Elimination of Anonymity in regard to Liability for Unlawful Acts on the Internet

Arnold Roosendaal

Student Assistant at the Tilburg Institute for Law, Technology and Society (TILT), Tilburg University, the Netherlands

Abstract:
Anonymous communication is one of the main facilities of Internet. However, challenging questions arise in relation to the scope of digital anonymity. For it is not difficult to abuse anonymity for defamation or other unlawful acts. In situations where the person posting defamatory information is anonymous, it is almost impossible for the victims of such defamation to start a lawsuit, because they do not know the identity of the other party. In the Netherlands the Supreme Court recently decided on this problem in the Lycos v. Pessers Case. This paper describes the problems on anonymous defamation and the Dutch point of view on how to solve these problems. The paper also includes a comparison between the European system and the systems of the United States and Canada. This paper concludes with some proposals for legislation to give a better protection to anonymity, besides enabling victims to open a lawsuit.
Keywords: Anonymity, unlawful acts, Internet, liability, Dutch Supreme Court decision

1. INTRODUCTION

Internet still enjoys an increasing popularity when it concerns communication and sharing knowledge and information. Due to its simple accessibility this "electronic highway" offers great benefits. Technical applications enable anonymous communication. Through anonymity and pseudonymity, views and opinions can be spread over the Internet without its sender disclosed to readers.

However, what if somebody is harmed by such communication? The information provided appears to be incorrect or defaming and the author hides himself behind a curtain of anonymity. How can this person be held liable for damages and how can he be subpoenaed?

On November the 25th of 2005 the *Hoge Raad* (Supreme Court of the Netherlands) in the Lycos v. Pessers case decided that under such circumstances, the Internet Service Provider (ISP) must identify the author by giving information about his name and address[1]. When this information is available, the author can be cited. However, this is not always advantageous because problems may arise during court cases, and there are also other consequences in relation to privacy and contractual liability.

In this paper I will discuss the abolition of anonymity in regard to liability for unlawful acts on the Internet. First, I will make some brief remarks on anonymity on the Internet (Chapter 2). In Chapter 3 I will argue that holding ISPs liable for the unlawful acts of users is not the right solution. The objective of these chapters is to sketch a background for reflection on the main issue of this paper.

Starting with Chapter 4, the main issue will be presented and discussed on the basis of the Lycos v. Pessers case. It will show which arguments pro and contra the elimination of anonymity have lead to the decision made by the Supreme Court of the Netherlands. Subsequent, in Chapter 5 I will discuss different problems and consequences that in practice might arise.

In chapter 6 I will make a comparison between the judicial systems in the Netherlands and those of the United States of America and Canada. For example in the US the so-called John Doe procedure has become common practice. After this comparison I will propose other possible solutions which were suitable for the Lycos v. Pessers case (Chapter 7). Finally in chapter 8, I will present the conclusions of this paper.

[1] http://zoeken.rechtspraak.nl/zoeken/dtluitspraak.asp?searchtype=ljn&ljn=AU4019&u_ljn=AU4019, retrieved 2006-01-24

2. ANONYMITY ON THE INTERNET

This chapter gives some brief remarks on anonymity on the Internet. How anonymous can someone be? And, are there legal borders that have to be taken into account? Or is anonymity completely justified, and is there even a right to anonymity?

Opinions on these questions might differ, but it can be noted that there are an increasing number of applications facilitating anonymity on the Internet, so at least there appears to be a market for anonymity. Especially from a privacy point of view in different occasions people want to remain anonymous. This anonymity can be specified in graduations such as anonymity, semi-anonymity, pseudonymity and semi-pseudonymity. Using, for example, anonymizers and remailers in combination with encryption can have the effect of being (almost) untraceable.

Assuming that there is a right to anonymity, one of the main issues for users is not being traced. Then the right is related to Article 8 of the European Convention on Human Rights (ECHR), arguing that people's acts on the Internet are their personal business and not public. In this context the right to anonymity seems justified. However, sometimes the protection of the real identity of the user is not the sole purpose. The interest at stake could also be to protect the act of communication itself and not the person who communicated. It is not difficult to imagine that sometimes political or religious opinions can be dangerous if made public. This is especially the case of some totalitarian regimes and strict religions. Therefore, in some situations anonymity is a necessary tool to enable views and opinions to be shared. In other words, anonymity is a crucial element in realizing freedom of expression.

