Evaluation of the Role of Access Providers

Discussion of Dutch Pirate Bay Case Law and Introducing Principles on Directness, Effectiveness, Costs, Relevance, and Time

by Arno R. Lodder and Nicole S. van der Meulen, VU UniversityAmsterdam, Department Transnational Legal Studies Center for Law and Internet, Amsterdam, The Netherlands

Abstract: Internet service providers (ISPs) play a pivotal role in contemporary society because they provide access to the Internet. The primary task of ISPs – to blindly transfer information across the network – has recently come under pressure, as has their status as neutral third parties. Both the public and the private sector have started to require ISPs to interfere with the content placed and transferred on the Internet as well as access to it for a variety of purposes, including the fight against cybercrime, digital piracy, child pornography, etc. This expanding list necessitates a critical assessment of the role of ISPs. This paper analyses the role of the access provider. Particular attention is paid to Dutch case law, in which access providers were forced to block The Pirate Bay. After analysing the position of ISPs, we will define principles that can guide the decisions of ISPs whether to take action after a request to block access based on directness, effectiveness, costs, relevance and time.

Keywords: Internet Service Providers; Pirate Bay; Access Providers, Effectiveness; Costs; Relevance

Recommended citation: Arno R. Lodder, Nicole S. van der Meulen, Evaluation of the Role of Access Providers Discussion of Dutch Pirate Bay Case Law and Introducing Principles on Directness, Effectiveness, Costs, Relevance, and Time, 4 JIPITEC 2, para 130.

A. Introduction

1 Traditionally, third parties facilitating communication and information exchange were mere messengers or neutral transporters. As a popular Dutch saying goes,[1] their policy should be to not take notice of the content of messages. Postal services do not open letters, telephone companies do not eavesdrop on communication, and even classic telephone operators simply facilitated the connection. Only with some services is knowledge of the content inherent, as in the case of telegrams and telex.

2 In the early days of the Internet, ISPs still fit into the tradition of communication neutrals. From the moment Internet access was provided to the general public in the early 1990s, however, crime slowly started to take off, and copyright infringements in particular increased quite exponentially. These developments led to a changing role for Internet service providers. No longer could they maintain a completely neutral position.

3 The initial attempts to regulate ISPs, with the prominent examples of the US Digital Millennium Copyright Act (DMCA)[2] and the European Union Directive 2000/31/EC on electronic commerce (Directive on E-commerce),[3] reflected a new dual role of Internet intermediaries: they deserved protection as neutrals, but they could also be called upon to assist with norm enforcement. The underlying reason for these regulations, however, was primarily to define exceptions or safe harbours that would protect ISPs against liability claims. Nevertheless, these laws also acknowledged that, under certain circumstances, ISPs should assist in stopping copyright infringements, for example.

4 Both the DMCA and the Directive on E-commerce[4] regulated three types of ISP services: the transport, temporary storage, and hosting of information. In addition, the DMCA also regulated search engines. Presently, there is a tendency to put pressure on ISPs to co-operate in addressing norm violation, in particular in their role as access provider. For instance, courts in several countries (Netherlands, Finland,[5] UK,[6] etc.) ordered ISPs to filter Internet traffic; the French HADOPI Act has a so-called three-strike policy regarding downloading; and the controversial ACTA is infringing on human rights in a serious way.[7] The secrecy surrounding this last initiative added to the controversy regarding its content. Much media attention was also paid to the US initiatives SOPA and PIPA.[8] These initiatives were abandoned in February 2012, but by April 2012 the comparable CISPA had already passed in the House of Representatives.[9] Since the Senate did not accept the CISPA, it was re-entered and passed again in April 2013.[10]

5 Are the times changing? Are we entering a new era? This paper aims to answer this question by focusing the discussion on ISPs in their role as the access provider.[11] The paper is structured as follows: In section 2 the liability exemptions of the US DMCA and the EU Directive on E-commerce are introduced. Next, we will discuss a series of Dutch court cases concerning The Pirate Bay that ended in 2012 with court orders against several ISPs to filter out websites belonging to Pirate Bay. In the third part we will evaluate which role fits access providers best. Viewed from different angles, the access provider as the intermediary merely providing access to the Internet will be weighed against the access provider as a full-time norm enforcer, and we will provide principles that can help in striking a balance.

