# Notice and Take Down

*Towards a central system in the Netherlands*

By: Carlijn Dohmen

Supervisors: Mr. A.P.C. Roosendaal

Dr. Mr. C.M.C.K. Cuijpers

Master Thesis 2008 for the master Law and Technology

Tilburg University

Faculty of Law

Department TILT

# 1. Introduction

The liability of Internet Service Providers is a well-known topic in the world of law and ICT. When should an ISP be held liable for actions of their clients? Do ISPs have any responsibility at all or is it impossible for them to monitor content on their servers in any way? In Europe the E-Commerce Directive was introduced in 2000, in 2004 it was implemented into Dutch law.[1] This directive contains a small number of articles offering a guideline on how to handle ISP liability.[2] In the articles a notice and take down procedure is implicitly given. Whenever an ISP receives a complaint –a **notice**- about illegal or unlawful content, the ISP has to decide whether the information is indeed illegal or unlawful and if so, it should remove the website from its server or block access to it –**take down**-. During the same period the directive was implemented in the Netherlands, voices were raised to develop a Notice and Take Down system,[3] which was supposed to be up and running in January 2006.[4] However, two and a half years later, the system is still not working. This has attracted my attention and I decided that I wanted to know more about this subject. Why is this system not working yet? What are its flaws and are there ways to make this system operational?

This leads to the main question of this research: *How can we achieve a sufficient Notice and Take Down system in the Netherlands?* In order to answer this question I will first give an oversight of how ISP liability in the Netherlands is regulated at this moment in section 2. In this section I will also explain the applicable articles in the E-Commerce Directive and I will discuss some Dutch cases which have been of importance to this subject. In section 3 I will address the current status of a Notice and Take Down system in the Netherlands. Why I believe such a system is desirable in the first place I will explain in section 4. In section 5 I will take a comparative approach and see how NTD is regulated in the United States and the United Kingdom. The reason I have chosen these two countries is that they both use a Notice and Take Down procedure, but in different fields and different ways. In Section 6 I will present my view on how a NTD system should be set up in the Netherlands. I will briefly discuss some opinions by authors who have written about this subject and I will give a short repetition of the NTD procedures in the United States and the United Kingdom. I will also take a quick look at the NTD-procedure Dutch provider XS4ALL uses, I have chosen XS4ALL

[1] *Stb.* 2004, 285
[2] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain Legal aspects of information society services, in particular electronic commerce in the Internal Market, O.J. 2000, L178
[3] Kamerstukken II 2003/04, 28 197, nr. 15
[4] Kamerstukken II 2004/05, 28 197, nr. 22

because they are well-known in different cases concerning ISP liability and because their procedure for complaints has become the standard model for Dutch ISPs.[5] In this section I will also sum up the conditions I believe are crucial for a sufficiently working system, what subjects should fall under the scope of a Centre for Notice and Take Down, who should be involved and I will give an overall picture of how I think a Dutch Centre for Notice and Take Down could become reality; The Dutch Centre for Notice and Take Down will be presented. Finally in section 7 I will come to a conclusion, where I will sum up the most important findings and give an answer to the research question.

# 2. The current status of Internet Service Provider Liability in the Netherlands

Before getting to an explanation of how the Dutch Notice and Take Down system was designed, it is useful to first have a look at the legal framework regarding ISP liability in the Netherlands. Once the legal framework is explained, the reasons why a central system is desirable will be more evidently. Directive 2000/31/EC (E-Commerce Directive) addresses the issue of ISP liability in four articles.[6] Also, a number of Dutch court decisions were given on different aspects of liability for ISPs. I will first address the articles of the E-commerce Directive. Next, I will illustrate some Dutch cases in section 1.2 and in section 1.3 I will explain why this legal framework, in my opinion, is not enough.

## 2.1 The E-Commerce Directive

The E-Commerce Directive was designed to harmonize European rules on electronic commerce. Four of its articles, art. 12 through 15 are specifically directed to Internet Service Providers and their liability. The directive makes a distinction in three different roles for the ISPs and connects different levels of liability to these roles. The first three articles that will be explained have been implemented into article 6:196c *Burgerlijk Wetboek* (Dutch Civil code, hereafter referred to as BW) in 2004.[7]

The first article, article 12, is for the ISP that is involved in so-called 'mere conduit'. Member States shall not hold an ISP liable on the condition that it gives access to information of which the ISP has not initiated the transmission, has not selected the receiver of the transmission and has not selected or modified the information contained in the transmission.

[5] *Infra* note 61 at p. 167.
[6] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain Legal aspects of information society services, in particular electronic commerce in the Internal Market, O.J. 2000, L178
[7] Wetsvoorstel Aanpassingswet Richtlijn Inzake Elektronische Handel, Kamerstukken II 2002/03, 28 197, nr. 1, p. 4

Automatic, transient and intermediate storage of information is also included as long as its sole purpose is to carry out the transmission and provided that the information is not stored longer than reasonably necessary. In this and the next articles it is mentioned that these "*shall not affect the possibility for a court or administrative authority, in accordance with Member States' legal systems, of requiring the service provider to terminate or prevent an infringement*". This even though an ISP has removed or blocked certain information, or when they did not and were not supposed to know that the information was illegal or unlawful, a court or administrative authority can still require an ISP to stop or prevent an infringement.

The second article on ISP liability, article 13, addresses ISPs in case of 'caching'. Member States shall not hold an ISP liable for automatic, intermediate and temporary storage of information, performed for the sole purpose of making the onward transmission of the information more efficient on the condition that: a) the provider does not modify the information, b) it complies with conditions on access to the information, c) it complies with rules regarding the updating of information, d) the provider does not interfere with the lawful use of technology to obtain data on the use of the information and e) the provider acts expeditiously to remove or disable access to the information once it obtains actual knowledge that the information has been removed from the network at its initial source, access to it has been disabled or that a court or administrative authority has ordered such removal or disablement. Like in article 12, the ISPs face only a very 'mild' form of liability. As long as the ISP has not influenced the information in the ways mentioned and acts immediately once they find out information should be removed, they will not be held liable for the content.

Article 14 of the directive is the third article to mention ISP liability, addressing the ISP in the role of 'hosting' provider. If a provider stores information provided by the recipient of the service it shall not be held liable by the Member States on certain conditions. These conditions are that the ISP did not have actual knowledge of the illegal activity or information and is not aware of facts or circumstances from which the illegal activity or information is apparent. Or, once it has obtained knowledge about above mentioned activities or information immediately removes or disables the access to the information. According to the second paragraph of the article, the ISP will be held liable if the recipient of the service was acting under the authority and control of the ISP. In this case a more stringent liability is applied. However, as long as the ISP removes illegal content as soon as it has noticed the information and the information was not put online under the authority of the provider, it will not be held liable.

Article 15, the last to address ISP liability, prescribes that Member States cannot oblige ISPs to monitor information which they transmit or store, nor can they be obliged to actively seek facts or circumstances indicating illegal activity. In section 6.3, where the possibility of techno-regulation will be discussed, I will examine whether in the future this last provision could be removed or adjusted. Article 15 also states that Member States are allowed to establish obligations for ISPs to inform the competent public authorities once they have knowledge of illegal activities or information and they can be obliged to communicate to the competent authorities about information enabling the identification of recipients of their service with whom they have storage agreements. In some of the case law dealt with in the next section, the obligation to provide national authorities with identifying information is expanded to other parties as well.

On first sight, these articles merely describe how the liability of ISPs should be regulated. But, when having a closer look, one can clearly distinguish the basis of a NTD-procedure. Articles 13 (1 b) requires the ISP to remove or disable access to information as soon as they find out that the information has been removed from the network of the initial source of transmission, access has been disabled or a court or administrative authority has ordered removal or disablement. In 14 (1 b) the ISP has the duty to remove or disable access to information expeditiously once it has obtained knowledge of illegal or unlawful activity or content. Because according to article 15, ISPs do not have an obligation to monitor. Hence, they will usually be notified by a third party about the allegedly illegal or unlawful information. ISPs have to check whether the notification is correct and if so, remove the information from their servers. Thus, a notice and take down procedure comes into existence.

## 2.2 Case law

Before going deeper into Dutch case law that relates to ISP liability, it is important to point out that these cases stress different aspects of ISP liability. In some cases, the ISPs were only obligated to enclose certain data of their users to a third party, in others the ISP itself was held liable for not removing unlawful content.

### *2.2.1 Lycos/Pessers*[8]

Pessers was a well-known seller of stamps on eBay with a high number of positive feedbacks. Despite his reputation, one of his buyers was not satisfied at all and decided to design a website on which he told about how he said he was deceived by Pessers and asked for others

[8] HR 25 November 2005, LJN AU4019 (Lycos/Pessers)

whose transactions also went wrong to respond by e-mailing their story. The website was hosted by the Dutch provider Lycos. Pessers has first tried to contact the maker of the website, asking him to reveal his identity and take the website offline. When no response came, Pessers contacted Lycos and asked for the name and address of the person who made the website containing alleged defamation towards Pessers. Lycos refused to do so, which led to Pessers applying for a court ruling against Lycos in order to retrieve the name and address of the wrongdoer so he could get his damages recovered.

Lycos claimed that it was not evidently made clear that the content of the website, which in meantime was deleted by its creator, was in fact unlawful and that they therefore did not have to provide Pessers with the name and address of the alleged wrongdoer. The *Hoge Raad* (Dutch Supreme Court) disagreed with Lycos, stating that in some cases, there is no other way of retrieving a person's name and address. Thus a particular group of victims would never be able to go to court and file a lawsuit. Lycos should have given the name and address to Pessers because he had no other way of retrieving that information, in court would be decided whether the information was in fact unlawful.

Lycos also claimed that they themselves had to be liable for the unlawful act itself, in order to be obligated to provide the name and address of their client. Again, the court disagrees, arguing that refusing to provide the name and address can be an unlawful act itself because it goes against the duty to care in social behavior. This means that each situation has to be taken into consideration separately and that there is no general rule.[9]

Furthermore, Lycos brings forward that there is a discrepancy because they did not have to remove the website, but they do have to give out the name and address of the creator of the website, which is a breach of privacy towards Lycos' client. This argument does not hold, since the court said that in different circumstances different interests prevail. The last argument by Lycos I will discuss is that of the right to freedom of expression. Anonymity should also be protected by this right. Although the court acknowledges that the freedom of expression is important, it is not an absolute right. The court decided that Lycos should reveal the name and address of the person who was behind the defamatory website. A painful detail is that the data turned out to be false, thus Pessers was still unable to trace the person who created the website and was unable to recover his damages.

[9] Roosendaal 2006, p. 219

### *2.2.2 Teleatlas*[10]

Another Dutch case is that of Teleatlas, a company offering navigational software, wanted to take judicial steps against Internet users who are selling illegal copies of Teleatlas-software on auction websites such as eBay. Teleatlas demands the names and addresses of these persons of the Dutch ISP Planet Internet, who is supplying them with e-mail addresses. Planet Internet defends itself by saying that a. they would be acting unlawfully against their clients if they would provide Teleatlas with their names and addresses and b. that Teleatlas does not have a legitimate ground in demanding these data from Planter Internet, because they have not tried other ways first.

The court agrees with Planet Internet, stating that the question whether there is a justification for demanding the name and address of someone should be answered in light of article 8 *Wet bescherming persoonsgegevens* (Dutch Personal Data Protection Act; hereafter referred to as Wbp). Part f of this article emphasizes that processing of personal data is only allowed when it is strictly necessary to concede to the interests of the responsible person for this data or a third party and when the interests of the person whose data is being processed do not prevail. In order to decide on whose interest should prevail, one should also look if there were other ways to retrieve the person's data. In this case, Teleatlas could have contacted the website through which the illegal copies were sold and did not have to go straight to the provider of the e-mail addresses. Hence, Planet Internet was not obligated to disclose the personal data of its clients. Continuing on this subject, the court has decided in the Ruthlo vs. Concept ICT case that there is no general rule that obliges ISPs to disclose the name and address of its clients once unlawful content has been found. In some cases deleting the content of the webpage is enough.[11]

### *2.2.3 Deutsche Bahn/XS4ALL*[12]

In contrast to the cases above, the information on the website hosted by the ISP was clearly illegal and therefore the ISP faced stricter liability. In this case German activists had made a webpage containing detailed information on how to sabotage the German railways owned by Deutsche Bahn, this webpage was hosted on a Dutch server from Internet Service Provider XS4ALL. By letter Deutsche Bahn asked XS4ALL to delete the webpage and disclose the name and address of the creators of the website. XS4ALL denies that the content of the webpage is unlawful and refuses both requests. They mention that they receive many notices of unlawful

[10] Vzr. Rb. Utrecht 9 July 2002, *LJN* AE5537 (*Teleatlas*)
[11] Hof Den Bosch 25 July 2002, *KG* 2002, 259 (*Rutloh/Concept ICT*)
[12] Rb Amsterdam 25 April 2002, *LJN* AE1935, Hof Amsterdam 7 november 2002, *LJN* AF0091 (*Deutsche Bahn/XS4ALL*)

content on webpages hosted by them on a daily basis, and that they cannot check each complaint individually. The court decides that the content of the website was clearly unlawful and that XS4ALL should have immediately deleted the website after having received and investigated the complaint from Deutsche Bahn. The court acknowledges that XS4ALL should handle personal data of its clients cautiously, but because in this case it is obvious that the behavior of the client is unlawful, they have to disclose the data of the creator. The fact that the creators of the website are likely to publish the harmful information through another host contributes to the duty of the ISP to provide Deutsche Bahn with the demanded information.