Concluding, it can be said that there are several reasons for claiming the right to anonymity. This is a good starting point. However, within the scope of this paper it should be pointed out that there are also limitations to the right to anonymity, given that there may be other interests at stake. As a result there may be legal limitations for upholding anonymity. Anonymity e.g. should not allow persons to harm others using the Internet. Victims of anonymous defamation or other forms of unlawful acts cannot react or defend themselves. Therefore, this abuse is a legal border which has to be maintained. In these cases this can be done by lifting anonymity. Besides problems that might arise in case of lifting of anonymity there is also the preceding problem of how to eliminate the anonymity. Or can ISPs be held liable for their users acts?

3. LIABILITY OF ISPS

ISPs are essential to identify users. Providers know the primary information that can lead you to the defaming party you want to trace. However, ISPs are not very willingly to provide this information, arguing that the trust of their users to remain anonymous is the main pillar supporting their contract. When anonymity is no longer guaranteed the number of clients immediately will decrease. This antipathy for this option results in a search for other possibilities to claim damage from defamation. The path to the user is blocked.

This brings us to the liability of ISPs; Can they be held liable for the acts of their users? At first sight this seems to be a favourable solution. ISPs can be easily tracked, so the problem of anonymity is placed at the background. But what will be the starting point to serve a subpoena? The ISPs are not acting unlawfully, at least not directly, they only facilitate the unlawful acts of users. Or, in general, they facilitate information to be made public.[2] Unlawfulness is not a motive. The Dutch court made the same consideration in the Scientology case. "The Court is of opinion that service-providers only provide the technical facilities to enable publication of content by others. Therefore it seems not correct to put them on a level with publishers who, presumably, publish themselves. This opinion is in conformity with the Agreed Statement at article 8 of the WIPO Copyright Convention: "It is understood that the mere provision of physical facilities for enabling or making a communication does not in itself amount to communication within the meaning of this Treaty or the "Berne Convention." " [3]

Furthermore, it can be questioned whether ISPs should be expected to check all information provided by their users. One way to address liability is on the basis of a risk responsibility. But liability based on a risk for illegal content might disable the freedom of expression as guaranteed in Article 10 ECHR. ISPs might

[2] Schellekens 2001, p.61
[3] Hof 's-Gravenhage, 11 september 2003, *AMI* 2004, p.76, r.o.12

restrict access to their applications or reduce their capacities to a lower level so that they are able to check all contents. This means that there will be a clash of interests. In the Autronic case, the European Court of Human Rights stated that "any restriction…necessarily interferes with the right to receive and impart information"[4]. If ISPs have a too big responsibility this interference cannot be avoided. Therefore it can be concluded that liability of ISPs is not the solution to the problem we are dealing with in this paper. There is such a mass of data which can be changed every second[5] that pro-active research to avoid liability seems impossible. Especially if there is a mere conduit function. To compare the situation, publishers can only be held liable if they have had influence on the content of books. As it concerns websites or e-mail messages ISPs do not have this influence.

Therefore the liability of ISPs in the Netherlands is restricted to specific situations. In general a provider acts unlawful if he hosts defaming or infringing content while he is been acquainted with the existence of these materials, there is no reasonable doubt about the acquaintance and he does not remove the content as soon as possible (Scientology v. Spaink)[6]. The legislative framework for this can be found in European legislation and its national implementations.

At European level Directive 2000/31/EC[7] is applicable, in particular Articles 14 and 15. Article 14 ensures that providers are not liable for information stored by recipients of their services "on condition that: (a) the provider does not have actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of facts or circumstances from which the illegal activity or information is apparent; or (b) the provider, upon obtaining such knowledge or awareness, acts expeditiously to remove or to disable access to the information." Article 15 states that there is no general obligation to monitor the information transmitted or stored by service providers.

The Dutch national legislation applicable is Art. 6:196c *Burgerlijk Wetboek* (Civil Code) which is the national equivalent of Art. 14 of the Directive on electronic commerce[8]. In addition, Art. 8 *Wet bescherming persoonsgegevens* (Personal Data Protection Act, Wbp) determines the circumstances under which personal data may be processed. This applies if processing of data is necessary to fulfill a legal obligation (sub c) or if processing of data is necessary to promote the justified interest of the responsible or a third to whom the data are being provided, unless the interest or the fundamental rights and freedoms of the involved, in particular the right of protection of privacy, prevails.

