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 © 2009 W.Ph. Stol, H.K.W. Kaspersen, J. Kerstens, E.R. Leukfeldt & A.R. Lodder. Published by Elsevier Ltd. All rights reserved.
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 supply of information on the internet changes continually, and because that same information may be supplied from varying places. Dynamic filtering intends to meet these objections.

The principle of dynamic filtering is that the filter software checks whether components of the information flow to be filtered contains certain (combinations of) features, such as certain words ('pre-teen' and 'sex') and/or certain pictures, such as pictures with characteristics of nude photography. When filtering the pictures on the basis of general criteria, colour, texture and shape are looked at (Shih and Lee, 2007). Various detection techniques have been developed to detect pornography, such as a method to identify nude skin (Fleck et al., 1996), to discern skin from non-skin (Jones and Rehg, 1998; Zeng et al., 2004), to detect pornographic shapes (Yang et al., 2004), as well as techniques based on the comparison of unknown pictures with known pictures (Wang et al., 1998; Yoo, 2004).

We have just discerned between blacklist filtering and dynamic filtering. A traditional, substantial difference between the two is that with *blacklist filtering* the information to be filtered is judged by people, while that is not the case with *dynamic filtering*. With the latter method, the information to be filtered is detected by a software program by means of a combination of search criteria (a certain algorithm). Based on that difference, the expected accuracy of *blacklist filtering* will be significantly larger (and so, the extent of overblocking will be significantly smaller) than that of *dynamic filtering*. Haselton (2007) observes that it was common practice between 1995 and 2002 for companies who made filters to pride themselves on the fact that all the sites on their blacklists had been reviewed by their employees (*human review*). Nowadays, blacklists are also generated automatically: based on certain criteria a search engine searches sites that apparently belong to a category to be filtered. The found sites are automatically placed on the blacklist (*automated review*). Thus, a blacklist is generated on the basis of *dynamic filtering*. In this way the difference in accuracy between *blacklist filtering* and *dynamic filtering* is eliminated.

There are various dynamic filters for detecting and blocking pornography.[1] Insofar as we now know, there is no dynamic filtering system to automatically detect *child* pornography. The additional problem would be the automatic assessment, through general criteria, of the (apparent) age of the depicted person. According to the interviewed experts it is frequently impossible to assess the age with some degree of certainty, even after a thorough study of the picture. In order to prevent interpretation errors, the Dutch police team responsible for the maintenance of the blacklist, focuses on the patently obvious cases.

A filter can be installed in various places or levels:

1. At a national level (all users in any country). The filter should then be placed between the national internet backbone and the digital world beyond. In various non-Western countries filtering is done like this, such as Saudi Arabia and China (Zittrain and Edelman, 2002; Deibert et al., 2008).
2. At the level of an ISP (all customers of an ISP).
3. At the level of a central server (all users of that server, for example all employees of an organisation).
4. At an individual level (the user of a certain computer).

Blocking through a blacklist is possible on the basis of:

a. IP-address (Internet Protocol). All information in the IP-address level is blocked, so of an entire web server. A web server usually hosts various domains (Clayton, 2005; Edelman, 2003). In that case, they are all blocked.

b. Domain name. An entire internet domain is blocked, for example www.preteensex.nl.

c. URL (Uniform Resource Locator) of a file or hashcode of a picture. A file on a certain location, for example www.pornography.nl/pics/lolitas.html or www.pornography.nl/pics/firstlolita.jpg, or a certain picture with a specific hashcode is blocked.

In our research we encountered three ways in which filters are embedded in internet traffic:[2]

i. DNS-filter. A DNS (Domain Name Server) finds the corresponding numerical IP-address (such as 123.123.123.123) for every linguistic domain name (such as www.cybersafety.nl) someone enters. The browser needs an IP-address to find the domain searched. If a domain is on a blacklist, the DNS-server will not give the correct IP-address for a linguistic domain name, but the IP-address of a so-called police *stop page*.

ii. Simple proxy filter. All internet traffic is led by a separate computer (a so-called proxy-server, or proxy for short) on which a filter has been installed which checks for every URL or hashcode whether it can be admitted or not.

iii. Two-step proxy filter. All internet traffic is led through a proxy first onto which a filter has been installed that basically discerns, i.e. on the basis of an IP-address, between suspected and unsuspected information flows. The suspected flows are diverted to a second proxy with a filter that checks on a detailed level (URL, hashcode) what can be admitted or not.

The above-mentioned illustrates that technically, there are quite a number of possibilities to realise a filter. The Dutch filtering system is based on DNS filtering on ISP-level (subsequently: 2, b, i). The police experts (read: the government) compose and maintain the blacklist and thereby determine what should be blocked. The co-operating ISP realises the actual filtering and blocking.

[1] Several of these have been subject to testing. It turned out that the quality of the filters is not very good; (considerable) underblocking or overblocking continuously occur (Greenfield et al., 2001; Richardson et al., 2002; Resnick et al., 2004; Kranich, 2004; Deshmukh and Rajagopalan, 2005; Stark, 2006; Haselton, 2007).

[2] Let it be remarked that we have not been able to find out exactly how the filter systems in non-Western countries work.

4. Effectiveness

Effectiveness of a measure is judged against to what extent that measure helps to achieve a certain preconceived goal. Fundamentally, before one starts filtering and blocking child pornography on the internet there should be an understanding of exactly how this material is being spread. However, exact figures about the size and the routes along which distribution takes place are unknown. Interviewed experts emphasize that P2P-networks substantially contribute to the spread of child pornography and hold that this way of spreading child pornography will be the most important one in the future. Notwithstanding these views no concrete information was found to judge the effects of filtering and blocking certain parts of the internet (web pages) on the *total* spread of child pornography, because it is unknown how much child pornography is being spread through which internet facility.

Furthermore, when assessing effectiveness it should be clear what targets are envisaged with the deployment of the filtering instrument. We have not found any governmental policy documents in which explicit targets for filtering are specified. Therefore, we base ourselves on media quotes from police spokesmen, internet providers and representatives of the authorities involved. Frequently mentioned objectives given in Norway, Sweden, England and The Netherlands are: preventing sexual abuse of children, making commercial offering of child pornography on the internet unattractive, preventing that 'internetters' search child pornography out of curiosity, and protecting innocent users from unwanted confrontation with child pornography on the internet.