B. Early days: DMCA and Directive on E-commerce

6 The spirit of the mid-1990s is well reflected by Kaspersen:[12] '(...) the duties of access-providers do not embody anything else but giving access to the Net and all the information in it, just as it is'.

7 Stated simply, an access provider should just provide access to the Internet. This basically was the background of the legislation proposed during the late 1990s, although besides this main focus on creating a safe harbour it was also acknowledged that under certain circumstances ISPs should assist in combating (in particular copyright) infringements.

I. DMCA

8 Prior to the DMCA, in 1996 Section 230 of the Communications Decency Act regulated immunity for ISPs and others regarding hosted content.[13] For the present paper with its focus on access providers, this controversial and much-debated Act[14] is not directly relevant.

9 On December 1998 the DMCA entered into force. This Act included in Title II the addition of paragraph 512 to the US Code, better known as the Online Copyright Infringement Liability Limitation Act (OCILLA). OCILLA defines four categories of exemptions applicable to ISPs: services related to (1) information location tools (search engines), (2) storage of information at the direction of users (hosting), (3) system caching and (4) transitory communications.[15] The transitory communications category is relevant for the present paper since it concerns 'transmitting, routing, or providing connections'. Whereas in doctrine, access providers are normally distinguished as a special category of providers, in regulation this is not necessarily the case. Although all types of transitory communication providers are crucial to a proper functioning of the Internet, the doctrinal treatment of access providers as a single category is understandable. For anyone on the Internet, it always starts with getting access.

10 Instead of enforcing norms on the Internet – regulating behaviour in cyberspace – it is sometimes easier to control at the source: make sure that people never get to (parts) of the Internet, or that people cannot use particular applications. As such, the ISP can function as a single point of contact for all of its users, and these users are regulated at a single instance. Access providers are the gate to the virtual world, and consequently are an obvious party to appoint as norm enforcer or gate keeper. As Mann & Belzey state:[16] 'Internet intermediaries (...) are easy to identify and have permanent commercial roots inside the jurisdictions that seek to regulate the Internet.'

11 As a shelter for such claims, the DMCA/OCILLA determines that the transitory communication provider is not liable if (1) the provider does not initiate the access, (2) the process is automatic without selection of the material, (3) the provider does not determine recipients, and (4) the information is not modified. Besides these topics related to the core activity of an ISP, OCILLA sets two other conditions: (5) providers should have a policy of account termination of repeat infringers and (6) should not interfere with technical measures (e.g. Digital Rights Management software).

12 Access providers almost intrinsically satisfy all these conditions expect for the fifth. Basically, in a normal course of action, access providers cannot be held liable as long as they define and apply a policy of account termination. The above applies to monetary relief. There are some circumstances under which injunctive or other equitable relief is possible,[17] and

we will discuss them after introducing the E-commerce Directive.

II. Directive 2000/31/EC on E-commerce

13 The E-commerce Directive was drafted against a different background than the DMCA. The opening words of the proposal for the E-commerce Directive are illustrative: 'Electronic commerce offers the Community a unique opportunity for economic growth, to improve European industry's competitiveness and to stimulate investment in innovation and the creation of new jobs.'[18]

14 This Directive formed the central pillar in the regulation of e-commerce within the EU, as was outlined in a policy document from 1997.[19] As part of the same legal package, Directive 2001/29/EC on copyright in the information society is more directly related to the DMCA, but it did not cover liability:[20] 'Liability for activities in the network environment concerns not only copyright and related rights but also other areas, such as defamation, misleading advertising, or infringement of trademarks, and is addressed horizontally in Directive 2000/31/EC (...) on E-commerce.'