What are the implications for anonymity as well as liability when looking at the recently decided Dutch Lycos v. Pessers case?

4. THE DUTCH JUDGEMENT

In the Netherlands the Supreme Court decided on the anonymity issue in the Lycos v. Pessers case. In this case a trader (Pessers) sold stamps via the virtual auction website "www.ebay.com". On this website buyers can give their feedback on the business transaction. The seller can, also in one line, give a reaction on this. Feedback and reactions are open to the public. The trader had a rating of 24787 positive, 299 negative and 217 neutral feedbacks.

The other party was Lycos, a globally operating Internet company. As a provider Lycos hosts websites on the Internet. Their domain, http://members.lycos.nl, contained a website called "stop the fraud". Up until the 4th of August 2003 this website contained the following text: "Have you ever been ripped of by Pessers on E-bay, join our quest for justice!! How does he work? You buy a small lot. Which he ships directly. So he gains your trust. You feel confident to buy a more expensive lot. That's when he strikes. He will keep your

---

[4] ECtHR, may 22 1990, CEDH, Serie A, vol.178, §47

[5] Van der Net 2000, p.56

[6] Rb. 's-Gravenhage 9 juni 1999, *Mediaforum* 1999, p.205-209 m.nt. D.J.G.Visser

[7] 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 (Directive on electronic commerce)

[8] Wet van 13 mei 2004 tot aanpassing van het Burgerlijk Wetboek, het Wetboek van Burgerlijke Rechtsvordering, het Wetboek van Strafrecht en de Wet op de economische delicten ter uitvoering van richtlijn nr. 2000/31/EG van het Europees Parlement en de Raad van de Europese Unie van 8 juni 2000 betreffende bepaalde juridische aspecten van de diensten van de informatiemaatschappij, met name de elektronische handel, in de interne markt (PbEG L 178) (Aanpassingswet richtlijn inzake elektronische handel) (Adaptation Act Directive on electronic commerce) http://wetten.overheid.nl/cgi-bin/sessioned/browsercheck/continuation=05153-002/session=729822466929558/action=javascript-result/javascript=yes, retrieved 2006-01-26

money and no stamps for you. That's not all. According to some of his victims he also sends fakes. Have you been ripped off and you want also to publish your story? MAIL your story to => stopthefraud@hotmail.com (…)."

There were a few 'stories' on the website from persons indicated only by their initials, telling they had had problems when they ordered stamps from Pessers.

On August 1st Pessers has sent an e-mail message to the website requesting the user to stop these activities and to make himself known. Because there was no response Pessers summoned Lycos by fax to remove the website and to provide him with the name, address and date of birth of the website holder. On the 4th of August Lycos reacted by letter, stating that they would not comply with the request. On the same date the website holder placed the following text on the website: "Site removed to avoid legal actions!!"

Pessers applied an immediate court ruling against Lycos. In the first instance there has already been made a distinction between two parts of the claim. The website had been removed by the holder so this part was dismissed. The other part concerning the name and address was taken into account. The date of birth of the holder was ruled to be irrelevant. Pessers claimed the name and address to be able to serve a subpoena on the website holder to recover his damage. The Supreme Court decided that Lycos had to provide these data. But what considerations led to this decision?

The Supreme Court makes a step-by-step approach to the root of the case, judging each step in relation to the E-Commerce Directive liability regime. Lycos stated that the Directive resists to a conviction to provide identifying data, at least if the incriminated content is not unmistakable unlawful against the person who brings the claim. This argument is based on the conception that the Directive has a limitative regulation, meaning that certain convictions are only permitted if the conditions in Article 14 are not fulfilled. The Court rejected this opinion. There are more opposite indications in the Directive, supporting a non limitative interpretation. The restriction of liability for ISPs does not exclude the obligation to assume responsibility for tracking and avoiding illegal activities. This follows in particular from the preamble sub 48 and confirmations in part 25, 45 and 52 of the preamble. Part 54 also effects that the prescribed sanctions in the Directive do not stand in the way of national sanctions or claiming facilities. Furthermore, according to the Directive, there has to be a high level of protection of general interests, in particular protection of human dignity and consumers (preamble part 10). This has to be guaranteed by effective remedies for victims of unlawful acts on the Internet (part 52). The Dutch legislator emphasized this by stating, "Service providers can be bound to provide information by which the users of their service can be identified. (…) For completeness sake, also in civil law the opportunity exists that the judge may rule that the service provider must make the source of the information known."[9]