It is indeed possible to reduce the availability of certain internet information through filtering, although no filtering system has appeared to be waterproof. We learn this from the situation in non-Western countries such as Saudi Arabia, Iran and China (ONI, 2004, 2005a, 2005b; Deibert et al., 2008). We have no reasons to assume that less rigorous filtering systems – as currently used in Scandinavian countries, England and The Netherlands – have no effect whatsoever: at any rate they cast a certain barrier. But, it remains to be seen if reducing or hindering the access to child pornographic material on the internet will lead to a decrease of sexual child abuse. We have not found any indication that filtering techniques against child pornography bring that effect about. No research has been conducted in this field, and it remains to be seen if meaningful research is at all possible. The interrelationship between filtering and child abuse is probably too vague.

Another, much-mentioned objective is to make the commercial offering of child pornography unattractive. The market for child pornography has increased due to the internet and online paedophiles who are prepared to pay money for child pornographic material. Filtering and blocking techniques – as the assumption goes – will cast an additional barrier against this lucrative trade: suppliers and consumers can no longer reach one another easily, which will cause the sale, and so the turnover, to decrease. Suppliers will perhaps find another source of income, less child pornography will be made, and so also – and that remains the final goal – the abuse of children will decrease. We have not found any facts in this research to corroborate the above-mentioned chain of cause and consequence. We also have not found any information based on which we could say to what extent the number of abused children corresponds to the commercial market and to what extent that number corresponds with the 'enthusiasts market'.

Our findings indicate that filters are not effective against 'enthusiasts' who mutually exchange pornographic material. They know how and where to make contact with each another anyway. Prior research shows that repressive measures against the commercial spread of child pornography will cause the suppliers to explore other, less risky ways to offer their material (Stol, 2004b). As far as we know, no research has been undertaken to the question whether repressive measures indeed lead to a *decrease* of the supply.

As mentioned before, a filtering system could reduce the availability of certain information, and therefore, it may prevent persons who are looking for pornography on the internet to extend their search to child pornography, just out of curiosity. Before this group, a filter could be a signal that child pornography is unacceptable in our society, as some respondents argued. The size of the group of 'rubbernecks' is unknown; however, nor do we know how they behave on the internet and, if so, how a filter would affect their behaviour. This is also a factor that prevents us from assessing the effectiveness of the measure of filtering.

A more modest objective of filtering seems to be the protection of innocent users against child pornography on the internet. Our findings raise the question to what extent the average internetter may unexpectedly or unwantedly be confronted with child pornography. Where internetters use a spam filter, are not searching for sex sites, do not participate in sexual news groups or panels and do not take notice of obscure messages that always seem to pass despite safety precautions, the chance of encountering child pornography seems minimal. Employees of the Dutch private Meldpunt Kinderporno op Internet (Registration Child Pornography on the Internet) believe that 'decent' internetters sometimes make a report of child pornography on the internet, although they say they also have experiences with less innocent reporters (persons who are looking for pornography with youngsters on the internet, but think some material goes too far). However, no research has been conducted into the surfing behaviour of netters who report child pornography. In this light, it remains to be seen whether 'the protection of innocent internetters' indeed is a realistic objective of filtering. The filters discussed in this report are aimed at websites. No interviewed expert, authority or other person involved was able to refer to a case in which a 'decent' internetter was unexpectedly or incidentally confronted with child pornography on a website, including representatives of the Registration Child Pornography on the Internet.

Where an instrument like a filter is to be deployed for a certain goal, one has to consider whether the instrument works as intended. In the US the accuracy of the filters in general has been object of continuous research. Filters can make two kinds of errors: block permissible websites (false positives or overblocking) or allow inadmissible websites (false negatives or underblocking) (Deshmukh and Rajagopalan, 2005). In the first instance, the filter can only be partly effective, in the second instance a tension with freedom of speech (and the chance of damage claims) is generated. Accuracy tests show that the ultimate filter does not exist, and that it is always a matter of finding a balance between *underblocking* and *overblocking*. Dynamic filtering techniques especially cause problems in this respect. They never perform properly on both criteria. The fewer *overblocking* a filter shows, the more *underblocking,* and the other way round (Greenfield et al., 2001; Richardson et al., 2002; Kranich, 2004; Resnick et al., 2004; Stark, 2006; Haselton, 2007).

We have not found any concrete information about research into the performances of blacklist filters based on human review, such as the child pornography filters that are the subject of this study. Yet, it is possible to make some observations on the matter. A child porn blacklist can only have a substantial effect if it has a certain size. Furthermore, in order to prevent overblocking, it must be up-to-date and error-free. Information that is offered on the internet is subject of continuous change. What is being rightfully blocked may be wrongfully blocked a few moments later. As a consequence, any filter will inevitably lack behind. It is, therefore, hardly possible to manufacture a filter that stops child pornography 100 per cent and at the same time passes all other information. Even if experts would check the correctness of a blacklist on a 24-h basis it has to be accepted that a child porn filter causes a certain amount of *structural* overblocking. For a filter that blocks using domain names, such as the Dutch DNS-filter, the filtering authorities should take into account that a domain seldomly contains solely child pornographic material, and that the decision to block a domain implies that all legal information the domain contains other than child pornographic material is also blocked.

Testing the accuracy of the filters is valuable, but it does not give conclusive information about the effectiveness of the filter. A filter may be highly accurate, but if users are able to bypass it, it may not be effective. Moreover, effectiveness cannot be demonstrated where a filter is deployed for a non-existing problem (such as, for example, the innocent user who is unexpectedly confronted with child pornography) or for a problem of which the filter has no or no verifiable influence upon, such as the number of abused children.

Filtering authorities collect information about the number of times a filter is activated (number of hits). From these statistics no conclusions can be drawn about the scope of the child pornography problem. It is unclear what these figures really mean. The number of hits tells even less about the effectiveness of the filters. No research exists into exactly who are or what is blocked by the filter, and so how to interpret the number of hits. It is therefore simply unwise to put down numbers of hits as an argument in favour of or against filtering.