15 In the proposal for the E-commerce Directive, the European Commission identified five key issues, referred to as obstacles. One of them concerned the liability of intermediaries: 'To facilitate the flow of electronic commerce activities, there is a recognised need to clarify the responsibility of on-line service providers for transmitting and storing third party information (i.e. when service providers act as 'intermediaries').'[21]

16 The angle is basically economic. The aim is to stimulate e-commerce within the European Union by protecting ISPs against liability, thus preventing them from being hindered by all kinds of liability claims when providing their services. Nonetheless, the Directive on E-commerce[22] takes a similar approach, and as McEvedy correctly observes[23] 'closely resembles the DMCA in that it provides "limitations of liability" while leaving the underlying law unaffected'. The scope of the E-commerce Directive is broader, in that it covers all legal fields, not only copyright. Surprisingly, the proposal for the E-commerce Directive does not mention the DMCA, but in certain parts it follows it almost verbatim.

17 The E-commerce Directive's well-known triad of services provided by ISPs is mere conduit (Article 12), caching (Article 13) and hosting (Article 14). At first sight it may seem that the role of access providers is left unregulated. However, just as the DMCA covered access under 'transitory communications', the mere conduit of Article 12 regulates not only 'the transmission in a communication network' but also 'the provision of access to a communication network'. The proposal also clearly indicates the different scope depending on the provider's role: 'establishes a "mere conduit" exemption and limits service provider's liability for other "intermediary" activities'.[24]

18 In order to be not held liable, the access provider should not (a) initiate the transmission, (b) select the receiver of the transmission and (c) select or modify the information contained in the transmission. For an access provider, this set of conditions is even easier to comply with than the six conditions of the DMCA/OCILLA just discussed.

III. Court orders and other observations

19 The fact that mere transmission and providing access are headed under the same category can be considered an underestimation of the role of access providers, as was indicated above. However, one could also argue that now that both the DMCA and the E-commerce Directive take this approach, there must be a reason why these services should be judged similarly. If we proceed from this assumption, we could argue that intervention of access providers should be treated similarly to intervention by providers of servers that just pass IP packets through. It is hardly imaginable that such a provider that only transmits information over the Internet would ever be called upon. So, if this provider is headed under the same category as the access provider and never asked to assist with the enforcement of norms, why would the access provider be?

20 An obvious difference between the two providers is that the access provider has a contractual relationship with the user, while the provider merely passing through IP packets does not. However, the court cases discussed in this paper concern blocking access to certain sites, so the contractual relation is not relevant in that respect. Another difference has to do with the Internet infrastructure. If an access provider blocks access, this can be effective[25] for their users, and for the other provider the effect is not guaranteed. Moreover, all users worldwide could be affected by the latter measure, whereas actions from the access providers affect only their users.

21 The safe harbors created for access providers by both the DMCA and the E-commerce Directive are not absolute. The DMCA is different in that it has an explicit notice-and-take-down (NTD) procedure,[26] and providers can be forced to reveal the identity of subscribers. The E-commerce Directive has no explicit procedures. As a consequence, ISPs need to carefully

weigh the pros and cons after a complaint without the certainty of not being held liable by either the party complaining or the opposing party. For the present paper this is not directly relevant, since access providers are never confronted with NTD requests, at least not in their role as access providers. Identity requests ask difficult decisions of ISPs, and these requests go even beyond the classic roles of ISPs to include web 2.0 providers.[27] Identity requests also fall outside the scope of the present paper.

22 An importance difference between the two regulatory frameworks is the way court orders are regulated. Whereas the DMCA defines many conditions that have to be met before a court can order an access provider to block certain content,[28] the E-commerce Directive sets no specific conditions,[29] generally stating in Article 12(3): 'This Article shall not affect the possibility for a court (...) requiring the service provider to terminate or prevent an infringement'.

23 This might explain why it is relatively easy to get a court order within the EU and hard to get one in the US. It might also explain why the tendency within the EU is for the entertainment industry to go to court, and in the US they focus on the introduction of new legislation. Illustrative are the Dutch court cases concerning The Pirate Bay, which we will discuss next.