### *2.2.4 Scientology/XS4ALL*[13]

This next case is about three questions; whether merely a link to copyright infringing information is a copyright infringement itself, whether an ISP is acting unlawful if it does not remove the link after having received a complaint and if an ISP can be held liable if it refuses to reveal the name and address of its client who is the alleged wrongdoer.

Scientology has accused XS4ALL of infringing the copyrights on a text that was written by Scientology founder Hubbard. What XS4ALL did, was to host a website which contained a link to another webpage where the text was put online and after having received a notice of Scientology that there was no permission to publish the text they did not take the webpage with the link offline. Scientology claims that having a link online to a webpage with unlawful content is also copyright infringement, because through the link third parties are able to access a copy of the text.

The court rules that ISPs are not publishing information themselves, they are merely providing the means for others to publish and therefore they are not infringing any copyrights. Nevertheless the court does say that an ISP has the duty to take the necessary steps when their client has put information online that is illegal. The court also states that, once an ISP has received a notice of illegal content on a webpage and the content is illegal beyond reasonable doubt, the ISP itself is behaving unlawful if it does not immediately remove the illegal content. Finally, the court also rules that an ISP can be obliged to provide a third party with the name and address of its clients. Koelman points out that the court could also consider that the refusal of disclosing these data can be unlawful.[14] This case shows that the Dutch court handles stricter rules than the E-Commerce Directive, in which enclosing the

[13] Rb. 's-Gravenhage 9 June 1999, *LJN* AA1039, Hof s'-Gravenhage 4 september 2003, *LJN* AI5638 (*Scientology/XS4all*)
[14] Koelman 1999

name and address of a client is not a condition to avoid liability. In the end, there was in fact no infringement of copyrights because the documents had been made public in a library in the United States.

### *2.2.5 IS InterNed Services*[15]

The most recent case that touches upon the topic of ISP Liability is that of an asylum seeker X who was denied a Dutch passport. Together with his partner he ran a used car company called A-Group. The Dutch Tax Authority imposed a high tax assessment and because they feared that X was about to leave the country without paying the assessment they had seized goods and money from A-Group and X. X accused the Dutch Tax authority and the involved tax inspector of basing this assessment and seizure of goods on racist motives and made a webpage, hosted by IS InterNed Services, accusing the involved parties of threats and racism. The Dutch State Secretary of Finance notified IS InterNed Services of this webpage, claiming that it was defamatory to the Dutch Tax Authority and the inspector who was involved. The ISP was asked to immediately remove the information, on which it responded with the message that they would investigate the complaint, but that they would not instantly remove the information. The State goes to court demanding that the ISP and/ or A-Group remove all defamatory content within 24 hours. The ground for this demand is that the accusations lack any factual basis and because there is no legal justification, the accusations are unlawful to the Dutch Tax Authority. IS InterNed Services defends itself by stating that in principle they are not responsible for any messages posted on websites they host. Their policy is to remove content immediately from their server as soon as they have become aware of the evidently unlawful nature of the information. The State could have sued A-Group; the verdict would have been reason enough to expeditiously remove the message from the website.

The court rules that article 6:196c paragraph 4 BW does not hold an ISP liable if he did not know of unlawful content stored on their server and removed the illegal information as soon as they are aware of it. However, in this case it was not evidently clear to IS InterNed Services that the content of the message was unlawful. The fact that the letter of the State Secretary said the information was unlawful does not mean that the ISP could know beyond reasonable doubt that the information was in fact unlawful. The decision to await a court order was not unlawful and the court assumes that, now it has ruled the information unlawful, the ISP will remove it instantly.

[15] Vzr. Rb. Haarlem 14 May 2008, *LJN* BD1446

## 2.3 Article 54a Dutch Criminal Code

The liability that was discussed in the previous chapters was mainly civil liability. However, ISPs could also face criminal liability; e.g. in the case of child sexual abuse or terrorist information. In implementing the E-Commerce Directive into Dutch Law, article 54a *Wetboek van Strafrecht* (Dutch Criminal Code, hereafter referred to as Sr) was formulated. The article states that the intermediary that supplies services that consist of the transmission or storage of information can avoid criminal liability by taking all measures that can reasonably be expected of him to block information on command of the public prosecutor, who has a written authorization of the investigating judge. The article has two purposes. The first is to restrict ISP liability, so ISPs can focus on providing their services and not have to worry about possible liability.[16] The second purpose is to protect the freedom of expression. It will prevent ISPs from removing everything that could possibly be illegal to avoid liability.[17] This liability is based upon art. 48 Sr, which says that a person may be an accessory to a crime if he provides the means for committing one. An ISP who knows about certain information because of a notification but does not act against it could be held criminally liable. Thus, a similar Notice and Take Down procedure is introduced, only now the notifier will be the public prosecutor who also gives the ISP an order to take down certain content. Not following that order can result in criminal liability for the ISP.

However, in their report Koops, Schellekens and Teepe come to the conclusion that there actually is no adequate legal ground for a Notice and Take down order given by the public prosecutor.[18] They come up with four arguments to defend this conclusion. The first argument is that, when looking at the history of article 54a, it was never meant as an independent ground.[19] Secondly the article was placed in the Dutch Criminal Code, while all other competences in relation to criminal law exist in the Code of Criminal Procedure, this could indicate that it was not meant as an independent competence for the public prosecutor.[20] Thirdly the article does not provide adequate legal protection for the parties involved, the content provider will not be notified there is no room for objection and it is not guaranteed that prosecution will actually take place, thus there may never be a judicial decision.[21] The last argument is that the actual text of the article only says that the ISP will not be held liable if he follows the order, but it does not say that the prosecutor is authorized to

[16] *Infra* note 17 at p. 9
[17] Koops, Schellekens & Teepe 2007, p. 5
[18] S*upra* note 17 at p. 42-43
[19] *Supra* note 17 at p. 18
[20] S*upra* note 17 at p. 19
[21] Ibid.

give such an order.[22] The article on which 54a Sr was built is art. 125o Code of Criminal Procedure, but when looking closer at this article the authors of the report say that 125o Sv does not provide an adequate ground either.[23] Although article 54a Sr may be used, it does not actually provide a sufficient legal ground for the public prosecutor to order an ISP to block access to materials. This, in my opinion, only leads to more unclarity about the status of the ISP. Because a third person, the ISP, is ordered to cooperate, there should be a better legal basis.[24] It would not be fair to force an ISP to cooperate without a legitimate ground. The ISP would then have to make a choice between not obeying the Public Prosecutor and protecting its clients' interests.

## 2.4 Difficulties

Despite the E-Commerce Directive and its implementation into Dutch law, the matter of ISP liability is not entirely solved. Different issues arise when looking deeper into the subject. First, there is the problem of the contracts the ISPs conclude with their clients. According to art. 8 Wbp they are not allowed to process personal data from their clients unless one of the exemptions applies. Disclosing a clients name and address would thus mean a breach of contract, unless the client consents beforehand with a clause giving the ISP the right to disclose personal data in certain circumstances. The exemption in art. 8 that is relevant to this is the aforementioned paragraph f: the processing of personal data is only allowed when it is strictly necessary to concede to the interests of the responsible person for this data or a third party and when the interests of the person whose data is being processed do not prevail. As illustrated by the court cases above, the ISP can be obliged to disclose certain data when the information their client has published is evidently unlawful. The same goes for taking websites offline or blocking the access to a webpage. If an ISP has unjustly removed a website, their client can hold them liable for the damages because the ISP has breached the contract. In the case of art. 54a Sr the ISP can argue that the circumstances are beyond their control, they were ordered by the public prosecutor to remove the illegal content. Besides, it is not always clear whether information is unlawful or not. As Kuilwijk remarks rather rudely: "And then the 14 year old Czech boy on the photo turned out to be 18 years after all."[25]

If the ISP discloses personal data or removes the website of its client and the information turns out to be legal, their client can hold them liable for breaching the contract. Once personal information has been disclosed, it cannot be reversed. Anonymity cannot be

[22] Ibid.
[23] *Supra* note 17 at. pp. 19-22
[24] *Supra* note 17 at p. 23
[25] Kuilwijk 2004

restored, which is why the ISPs have to be very careful in taking such decisions.[26] On the other hand, if the ISP does not disclose these data and the information is unlawful, they can be held liable by the harmed party.[27] The ISP has to make a choice between two parties and will most likely chose the option that involves the least risk for them.[28] This might result in a chilling effect on the freedom of information.[29]

Continuing on the previous paragraph, it can be said that the knowledge of ISPs is often not sufficient to decide on the nature of information they store. A Dutch project called the Multatuli-project proved this lack of knowledge with the ISPs by putting a text of the Dutch author Eduard Douwes Dekker (1820 – 1887), whose pseudonym was Multatuli, on different webpages with different ISPs.[30] They then sent e-mails from a hotmail address summoning the providers to take the website offline because the text was protected by copyrights owned by the E.D. Dekkers Foundation. Out of the ten approached providers, one never responded to the e-mails sent. Seven of them took down the text after being notified. UPC responded to the message with an e-mail asking the notifying party to sufficiently verify that he was acting on behalf of the E.D. Dekkers Foundation, because the complaint was sent from a free and anonymous hotmail address. UPC said they would not process the complaint until further verification. The only provider that had the right answer was XS4ALL, which responded that the text of Multatuli belonged to the public domain since the author had deceased over 70 years ago.

The project also pointed out that, at that time, none of the approached providers have any information on complaints or a notice and take down procedure on their websites.[31] This ahs now been changed, XS4ALL for example now does have such a procedure. Users do not know how to file a complaint or how to respond in case of illegal or unlawful content. ISPs often only refer to the general terms and conditions, allowing them to do whatever they think necessary; including removing accounts. This could be unfair against their client and could result in liability on the basis of the contract that was closed.[32]

This project has shown that the knowledge of ISPs is poor when it comes to copyright protected works. But at least it is possible to verify some facts and decide whether copyright infringements were made or not. A bigger problem is that the nature of certain information is

[26] S*upra* note 9 at p. 223
[27] Duthler Associates 2004, p. 9
[28] Clayton 2000
[29] Schellekens 2001, p. 63; Julia-Barcelo 2000, p. 108
[30] Nas 2004
[31] *Supra* note 30 at p. 8
[32] Ibid.

hard to identify. When is a statement actually defamatory? In the case of child sexual abuse one cannot always see whether a person is 18 or over. And do pictures of a baby girl playing naked in the garden also qualify as child pornography? Also, what about the freedom of expression? Judgments like these ask for careful consideration and should not be made lightly. Hugenholtz points out that according to the jurisprudence the ISP may await a court order before taking down information.[33] However, in many cases parties will not go to court and even if they do, this would take up a lot of time and money. It is simply not feasible to wait for court decisions, which may never be taken, when deciding on the illegal or unlawful nature of information. In my opinion deciding on matters like these is not the task of ISPs; they do not have the knowledge nor the capacity to handle these issues. A balance should be found between the rights of the victims of unlawful activities on the Internet, those who are being accused of these activities and the ISPs who have to handle the complaints.[34]

There is also another problem involved; because of the international and deterritorialisational features of Internet, illegal content can be hosted in a foreign country. The prosecutor cannot order a foreign ISP to remove information purely on the basis of art. 54a Sr. A Dutch ISP can be asked to block the information from the foreign ISP. This, however, brings along the risk of blocking legal information as well.[35]

In the next chapters a solution will be sought for the problems I have described above. In my opinion this solution lies in a Notice and Take Down System, with a central authority to handle complaints. Such a system has been designed in the Netherlands, but has never actually been realized. How this system was designed, why it was not realized, how other countries handle the NTD matter and why I believe a central NTD-system should be realized will be elaborated upon in the next three chapters.