This means that the Directive should be interpreted as non limitative. Another conception would also lead to the unfavorable result that a restricted group of victims of defamation on the Internet on present showing would have no effective judicial remedy, in contrary to the function of article 3:296 paragraph 1 Civil Code.

The second argument of Lycos was that a claim to provide identifying data is only allowed as a subsidiary claim, next to a primary claim for unlawful acts. Therefore, Lycos had to be liable for an unlawful act, besides their refusal to provide the identifying data. This argument was also rejected by the Supreme Court. A claim to provide identifying data has to be judged separately from an unlawful act. In certain circumstances, refusing to provide this information can be an unlawful act itself, because it is contrary to the duty to care in social behavior. This means that there is no general rule, but each particular situation has to be taken into consideration.

The third argument stated by Lycos consists of two parts. The first part relates to the standard on which the unlawful act of Lycos is judged. Lycos believes that if the content is not unmistakably unlawful, in principle, the identifying data do not have to be provided, unless there is an exceptional situation. In addition, the used standard is so generalizing that it will have unfavorable applications outside the Internet environment. Furthermore, Lycos considers that there is a contradiction because Lycos did not have to remove the content from the website, but on the other hand there is the legal obligation to "disclose the identifying data, thereby breaking down the confidentiality towards the client"(r.o. 5.3.3). The Court reacted

[9] Explanatory memorandum at the Adaptation Act Directive on electronic commerce (Kamerstukken II 2001-2002, 28 197, nr. 3, blz.28)

by stating that the ruling is applicable to the present case. The objections made by Lycos were dismissed because in every instance it is important which circumstances or interests prevail.

The second part refers to privacy and freedom of expression and the proportionality of the claim. Anonymity should also be protected by the right to freedom of expression by Article 10 ECHR if published content is harmful to others and not related to a serious abuse. According to the Supreme Court the interest of freedom of expression may not be thoughtless disregarded, however it is not an absolute right.

Furthermore Lycos stated that there was no risk of further spreading[10] and there was a realistic alternative in criminal law to claim the identifying data. The risk of further diffusion of the materials has to be seen separately from the claim of providing the identifying data. In addition, the use of the criminal law does not guarantee a quick and effective remedy. "In legal provision 126a of the Criminal Procedure Act, strict conditions are mentioned for the use of the described competences, which implies that the application of these competences should be very restrictive."[11] The last argument Lycos presented was that Article 8 of the Wbp does not satisfy the requirements from Article 8 paragraph 2 European Convention on Human Rights and that the restriction of the rights of Articles 8 and 10 ECHR was not necessary in a democratic society. The Supreme Court rejected this argument because the Wbp explicitly prescribes weighing the involved interests, in particular the interest of privacy protection.

Result is that Lycos had to provide the identifying data enabling Pessers to serve a subpoena on the defaming party. Most of the decision depends on weighing the involved interests, in relation to the legal provisions. However, it seems that there has to be decided as each case arises. The general principle is that the right to anonymity is not an absolute right in case of misuse of anonymity for defamation. There are still some effects of this decision which will be discussed in the following chapter.

5. CONSEQUENCES OF THE DUTCH DECISION

The Dutch decision in the Lycos v. Pessers case is related to legal provisions. However, it seems clear that there are no strict rules on liability of ISPs. The EU Directive gives some indications, but in the first report of the Commission on the application of the Directive it has already been remarked "that one or two adopted laws contain problems related, in particular, to the transposition of the provisions concerning the liability of internet intermediaries".[12] Besides the lack of clarity on the occasions as described in the Directive there is the freedom for Member States to regulate other situations as well.[13] What is clear, is that the EU in Article 15 of the Directive prevented "Member States from imposing on internet intermediaries, with respect to activities covered by Articles 12-14, a general obligation to monitor the information which they transmit or store or a general obligation to actively seek out facts or circumstances indicating illegal activities. This is important, as general monitoring of millions of sites and web pages would, in practical terms, be impossible and would result in disproportionate burdens on intermediaries and higher costs of access to basic services for users."[14] A general obligation to monitor is not the Commission's aim. There can be an ISPs liability, but under what conditions this will be is entirely left in the hands of national case law. From this point of view, the Dutch Supreme Court made the right decision by weighing all the relevant interests to reach its ruling.