C. Dutch case law or the Pirate Bay saga

24 In 2012 the Dutch anti-piracy organization BREIN, a foundation that aims to enforce intellectual property rights for the entertainment industry, obtained several court orders that forced ISPs to block access to The Pirate Bay. The Dutch Pirate Bay cases nicely illustrate the legal grounds underlying the blocking of access by ISPs. Therefore, we will discuss the main arguments used in the various cases that started with court proceedings against The Pirate Bay in May 2009.

I. BREIN v The Pirate Bay 2009-2010

25 The case against The Pirate Bay began well before the judge handed down its verdict in the Netherlands. Early in 2009, charges were filed in Sweden against the people behind The Pirate Bay, followed by a conviction of one year of imprisonment for Fredrik Neij, Gottfrid Svartholm, Peter Sunde and Carl Lundström on 17 April 2009.[30] The criminal conviction in 2009 led to a court initiative by BREIN that sued the Pirate Bay people in the summer of 2009 for copyright violation.

26 The summons was delivered at the address as recorded in the Swedish population register but was returned. The defendants did not show up in court, but the judge allowed the proceedings to take place in absentia.[31] This is allowed in summary proceedings if the plaintiff has put sufficient effort in trying to reach the defendant. It is interesting in this case that the effort consisted, amongst others, in sending the court order via e-mail, Twitter and Facebook (the plaintiff was de-friended minutes after the court order was left on the Pirate Bay-owned Facebook page). The reaction of one of the defendants was decisive when the press confronted him with the upcoming court case: 'Having a court case in Amsterdam on July 21 does not ring a bell.'

27 In the 30 July 2009 verdict, the court ordered The Pirate Bay to

1. stop copyright infringements in the Netherlands and

2. make websites thepiratebay.org, piratebay.se, etc. inaccessible to Dutch users.

28 The verdict is somewhat ambiguous. What is probably meant by 'Dutch users' and 'copyright infringements in the Netherlands' is Dutch IP addresses. One could argue that if the websites mentioned are inaccessible in the Netherlands, copyright infringements are stopped as far as The Pirate Bay is concerned so the first order does not add anything. However, the reason for the first point might be that changing domain names will not work to undermine the second point. Clearly, if a proxy were used the second ban could be circumvented, allowing users to access The Pirate Bay and infringe copyrights.

29 After this verdict, Pirate Bay started summary proceedings against BREIN, arguing that due to the technical complexity, this case is not suited for summary proceedings. The judge indicated that despite the complexity, balancing the opposing interests of The Pirate Bay and BREIN remains possible. The result: The Pirate Bay did not violate copyrights, but the judge decided that the act of facilitating copyright infringements by others is illegal. The judge ordered the following on 22 October 2009:[32]

1. The Pirate Bay should delete all torrents that refer to material that infringes on copyright material relevant to BREIN.

2. The Pirate Bay should block access of Dutch Internet users on the various Pirate Bay websites to the torrents under 1.

30 The idea behind this court order change was to allow references to material that does not infringe on copyrights of the parties BREIN represents. This is in favour of the freedom of speech as far as non-infrin-

ging material is concerned. However, since the court orders the deletion of torrents, people not using a Dutch IP address would also no longer be able to access them. In this respect the order reaches further than the previous court order. Another problem with the verdict is how The Pirate Bay can establish whether a torrent infringes on the copyright of the parties BREIN represents.

II. Intermezzo: International hosting providers

31 The Pirate Bay did not follow the court order, so BREIN turned to the access providers. In previous court cases in other countries, The Pirate Bay hosting providers had been sued. First, the Swedish courts decided that hosting The Pirate Bay was not allowed. The Pirate Bay was offline for a couple of days but then reappeared on German servers. The German judge also ordered a cessation of hosting The Pirate Bay. The race to the bottom stopped in Ukraine, which has hosted the Pirate Bay servers since then. In addition to the fact that suing in Ukraine would not necessarily have the same results as in Sweden and Germany, it became clear that even winning in Ukraine would only mean that The Pirate Bay would seek yet another country to host their websites.