The Dutch government uses, just like the Norwegian, Swedish and Danish governments do, a DNS-filter (see above) with which internet domains are blocked on ISP-level, based on a human reviewed blacklist. Bypassing any such filter is relatively easy. The user can subscribe to a (foreign, if necessary) provider that does not use such a filter. The user could also enter the IP-address of the blocked site. In that case the browser will not go to the DNS-server with the filter, but will directly go to the specified address. Users can also connect their own DNS-server to their computer and bypass the server-with-filter of their own provider. Technical experts drew our attention to a whole repertory of websites where commercial suppliers put DNS servers up for sale for home use, and explain in detail how a DNS-filter can be bypassed. To put the above into perspective, it should be observed that a more than average technical knowledge is required to bypass a DNS-block. At the same time, it must be held possible that filtering-antagonists place anti-filter software on the internet which is also easy to install on a computer by a lay-person.

For the Dutch (Norwegian, Swedish, Danish) filtering practice the general effectiveness question applies (which goal has actually been achieved?). What is more, a DNS-filter is fairly coarsely-woven. The filter blocks at domain-level, so there is a considerable risk of overblocking. And the filter can be bypassed easily. There are no 'effect' studies; the filters have not been submitted for accuracy or effectiveness tests. This means that the deployment of filters by or on behalf of the Dutch government is not based on any founded knowledge concerning effectiveness of the measure.

5. Legal context

Under Dutch Law the criminalisation of child pornography in article. 240b Penal Code was firstly aimed at the factual abuse of youngsters. Under the influence of international developments, also Dutch parliamentarians and criminal policy makers became aware that it is at least as important that youngsters are being protected from behaviour that encourages or tempts them to participate in sexual intercourse or against behaviour that can become a part of a subculture that encourages sexual abuse of youngsters. From that consideration, also virtual child pornography (child pornography created with computer-animated children instead of real children) has been brought under the criminal offence. The current text of article 240b PC reads as follows:[3]

1. The person who distributes, publicly displays, makes, imports, passes through, executes or possesses a picture – or an information carrier containing any such picture – of a sexual conduct, with which a person who apparently has not yet reached the age of eighteen years is involved or apparently involved, will be punished with a prison sentence of four years at the most or by a fine of the fifth category.
2. The person who has made a habit or a profession out of committing one of the criminal offences as described in the first paragraph is punished with a prison sentence of six years at the most or by a fine of the fifth category.

Internationally, efforts have been made to harmonize legislation on child pornography.[4] Although these efforts have

[3] All translations of Dutch rules of law are ours, unless otherwise indicated.

[4] Article 9 Cybercrime Convention 2001, Council of Europe, ECTS 185. Europe Union Framework Decision, article , OJ L 13, January 20, 2004, 13.

not been without result, major differences between countries continue to exist (Stol et al., 2008). The differences concern the criminalised acts in relation with child porn (such as the production, distribution, making available and procurement of such material), the nature of child porn and the age limit of the child involved. For example, virtual child pornography does not qualify in many countries as forbidden material. Seen from an international perspective the Dutch provision of article 240b Penal Code has a rather wide scope. This, however, will not ensure that international co-operation is possible with countries with no law on the matter or with a more restricted law.

Domestic law generally will authorise law enforcement to prevent the commission of a crime within the territory of that State. Similarly, domestic law will authorise to take reasonable measures – within the territory of that State – to prevent or reduce the impact of criminal conduct committed abroad. *In casu,* child porn material may lawfully be made available on the internet from some States, but it may be blocked by other countries because it is part of a criminal act according to the law of that State. The opposite may also be the case.

The application of filtering or blocking of internet traffic means that the content of certain flows of traffic has to be put under (automatic) surveillance. The communication between an internet user and a website is as being confidential protected by article 8 of the European Convention on Human Rights and Fundamental Freedoms (ECHR), like it is under article 13 of the Dutch Constitution. As a consequence, filtering internet traffic by a public authority can only legally be undertaken on the basis of a formal statutory authority. This Constitutional safeguard has also legal effect in horizontal relationships. The Dutch Telecommunication Act in its article 18.13, orders communication service providers – as is an ISP – to respect the confidentiality of electronic of communications facilitated by them. Therefore, an ISP is only authorized to monitor the communications of a user of its communication services if agreed upon. Such an agreement usually is part of the General Contract Terms of the service contract.

Based on the European E-commerce Directive (article 12–15), internet providers are not liable for the traffic of data they have not initiated or cannot influence with respect to content. They are not obliged to verify if they host information of a criminal nature or host information in violation of the law, but they are supposed to take action in case they have knowledge of the unlawful character of the information being hosted by them. These principles form the basis of so-called *notice and take down* procedures: as soon as an ISP has knowledge of the presence of illegal content on its server, for example because the police have informed the ISP, it is responsible for the removal of this content.

There is no legal basis for the deployment of internet filters by or on behalf of the Dutch Government in the servers of Dutch providers. The road to take in these cases is to have the information removed and to track down the offenders. Removing and tracking is also the first road to take in case of child pornography that is offered on websites outside The Netherlands. If this appears not to be feasible, for example because the authorities abroad cannot or do not wish to cooperate, consideration may be given to blocking the child pornography for Dutch internetters.[5]

The fundamental right of freedom of speech as well as the right of privacy may be restricted only on the basis of statutory law. The task of the Dutch police is worded in article 2 of the Dutch Police Act 1993: 'The police have the task, subordinate to the competent authority and in accordance with the applicable rules of law, of upholding the rule of law and rendering assistance to those who need it.' 'Upholding the rule of law' includes law enforcement (fighting crime) as well as the maintenance of public order. Another aspect of police work is the performance of policing tasks for the justice authorities (BZK, 2004). The Act provides for some specific powers concerning use of weapons, frisking, arrest, etc but no power under which a preventive measure as filtering could be subsumed. The wordings of article 2 are too general to serve as a legal authorisation to interfere with the given fundamental rights, as has been confirmed by case law.