# 3. The present status of a central Notice and Take Down system in the Netherlands

In this chapter I will first have a look at the history of the plan for a central Notice and Take Down system. Next I will explain what the NTD system as it was designed comprehends;

[33] Hugenholtz 1999
[34] *Supra* note 25
[35] *Supra* note 17 at p. 37

who are held liable, what kinds of infringements are covered under this system and who are involved. I will then explain why the plan for a central NTD-system has not yet been realized.

## 3.1 The history of the Dutch NTD system

Since 2003 the Ministry of Justice has tried to bring together some important authorities in the field of Internet Service Providers in order to come to a form of self-regulation. The parties involved were: *NLIP* (Dutch Association of Internet Providers), the Department of Public Prosecution, *Meldpunt Discriminatie* (Dutch Complaints Bureau for Discrimination on the Internet), *Meldpunt kinderporno* (Dutch Bureau for reporting child sexual abuse) and *Stichting Brein* (a Dutch authority that protects intellectual property rights in the entertainment industry). In November 2003 Dutch members of Parliament van der Laan and van Dam advocated for government involvement to come to some sort of co-regulation. In 2004 a report was written on the feasibility of a central NTD system in the Netherlands.[36] The report provides an insight of how such a system might be realized and what its bottlenecks are, section 3.3 will have a closer look on these findings. In a letter to the Dutch Parliament the Minister of Justice Donner indicates that the system should be operational in the beginning of 2006. However, the system as Donner describes it is not the system the ISPs were presented with, this will be further explained in section 3.3.[37] In the same period the NLIP ceased to exist, part of its providers had already left this organization and started *ISPO* (a consultation organ for ISPs). The co-operation fails and to this date the original NTD-system is not operational.

## 3.2 The NTD system as it was meant to be

This chapter will provide an overview of how the original model for a central NTD-system was designed. It will illustrate what parties are involved, what kinds of acts fall under its scope and how the system processes complaints.

### *3.2.1 The original model for a central NTD-system*

In the aforementioned report on the feasibility of a central NTD-system a model for this system is described in chapter two.[38] The central system will consist of two groups: The Centre for Notice and Take Down that will function as a central point for receiving complaints and notifications and a communication platform for all parties involved. The second group will be the different organs to decide upon the complaints.

---

[36] *Supra* note 27

[37] Bits of Freedom newsletter, nr. 3, 16-17 August 2005, <http://www.bof.nl/nieuwsbrief/nieuwsbrief_2005_16.html>

[38] *Supra* note 27at p. 15-26

A person can send its complaint to the Centre for Notice and Take Down, which will send the complaint to the relevant organ. This organ will investigate the complaint and report its findings to the Centre for NTD, which will then inform the ISP and the person who sent the complaint. In case of illegal or unlawful information the ISP will remove or block the information. The obligation to block information will not exist until the complaint has been investigated. The system will operate in different areas of illegal information, those area's are: child sexual abuse, racism and discrimination and intellectual property rights. In the letter of Donner to the Parliament terroristic information and activities are also subject to this system. ISPs will not be held liable if they cooperate. If they chose to ignore the centre's advice, they can be held liable for their action or inaction.[39]

For example: if a person accidently finds child sexual abuse on the Internet, he can notify the Centre for NTD. The centre will look at the complaint and send it to the organ that is specialized on this subject. The organ will then decide whether the complaint is correct and consider the measures to be taken. These may involve leaving the illegal content online, so an investigation can be started. The specialized organ will report its findings back to the centre, which will act on the organs advice. If necessary the centre will summon the ISP to take the content down.[40]

The burden of proof is on the notifying party. In the case of child sexual abuse this will be obvious, but in some cases it will be harder to proof that a complaint is correct. To come to an operational situation, the complainer will at least have to provide some of the proof that the information is unlawful.

In the report a number of matters are summed up that need further elaboration. Some of these are the identification of the notifying party, the data needed for processing a complaint, the maximum period of time for processing a complaint, the necessity to report the findings to the notifying party, the maximum amount of time for blocking the information, the expected frequency of complaints and the allocation of costs over the actors involved.[41]

### *3.2.2 Conditions for a successfully operating NTD-system*

The system will need to meet a number of conditions in order to be effective. The system needs to be trusted by all parties, transparency is therefore an essential condition. The system should have a stable legal basis because if it does not, the status of the decisions taken by the centre and organs will be unclear. Another important condition is that ISPs will not have to

[39] *supra* note 27at p. 25
[40] *supra* note 27at pp. 16-17
[41] *supra* note 27at pp. 16-19

face liability if they cooperate, otherwise there would be no reason for them to participate. The organs handling the complaints should have a sufficient legal basis and the system needs to be accepted at both a political and societal level. The decisions made within the system should be taken objectively and independently by experts in the relevant fields. And, the system should be exclusive. If there are other authorities or systems that work with a similar system, the weight of the decisions will be decreased.[42]

The report also leaves some room for the alleged wrongdoer. He should be treated fairly; his interests should be handled with care. Thus the centre for NTD has to make sure that the complaint is correct and that it is handled confidentially. The process needs to be transparent so the 'suspect' can defend himself.[43] However, how exactly these conditions should be fulfilled is not explained in the report.

The report emphasizes that international collaboration is needed to ensure the system operates as effectively as possible. Countries can share their knowledge and thus improve their models. In section 5.3 the United Kingdom will be discussed, this country has a well developed NTD system that is fully operational.[44] Other countries that currently have initiatives on NTD-systems are Belgium, Iceland, Spain and Finland.[45] My focus will be on the United States because in their Digital Millennium Copyright Act, a NTD procedure is described for complaints concerning copyrights. The United Kingdom will be discussed because they have a fully operational NTD system, which focuses on child sexual abuse, criminally offensive content and incitement to racial hatred.

### *3.2.3 The legal status of the system*

Whether the system should be private or public is addressed shortly in the report. Because it is the state that combats illegal information on the Internet, this part of the system should be publicly operated.[46]

The complaints can be of criminal or civil nature, in case of unlawful content the civil regulations will be applicable, illegal content will be processed under criminal law. The Centre for NTD is considered a public entity, also for complaints concerning unlawful information.

About the status of the processing organs there is a difference of opinion between the ISPs and the Ministry of Justice. The ISPs think that the organs should have a public status,

[42] *supra* note 27at pp. 20-21
[43] *supra* note 27at p. 23
[44] *supra* note 27at p. 26
[45] *supra* note 43
[46] *supra* note 27at p. 27

since complaints about illegal content are automatically a public matter. They believe it would be irresponsible to leave such judgments up to private organs. They also argue that in civil cases the final decision is not made by private parties and that it would be undesirable to leave the development of 'jurisprudence' to the market. The Ministry of Justice, however, argues that the organs should have a private status. In their opinion the law starts from responsibility for the ISPs, this responsibility should not be shifted to public entities.[47] In section 6 I will clarify how I think this should be solved.

#### *3.2.4 Liability for the ISPs and the Centre for NTD*

There is always the possibility of the alleged wrongdoer holding the ISP liable for damages; the goal of the NTD-system is to avoid this kind of consequences. But how can this be achieved? The most obvious action would be to provide a legal guarantee that if an ISP or the centre for NTD have carefully followed the procedure, they are not held liable. However, an amendment of law is necessary and will most likely not happen any time soon. Another possibility would be to set up a standard regulation for the ISP industry, designed by the industry, the centre for NTD and the clients of the ISPs. A third option is the centre for NTD taking on all liability if an ISP handles correctly. This asks for a careful spreading of risks. The last option in the civil framework is to record a provision in the general terms and conditions of the contracts ISPs close with their clients. This provision can protect the ISPs from being held liable by their clients. However, in the latter case ISPs can still be held liable by third parties.[48] My view on this matter I will discuss in section 6.

To avoid criminal liability an ISP has to remove or block illegal content on the basis of art. 54a Sr. Naturally the centre for NTD cannot order ISPs to block content on the basis of this article, only the public prosecutor has the authority to do so. The centre can give an advice to take down a website, but unless legislation would be changed, this cannot be enforced. Still, it is advisable to ensure the ISP that it will not be held criminally liable if it follows the advice given by the centre for NTD. [49]

### 3.3 Complications

The original plan for the NTD-system was generally accepted by the ISPs, but to become operational it did need some further elaboration. When Donner, Minister of Justice, in his letter to the Parliament,[50] shifted the balance from the issues that were originally in the plan,

---

[47] *supra* note 27at p. 29
[48] S*upra* note 27at pp. 30-31
[49] *Supra* note 27at pp. 31-32
[50] Kamerstukken II, 28 197 nr. 5 vergaderjaar 2004-05

child sexual abuse, discrimination and intellectual property rights, to terroristic and hateful messages, the ISPs were 'not amused'.

The first complaint the ISPs have is that the system is not yet fully developed. Donner wanted to launch the system and solve the problems they come across during the progress.[51] There are no concrete solutions available to fill the gaps in the proposed model. Complications will be solved with the battle against terrorism as a leading factor, this in contrast to the report, which put the three above mentioned issues first.[52] The ISPs fear that terrorism and hateful messages playing such an important role in the new system will lead to an even stronger grip of justice and police on the NTD-system, threatening the independence of the centre for NTD.[53]

This leads to the next argument ISPs have against the system as it was proposed. Justice and police are the ones to decide when illegal content is involved, they can also decide to leave certain content online to make monitoring activities easier. Also, the National High Tech Crime Centre[54] mentioned the so-called honey pots; websites purposely attracting radical-fundamentalists, making the monitoring of these groups easier. This, again, leads to a much stronger grip of justice and police on the Centre for NTD.[55]

Another point of discussion is that of a fair hearing for the alleged wrongdoer. The report does not mention a procedure in which the alleged wrongdoer gets a chance to defend himself against the complaints. The report stays vague when discussing this problem, before the ISPs will agree to the proposed system this issue needs to be solved.[56]

In the report, several sources of financing are summed up which can be of financial means for a Centre for NTD.[57] One of them is donations from pressure groups. It is likely that especially groups protecting intellectual property rights are willing to invest. However, if the main focus is on the battle against terrorism and hateful expressions, the groups might be less interested.[58]

---

[51] S*upra* note 50 at p. 2
[52]Bits of Freedom newsletter, nr. 3, 20-26 October 2005, <http://www.bof.nl/nieuwsbrief/nieuwsbrief_2005_20.html>
[53] *Rechtennieuws.nl* 31 October 2005, <http://rechtennieuws.nl/5032/haalbaarheidsonderzoek-centrum-voor-notice-and-take-down.html>
[54] The National High Tech Crime Centre was founded in 2004 as a collaboration between the Ministry of Internal Affairs, the Ministry of Economic Affairs, the Ministry of Justice and the Dutch Police to fight ICT criminality. Merely a year after it was founded, the NHTCC was closed by the government after complaints of the economic industry that it was not doing enough against computer criminality. See: <http://rechtennieuws.nl/1445/national-high-tech-crime-Centre.html> and
<http://www.security.nl/article/12866/1/Criminelen_vrij_spel%3F_Overheid_sluit_High_Tech_Crime_Centre.html>
[55] *supra* note 52
[56] ibid.
[57] *supra* note 27 at p. 41
[58] *supra* note 52

Overall, the ISPs did not agree with the system as Donner proposed it in his letter. It was their belief that some crucial points of discussion should be solved before the system would become operational. As of yet, the problems have not been solved and the system was unable to meet its deadline at January 2006. There has been no further progress towards a central NTD system since then. There has been a meeting in June 2007, where the Ministry of Economic Affairs and the *EPC. NL* (platform voor E-Nederland; platform for E-Netherlands) met to discuss a national regime which should focus on the notice-part of a Notice and Take Down regime.[59] The NTD procedure used by XS4ALL, which will be discussed under 6.1.2, should serve as an example. This meeting was confidential, so no conclusions can be drawn from it. Veenman, chairman of the Dutch association for ISPs ISPConnect Nederland, who was present at the 2007 meeting, does mention a Code of conduct for Notice and Take Down regimes, but this code has not yet been made public.[60]

# 4. The desirability of a central Notice and Take Down system

After having discussed the original model for a Dutch NTD-system and before going deeper into how such a model could become operational, it is useful to show why I believe such a system would be desirable. First I will list some arguments that support the realization of a central NTD-system. Next I will give some arguments against such a system and prove that not all these arguments hold up.