However, the problem is that this ruling, which is supported by European legislation, opens the way for lots of almost similar claims. Organizations like BREIN, the Dutch organization for promotion of interests of authors from music, films and interactive software, already stated that this is a principle judgment. "The Lycos v. Pessers case deals with the question as to whether a victim can hold somebody liable for defamation. The same principle is applicable if BREIN questions ISPs to provide identifying data of

---

[10] In contrast with the case Deutsche Bahn/XS4All (Vzr.Rb.Amsterdam 25 april 2002, *Mediaforum* 2002-6, nr.24 and Hof Amsterdam 7 november 2002*, Mediaforum* 2003-1 m.nt.A.H.Ekker), where refusing to identify the client was judged unlawful *because of* the risk of further spreading

[11] Vzr. Rb. Utrecht, 12 juli 2005, KG-nr.194741/KGZA 05-462 (BREIN/Providers), r.o. 4.6

[12] REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL AND THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE - First Report on the application of 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 (Directive on electronic commerce), §3.3

[13] Id. at §64

[14] Id. at §72

infringing persons, so they can be sued for illegally circulating music, films and interactive software."[15] According to the judgment, ISPs have to provide the data if "the unlawfulness is credible and the injured party has a justified interest. The injured party does not have to go to law for this."[16] In fact, BREIN has already tried to claim identifying data of users of peer2peer software from ISP's. All the conditions to claim these data were fulfilled. However, the lawsuit ended in a deadlock because BREIN had used an illegal data processing method which was not allowed by the Wbp and conditions of the Dutch Data Protection Authority (Dutch DPA). To collect IP-addresses they had enlisted the services of an American private company. The Court considered: "The United States of America cannot be regarded as a country with an appropriate protection level for personal data."[17] Furthermore, the American company had researched the files in the 'shared folders' of the involved IP-addresses. "Between these files there can also be files which are not infringing the rights of others or which can have a personal character."[18]

If the conditions had been adhered to, the claim might have been successful. This means that, if identifying data are being requested by defamed parties (or persons who are claiming to be a victim of defamation) the ISPs have to judge the different interests themselves. On the one hand there is the interest of the anonymous information provider to spread information or content, based on the freedom of expression. On the other hand there is the interest of the party claiming to be injured, to stop defamation and to claim his damage from the defaming party. The position of the ISP is rather difficult. The judgment on the unlawfulness of the content has to be based on his personal view and eventually some references of specialists. However, there always remains the risk of a 'wrong' decision. If the ISP does not remove the content and provide the identifying data, there might follow a legal decision on the case, stating that the ISP is liable for not avoiding further spreading. And, if the ISP does remove the content and provide the identifying data, afterwards the content might be judged not to be defaming, so the right to anonymity and freedom of expression of the information provider is being harmed. Therefore the ISP can also be held liable. The ISP will take the lowest risk. The acts of ISPs in practice will have impact on the freedom of information. This means that stringent rules on liability can result in a "chilling effect" on the information society.[19] ISPs will be too reserved with the effect of a self-regulated restriction on the providing of information on the Internet. To avoid this problem in the Netherlands the Minister of Justice has proposed the introduction of a national institute with experts to make this judgment. This institute will be developed by the National High Tech Crime Centre (NHTCC).[20]

The above also draws attention to an aspect which is strongly interwoven with anonymity. A decision to lift anonymity has to be taken with caution because the result of this decision is irreversible.[21] Anonymity cannot be restored if afterwards the decision appears to be incorrect. Therefore, anonymity is a very sensitive value. ISPs should not be made responsible for decisions on the interests of different actors on the Internet related. Other solutions to solve this problem are welcome. The Dutch solution is generally favorable, but it does not cover the whole issue satisfactorily. In the next chapter there will be a closer look at other judicial systems to compare different options.