A next question is whether preventive measures like filtering could be based upon powers in Dutch penal legislation? Two articles can be linked with filtering and blocking information: article 125o Code of Criminal Procedure (CCP) and article 54a Penal Code (PC).

In case of (among other things) *délit fragrant* or suspicion of a crime to which a prison sentence of four years or more applies, the police are authorized to search a data storage location where data have been stored or recorded on a data carrier (articles 67, 96b and 125i CCP). Article 125o CCP subsequently determines that:

> *'If after searching of an automated work data are encountered in relation to which or with the help of which the legal offence has been committed, the public prosecutor or, in the course of the preliminary investigation the examining judge, can determine that these data are made inaccessible insofar as this is deemed necessary for the termination of the penal offence or to prevent new penal offences.'*

This condition authorizes the police to make child pornographic pictures that have been found on a computer inaccessible, which can be effectuated by blocking access to that material. Direct application of the power to an ISP who is hosting child pornography would only be possible if the ISP itself is the suspect of a crime, which could be the case, e.g. when the ISP would fail to take down the website after being notified. Moreover, the power of article 126°CCP is not applicable to the blocking data flows.

The Dutch Penal Code, first book, article V, deals with liability of editors for criminal content. Article 53 PC determines that a publisher will not be prosecuted for 'crimes committed by means of a printing press', in case the perpetrator is known or, after certain preconditions during the criminal investigations have been met, is made known by the publisher. Article 54a says:

[5] This line of policy was confirmed again by the Minister of Justice, after our visit. See *House of Commons Publications* 2007–2008, 28684 and 31200 VI, nr. 166, page 4.

> *'an intermediate person who renders a telecommunications service consisting of the passing on or storage of data originating from someone else, will not be prosecuted as such if he carries out the order of the public prosecutor, after written leave of the court upon claim by the public prosecutor to be rendered by the examining judge, to take all measures that can be expected of him within reason, to make these data inaccessible'.*

As a consequence, an ISP who makes criminal content available to the public – e.g. by hosting a website that contains such content – is indemnified against criminal prosecution, if he takes measures to make these data inaccessible when so ordered by the public prosecutor. Such a measure could be removal or blocking.

The text of article 54a PC raises, however, some questions. The wording of this article implies that the public prosecutor has the legal power to order ISPs to make information inaccessible. But article 54a PC does not refer to an article in the Criminal Procedural Code that provides the public prosecutor with this legal power and that describes the corresponding conditions and safeguards (grounds, time, appeal), as is customary and required by the principles of fair proceedings. An interpretation that 'making inaccessible' could consist of filtering and blocking of internet traffic overstretches the meaning and the scope of the provision.

From the above it is evident that Dutch law enforcement authorities, in particular the police, do not avail over legal powers to filter and to block internet traffic in general, including traffic to and from internet sites that hold child pornographic material.

6. Dutch filtering practice

Prior to the start of Dutch filtering project (beginning of 2007), a copy was obtained of the blacklist composed by the Norwegian police. The list contained some 2500 internet domains. On behalf of the Dutch filtering project the list was reduced to approx. 250: criminal standards concerning child pornography differ between Norway and The Netherlands. Further, it was chosen only to include domains in the list with an outspoken undoubted criminal nature. The filtering itself was organised along the lines of the Norwegian approach. The police entered into agreement with an individual ISP. At the time of our study, an agreement had been arranged with three out of approximately 300 Dutch ISPs: UPC, Kliksafe and Scarlet. The agreement obliges the police to maintain and to supply a blacklist. The ISP takes the obligation to apply the blacklist without change, and run the software that delivers the factual filtering and the blocking on the basis of the blacklist (DNS filtering, see above). The ISP agrees to keep the list confidential. The police will indemnify the ISPs against possible damage claims from customers or third parties. As a consequence the ISP in question is filtering on direct instruction from the police.

To get a better picture of the filtering practice in The Netherlands, we carried out two on-site reviews; the first on 21 February and the second on 14 March, 2008. We asked policemen of the department involved about their working procedures, and we asked them to show the internet sites that had been added to the blacklist, and we gave the contents an assessment. The first time we selected a series of 36 out of the list of 110 sites and the second time we selected a series of 34 out of a list of 103 sites. Both times we selected each third site on the list. A KLPD employee showed us the site, which we subsequently assessed on the basis of a research protocol. Apart from the researchers, detectives of the KLPD and employees of the private Registration Child Pornography on the Internet were present during the first review. The second review was conducted by one of the researchers and a KLPD detective. All selected sites appeared freely accessible. The policemen determined the countries in which the sites were hosted.

The KLPD[6] uses the following procedure and criteria to determine whether the contents of a website might be criminal in the sense of article 240b PC:

- A detective determined whether a picture concerning a sexual act in which a minor ('someone who apparently had not yet reached the age of eighteen years') was involved (in accordance with the text of article 240b);
- If there was no explicit *sexual act*, the character as well as the context of the picture were considered (among other things: unnatural pose, presence of objects with a sexual character). This elaboration on the concept 'sexual act' as mentioned earlier was implemented on instruction by the Attorney Generals College. If the character as well as the contents were considered strongly sexual, the picture was still considered child pornography. In case of doubt, sometimes a second detective would be consulted.

The police had a list of criteria at its disposal for criminal investigation purposes, in order to assess child pornographic material. The list was drawn up by the Attorney Generals College, and is valid as from 1 September 2007.[7] The KLPD detectives did not use this list when assessing child pornographic sites. The KLPD had not laid down procedures concerning the maintenance of the blocking list, nor for any other procedure, and they had no protocols with criteria on the basis of which a specific site was assessed as to whether or not to add it to the blacklist. During the first review the blacklist consisted of 110 sites. Since the start of the filtering project, the list has been more than halved. The criteria upon which this was done remain unknown.

All websites visited by us were freely accessible: the user would not need authorisation to be able to see the content of the website. If the site contained child pornographic material, this was directly present on domain-level; the user did not have to click through to an underlying level in order to obtain access to the punishable content. KLPD detectives indicated that most blocked sites act as central portal, intended to arouse the interest of the users. When the user tries to obtain

[6] As specified by the head of the team Child Pornography Control of the KLPD.