## 4.1 Arguments pro a central NTD-system in the Netherlands

The first reason why I believe a central NTD system could be part of the solution to the problems with ISP liability is that ISPs no longer need to decide on matters they do not have enough knowledge about.[61] Whether a copyright is infringed may not be too hard to see - although the Multatuli-project showed that even the ISP's knowledge of intellectual property rights is very poor.[62] But when is a statement defamatory? And when is something child sexual abuse? Think of the example above; are pictures of a baby girl playing naked in the garden child pornography? These are subjects that the employees at ISPs are not skilled in and one cannot expect them to always make the right decisions,[63] whilst specialized organs do possess the knowledge necessary to make the right decisions.

[59] Veenman 2007b
[60] Veenman 2008
[61] Heinemann 2005
[62] S*upra* note 30
[63] Nas 2003, p. 167

The second argument in favor of a central NTD system is that ISPs can avoid liability by operating on the advice of the Centre for NTD. Once the model is fully developed and operational, the only task for ISPs is to act when the centre advises them to take down or block access to a website containing illegal or unlawful information. Thus, the risk of ISPs taking information down too easily to avoid liability is reduced.[64] This also reduces the risk of ISPs threatening the freedom of expression.

Looking back at the case law that was discussed in section 2, one can see that the protection of anonymity is also in danger when it comes to ISP liability. A court can enforce an ISP to reveal the name and address of its client, so a right holder or victim can go to court. Not revealing such data can result in liability for the ISP.[65] But, if the court decides that the complaint was wrong, the anonymity of the client is already gone. As said, anonymity cannot be restored.[66] But anonymity is not only a valuable asset for the alleged wrongdoer; the notifier may want to stay anonymous as well.[67] This can be avoided by setting up a Centre for NTD which receives complaints on a central hotline. Because the Centre and its organs handle the complaints, the notifier does not need the name and address of the wrongdoer right away. He can await the decision of the Centre for NTD and if the complaint is correct, the Centre can provide the notifier or the Public Prosecutor with the necessary data to start a judicial procedure.

Working with a central authority would also take some of the burden off from the courts because they no longer have to decide in the 'first phase' of a complaint. Only if one of the parties wants to go to court *after* the Centre for NTD has decided, the legal system will be burdened. Because the Centre protects anonymity, parties also do not have to start a legal procedure for disclosure of personal data of the alleged wrongdoer.

Not only would a central authority take some of the burden off of the courts. It could also result in lower costs for the ISPs. They do not have to spend time on investigating complaints, fewer costs will have to be invested in judicial procedures and there is also the possibility of lower costs for insurance against liability.[68]

In the United Kingdom the number of websites containing child sexual abuse hosted on UK servers has dropped dramatically from 18% in 1997 to 0.4 % in 2006, since the founding of the Internet Watch Foundation (IWF) in 1997.[69] What this foundation exactly is

---

[64] Schellekens 2001, p. 63
[65] *Supra* notes 9, 12 & 13
[66] *Supra* note 26
[67] *Supra* note 27 at p. 35
[68] S*upra* note 27 at p. 26
[69] Internet Watch Foundation 2008, *Success Stories*, Internet Watch Foundation, United Kingdom, <http://www.iwf.org.uk/public/page.34.htm>

and how it operates will be explained in section 5.2. For now it is important to know that this foundation has set up a NTD system with special attention to child sexual abuse. As the numbers show, this system is certainly successful. Taking this foundation as an example could be of great interest to the Dutch system and might result in success ratings similar to those in the UK.

Of course there are also some counterarguments. In the next paragraph these arguments will be dealt with and I will show why these arguments are insufficient to oppose a central NTD system.

## 4.2 Arguments against a central NTD-system

The first argument against a central NTD system in the Netherlands is that a national system is simply not enough. A lot of information one can access is not hosted with Dutch ISPs, but on foreign servers.[70] A national system could only battle national issues and would therefore only be useful to a limited extent. However, if a system is working sufficiently on a national level, it could serve as an example for other countries or even international solutions. Working towards a certain level of harmonization could make national systems interoperable and thus much more effective. Initiatives could be taken at European or global level. Mainly cases like child sexual abuse images and terrorism can be taken on much more effectively on an international level. Important roles could be played by e.g. the United Nations or the European Community. The latter has already tried to harmonize some of the rules with directives such as the E-Commerce Directive. Besides, even though only a smaller level of success would be reached in operating on a merely national level, this would be better than no success at all.

The second argument against a Centre for NTD in the Netherlands would be the threat to the freedom of expression. Depending on how the system would eventually be organized, governmental authorities such as the police and the department of justice will have less or more influence on the procedures. As the ISPs argue, the original model and the new proposition Donner made both leave too much room for the department of justice and the police.[71] This could result in a strict limitation of the right to freedom of expression, especially in cases where terrorism is involved. If the centre for NTD could be guaranteed a certain amount of independence, ensuring the freedom of expression there would not be a problem. If, and how this is possible will be discussed in section 6. Leaving NTD procedures

[70] *Supra* note 17 at p. 36
[71] *Supra* note 52

to ISPs exclusively could just as much result in a restriction of the freedom of expression. As stated above, ISPs could take down too much in their eagerness to avoid liability.[72]

Thirdly, one could argue that ISPs can simply implement a provision in their general terms and conditions that relieves them from any kind of liability and thus a central system would be redundant. If a client does not want to take this risk, he can look for another provider. In my opinion this argument is weak because first of all, the ISPs can then stretch this provision as far as they want. That could result in unfair practices, ISPs, choosing the lowest risk possible, will take down anything that is not clearly legal. The case should go to court to be solved, which results in higher pressure on the judicial system and higher costs for the ISPs and its clients. Secondly, it is likely that all ISPs want to waive themselves from liability, thus leaving the client without a realistic option of going to another provider.

The fourth argument against a Centre for NTD starts from a financial point. How will such a centre be paid for? The report mentions different groups who are of financial means to a central system.[73] The income of the centre would, according to the report, consist of contributions paid by the concerned parties (mainly the government and the ISPs), donations by interest groups and in case of complaints related to intellectual property rights the costs can be transferred to the complainant.[74] Once the centre is up and running, the costs of investigating complaints that are usually made by the public prosecutor can be transferred to the Centre for NTD. By separating the obvious cases from the more difficult ones, the centre can distribute its employees and resources more efficiently and rubricating different cases will also save the department of public prosecution time and effort.[75] I believe this last option to be a realistic view on how to save costs. But I am not sure whether and how much different groups are willing to invest in a central system. And although the report does offer some solutions as how to financially make this Centre possible, it does not address the issue of false complaints. If a case goes to court after the Centre has ordered the removal of certain content and the court decides this removal was incorrect, who will pay for the damages then? Or when the Centre decides that information should stay online and this is later overruled by the court, damages will also have occurred. In case of a false complaint one could try to retrieve the damages from the complainant, but this does not seem reasonable if the complainant was acting in good faith. The report does not offer a solution for this problem, which could eventually lead to financial problems. Although I do not have a clear solution to this problem, I do see some options such as EU funding, which is also the case with the *Internet Watch*

[72] *Supra* note 29
[73] *Supra* note 27
[74] *Supra* note 27 at p. 41
[75] *Supra* note 27 at p. 48

*Foundation*, on which I will elaborate under section 5.2, and the saving of costs by other means, which I will discuss in section 6. Overall I think the options for financing a central system given by the report are realistic, although I am not completely sure whether they will be enough to finance the entire system.

The last counterargument that will be discussed is that of the pressure that could be put on a central system. It is imaginable that the Centre would have to handle a lot of complaints, resulting in high pressure on its employees and longer reaction times on complaints. The *College Bescherming Persoonsgegevens* (The Dutch Data Protection Authority, hereafter referred to as CBP), to name an example, has mentioned in its annual report of 2005 that pressure is increasing among other reasons because of the growth of complaints.[76] Too much work will lead to long responding terms, this could cause damages because illegal content is left online too long. Because I will go deeper into these matters in section 6, I will only briefly discuss some solutions to this problem in this section. Of course there is always the risk of too much pressure, but there are ways to reduce this risk. One of those could be to let law-students handle the simple cases. Also, because complaints are distributed over different organs, the pressure could be minimized.

Overall, I believe that the counterarguments are weaker than the arguments pro a central system. Most parties seem to agree on the statement that there should be a central system, it are the details of how to organize such a system that lead to conflicts.[77]

Now that the pro- and counterarguments have been discussed and that I have made my position in these matters clear, it is time to demonstrate how I believe a Centre for NTD can be realized. But before going deeper into that subject, it is useful to first have a look at how other countries have organized their NTD procedures or (and) systems.

# 5. Notice and Take Down in other countries

This chapter will provide an overview of how ISP liability and NTD procedures are regulated in two other countries and point out the differences and similarities with the Dutch approach. I will first discuss the United States and its policy on Notice and Take Down procedures, and then I will look at how the United Kingdom deals with this subject. I have chosen these two countries because both handle NTD-procedures in a different way. As I will show, the US is

[76] College Bescherming Persoonsgegevens 2006, p. 55

[77] Compare the opinions of the Centre in the Bits of Freedom newsletters and those of parties involved in the Duthler Associates report from 2004

mainly focused on intellectual property rights, whereas the UK has put its focus on child sexual abuse materials.

## 5.1 United States

In 1998 the United States implemented a new copyright act; the Digital Millennium Copyright Act (DMCA). This act was enacted to comply with international private law, in particular with the WIPO Copyright Treaty and the WIPO Performances and Phonograms Treaty of 1996.[78] The part relevant for ISP liability is Title II, which was actually the Online Copyright Infringement Liability Limitation Act, now incorporated into the DMCA.[79] The DMCA provides four so-called 'safe harbours' for ISPs, provided that they act as "*"good citizens" who err in favor of removal of the material complained of."*[80] The four safe harbours are: Mere conduit, caching, user storage and information location tools. As one can see, three out of these four safe harbours use the exact same terms as the E-Commerce Directive. The only safe harbour that is not in the E-Commerce Directive is that of information location tools. Information location tool providers are providers that identify and index new websites and that display lists of links with websites containing information a user has requested.[81]

The other three safe harbours have the same meaning as the terms have in the E-Commerce Directive, to keep things clear I will briefly repeat these meanings. Mere conduit means that the ISP is transmitting, routing or providing connections for information. Caching is the automatic storing of material made available by others. User storage, referred to as hosting in the E-Commerce Directive, is the storing of material at the direction of a user.[82] Information location tools, not mentioned in the E-Commerce Directive, comprehend referring or linking users to online locations by directory, index, reference, pointer or hypertext.[83]

To be protected by one of the safe harbours the ISPs have to meet certain conditions. For mere conduit and caching these conditions are roughly the same as the conditions in the E-Commerce Directive, which are described in section 2.1 of this thesis.[84] In the case of user storage and information location tools the conditions for a safe harbour resemble those of the conditions required in art. 14 of the E-Commerce Directive. These conditions can be found under paragraphs 512 (c) and (d) of the DMCA, summarized: the ISP does not have actual

[78] McEvedy 2002, under FN1
[79] *Supra* note 78
[80] *Supra* note 78 at p. 66
[81] Julia- Barcelo 2002, p. 112
[82] *Supra* note 78 at p. 66
[83] *Supra* note 78 at p. 66-67
[84] For a full description of these conditions see section 512 (a) and (b) of the DMCA

knowledge that material is infringing, is not aware of circumstances from which infringing activity is apparent or acts expeditiously to remove the infringing material once it does obtain such knowledge. The ISP does not receive financial benefits directly attributable to the infringing activity where the ISP has the right and ability to control such activity and acts expeditiously to remove or disable access to the infringing materials upon notification of claimed infringement.