III. BREIN v the largest ISP, summary proceeding 2010

32 Based on this verdict, BREIN asked Dutch providers to filter out Pirate Bay Internet traffic. The providers did not grant this request. Therefore, in what they called a test case, BREIN decided to sue only the ISP that facilitated the most Pirate Bay traffic. This appeared to be Ziggo. On the grounds of principle, XS4ALL joined Ziggo as a defendant in this case.[33]

33 The subtlety of the 2009 verdict (not providing access to infringing material) was replaced by BREIN and became mere access. In summary proceedings, BREIN applied the Dutch implementation of Article 11 of Directive 2004/48/EC on the enforcement of intellectual property rights (see also Article 8(3) Directive 2001/29/EC on the harmonisation of certain aspects of copyright and related rights in the information society): '(...) rightholders are in a position to apply for an injunction against intermediaries whose services are used by a third party to infringe an intellectual property right (...)'.

34 The third party are the subscribers of the ISP. The judge did not grant the request, arguing that the injunction is allowed only in cases of direct infringement, and the order would apply to all users of the provider, not only those infringing copyrights after accessing The Pirate Bay. This ruling is a bit odd: people who do infringe are banned, and people who do not infringe did not go to The Pirate Bay anyway. The argument could be that those who do not use The Pirate Bay might want to go there for lawful activities as well. However, in practice most, if not all, Pirate Bay users go there to obtain copies of works violating copyright.

IV. BREIN v the largest ISP, proceedings on the merits 2010-2012

35 In the proceedings on the merits that BREIN started after they lost the summary proceedings, they basically claimed the same.[34] The judge followed the European Court of Justice (ECJ) ruling from 12 July 2011[35] (L'Oreal v eBay), and stated that Article 11 of Directive 2004/48/EC on the enforcement of intellectual property rights can also be used to prevent infringements. In a later case (Scarlet v Sabam) on 24 November 2011,[36] the ECJ indicated that active monitoring for illegal content cannot be asked from access providers.

36 This last decision is interesting, since the Dutch judge's verdict in the summary proceedings asked precisely this from the providers XS4ALL and Ziggo. If this verdict were to be translated to ISPs, it would not be allowed according to the Scarlet v Sabam case. However, since BREIN chose a different strategy, in which it requested the mere banning of domain names and IP addresses, this EU court ruling could not be applied directly. This actually means that because BREIN claimed too much (hence also blocking legal Internet traffic), the active monitoring prohibition could be circumvented. Blocking websites or IP addresses of The Pirate Bay is ordered from the ISPs.

37 On the subsidiarity question, the judge in the summary proceedings indicated that at least suing some consumers – i.a. because they could then have the opportunity to defend their position – could be asked from BREIN. Now the judge indicated that this was not necessary, and that after the lawsuits against The Pirate Bay and the hosting providers, the logical next step concerned access providers.

38 On the proportionality question, the judge indicated that given the amount of illegal opposed to legal content, the interests of the copyright holders outweigh the interests of the ordinary Internet users. Still, the blocking of access to the complete website is less proportional than what was previously ordered by the court: not providing access to illegal material. Interestingly enough, downloading music and movies is allowed in the Netherlands, but uploading

of infringing material is illegal. Most – though not all – users do both on a torrent site.

39 During the proceedings, BREIN claimed that blocking had been effective in Denmark and Italy. Still, it is easy to circumvent the blocking, and the people who really want to use The Pirate Bay can do so. Interestingly enough, research carried out by the University of Amsterdam showed no difference in Pirate Bay Internet traffic after the ban.[37]

40 The judge briefly addressed whether the current measure was necessary in a democratic society (cf. Article 10 ECHR). He referred to the proportionality and subsidiarity considerations just discussed, in particular regarding the interests of the subscribers in relation to the copyright holders. One might claim that the necessity considerations should at least include how the entertainment industry operated during the last 15 years.[38] Another point that could have been covered is what role access providers should have on the Internet. The outcome might still have been the same, but it would have been better grounded.