[7] In the list of criteria referred to the pictures are characterized as follows: (1) (pre)pubertal (<14 years) or postpubertal (14–18 years); 2) unfamiliar or familiar material; (3) old, recent or new material; (4) presence investigatable elements in the picture; (5) familiarity with perpetrator and/or victim; (6) check by digital expert; (7)description of material: acts-violence-posing-character-context-age.

access to more pornographic material through clicking on the offered links, in most cases he has to pay in advance. By blocking on domain-level the user can no longer obtain access to the underlying (mostly) commercial sites.

As appears from the data recorded in the list, the police had updated the list for the last time six weeks prior to the review. The blacklist contains sites that no longer exist, that have lost their content or that contain no child pornography (any more).

The blacklist contains sites with child pornography that are hosted in The Netherlands (Table 1). These sites were not reported to the ISPs concerned by the KLPD. No criminal investigation was started to track and prosecute the perpetrators. One foreign site with child pornography is hosted in England; all other sites are hosted in the USA. The Netherlands work closely together with these two countries in the fight against child pornography.[8] So, it is possible in these cases to report them to the law enforcement organisations in these countries, after which the sites would be removed and criminal investigations could be started in these countries. But apparently, this has also not happened.

Table 1 – Content of the blacklist of the Dutch police.

Site	Contains child pornography?	Hosting country	
First on-site review (21st of February 2008)			
Does no longer exist	n.a.	VS	1
		NL	2
		Unknown	1
Site does exist, no content	n.a.	VS	1
Site does exist, content	No child pornography	VS	2
	Child pornography	UK	1
		NL	4
		VS	24
Total			36
Second on-site review (14th of March 2008)			
Does no longer exist	n.a.	NL	1
		Unknown	1
Site does exist, no content	n.a.	–	–
Site does exist, content	No Child pornography	VS	1
	Child Pornography	Belize	1
		France	1
		Russia	1
		Ukraine	1
		Korea	2
		UK	3
		VS	22
Total			34

To our question to the KLPD detectives as to why the blacklist contained many sites from countries that The Netherlands legally cooperated with, and where also cooperation existed within an international police project against child pornography, the answer was that the spreaders of child pornography often changed the server or the provider that hosted their sites. Sites will also be hosted in countries The Netherlands does or cannot cooperate with. To check this information a second review was held, but our findings from the first review were only confirmed. Again, the sites on the blacklist appeared to be hosted mainly by countries that The Netherlands officially cooperates with in fighting child pornography (Table 1). The conclusion can only be that the blacklist seems to function as an alternative for tracking and prosecution.

The policemen of the KLPD feel that the length of time it takes to maintain the blacklist properly is disproportionate given the available staff. One detective said: 'This experiment has gone, also in view of the fuss around it, somewhat out of control. We have entered on a road that seems irreversible and the results of which seem unclear, for now.' The team Child Pornography Control does not consider the maintenance of the blacklist as one of its primary tasks: 'Our first priority is to find the victims and to prosecute the perpetrators.'

The above raises the question as to how the maintenance of a blacklist relates to the so-called core tasks debate (van der Vijver et al., 2001; PVP, 2005). The essence of that debate is the question which tasks the police should definitely perform in view of their legal tasks, which tasks should end and which left to others so as to secure more time for their specific core tasks.

In their so-called core tasks letter of July 15, 2004, ministers responsible for the police indicate that the police should primarily deal with crime fighting and tracing criminals, and not as such with preventive activities. The police should choose a somewhat different role concerning prevention, according to the ministers: 'less executive, signalling more and giving advice where others are responsible'[9] In its coalition agreement, the fourth (current) cabinet Balkenende mentions safety to be a core task of the government. It is translated directly into crime fighting, of which the prevention of criminal behaviour is a part. According to the coalition agreement, crime prevention is part of safety policy. But this should not lead to a new burden for police and the justice department: 'The performance of police and public prosecution is strengthened; new technology will be used optimally to improve the clearance rate [an investigation target – our addition]. Bottlenecks will be removed and there will be no new barriers, procedures of limitations.'[10]

From the policy principles mentioned above, the maintenance of a blacklist cannot be considered as a police task. Instead, investigation to the perpetrators should have priority.

7. Connecting the different perspectives

The confidentiality of Internet traffic is protected by article 8 of the European Convention on Human Rights and Fundamental Freedoms (ECHR) and the corresponding provisions of

[8] Countries mentioned participate in the CIRCAMP project (Cospol Internet Related Child Abusive Material Project – where Cospol stands for Comprehensive Operational Strategic Planning for the Police).

[9] House of Commons Publications, 2003–2004, 29628, nr.4, pages. 6–7.

[10] Coalition agreement between Lower Chamber Fractions of CDA, PvdA and ChristenUnie, 2007. (*Coalitieakkoord tussen de Tweede Kamerfracties van CDA, PvdA en ChristenUnie.* 2007).

the Dutch Constitution (Article 13). Therefore, infringement of this fundamental right by filtering and blocking information requires an explicit legal basis. Today, such a basis is lacking in The Netherlands. Filtering and blocking of internet traffic without permission of the persons concerned cannot be undertaken by the police or other government body. Under Dutch Administrative Law the principle has been developed that the Government may conclude civil agreements with non-governmental bodies for the purpose of public tasks. However, government or a government body may not use civil agreements to circumvent or avoid limitations of administrative law. In other words, government may not use a civil agreement to realise certain aims where government has no authority to realise such aim.[11] The sanction provided for is that such an agreement is void. Above it was discussed that the law does not provide the police with an authority to filter and to block internet information. A contract that instructs ISP's – on behalf of the police – to filter, etc. lacks therefore legal validity.