Under the DMCA the ISP does not have the obligation to monitor or to actively seek for infringing activities. However, the ISP cannot hide behind the absence of these obligations. Once it has received a notice of infringing material it has to act immediately, otherwise it will lose the benefits of the safe harbour.[85]

So far the E-Commerce Directive and de DMCA show various similarities in their views on ISP liability. Both provide the same kind of liability limitations, there are however two differences. The first difference is that the E-Commerce Directive does not have a provision for information location tools. Because this thesis focuses mainly on ISPs in the role of hosting provider, the issue of the ISP acting as an information location tool will not be further discussed. The second difference between these two legal frameworks is that the DMCA provides a Notice and Take Down procedure, whereas the E-Commerce Directive does not explicitly contain such a procedure. In the next paragraph the NTD procedure from the DMCA will be further explained.

A NTD procedure under paragraph 512 of the DMCA starts with a notification by a right holder that a copyright is infringed. The ISP must act immediately by removing the content or blocking access to it. Paragraph 512 (c) (3) lists a number of elements the notification should contain: it must be a written notification to the designated agent including an electronic signature from the right holder or a representative of the right holder whose right is infringed. The copyrighted work that was infringed and the actual material need to be identified and the notifier has to provide sufficient information for the ISP to locate the content. The complaining party should also give the ISP enough information on how to contact him, such as an address, a telephone number and an e-mail address at which he can be contacted. The notification should contain a statement by the complainant that he has a 'good faith belief' that the use of the material was not authorized by the copyright owner, its agent or the law. The complaining party also has to add a statement that the notification is accurate and that he is authorized to act on behalf of the right holder. The complaining party has to make these

[85] *Supra* note 78 at p. 67

statements under the penalty of perjury.[86] The ISP should have a designated agent to whom the notification should be sent, a notification sent to someone else than the designated agent is a non-conforming notice. However, even a non-conforming notification will usually be taken care of, because the ISP will lead the complainant to the designated agent if the first complaint was sent to the wrong address.[87] According to paragraph 512 (g) of the DMCA, the ISP cannot be held liable for removing content, even though the material was in fact not infringing.

The ISP can only waive the above mentioned liability if it also notifies his client that material was blocked or removed. If the client sends the ISP a counter-notice, the latter is obligated to restore the material within ten days and the ISP should send the complainant a copy of the counter notice and inform him that the material will be restored. The ISP does not have to restore the material if it receives a notice from the complainant that he has issued a law suit. Then access to the allegedly infringing material will continue to be disabled until the court has ordered otherwise. After a counter-notice from the alleged infringer, the complainant cannot send another counter-notice. Thus the ISP does not have to continue blocking and de-blocking access to the material, the parties should go to court.[88]

The most positive point of this procedure is that the ISP does not have to decide whether or not the content complained about is infringing or not. There is no qualitative decision required, the ISP merely acts upon notifications.[89] This contributes to a faster process of removing and replacing materials, saving the ISP time and money. Another positive aspect of this framework is that the ISP is not liable for removing content that was not infringing. Not having to choose between the possibility of being held liable for copyright infringing materials and the possibility of facing liability for unjustly removing materials will take some of the burden off the ISPs, both financially and physically. In case of an untrue complaint, the complaining party will be held liable for the damages instead of the ISP.[90]

A negative aspect of this regime is that for a substantial decision, parties have to go to court. This puts an extra burden on the judicial system, which is undesirable. Another downside of the DMCA's NTD procedure is that both parties can be acting in good faith, this could especially occur when the allegedly infringing party is relying on the fair use of materials.[91] The fact that the complainant who made an untrue statement will be held liable

[86] *Supra* note 78 under FN37
[87] *Supra* note 78 at p. 68
[88] Clayton 2000
[89] Ibid.
[90] *Supra* note 81 at p. 112
[91] *Supra* note 78 at p. 69

for the damages may in that case also turn out unfair. Finally, the DMCA only covers the subject of copyrighted materials. For other topics such as child sexual abuse images or defamation there is no such procedure available. As I will show in section 6 some elements of the US system can function as an example for the Dutch system, both in a positive and a negative way.

The Communications Decency Act of 1996 provides a framework for ISPs in case of offensive material. ISPs removing or blocking access to content that falls under this act will not be held liable for defamation or other causes of action.[92] This leaves the victims of so-called cyberbullying without a proper action, because approaching the wrongdoer is often almost impossible and the ISPs enjoy full immunity under the CDA.[93] If the US government were to implement a NTD regime similar to that of the DMCA, these victims can start a legal procedure in order to get their damages paid for.[94]

In the next paragraph another regime will be illustrated, namely that of the United Kingdom. Whereas the US focuses on intellectual property rights, the UK system focuses on child sexual abuse images, criminally obscene content and incitement to racial hatred.

## 5.2 United Kingdom

Child sexual abuse images hosted anywhere in the world, criminally obscene content and incitement to racial hated hosted in the UK are the three main categories the *Internet Watch Foundation* (IWF) focuses on. The IWF was founded in 1996 and is a self-regulatory body that co-operates with several other bodies, both governmental and non-governmental. Its goal is to work in partnership with these different bodies to minimize the availability of online illegal content, with special attention to child sexual abuse images.[95]

The IWF offers a so-called hotline where complaints can be made about potentially illegal content. It also promotes wider education and awareness of its role and the role of other players in the field such as consumer bodies, government departments and law enforcement bodies. The IWF also assists national and international law enforcement in the fight against criminal content on the Internet by working together with police and other

[92] Deturbide 2000, p. 6
[93] Areheart 2007, p. 42
[94] *Supra* not 93 at p. 43
[95] Internet Watch Foundation 2007, *About the IWF*, Internet Watch Foundation, United Kingdom, viewed 10 July, 2008, <http://www.iwf.org.uk/public/page.103.htm> and Internet Watch Foundation 2007, *Mission and Vision*, Internet Watch Foundation, United Kingdom, viewed 10 July, 2008, <http://www.iwf.org.uk/public/page.114.htm>

relevant authorities.[96] How the IWF handles complaints will be described in the next paragraph.

Once someone encounters illegal content on the Internet that falls under one of the three categories the IWF handles, one can make an online report to the IWF hotline. After receiving the report the IWF will see whether it falls under one of its categories and assess what should be done with it, the reporter will receive a reply that action will be taken. If the content is not illegal under UK law no further action will be taken, if the content is potentially illegal the IWF will trace the source of the server of the content. This tracing is done by employees who are trained and advised by the police. If the content is not hosted in the UK, the IWF can only take action in case of child sexual abuse images. If the content is hosted in a country that is also a member of INHOPE, the IWF will notify the relevant hotline.

> **INHOPE** is the International Association of Internet Hotlines, an organization founded under the European Commission's Safer Internet Action Plan[97] to help combat the growing concern of illegal content on the Internet.[98] Connected to INHOPE are many different countries, each working with their own hotline. The Dutch organization connected to INHOPE is the *Meldpunt Kinderporno op het Internet*.

A notification will also be sent to the Child Exploitation and Online Protection Centre (part of the UK police, dedicated to protecting children from sexual abuse)[99] and the case will be disseminated to Interpol. If the content is hosted within the UK, in this case criminally obscene content and incitement to racial hatred can also be attended to. The IWF will send a Notice and Take Down notification to the ISP that there is potentially illegal content on their server and a notification will be sent to the police. The IWF inform the complainant of the assessment and the action taken.[100] In their FAQ-section the IWF offers a list of other online materials that do or do not fall under the scope of the IWF. In case the subject does not belong to the IWF's field, they redirect the user to the relevant website to take action. Reporting content can be done anonymously.[101]

When talking about the liability of ISPs, the IWF is operating in accordance with the framework given in the E-Commerce Directive. ISPs cannot be held liable if they immediately

---

[96] Internet Watch Foundation 2007, *Role and Remit*, Internet Watch Foundation, United Kingdom, viewed 10 July, 2008, <http://www.iwf.org.uk/public/page.35.htm>
[97] See: <http://ec.europa.eu/information_society/activities/sip/index_en.htm>
[98] INHOPE, *Delivering Global Security*, INHOPE, Ireland, viewed 10 July, 2008, <https://www.inhope.org/system/files/inhope_brochure.pdf>
[99] See: <http://www.ceop.gov.uk/>
[100] Internet Watch Foundation 2007, *What happens to my report?*, Internet Watch Foundation, United Kingdom, viewed 10 July, 2008, <http://www.iwf.org.uk/public/page.31.43.htm>
[101] Internet Watch Foundation 2008, *How to report*, Internet Watch Foundation, United Kingdom, viewed 10 July, 2008, <http://www.iwf.org.uk/howto/page.10.htm>

act after being notified of illegal content. The IWF plays the role that I have in mind for a Dutch Centre for NTD, it investigates the complaints and notifies the relevant parties. The ISP only has to follow the order given by the IWF to escape liability. According to the Sex Offences Act 2003, under S. 46: 8.12, the IWF is, next to UK Law Enforcement Agencies, the only relevant authority to receive and assess potentially illegal images.

Numbers show that the IWF has had quite some success since it was launched in 1996. In 2000 the websites that were judged to be potentially illegal in the UK had decreased with 75%. That year the IWF processed 8942 reports; in 1997 only 1291 reports were processed. In 2001 it won an award for the most "Positive contribution to the Internet industry", awarded by the Internet Service Providers Association (ISPA). In 1997 18% of the illegal content assessed by the IWF was hosted on UK servers. In 2005 this percentage has dropped to just 0.4%.[102]

The most important advantage that IWF has in my opinion is its connections with other national authorities through INHOPE, making it possible for national systems to all co-operate on an international level. The statistics mentioned show that the UK system is working effectively and could be used as an example for other countries and other subjects. One of the downsides of the IWF is that its field is limited to child sexual abuse, criminally obscene content and incitement to racial hatred. Subjects such as harmful content, copyright infringements and defamatory content are left to other authorities. One organization covering and coordinating all these different subjects could prove an effective solution. And if that organization would work together with other national authorities through bodies such as INHOPE an international collaboration could be the result.

After having discussed these examples of how countries nationally use certain Notice and Take Down systems the time has come to investigate how a central system could be made operational in the Netherlands. In the next section I will shine a light on how I believe such a system could be made possible, what the options are and how I think it should be organized.

## 6. How to realize a central Notice and Take Down system

Is the plan as proposed in the 2004 report enough? What improvements should be made to successfully implement a central system? In what cases should content be removed? It is rather obvious that illegal content should be removed; think of obvious child sexual abuse

[102] *Supra* note 69

images or clearly terroristic information. But what about harmful information? And what qualifies as harmful? Should websites that encourage self-mutilation be removed from servers? And what about the current discussion on so called pro-ana websites, should those be taken into account as well? These questions I will try to answer in this chapter.

In section 6.1 I will first give an oversight of different suggestions that have been made by authors and I will look at some NTD-procedures that other countries or individual organizations have implemented. Next I will come up with some essential conditions that should be met in order to establish a functional system. Whether these conditions are realistic and achievable will also be discussed in this section. Under 6.3 I will look at what kind of subjects are suitable to place under the authority of a centre for NTD. Section 6.4 will be used to see what organizations could be involved to run the Centre for NTD. Next I will briefly discuss the possibility of techno regulation and finally, in section 6.6 I will provide a complete image of the Dutch Centre for Notice and Take Down as I believe it should be.

But before I start this chapter I will first explain what sufficient, as mentioned in the central question of this research, in my opinion comprehends. A sufficient NTD system should be one that is a) working efficiently and is able to handle complaints within a reasonable amount of time (usually within three working days), b) ensuring a fair process for all parties involved and c) relieves ISPs from liability if they cooperate.

## 6.1 Different views on NTD- systems and –procedures

This section is meant to show some different views on NTD-systems and procedures by different authors and organizations. For each opinion I will point out what aspects I think are relevant for the Centre as I have it in mind. I will also explain for each idea what I think the flaws are and how these might be solved. After having discussed the opinions of these authors I will shortly repeat the aspects of the US approach towards NTD as described in the DMCA and the NTD procedure used by the IWF. I will do this to point out which aspects I believe could be used as an example for the Dutch system. Finally I will look at the NTD procedure Dutch ISP XS4ALL uses for its clients. XS4ALL was chosen as an example because they have launched a new procedure for NTD in 2007. XS4ALL launched this procedure under a Creative Commons License and encouraged other ISPs to also use this procedure, in order to establish a harmonized working method.[103]

[103] Veenman 2007a

### *6.1.1 Solutions offered by authors*

In this section I will talk about the opinions of three authors who have written about the subject of ISP liability and NTD procedures. First I will discuss two suggestions made by Richard Clayton. I have chosen Clayton because the procedure he has designed greatly resembles that of the DMCA. Next I will briefly look upon the solution Kees-Jan Kuilwijk provides, because this solution seems to be based upon one of Claytons models. Then I will have a look at what Sjoera Nas has written about the subject of Notice and Take Down. Nas was chosen because she was behind the Multatuli-project and has worked as a spokeswoman for XS4ALL and for Bits of Freedom. She was also involved in the European Commissions Rightswatch programme, which attempted to work out a European self-regulatory framework for copyright infringements on the Internet.