6. THE JUDICIAL SYSTEMS IN THE US AND CANADA

As previously explained the Dutch decision is not completely satisfactory, albeit the best feasible solution. Within the legal framework of the Netherlands it might answer expectations. However, some aspects remain unsolved. It should be postulated that other solutions require changes in Dutch legislation. Therefore, in this chapter a comparison will be made with some other judicial systems. Can problems be solved and if so, in which way? And are there any disadvantages related to other solutions? I will focus on the systems of the United States of America and Canada.

First, a distinction should be made between the liability of ISPs, and their role in anonymity issues concerning the users of their services. As it regards liability, ISPs seem to be quite well protected. They

---

[15] Hoge Raad: ISP moet NAW-gegevens afstaan, http://www.anti-piracy.nl/Nieuws/Bericht_0064.html, retrieved 2006-01-29
[16] Id.
[17] Vzr. Rb. Utrecht, 12 juli 2005, KG-nr.194741/KGZA 05-462 (BREIN/Providers), r.o. 4.26
[18] Id.
[19] Schellekens 2001, p.63
[20] Kamerstukken II, vergaderjaar 2004-2005, 28 197, nr. 22
[21] Vzr. Rb. Utrecht 9 juli 2002 (Teleatlas/Planet), *KG* 2002,209; *Computerrecht* 2002/5 m.nt. W.A.M. Steenbruggen

cannot be held liable if they were not involved with infringing or defaming content. This was also seen in Chapter 3. Legislators acknowledged that service providers might "only contribute to distributing information that originates from third parties".[22] In the United States this protection is stipulated in Section 230 of the Communications Decency Act (CDA), providing that no ISP "shall be treated as the publisher or speaker of any information provided by another information content provider".[23] This protection seems to be quite absolute as can be seen in the Whitney Information Network v. Xcentric Ventures LLC[24] case. In this case the defendants operated websites that provided consumers with the opportunity to complain about businesses that allegedly "rip-off" consumers. "The defendants select which complaints they will publish on the Web site, but they do not verify the consumer's allegations."[25] However, the operators were immune on the basis of Section 230 of the CDA. Thus, even selecting these complaints does not create liability.

The other part regards responsibility of ISPs for identification of users. In Europe the legal framework for this can be found in Directive 2000/31/EC. If a complainant requests an ISP to provide identifying data, the involved interests of all parties, including the ISP will be taken into consideration. In the United States the legal framework is based upon the First Amendment. "Internet users in the United States derive an independent right to communicate anonymous from the First Amendment. This forces the judge to take constitutional claims serious and to involve them in his considerations. Through the protection of anonymous expression is been brought under one and the same doctrine, as well in the physical as in the digital world, there is a more consistent approach."[26] In the United States and Canada it is possible to start a claim against an anonymous person by filing a so called "John Doe" lawsuit.[27] This involves obtaining information from a third party that has this information so that the anonymous person can be identified. "In most cases implicating anonymous Internet speech, that means a subpoena directed against the ISP or bulletin board operator, or a related discovery request aimed at someone presumed to know the speaker's identity."[28] This also follows a balance of the interests. In John Doe v. 2TheMart.com Inc. the court stated four criteria for this balance, considering "Whether (1) the subpoena seeking disclosure was brought in good faith; (2) the information sought relates to a core claim or defense; (3) the identifying information is directly and materially relevant to a core claim or defense; and (4) the information sufficient to establish or disprove the claim or defense is unavailable from any other source."[29] In Canada there is a comparable system.[30] The conclusion is therefore that the European system and the American and Canadian system are based on the same principles. There has to be a legal claim and, depending on the interests of the involved parties, the ISP has to provide identifying information on the defaming person. Each system has its own guidelines to make the balance of interests and works on a case-to-case basis. However, there is one very important difference. In the United States and Canada the judgment on the defaming character of the content is made before the order to identify the anonymous party is given. This has the result that the defendant might not be aware of the procedure until there is an order to identify him. If the order is made, the defendant might try to contest the motion of the plaintiff. If he does not, the plaintiff can claim his damage from the defendant. The advantage of this system is that the defendant will remain anonymous if the claim is rejected by the court. However, there is also a disadvantage. The first opportunity the defendant has to defend himself is when the decision is already been made. Therefore, the parties in a procedure are not equal. In Europe, there is a weighing of interests related to lifting the anonymity, but the judgment on the damaging effect of the defamation is made in the procedure which follows if the 'identified anonymous' is being sued. Therefore there is a chance that the anonymity was lifted, but afterwards this appeared to be incorrect. To solve this problem, the next chapter I propose for another way of dealing with anonymity issues.

