. From the point of view of the constitutional law it is not acceptable that the authorities make use of instruments without sound legal basis in order to reach an otherwise legitimate goal. If the legislature's intention is to designate the blocking of child pornography as a duty of the police, then this should be provided in specific legal jurisdiction.

Scenarios

In order to indicate which possible ways the spread of child pornography on the internet in the near future can be prevented, we give a rough sketch of four scenarios. These scenarios are within the spectrum of spontaneous self-regulation up to internet traffic controlled by the government.

In the first scenario the government puts all its energy in core responsibilities and it leaves the development, management and operation of filters to private companies, non-commercial organisations and internet users. Developments abroad show that there is a growing (commercial) market of suppliers of all sorts of filters. By starting with the free market the government stays out of the discussion about internet censure, moreover there are no legal complications.

In the second scenario the government stimulates and facilitates the development of filters without taking on the executory duties itself. In this scenario the government up to a certain point itself has control and partially one can speak of a public-private cooperation (PPC).

In the third scenario the government takes care of the implementation of some of the tasks itself. In a PPC the police put a block list at the disposal of the market sectors that use those to develop child pornography filters. The police draw up protocol rules for managing the files that fall under their responsibility. They also take care of full transparency in the criteria on which the basis of the particular list has been put together.

In the fourth scenario the government makes the implementation of child pornography filter mandatory based on formal legislation. It requires ISPs to install filters with which websites with child pornography can be blocked. A variation on this is that the government forces certain persons or organisations to take action against the spreading of child pornography on internet. The government itself in this case does not the authority to filter, but forces employers or public libraries to take action.