In his article Clayton presents two solutions for the problem of ISP liability in NTD-situations.[104] The first solution Clayton offers is to give ISPs full immunity for the actions of others.[105] ISPs would have no liability at all for content that originates from their customers or anywhere in the world as long as it does not belong to corporate activities of the ISP itself. The reason Clayton gives for this immunity is that the actions are outside of the ISP's control.[106] In Claytons first model, ISPs only have to act upon the instructions of a court.

However, providing ISPs full immunity would mean that companies and individuals who wish to see certain information removed from the Internet would have to go through expensive procedures, because at any time a court needs to be involved.[107] The second argument that Clayton mentions against this option is that in certain cases it might be enough to notify the author of the content that is offensive or illegal to have the content removed by the author itself.[108] Sometimes messages can be posted in the heat of the moment, which is a typical characteristic of the Internet. After being warned an author might want to change his choice of words or remove the materials that were complained about. There is also a third argument against this model, which is not brought up by Clayton; if courts have to be involved materials could be available online for a greater period of time. The ISP can only act upon an instruction of the court, while these are usually long procedures. Defamatory statements can cause irreparable damage to someone's reputation, not to mention what kind

[104] *Supra* note 88
[105] *Supra* note 88 at p. 9
[106] Ibid.
[107] Ibid.
[108] Ibid.

of damage information as it was being spread in the Deutsche Bahn case could cause.[109] Considering these arguments I do not believe that full immunity would be the solution to the problem of ISP liability.

But Clayton also provides another solution which he refers to as R4; report, removal, response, replacement. These four R's represent the steps an ISP has to take to avoid liability and to be able to respond quickly to complaints. Clayton states this procedure should not only apply to civil actions but also to criminal matters where it would be usual for the police to issue the relevant report.[110] I will now describe each of the four steps as Clayton foresees them and comment on the usefulness of his system.

The first R stands for the **report** of material that should be removed. The party that is aggrieved reports the material they are complaining about to the ISP and gives the reason why it should be removed. In the report the complainant should be identified so the ISP can check whether the report is genuine. The ISP will have no liability for the complained of material as long as there is not a proper report.

The second step in this procedure is the **removal** of the material that was complained about. After having received a complete report the ISP removes the material from its servers and notifies the author of the material. The ISP will provide the author with the identity of the complainant so that they can form a good view of their legal position. The ISP is now indemnified against both the complainant and the author of the removed material. Clayton does not wish for the author himself to remove the material because this might cause delay, thus the information would be available for a longer period of time; ISPs can act more rapidly. If an author cannot be identified the ISP only has to take reasonable steps to find out the identity of the author, if this is not possible the material will be removed without a notification.[111]

The next step in Claytons procedure is that of **response** by the author. There is always the option that an author does not respond at all and will leave everything as it is. This does not mean that the complaining party will not go to court, but for the ISP the case will end at the previous step. However, it is also possible that the author does respond, stating that the material never should have been removed, a misidentification could be made or the material is simply not illegal. The author can then choose to go to court or to issue a replacement notice. This notice requires the ISP to put the material back online. A court can still decide

[109] See: section 2.2.3
[110] *Supra* note 88 at p. 9
[111] *Supra* note 88 at p. 10

that the material is illegal and that it should be removed again. Clayton adds that the author should be given the opportunity to respond to the complaint before the material is being removed at all. But in that case the ISP would have to take a substantive decision instead of merely respond to valid notices.[112]

The last step will be the **replacement** of material. If the ISP receives a response of an author as described above it should automatically act and replace the material. A notification should be sent to the original complainant and, of course, to the author that the material has been replaced. If the ISP acts within a reasonable period of time, they will not be liable.[113]

After replacement of material the material cannot be removed again. Parties will have to go to court to solve the issue. The ISP then has to act upon the instructions of the court, obeying the courts orders will free the ISP from liability.[114] The danger of this procedure is that it can be abused; complaining about smaller parts of a website, thereby taking the entire or the most important parts of a website down. Clayton suggests that in cases like these a restore-notice could cover the whole website and not just the one part the specific complaint is about.[115]

In his column, Kuilwijk suggests the same procedure Clayton has described, there is only one difference. Kuilwijk envisions a NTD Code of Conduct with which different parties can comply.[116] Complying parties oblige themselves to first follow this procedure before going to court.

As one can see, the procedure Clayton and Kuilwijk suggest greatly resembles the procedure used by the DMCA. But now a much greater range of subjects could be covered than in the DMCA. The advantages of such a procedure are that the ISP does not have to make a qualitative decision, the process will be faster and the limited liability of the ISPs will take some of the burden off of them. ISPs do not have to judge cases they do not actually have enough knowledge about and the risk of them taking everything down to avoid liability is also reduced. Disadvantages of this procedure are that for a substantial decision parties will still have to go to court, which is expensive and puts extra pressure on the judicial system. And, in this procedure there is no anonymity for the complainant. The user whose material is complained about will receive the identity of the complainant. In cases involving intellectual property rights or defamation this will not be problematic. But one can imagine cases in

[112] Ibid.
[113] *Supra* note 88 at p. 11
[114] Ibid.
[115] Ibid.
[116] *Supra* note 25

which anonymity of the complainant should be protected. Think of a Jewish girl offended by a website from skinheads. If she would send a notice, the ISP will forward some of her personal data to the website owners, which could get the girl in trouble.

It is this specific aspect of the procedure that I find too important to be neglected. It could prevent people from notifying the ISPs of allegedly unlawful material and if people do notify the ISP there is a chance the other party wants to take reprisals. Of course a complainant should sufficiently identify himself, but it would be better not to forward that information to the person who the complaint concerns. Without an organization in between, an ISP would be the one to act as an intermediary, which is not the role I would assign to them. A Centre for NTD can function as an intermediary between the author and the complainant, protecting the identity of the complainant. If the case goes to court, the Centre can provide the parties with the necessary data.

In my opinion the R4 as Clayton describes them can still be used, only not by the ISP itself but by a Centre for NTD. Instead of merely acting upon the notification and the counter notification the Centre can judge the complaints substantially and then come to a decision. The ISP will be notified if content has to be removed and as long as the ISP obeys the Centres instructions it will not be held liable in case of damage.

Sjoera Nas is of the opinion that ISPs should not have to deal with complicated decisions, especially when it involves the freedom of expression. In her opinion all these cases should go to court.[117] She says it will only lead to a limited number of cases because in 90% of the cases the complaint originates from a major right holder, which can easily be verified and in 95% of those cases the user will immediately remove the content after 'being caught'. The other complaints are usually incorrect, she states. The remaining 10% of the complaints deserve closer attention and again she believes that in 90% of those cases the users will remove the content from their websites instantly. What is left are the cases that are crucial to the freedom of expression and those should be decided upon in court. ISPs should be able to leave that content online without having to face liability until a court has decided what should happen.[118]

Nas also advocates a central body to handle complaints, it should be similar to the existing hotlines for child sexual abuse images and online discrimination. The central body should be able to take care of simple cases and the complicated cases should go to court.[119]

---

[117] *Supra* note 63 at p. 170
[118] Ibid.
[119] *Supra* note 63 at p. 171

When looking at the above mentioned solutions I agree with Nas that a central body would be part of the solution to the problem of ISP liability. Indeed, cases that are too complicated should go to court. The 4 R's by Clayton are also useable when working with a central body, although complainants should be able to stay anonymous. The next section will briefly repeat the US and UK procedures and introduce the procedure used by Dutch provider XS4ALL, again I will point out the advantages and disadvantages of these procedures to show how they can be useful for designing a Dutch Centre for NTD.

### *6.1.2 Existing procedures*

Because both the US and UK procedures for NTD have been described under sections 5.1 and 5.2 I will not repeat them here. I will simply point out which features of these procedures I believe to be useful as an example for a Dutch central system.

Under the DMCA a notification needs to meet certain demands in order to be valid; the written notification must contain an electronic signature from the right holder or its representative. The copyrighted work that is allegedly infringed must be identified, as well as the actual material and sufficient information should be provided for the ISP to locate the concerned materials. Also, the complainant has to provide the ISP with relevant information on how to contact him. The notification has to contain a statement that the complainant has 'a good faith belief' that use of the material was not authorized by the copyright owner, its agent or the law and it should include a statement that the notification is accurate and that the complainant was authorized to act on behalf of the right holder. These demands ensure that a complainant walks through several steps before filing a complaint, thus forcing him to consider his complaint carefully. This, I believe, will reduce the number of false complaints. The other aspect of the DMCA that is useful is that ISPs are not held liable if they follow the NTD procedure prescribed in the act. This is how it should also be in a Dutch system.

The procedure the IWF uses is a good example on how to help harmonize procedures internationally. If content is potentially illegal the IWF will trace the source of the server, if it is located in another country the relevant INHOPE hotline will be notified; the Child Exploitation and Online Protection Centre and Interpol will also be notified. This way content hosted outside the Dutch borders could also be battled.

XS4ALL has introduced its own procedure for NTD in 2007. Even though XS4ALL is known to be very protective of personal data from their clients -they would not provide a

complainant with personal data of their clients unless there is a court order- in the new procedure they can provide a complainant with the name and address of their client in case of unlawful content. [120] Niels Huijbregts, XS4ALL spokesman, explains that they have abandoned the policy of extreme protection of its clients because it was no longer attainable.[121] From the court rulings has followed that material does not have to be apparently illegal before an ISP is obliged to give out the name and address of its clients. What matters is, according to the courts, that a complainant has the opportunity to file a lawsuit –for which he needs the name and address of the client-. As long as the ISP and complainant are acting carefully, the complainant should be able to file a lawsuit. It is for this reason that XS4ALL has decided to change their policy, but Huijbregts points out that they will still be careful with personal data of their clients.[122]

In the current procedure XS4ALL will notify its client of a complaint and give the client a chance to respond to the complaint. Complaints need to be sufficiently specified and based upon valid arguments. In case of intellectual property right infringements the complainant has to verify that he is the right holder or an authorized representative of the right holder. After receiving a notification the client can decide to take the material offline himself, this way parties will not have to go to court and the client can stay anonymous. If the matter is not solved at this point, XS4ALL will deal with the case more in-depth, it will do so with court decisions as examples. Unless it is unreasonable, XS4ALL will decide upon a complaint within three working days. Material that is obviously unlawful or illegal will be removed immediately, both the complainant and the client will be notified of the actions taken. Clients can object to the complaint, XS4ALL will forward the objections to the complainant within two working days. Within ten days the provider will send a motivated decision to the complainant and client. If a complainant wants to receive the name and address of a client he has to meet a range of strict conditions summed up in article 6 of the XS4ALL policy on complaints concerning unlawful content on the Internet. [123] These conditions are: 1. the complainant has asked the client via XS4ALL to voluntarily supply him with his name and address and the client has not responded within 5 days. 2. The complainant himself has not acted unlawfully in collecting data from the client. 3. It is likely that the behaviour of the client is indeed unlawful. 4. The complainant has a realistic interest in receiving the clients name and address. 5. It is plausible that there is no less radical way of retrieving this person's data. 6. When weighing the interests of both the complainant and the

[120] See the cases Deutsche Bahn vs. XS4ALL and Scientology vs. XS4ALL in sections 2.2.3 and 2.2.4.
[121] Huijbregts 2007
[122] Ibid.
[123] *Infra* note 124

client, the complainants interest has to be clearly more. 7. It is beyond reasonable doubt that the information given by the complainant concerns the client involved. In case of protest by the client XS4ALL will not provide the information until a decision has made on the protest. In the more complicated cases XS4ALL will use the help of an independent commission of experts.[124] As one can see at number 6, the ISP still has to make a substantive decision when weighing the interests of both the complainant and the client. Thus, in my opinion this procedure is still not satisfactory.