It remains to be seen whether filtering and blocking would be legally possible even if a specific power was enacted. Under the Dutch Legal System application of a coercive power should meet requirements of subsidiarity and proportionality (Michiels et al., 1997; Muller et al., 2007). Subsidiarity means that an instrument can only be implemented if the aimed goal could not be achieved with less invasive measures. Proportionality means that a measure should be in reasonable proportion to the problem, and it cannot be used more often than necessary. In the definition of a legal power to filter and to block, a careful choice should be made of the instrument to be used accompanied by a permanent assessment whether the measure (still) meets its goals. As demonstrated above, the applied filtering technique (DNS-filter) filters on domain-level and therefore is rather inaccurate. Structural overblocking is inevitable, because every internet domain with child pornography also contains, and sometimes probably mainly contains, information that does not fall under article 240b PC. Furthermore, because the continuous change of the internet information flow, the use of an imprecise filter would bring a need to check frequently whether a domain is still justifiably blocked. In addition, the assumption may be that the filtering contributes to the fighting of child pornography: to what extent and in what way it solves the problem is unknown, and so it is unclear what the instrument means when it refers to 'fighting of the problem'. This makes it difficult, if not impossible to judge whether the inherent structural overblocking of the filter is or will be still in accordance with proportionality requirement.

A legitimate question therefore is whether a more precise filtering technique would be available that reduces overblocking to an absolute minimum. In Great Britain, British Telecom uses a technique we referred to as two-step proxy filter on ISP-level, for blocking separate files (2-c-iii). It is a more complex and therefore more expensive system than the Dutch one, but it blocks more precisely. But it is also more laborious. Precise blocking requires extra accuracy in composition and maintenance of the blacklist, which should in that case be based mainly on URLs instead of domain names.[12]

Anyway, the careful maintenance of a blacklist would require a substantial editorial effort. Police priorities should lie with tracking perpetrators and identifying victims. Performance of special efforts for the composition and maintenance of an internet filter will absorb investigative capacity and, therefore is not in line with police policy. Where another government body takes care of the maintenance of the blacklist, the tension or conflict with fundamental rights continues to exist, because of the structural overblocking that is inextricably bound up with filtering.

Private bodies in this respect have more room for manoeuvre. A private body could act as editor of the blacklist. This body could agree with ISP's to apply the list and filter software, provided that the ISP has obtained the consent of the subscribers. This can be easily achieved by (amendment to) the General Terms. This scheme is applied in Great Britain: the blacklist's editor is the private institution the Internet Watch Foundation, ISPs filter on the basis of that list. And they do that with a two-step proxy filter, as mentioned before. Employers can also filter the internet on the basis of a blacklist maintained by a private institution.

Other measures are possible: in Norway, employers and supervisors are even legally obliged to prevent employees from breaking the child pornography laws. In Sweden, the government has set an example by placing an URL-filter in their own computers against, among other things, child pornography.

8. Evaluation of the Dutch filtering policy

As a reaction to questions in Parliament, the Dutch government (police) has taken the initiative to filter the internet. Taking policy measures could be subjected to quality requirements. Already in the 1930s, Shewhart developed the Plan-Do-Check-Act (PDCA) circle (Shewhart, 1939). The PDCA-circle was adopted by Deming in the 1950s, who later made it the Plan-Do-Study-Act (PDSA) (Deming, 1993). In the first phase of this model (plan) the targets should be defined; in the second phase (do) the policy is executed. During the third phase (study) the results should be studied and in the fourth phase the actions are set out on the basis of the findings, in order to improve the results. Various policy techniques have been developed that use the principles form the PDSA-model (e.g. Mazmanian and Sabatier, 1980; Geul, 2005; Hoppe et al., 2004; Hoogerwerf, 2008). According to Hoogerwerf policy recognises eight sub processes:

1. Listing: the process which gives social problems the attention of the public and of policy makers.

[11] Supreme Court, January 26, 1990, NJ 1991, 393, AB 1990, 408.

[12] It is conceivable that the BT-filter will sometimes also block on domain-level, but we do not know for sure because the exact operation of the filter was not released.

2. Policy preparation: collection and analysis scientifically obtained information and defining advice with the view of the policy to be executed.
3. Policy determination: taking decisions about the content of policy. Mainly choosing and specifying the targets, the means and the times are included.
4. Policy implementation and execution: applying the chosen means for the chosen targets.
5. Observance of the policy and policy maintenance: taking care that the behavioural norms that are set are actually observed.
6. Policy evaluation: examining the contents, the process, and the effects of a policy for certain criteria.
7. Feedback: processing the findings of the evaluation with regard to content, the process and/or the effects of the policy, and on that basis re-determination of the policy or policy process
8. Policy termination: terminating executed policy. With the feedback the policy process can start again, unless the policy is terminated.

The policy concerning filtering and blocking of websites with child pornographic material studied by us, has proven to be of insufficient quality on a number of points, according to the research presented here. There seems to be hardly any policy preparation. For example, prior to the measure, no research was performed into the legal and technical possibilities. With regard to the policy determination, we can remark that no concrete measurable targets were defined, and with regard to the policy maintenance we can remark that the police have maintained the blacklist rather superficially, and included mainly sites from countries The Netherlands has a close cooperation with – which made the blacklist an alternative for tracking, which was explicitly not the Minister's intent.

The essence of policy evaluation is assessing effects. This study has paid attention to that. This study also contains parts that, according to the phases of Hoogerwerf, should have been performed prior to the policy implementation, such as the legal and technical analysis, an analysis of police policy and an inventory of experiences from abroad. The outcomes have led to changes in the policy, or if you like, a partial policy termination.

The reaction of the Minister of Justice to this research report was 'what does not change [is] the starting point that children should be protected from this horrible form of abuse.'[13] In order to reach that, criminal investigation remains crucial in the view of the Minister. The thing that also does not change is: 'stimulating international cooperation in this field'. In addition 'the access to websites with child pornographic material should be blocked'. What does change is 'the role of the police in this. The task taken up by the KLPD, maintaining a blacklist will be terminated, after the activities have been performed by the ISPs.' The most important policy change is that the government no longer blocks websites itself.