---

[22] Koops, Prins & Hijmans (ed.) 2000, p.164
[23] CDA § 230 (c)(1), *codified at* 47 USC. § 230(c)(1)
[24] Whitney Information Network v. Xcentric Ventures LLC, M.D. Fla., No. 2:04-cv-00047, 7/14/05
[25] *Electronic Commerce & Law Report*, 8-3-2005, Vol.10, No. 30, p.760
[26] A.H.Ekker 2006, p.224
[27] A.H.Ekker, Anonimiteit en uitingsvrijheid op het internet; het onthullen van identificerende gegevens door internetproviders, *Mediaforum* 2002-11/12, pp.348-351
[28] A.Michael Froomkin in Nicoll, Prins & van Dellen 2003, p.26
[29] John Doe v. 2TheMart.com Inc, 140 F.Supp.2d 1095 (W.D.Wash.2001)
[30] See www.cippic.ca/en/faqs-resources/online-anonymity/, retrieved 2006-01-26

7. PROPOSALS

This chapter covers some proposals related to dealing with anonymity. In all of the previously mentioned systems, anonymity is eliminated before a final judgment on the liability of the defendant. In the US only, there is a possibility to argue the order. However, most of the times there is too little time to do this in practice. The result is that there is some sort of restriction on anonymity if someone claims to be injured by anonymous defamation on the Internet. How can this be solved?

As already stated in Chapter 2, it is not clear if there is a right to anonymity. In my opinion, there is no need for a constitutional right to anonymity. This would result in too many disadvantages because of the restrictions that have to be made in cases of unlawful or illegal acts. However, in different judicial systems the courts have drawn up conditions regarding the duty of ISPs to provide identifying data. Therefore, it would be favorable if legislators made national, or even European, provisions to create an independent test for unlawful acts on the Internet.[31] A legal basis will promote clarity and strengthen authority. For certain other legal fields such as copyright infringement or child porn on the Internet, there already are such legal provisions.

Another possibility of dealing with anonymity issues in liability for unlawful acts on the Internet is strongly related to the John Doe procedure. In the John Doe procedure the ISP hands on the subpoena. The ISP also has to provide the identifying data to the applicant to enable him to claim damages. Then the civil procedure follows. Anonymity will have been lifted by then. However, the ISP can act as a point of transfer. The procedure can start and the defendant can defend himself by communicating his opinion and arguments to the court, via the ISP. An adverse effect is that the procedure must be in writing, at least in the beginning. Another negative effect is that the ISP's have a new task which they did not ask for. This can be solved by creating a national institute which takes care of communications. The ISP then has to provide identifying data or merely an e-mail address to this institute. These data remain confidential. By using this system, the anonymous is able to defend him self and to remain anonymous during the procedure. The task for the national institute, which can be an existing one like, for example, the NHTCC (see Chapter 5), is clear and the risk of eliminating anonymity unjustly is been avoided. The feasibility of this proposal requires further research, but at first sight it seems to be a favorable solution.

8. CONCLUSION

In this paper I discussed the elimination of anonymity in regard to liability for unlawful acts on the Internet. The Dutch Lycos v. Pessers case is of importance because there is a new point of view on this topic. The Supreme Court made a good decision by first making a weighing of relevant interests. Besides, there is a clear explanation of the legislative framework that led to the decision to order Lycos to provide the identifying data of the defaming anonymous. However, the problem is that anonymity now has to be eliminated before there is a judgment on the unlawfulness. This means that afterwards the elimination can appear to be unjust.

The American and Canadian system has John Doe procedures as a common practice. This procedure enables victims of defamation to serve a subpoena to an anonymous person. This seemed to be a solution, but here the defendant is not able to defend himself properly. Besides that, anonymity is also been eliminated before there is a judgment on the unlawfulness of the acts of the anonymous. It also appeared that all criteria to judge requests for identifying data are being developed in practical case law.