However, this procedure could prove to be of high value for a Dutch Centre for NTD. Using a strict procedure as the one XS4ALL uses could save the centre a significant amount of time in deciding upon complaints, which is important for an efficiently and fast working centre. Clients can remain anonymous for a reasonable amount of time and have the chance to solve the problem without further interference of the ISPs or a judge. The most complicated cases can always go to court, those decisions can later be used when encountering similar problems.

## 6.2 Conditions for a working NTD system

We have now discussed the legal frameworks that concern ISP liability and had a closer look at how the original Dutch NTD system was designed. We have seen the difficulties within the current legal frameworks and the reasons why a Centre for NTD is desirable have been discusses. The NTD procedures used by the US and the UK have been discussed and the XS4ALL procedure has been explained. Now the time has come to sum up –in random order- the conditions that I believe at least should be met in order to establish a Dutch Centre for Notice and Take Down.

The first condition that should be met is that the Centre should be able to work independently. Governmental involvement should be restricted as much as possible. This to ensure the freedom of expression. Only in cases of criminal content the department of Justice should be involved. Financially the government may be of great importance for the Centre, if it were to subsidize the Centre this should be done under strict conditions. As I have described in section 3.3 part of the problem with the system as Donner proposed it was that the focus was on terrorist information and not on the other subjects as well. This could lead to too much involvement of the department of justice, which led to great resistance among other parties. One of the options would be to use a model simillar to that of the Dutch Data

[124] For the complete XS4ALL policy on complaints concerning unlawful content on the Internet see: <http://www.xs4all.nl/overxs4all/contact/media/beleidsregels_klachten.pdf> (in Dutch).

Protection Authority. This is an independent body that monitors the compliance with different data protection laws. It cooperates with different other bodies on both national and international levels.

The second condition is that anonymity for the ISP's client is guaranteed insofar as this is possible. As I have described in section 6.1.1. in some cases it can be unfair or dangerous to provide a complainant with the personal data of a client. Besides, a person also has the right to privacy which should be protected as far as possible. Of course full anonymity could lead to unfair outcomes. As the courts have ruled; a complainant should have the opportunity to take the case to court and therefore he needs the name and address of the person he want to file a lawsuit against. The procedure XS4ALL uses could be a solution to the problem of anonymity. The client will stay anonymous for a reasonable period in which he can decide to take the concerned material offline or solve the problem in another manner. If the problem is not solved the complainant will be provided with the name and address of the client, but only if the conditions summed up in the XS4ALL policy are met.

The third condition would be transparency. A system that is not transparent will never be trusted by all parties, the report on the feasibility of a central NTD system in the Netherlands emphasizes the importance of this condition.[125] There have to be clear procedures and the legal status of the Centre should be made clear through legislation. This way the status of the Centre's decisions will also be clear.

Efficiency is the next term that should be met. If the Centre is not working efficiently it will soon drown in complaints. First of all the complaints should be distributed throughout the different organs within the Centre. If standardized forms are used for complaints the complainant can already indicate which part of the Centre should decide upon the complaint. The form used by XS4ALL, is an example of how this can be achieved. Another way to make the Centre work efficiently would be to separate the easier complaints from the more complicated ones and let the easy complaints be handled by e.g. law-students. Students can do an internship in the Centre and thereby become acquainted with subjects such as intellectual property rights, defamation and criminal content. I agree with Nas that most of the cases will be rather obvious and thus students in the last phase of their education should be able to solve these issues.[126] Cases that can be identified as simple are the ones with obvious copyright infringements, such as enabling the downloading of movies or music. Information like that of the Deutsche Bahn case, which is without a doubt damaging would also be simple to solve. In other cases the illegal nature of content will also be obvious, think

[125] *Supra* note 27 at p. 23
[126] *Supra* note 63 at p. 170

of terroristic content, child pornography that is undoubtedly child sexual abuse or incitement to racial hatred. But also the complaints that are not correct can be of simple nature, think of the aforementioned Multatuli-project. Having students solve these complaints could save time and money. Whenever a complaint is not that easy to solve, the student can forward the case to an expert. This would take some of the pressure off for the organs within the Centre and could help prevent the Centre from colliding under the pressure of too many complaints.

To make sure the ISPs will cooperate with a Dutch Centre for NTD they have to be guaranteed that they will not be held liable if they obey the instructions given by the Centre. If this cannot be guaranteed, it is rather obvious that ISPs will not be willing to participate, because there is not much to gain for them. But who will be held liable? In most of the cases this will be obvious. Either the client who has done something wrong or the complainant who was not acting in good faith. If the Centre cannot decide, a court should. But what if the Centre has taken content offline and later a court decides that this should not have been done? In that case the court shouldn't only decide upon the problem itself, but it should also see whether the Centre has made an obvious mistake or not. If so, the Centre can be held liable for the damages. If not, the problem remains of who will pay for damages caused by the removal of the information. Possibly the court can come to some distribution of the damages among the parties involved.

The next important condition would be fair treatment for all parties. Both the complainant and the client should have the opportunity to defend themselves and to solve the issue without further interference of the ISP or a judge. Complaints have to be verified sufficiently and so do the counter notifications. If there is reasonable doubt among any of the parties, both the complainant and the client, they can start a legal procedure. But because there are strict and transparent procedures this, in my opinion, this will not be likely to occur very often.

The Centre also needs to be very careful to protect the freedom of expression. It is of great importance that the Centre will not turn into a censoring organ. If a case is not entirely clear on whether the freedom of expression in unreasonably restricted, it is best to let a judge decide as to ensure the freedom of expression is respected.

The last condition for a fully operational Centre for NTD is one that should be further evolved once the Centre is up and running. Internationally the procedures surrounding Notice and Take Down should be harmonized as far as possible so illegal and unlawful content cannot be battled only within the Netherlands but also in other countries. The example of the IWF who cooperates with INHOPE is one that can be used to establish a

procedure that involves other countries as well. If material is located outside the Dutch borders, the Centre should be able to contact the relevant authorities in that country and provide them with the information that has so far been collected. The foreign authority can then resume the case and thus the activities of the Dutch Centre have not been a waste of time. Internationally this could lead to a more effective way to fight online crimes and unlawful content.

In my opinion the above mentioned conditions are not unrealistic. With proper consultation and close cooperation between the Centre and the different organs these conditions can be met. The next question would be who these organs should be? But before answering that question it is necessary to decide what subjects should and what subjects should not fall under the scope of the Centre. This will be done in the next section.

### 6.3 What subjects should be covered and who should be involved?

In order to know who should be involved as separate organs under the authority of a national centre we first need to address the subjects that should be covered by the Centre. For each subject I will explain who I think should be involved when working with the Centre for NTD.

The first and most important subject is, in my opinion, child sexual abuse images. Because of the nature of this subject anything should be done to effectively fight these practices and to protect children from being harmed. As shown, the IWF has been very successful in combating child sexual abuse images hosted on UK servers. The cooperation with INHOPE is also a good way to fight this problem internationally. In the Netherlands the Meldpunt Kinderporno would be the right authority to involve. This hotline is already cooperating with INHOPE and its tasks would be the same as before. Only now complaints will first be sent to the Centre for NTD, there the complaints will be looked at. If a complaint is serious it will be forwarded to the hotline, which can follow its own procedure. The hotline is also cooperating with the department of Justice. In this case not much would have to be changed, except that the hotline will no longer be the front desk. The Centre for NTD will be the one filtering the complaints, thus saving the hotline time and effort.

The second subject to be covered is illegal content, this organ could be divided into three departments namely one for child sexual abuse images, one for discriminating content and one for other kinds of criminal online content. The covering organ would be the

department of Justice. Meldpunt Kinderporno and Meldpunt Discriminatie can function under this organ, cooperating with Justice in order to work as efficiently as possible.

Intellectual property rights is the third subject to be covered. The Centre should establish its own department to look into complaints related to intellectual property rights. If the Centre develops internships for law-students they have an effective means to handle simple complaints, in the meantime these students can get acquainted with that area of law and gain some experience. For the more complicated cases they can turn to the experts who will look into the case. This could be done together with the student so he can learn at the same time.

The same method as the one described above can be followed for the fourth subject that should be covered by the Centre for NTD; defamation or other unlawful content. Complaints can be handled by an organ that should be established by the Centre for NTD. Students can take on the easier cases and the more complicated cases can be solved by experts, possibly with the help of interns.

The four subjects described above are the subjects that deserve to be taken care of with this system. I have also given thought to other subjects that could fall under the Centre's attention. The subjects that I found interesting were those of what I will call harmful information. Recently so-called pro-ana websites have been the centre of many discussions.[127] On this website young girls encourage each other no to eat and they share tips on how to loose weight as fast as possible. These girls consider anorexia as a lifestyle, not a disease. Research by scientists from Stanford University has shown that anorectic girls who visit those websites end up in hospitals more often than patients who do not visit them.[128] In France, these websites have been prohibited by law.[129] In the Netherlands there is no such law, but ISPs and blog communities such as Punt.nl have added warnings to pro-ana sites. Whenever someone wants to visit such a website, a warning will first appear that this person is about to enter a website that promotes anorexia and that this is dangerous. The warning also includes links to websites with more information and help for patients.

At first I thought it would be a great idea to have a special division within the Centre for NTD that could look into pro-ana websites and order ISPs to take them down when they are too extreme. However, when taking down these websites without a specific legal background the Centre would, in my opinion, be restricting the freedom of expression of

[127] See: <http://www.medicalfacts.nl/tag/pro-ana/>, <http://www.dag.nl/1070310/NIEUWS/Artikelpagina-Nieuws/Heb-jij-nog-een-kotstip-voor-mij.htm> and <http://www.artsenapotheker.nl/i95187> .
[128] Wilson e.a. 2006
[129] Moerland 2008

these girls. And where to draw the line? At first one might prohibit websites that are actually a danger to a person's health, such as the pro-ana websites or websites that promote self-mutilation. But who will guarantee that having tattoos or piercings will not be seen as self-destruction too? It will be hard to draw a clear line in these matters and because I believe that the freedom of expression is incredibly important I do not think that the Centre should become involved in these activities. The Centre should stick to the four above mentioned subjects because those are already regulated and offer more clarity than subjects that are not (yet) covered by law.

## 6.5 The Dutch Centre for Notice and Take Down

After having discussed all these aspects I believe are important for a complete image of how a Centre for NTD could be organized, I now want to provide an overview of how I imagine a Dutch Centre for NTD could be organized.

First of all there should be one organization, The Centre for Notice and Take Down, which covers several organs that work under the authority of or together with this body. The Centre should mainly work as a front desk; distributing the claims among specialists who will have a first look at what kind of notification it is and whether it should be taken seriously. If a complaint is valid the Centre will forward the complaint to the relevant organ. The organs covered by the Centre should be the department of Justice, Meldpunt Kinderporno, Meldpunt Discriminatie, an organ that looks into cases that relate to defamation and other unlawful content and a department for complaints related to intellectual property rights. The first three organs already exist at this point, but instead of having to filter complaints themselves, this can be done by the Centre. These organs cooperate with the Centre on the subjects that fit into their fields. The other organs should be established under the authority of the Centre for NTD. The employees working in these departments should consist of experts and students.

The funding of the Centre could be done by governmental subsidies, contributions from interested parties and donations made by pressure groups. Especially in the case of intellectual property rights, certain groups, such as Brein, may be willing to invest in a system that can battle infringements of intellectual property rights more effectively. For the government it will also be interesting to finance the Centre because all kinds of criminal online activities may be fought through a better coordinated system.

The legal status of the Centre for Notice and Take Down should be made clear. I believe that the Centre should have an exclusive position as to avoid confusion and competition between different private bodies. The Centre should be the only body authorized to give NTD-orders to ISPs, this could be implemented into different laws concerning the different subjects involved. The Centre should be independent from the government, this to avoid the risk of the government having too much influence on how the Centre operates. One of the reasons the original system never became operational was because the ISPs feared too much influence by the government because the focus had shifted to terroristic online activities.[130] The procedures should be clear and easy to access; transparency will stimulate the success of the Centre.[131] Some articles that could be adapted to the new situation are 6:196c BW, which should contain the procedure and the competences of the Centre for NTD. Also, article 54a Sr could be adapted, insofar that instead of the public prosecutor, the Centre can be the one to give the ISPs orders. Other laws that could contain articles related to the Centre are the Dutch Data Protection law, which could regulate how the Centre should handle data and in what cases data could be revealed to other parties.