The minister also states that:

> *'Every serious attempt to stop the spread of child pornography in the internet [will] have to be internationally coordinated. In connection with Europol and Interpol [...], the Dutch police will ask attention for countries that do not take sufficient action against child pornography. The Netherlands will invite the European Union to increase political pressure on countries outside the Union where many sites are hosted. The purpose of the pressure is to see to it that these countries will act to uphold the law.'*[14]

The minister does not mention countries by name, but says: 'countries with which cooperation is not possible'. The suspicion is that he is referring to countries that are also named by our respondents in this respect, i.e. countries that are not taking a tough enough stance against child pornography and with which cooperation in a legal context is difficult or impossible, such as White Russia and Ukraine. If, however, we consider the sites the Dutch police have put on the blacklist as an indication of where the problems mainly occur, the Minister should not only focus the political pressure on those two countries, but mainly on the USA. But before any political pressure is executed against any country, more in-depth knowledge of the problem seems necessary.

The question that perhaps pushes itself forward the most from the above is why the government, contrary to policy insights, takes measures without serious prior analysis. The fact that this concerns a technological measure probably plays an important role. Quite frequently, managers have little knowledge of the limitations of technological solutions, which pitches their expectations too high. (Frissen, 1989; Stol, 1995; Oey, 2001). A publication of the Expertise Centre for Maintenance Law and Order of the Ministry of Justice speaks of 'naive optimism' in this respect. (Stol, 2004a:23). The critical analysis of a control measure of an emotionally charged subject like child pornography can also lead the critic to be reproached that he has not wanted to do everything possible against child pornography – and so be grouped in the 'wrong camp'. Politicians cannot afford this just like that. In relation to the technical policy measure of camera surveillance, van Gestel (2006:49) – researcher for the scientific bureau of the Dutch Ministry of Justice – was struck by an irrational preference for more cameras. 'The policy process in this case does not seem to start with a signalled problem, but seems to start with the desires of the government with regard to specific policy'. Then Van Gestel refers to Kingdom (2003) who states that a policy agenda is created in a force field of problems, solutions and political events. Policy can find its origin in any of these three. In a society where child pornography is judged with abhorrence, in which safety is rated higher than 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.

In this context, the Dutch minister of Justice primarily gave his support to internet filtering by the police. Contrary to the mayor in the case of Van Gestel (who expanded his measure despite unclear results), the minister has transformed his

[13] *House of Commons Publications* 2007–2008, 28684 and 31200 VI, no. 166.

[14] *House of Commons Publications* 2007–2008, 28684 and 31200 VI, no. 166, page 4.

policy on the basis of an evaluation which, among other things, imposes targets upon the policy measure.

9. The Dutch case: international relevance

In the above we have discussed the Dutch case in filtering the internet. Although this paper refers to the situation and policy in The Netherlands it includes a number of elements and issues that are relevant for other European Member States as well. We might expect a further spread of filtering practices in the EU. The European Commission is presently working on a proposal to update Framework Decision 2004/68 on child exploitation, etc., due for March/April 2009. The issue of blocking websites may be part of this proposal. The issue is controversial. Some member states have strong objections, while some already are filtering the internet (e.g. Sweden, Denmark, Italy, The Netherlands) and for example Belgium is about to introduce a compulsory blocking system based on a blacklist, and similar plans are discussed in Germany and possibly in France.[15] At this point it should be noted that the actual exchange of views is not restricted to the filtering of child pornography, it also has to do with the filtering of, for example, sites with content related to hate/racism, fraud, bestiality, and woman trafficking (Stol et al., 2008; Webwereld, 12-01-2009). For all Western states that are involved in the debate about filtering the internet, the following findings of our study are relevant to at least some degree:

- The introduction of a filtering system in the European countries in our study (Norway, Sweden and The Netherlands) was not preceded by any independent research into the legal, technical and practical possibilities – as a result of which the discussion includes suspect arguments, such as 'filtering is effective because the filter produces so many hits' – recently used again by the German Minister of Family Affairs, Ursula von der Leyen (Der Spiegel Online, 15-01- 2009).
- Internet filters have clear technical limitations, as a result of which they always cause a certain amount of *structural* overblocking (structural blocking of legal information, that is).
- The European Convention on Human Rights and Fundamental Freedoms (ECHR) guarantee the confidentiality of information flows. On top of that national constitutions of Western states tend to include basic laws such as with respect to freedom of speech, privacy and the freedom of information gathering. That means that filtering the internet by or in name of the government demands a specific legal basis. We studied the introduction of governmental filtering systems in Norway, Sweden and The Netherlands, and in none of these countries we have observed that the government provided the filtering system with such tools. We carried out an in-depth investigation into the legal context in The Netherlands and we came to the conclusion that the Dutch filtering practice was unlawful. We did not find similar in-depth studies with respect to other countries.
- Managers and politicians have little knowledge of technological solutions, which pitches their expectations too high and prevents them from being critical towards technology. Recently the German Minister of Family Affairs, Ursula von der Leyen, demonstrated this by claiming that the filtering of child pornographic material is not a matter of censorship because it is clear ('klar abgrenzbar') what should be labelled child pornographic material and what not (Der Spiegel Online, 15-01-2009). No word about the problem of structural overblocking was mentioned.

We hope that this article provides European countries with adequate information and arguments for a Europe-wide and informed discussion on governmental filtering of the internet and the blocking of websites.

W.Ph. Stol (*w.ph.stol@ecma.nhl.nl*) **J. Kerstens, & E.R. Leukfeldt,** *NHL-University of Applied Sciences Leeuwarden, Chair Cybersafety.* **H.K.W. Kaspersen** (*H.W.K.Kaspersen@rechten.vu.nl*) & **A.R. Lodder,** *Free University Amsterdam, Computer Law Institute; All the authors are members of the Cybersafety Research and Education Network (CyREN; www.cybersafety.nl)*

REFERENCES

BZK (Ministry of the Interior and Kingdom Relations). Policing in the Netherlands. Den Haag: BZK; 2004.

Clayton R. Failures in a Hybrid Content Blocking System. Cambridge: Cambridge MIT Institute (CMI); 2005.

Deibert RJ, Palfrey JG, Rohozinski R, Zittrain J. Access Denied; the Practice and Policy of Global Internet Filtering. Cambridge, Mass: The Mitt Press; 2008.