Finally, in chapter 7, I have made some proposals to solve these problems. First, there ought to be a legal provision with criteria to judge a request for identifying data. Secondly, there ought to be a national institution which will act as a point of transfer to enable written civil procedures to take place without eliminating anonymity. In conclusion, there are some guidelines on dealing with Internet anonymity, but these have been developed on a case-by-case basis. Further legislation would be a first step towards keeping-up with technical developments on anonymity.

---

[31] As also proposed by W.A.M.Steenbruggen in "Annotatie Teleatlas/Planet Media Group", *Computerrecht* 2002-5, p.297-298

BIBLIOGRAPHICAL REFERENCES

1. A.H.Ekker, *Anoniem communiceren: van drukpers tot weblog*, 2006 dissertation
2. Koops, Prins & Hijmans (ed.), *ICT Law and Internationalisation, A Survey of Government views*, The Hague: Kluwer Law International 2000
3. C.B.van der Net, *Grenzen stellen op het Internet*, Gouda: Gouda Quint 2000
4. Nicoll, Prins & van Dellen, *Digital anonymity and the Law, Tensions and Dimensions*, The Hague: T.M.C.Asser Press 2003
5. M.H.M.Schellekens, *Aansprakelijkheid van Internetaanbieders*,2001 dissertation
6. A.H.Ekker, Anonimiteit en uitingsvrijheid op het internet; het onthullen van identificerende gegevens door internetproviders, *Mediaforum* 2002-11/12, p.348-351
7. W.A.M.Steenbruggen, Annotatie Teleatlas/Planet Media Group, *Computerrecht* 2002-5, p.297-298
8. Kamerstukken II 2001-2002, 28197, nr.3
9. Kamerstukken II 2004-2005, 28197, nr.22
10. REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL AND THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE - First Report on the application of 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 (Directive on electronic commerce)
11. EctHR, may 22 1990, CEDH, Serie A, vol.178, §47
12. John Doe v. 2TheMart.com Inc., 140F.Supp.2d 1095 (W.D.Wash.2001)
13. Hof Amsterdam, 7 november 2002, *Mediaforum* 2003-1
14. Hof 's-Gravenhage, 11 september 2003, *AMI* 2004, p.76
15. Rb. 's-Gravenhage, 9 juni 1999, *Mediaforum* 1999, p.205-209
16. Vzr. Rb. Amsterdam, 25 april 2002, *Mediaforum* 2002-6
17. Vzr. Rb. Utrecht, 9 juli 2002, KG 2002,209, *Computerrecht* 2002/5
18. Vzr. Rb. Utrecht, 12 juli 2005, KG-nr.194741/KGZA 05-462
19. Whitney Information Network v. Xcentric Ventures LLC, *Electronic Commerce & Law Report*, 8-3-2005
20. Hoge Raad: ISP moet NAW-gegevens afstaan, http://www.anti-piracy.nl/Nieuws/Bericht_0064.html, retrieved 2006-01-29
21. Lycos v. Pessers, http://zoeken.rechtspraak.nl/zoeken/dtluitspraak.asp?searchtype=ljn&ljn=AU4019&u_ljn=AU4019, retrieved 2006-01-24
22. Wet van 13 mei 2004 tot aanpassing van het Burgerlijk Wetboek, het Wetboek van Burgerlijke Rechtsvordering, het Wetboek van Strafrecht en de Wet op de economische delicten ter uitvoering van richtlijn nr. 2000/31/EG van het Europees Parlement en de Raad van de Europese Unie van 8 juni 2000 betreffende bepaalde juridische aspecten van de diensten van de informatiemaatschappij, met name de elektronische handel, in de interne markt (PbEG L 178) (Aanpassingswet richtlijn inzake elektronische handel) (Adaptation Act Directive on electronic commerce) http://wetten.overheid.nl/cgi-bin/sessioned/browsercheck/continuation=05153-002/session=729822466929558/action=javascript-result/javascript=yes, retrieved 2006-01-26
23. www.cippic.ca/en/faqs-resources/online-anonymity/, retrieved 2006-01-26