Another option of regulating the Centre is to design one specific law to regulate all the competences and procedures. Some of the articles could refer to other relevant laws such as the ones mentioned above. This law could start with the competences of the Centre for Notice and Take Down, the competences of the other organs involved and how these relate to each other. Next the procedure should be made clear and the status of the involved parties if they correctly follow this procedure. Also, there should be a framework on how to handle complaints that relate to content hosted outside the Dutch borders. There also has to be a chapter with rules on what should happen if the procedure was abused.

Transparency is also important to ensure fair procedures, where both parties will be heard and have the chance to defend themselves. It is at this point where the original system failed. In the report on the viability of the system this subject was not mentioned, which led to resistance among ISPs.[132] In first instance anonymity should be guaranteed for both parties, if the case cannot be solved without revealing the identity of any of the parties, then the Centre can order the ISP to provide the name and address of their client and in certain cases reveal the identity of the complainant.

A procedure would go as follows: a person reports material he has found online through an online form in which he has to specify his complaint as clearly as possible. The

[130] *Supra* note 50
[131] *Supra* note 27 at p. 23
[132] *Supra* note 52

Centre receives the complaint and verifies it. The Centre will distribute the complaints to the relevant organs or dismiss the claim because it was not valid, in both cases the complainant will be notified that the complaint has been received and that steps have been taken. If a complaint is valid the Centre will order the involved ISP to take the concerned material temporarily offline and notify the content provider who will be given the opportunity to respond within 24 hours. The relevant organ will decide upon the complaint and if necessary –think of child sexual abuse images or undoubtedly criminal activities- legal procedures can be started. Decisions will have to be made within three working days to avoid materials unjustly being taken offline for too long. Once the decision has been made the access to the material can be restored or be blocked permanently. If parties do not agree with the outcome, they can start a legal procedure, the Centre can order the ISP to supply the complainant with the name and address of their client. The ISP that has obeyed the Centre's orders will not be held liable for any of the possible damages.

# 7. Conclusion

This thesis has looked into the possibility of a central system for Notice and Take Down to help solve the problem of liability for ISPs. At this point, ISPs can be held liable for content hosted on their servers if they were aware of it and did not take action to block access to it. The rule forces ISPs to choose between the interest of their clients and the risk of being held liable for damages caused by content their clients placed online.

Although the original plan for the system failed, I do believe that a central body for Notice and Take Down is desirable. It would relieve the ISPs from a task they never asked for and it would prevent them from taking everything they are notified of offline to escape liability. ISPs lack knowledge about subjects such as intellectual property rights or defamation, which could lead to unfair decisions. These decisions should be made by those who are specialized in the relevant fields; the employees of the Dutch Centre for Notice and Take Down.

The conditions I believe are crucial for a fully operational centre are: independence, anonymity for the ISP's clients and complainants, efficiency, transparency, no liability for ISPs if they cooperate, fair procedures in which all parties get the chance to defend themselves, a guarantee that the freedom of speech will be protected as far as possible and international harmonization.

By establishing a clear legal framework to clarify the competences of the central body, the first step towards a better NTD procedure can be taken. This framework could consist of

several new articles in existing laws such as the Dutch Civil Code, the Dutch Penal Code and the Dutch Data Protection Act. Or one specific law could be designed in which all the competences and procedures of a Centre for NTD could be specified. Having the Centre work as a front desk to verify the complaints and distribute the valid complaints among the relevant organs would ensure an efficient method of working. Fair procedures should be developed in which both the complainant and the ISP's client have the chance to be heard, the XS4ALL procedure would be a good example to use.

Although a central body may not be the perfect solution, it is my belief that with the right deliberation between all parties involved and the procedures as I have suggested it is not at all impossible to finally come to a sufficient Notice and Take Down system in the Netherlands: The Dutch Centre for Notice and Take Down.

## References

Areheart, BA 2007, 'Regulating Cyberbullies Through Notice-Based Liability', *The Yale Law Journal Pocket Part*, September 2007, viewed 5 October, 2008, <http://yalelawjournal.org/images/pdfs/581.pdf>.

Bits of Freedom newsletter, nr. 3, 16-17 August 2005, <http://www.bof.nl/nieuwsbrief/nieuwsbrief_2005_16.html>.

Bits of Freedom newsletter, nr. 3, 20-26 October 2005, <http://www.bof.nl/nieuwsbrief/nieuwsbrief_2005_20.html>.

College Bescherming Persoonsgegevens 2006, *Jaarverslag 2005*, Deltahage B.V., Den Haag

Clayton, R 2000, *Judge and Jury; How "Notice and Take Down" gives ISP's an unwanted role in applying the law to the Internet,* University of Cambridge, United Kingdom, viewed 10 March, 2008 <http://www.cl.cam.ac.uk/~rnc1/Judge_and_Jury.html>.

Deturbide, M 2000, 'Liability of Internet Service Providers for Defamation in the US and Britain: Same Competing Interests, Different Responses', *The Journal of Information, Law and Technology*, 2000 (3), viewed 10 April, 2008, <http://elj.warwick.ac.uk/jilt/--3/deturbide.html>.

Duthler Associates 2004, *Haalbaarheidsonderzoek Notice and Take Down; Eindrapport*, Duthler Associates, Den Haag.

Hardy, KK, Litt, FF, Peeble, R & Wilson, JL 2006, 'Surfing for Thinness: A Pilot Study of Pro–Eating Disorder Web Site Usage in Adolescents With Eating Disorders', *Paediatrics* 2006, pp. e1635-e1643, viewed 28 August, 2008, <http://pediatrics.aappublications.org/cgi/content/full/118/6/e1635 >.

Hugenholtz , PB 1999, 'Noot bij Rb 's-Gravenhage d.d. 9 juni 1999', *Computerrecht* 1999-4, pp. 200-205, viewed 9 May, 2008,<http://www.ivir.nl/publicaties/hugenholtz/noot-scientology-xs4all.html>.

Huijbregts, N 2007, 'Notice and Takedown', *XS4ALL Opinie Weblog*, viewed 17 August 2008, <http://www.xs4all.nl/opinie/2007/02/21/notice-takedown/>.

INHOPE, *Delivering Global Security*, INHOPE, Ireland, viewed 10 July, 2008, <https://www.inhope.org/system/files/inhope_brochure.pdf>.

Internet Watch Foundation 2007, *About the IWF*, Internet Watch Foundation, United Kingdom, viewed 10 July, 2008, <http://www.iwf.org.uk/public/page.103.htm>.

Internet Watch Foundation 2007, *Mission and Vision*, Internet Watch Foundation, United Kingdom, viewed 10 July, 2008, <http://www.iwf.org.uk/public/page.114.htm>.

Internet Watch Foundation 2007, *Role and Remit*, Internet Watch Foundation, United Kingdom, viewed 10 July, 2008, <http://www.iwf.org.uk/public/page.35.htm>.

Internet Watch Foundation 2007, *What happens to my report?*, Internet Watch Foundation, United Kingdom, viewed 10 July, 2008, <http://www.iwf.org.uk/public/page.31.43.htm>.

Internet Watch Foundation 2008, *How to report*, Internet Watch Foundation, United Kingdom, viewed 10 July, 2008, <http://www.iwf.org.uk/howto/page.10.htm>.

Internet Watch Foundation 2008, *Success Stories*, Internet Watch Foundation, United Kingdom, viewed 20 May, 2008, <http://www.iwf.org.uk/public/page.34.htm>.

Julia-Barcelo, R. 2000, 'On-line intermediary liability issues: comparing E.U. and U.S. legal frameworks', *European Intellectual Property Review*, 2000-22(3), p. 105-119.

Koelman, KJ 1999, 'Wat niet weet, wat niet deert: civielrechtelijke aansprakelijkheid van de provider', *Mediaforum*, July/August 1999, pp. 204-213, viewed 10 April, 2008, <http://www.ivir.nl/publicaties/koelman/aanspr.html> .

Koops, EJ, Schellekens, MHM & Teepe, WG 2007, *Wat niet weg is, is gezien. Een analyse van art 54a Sr in het licht van een Notice-and-Take-Down regime*, TILT and Cycris, Tilburg.

Kuilwijk, KJ 2004, '"Torn between two lovers, feeling like a fool..." Voorstel voor een simpele, doch evenwichtige, notice-and-take-down-procedure', *Netkwesties* 8 October 2004, viewed 6 March 2008, <http://www.netkwesties.nl/editie111/column2.html>.

McEvedy, V 2002, 'The DMCA and the E-Commerce Directive', *European Intellectual Property Review*, 2002-24(2), p. 65-73.

Moerman, R 2008, 'In Frankrijk beslist rechter over magerte', *NRC Handelsblad*, 16 april, viewed 26 August, 2008,

<http://www.nrc.nl/achtergrond/article1875129.ece/In_Frankrijk_beslist_rechter_over_magerte> .

Nas, S 2003, 'The future of freedom of expression on-line – Why ISP self-regulation is a bad idea', *Spreading the word on the Internet – 16 answers to 4 questions; Reflections on Freedom of the Media and Internet, Amsterdam Conference June 2003*, Representative on freedom of the media OSCE, Vienna.

Nas, S 2004, *The Multatuli Project, ISP Notice and Take Down*, Bits of Freedom, viewed 6 March 2008 <http://www.bof.nl/docs/researchpaperSANE.pdf>.

*Rechtennieuws.nl* 31 October 2005, <http://rechtennieuws.nl/5032/haalbaarheidsonderzoek-centrum-voor-notice-and-take-down.html>.

Roosendaal, APC 2006, 'Elimination of anonymity in regard to liability for unlawful acts on the Internet', in: *Legal, Privacy and Security Issues in Information Technology Volume 2: The First International Conference on Legal, Privacy and Security Issues in IT Hamburg, Germany, April 30 – May 2, 2006*, Institutt for Rettsinformatikk, Oslo.

Roosendaal, APC 2007, 'Opheffen van anonimiteit bij aansprakelijkheid voor onrechtmatige daad op het Internet', *Secure Master Special* 2007, pp. 40-42.

Schellekens, MHM 2001, *Aansprakelijkheid van Internetaanbieders*, Dissertation, Universiteit van Tilburg, Tilburg.

Veenman, A 2007a, 'XS4ALL introduceert nieuwe klachtenprocedure', *ISPam.nl* 2 February 2007, viewed 5 October, 2008, <http://www.ispam.nl/archives/513/xs4all-introduceert-nieuwe-klachtenprocedure/>.

Veenman, A 2007b, 'Vergadering Notice and Take Down in Nederland - 1 juni', *ISPam.nl* 6 May 2007, viewed 21 June, 2008, <http://www.ispam.nl/archives/690/vergadering-notice-and-take-down-in-nederland-1-juni/>.

Veenman, A 2008, 'ICTRecht lanceert Notice and Takedown adviesdienst', *ISPam.nl* 16 May 2008, viewed 21 June, 2008, <http://www.ispam.nl/archives/1889/ictrecht-lanceert-notice-and-takedown-adviesdienst/#more-1889>.

## Consulted literature

van Duuren, NAH, Kaspersen, HWK, Neppelenbroek, EDC & Stuurman, C 1999, *Contracten van Internetproviders:een adequate basis voor zelfregulering?*, Kluwer, Deventer.

Ekker, AH 2006, *Anoniem communiceren: van drukpers tot weblog; Een onderzoek naar de grondrechtelijke bescherming van anonieme openbare communicatie*, Dissertation, Universiteit van Amsterdam, Amsterdam.

van der Net, CB 2000, *Grenzen stellen op het Internet; Aansprakelijkheid van Internet-providers en rechtsmacht*, Dissertation, Universiteit Leiden, Leiden.

## Case Law

HR 25 november 2005, *LJN* AU4019 (*Pessers/Lycos*)

Hof Amsterdam 7 november 2002, *LJN* AF0091 (*Deutsche Bahn/XS4ALL*)

Hof Den Bosch 25 juli 2002, *KG* 2002, 259 (*Rutloh/Concept ICT*)

Hof s'-Gravenhage 4 september 2003, *LJN* AI5638 (*Scientology/XS4all*)

Rb Amsterdam 25 april 2002, *LJN* AE1935 (*Deutsche Bahn/XS4ALL*)

Rb.'s-Gravenhage 9 juni 1999, *LJN* AA1039 (*Scientology/XS4ALL)*

Vzr. Rb. Utrecht 9 juli 2002, *LJN* AE5537 (*Teleatlas*)