Deming WE. The New Economics: for Industry, Government and Education. Cambridge: Mass MIT Press; 1993.

Deshmukh A, Rajagopalan B. Performance analysis of filtering software using Signal Detection Theory. Decision Support Systems 2005;42:1015–28.

Edelman B. Web Sites Sharing IP Addresses: Prevalence and Significance. Harvard Law School: Berkman Center for Internet and Society; 2003.

Fleck MM, Forsyth DA, Bregler C. Finding naked people. In: fourth European Conf. on Computer Vision 1996;2:592–602.

Frissen PHA. Bureaucratische cultuur en informatisering. Den Haag: Sdu-Uitgeverij; 1989.

Geul A. Beleidsconstructie, coproductie en communicatie. Zes beproefde methodieken van beleidsontwikkeling. Den Haag: Boom Juridische Uitgevers; 2005.

Greenfield P, Rickwood R, Tran H. Effectiveness of Internet filtering software products. CSIRO Mathematical and Information Sciences; 2001.

Haselton B. Report on accuracy rate of FortiGuard Filter. Bellevue, WA: Peacefire.org; 2007.

Hoogerwerf A. Beleid, processen en effecten. In: Hoogerwerf A, Herweijer M, editors. Overheidsbeleid. Een inleiding in de beleidswetenschap. Alphen aan den Rijn: Kluwer; 2008.

[15] Personal information. See also online journals Webwereld, 12-01-2009 (http://webwereld.nl/articles/54321/belgen-willen-kinderpornosites-blokkeren.html) about Belgium and Nu.nl, 16-01-2009 (http://www.nu.nl/internet/1900725/ook-duitsers-krijgen-kinderpornofilter.html) and Det Spiegel Online 15-01-2009 (http://www.spiegel.de/netzwelt/web/0,1518,601440,00.html), about Germany. (All sites most recently checked at 09-03-2009).

Hoppe R, Jeliazkova M, van de Graaf H, Grin J. Beleidsnota's die (door)werken. Handleiding voor geslaagde beleidsvoorbereiding. Bussum: Coutinho; 2004.

Jones MJ, Rehg JM. Statistical color models with application to skin detection. Technical Report Series. Cambridge Research Laboratory; 1998.

Kingdom, J.W. (2003) Agendas, Alternatives and Public Policies. New York: Longman.

Kranich N. Why filters won't protect children or adults. Library Administartion and Management 2004;18(1):14–8.

Mazmanian DA, . Sabatier PA. A multivariate model of public policy-making. American Journal of Political Science 1980;24: 439–68.

Michiels FCMA, Naeyé J, Blomberg AB, Boek JLM. Artikelsgewijs commentaar Politiewet 1993. Den Haag; 1997.

Muller ER, Dubelaar MJ, Cleiren CPM. Algemene beginselen van behoorlijke politiezorg. In: Fijnaut CJCF, Muller ER, Rosenthal U, van der Torre EJ, editors. Politie, studies over haar werking en organisatie. Deventer: Kluwer; 2007. pp. 559–99.

Oey H. Criminaliteitspreventie: kansen zien, kansen benutten. Den Haag: Senter; 2001.

ONI (OpenNet Initiative). Internet Filtering in Saudi Arabia in 2004; 2004.

ONI (OpenNet Initiative). Internet filtering in Iran in 2004–2005; 2005a.

ONI (OpenNet Initiative). Internet filtering in China in 2004–2005; 2005b.

PVP (Projectgroep Visie op de Politiefunctie). Politie in Ontwikkeling. Den Haag: NPI; 2005.

Resnick P, Hansen D, Richardson C. Calculating error rates for filtering software. Communications of the ACM 2004;47(9):67–71.

Richardson C, Resnick P, Hansen D, Derry A. Does pornography blocking software block access to health information on the Internet? Journal of American Medical Association 2002;22: 2887–94.

Shewhart WA. Statistical method from the viewpoint of quality control. New York: Dover; 1939.

Shih JL, Lee CH, Yang CS. An adult image identification system employing image retrieval technique. Pattern Recognition Letters 2007;28(16):2367–74.

Stark Ph.B. Expert report of Philip B. Stark Ph.D. Civil Action no. 98-5591 (E.D. Pa) ACLU vs. Gonzales; 8 May 2006.

Stol WPh. Handhaven: eerst kiezen dan doen: technische mogelijkheden en beperkingen. Den Haag: Ministerie van Justitie; 2004a.

Stol WPh. Trends in cybercrime. Justitiële Verkenningen. 2004b; 30(8):76–94.

Stol WPh. Zin en onzin van politieautomatisering. In: Hilarides D, editor. Handboek Politiemanagement. Alphen aan den Rijn: Samsom H.D. Tjeenk Willink; 1995. sectie C4130, pp. 1–24.

Stol WPh, Kaspersen HKW, Kerstens J, Leukfeldt ER, Lodder AR. Filteren van kinderporno op internet. [(Filtering Child Pronography on the Internet)]. Den Haag: BJU; 2008.

van Gestel B. Lokale media en politiek over cameratoezicht: een case studie. Tijdschrift voor Veiligheid 2006;5(4):34–52.

van der Vijver CD, Meershoek AJ, Slobbe, DF. Kerntaken van de politie. Zeist: Kerckebosch; 2001.

Wang JZ, Li J, Wiederhold G, Firschein O. System for screening objectionable images. Computer Communication 1998;21: 1355–60.

Yang J, Fu Z, Tan T, Hu W. A novel approach to detecting adult images. In: 17th International Conference on pattern recognition; 2004;4:479–82.

Yoo SJ. Intelligent multimedia information retrieval for identifying and rating adult images. KES 2004:164–70.

Zeng Wei, Gao Wen, Zhang, Tao, Liu, Yang. Image Guarder: an intelligent detector for adult. In: Asian Conf. on Computer Vision; 2004. p. 198–203.

Zittrain J, Edelman B. Documentation of internet filtering in Saudi Arabia. Harvard Law School: Berkman Center for Internet and Society; 2002.