41 The judge ordered Ziggo and XS4ALL to block a list of 24 websites (of which several were outdated at the time of the verdict, and others later became outdated), as well as three IP addresses. It is curious that BREIN was granted the right to change the list anytime they believe it is necessary, without judiciary intervention. One could argue that the judge did not really take notice of the particular sites anyway, but in a trial opponents have the opportunity to object. Ziggo and XS4ALL now have to start a new trial if they do not agree with a particular IP address or website. If they do not comply, they have to pay a daily fine. The verdict does not pay attention to possible errors on BREIN's side.

42 Both Ziggo and XS4ALL have appealed, but a decision is not expected before the end of 2013.

V. BREIN v other ISPs 2012/5-

43 Based on the verdict, BREIN asked other ISPs to voluntarily start blocking The Pirate Bay. Since the ISPs refused, BREIN started new proceedings against other big providers, including KPN, UPC, T-Mobile and Tele2.[39] The verdict is lengthy but does not add much. A difference from the original verdict is that BREIN is not allowed to change the list of sites and IP addresses. The Pirate Bay has over 100 different IP addresses and has already announced that it might add one IP address at a time, meaning that BREIN would have to start over one hundred different procedures. Maybe, this Pirate Bay policy can change subsequent verdicts on this point.

44 One interesting observation is on the effectiveness of the blocking. The ISPs introduced the previously mentioned research by the University of Amsterdam[40] showing that the blocking did not have any effect. The judge stated: '[B]locking as such does not necessarily lead to less Pirate Bay traffic, but effectively combating infringements is possible only if this blocking is combined with other measures'.

45 This is a somewhat curious observation, in particular since one of BREIN's claims from the beginning has been that the blocking has at least some effect and as such contributes to fighting copyright infringements. Therefore, the argument is that the measures are a necessary element that works in combination with other measures. One of those other measures is to forbid proxy servers. In the course of 2012, BREIN sued a series of organizations and people that offered proxy servers, and did so ex parte.[41] One of the controversial cases was against the political Pirate Party. Although legally interesting and socially relevant, these cases are not within the scope of the present paper since it does not concern access providers.

D. What role fits access providers best?

46 The decisions discussed above are certainly not exclusive to the Netherlands. On 1 May 2012, the High Court in the United Kingdom ruled that the major ISPs in the UK must block access to The Pirate Bay. As the providers themselves noted, they do not want to be the judge and the jury of online content. Copyright-infringing material is the prime example of content ISPs are asked to intervene with and central in this paper.

47 The interest in ISPs commenced before the DMCA and Directive on E-commerce were enacted. Back in 1995, ISPs were considered to be the party most suited to control the dangers of the Internet; in fact, 'a task force created by President Clinton suggested imposing strict liability on ISPs'.[42] Moore & Clayton capture the complexity of ISP liability,[43] but recognize how '(...) ISPs are in an unrivalled position to suppress content held on their systems'.[44]

48 Before answering what role best fits the access provider, we will discuss ISP liability both related to Internet traffic (spam, cyber security) and concerning content (defamation, privacy breaches, child porn).[45] For each of these topics we will introduce a rule of thumb that can help ISPs in their decision whether to comply with a request.

I. Cyber security and spam: ISPs take initiative

49 In the field of cyber security, ISPs have realized over the years that it is in their best interest to act. The same is true for spam. If ISPs did not use spam filters, probably no one would use e-mail any longer. Can ISPs still claim to be neutral if they actively act, as in filtering spam or eliminating malware?

50 In a famous Dutch case, the Supreme Court judged on the position of an ISP in the case of spam.46 XS4ALL asked the direct marketer Ab.fab to stop sending spam to their customers. Ab.fab did not. Some argued that ISPs would lose their neutral position should they be allowed to reject messages. The Supreme Court decided that an ISP had the right to ask a party to stop sending spam.[47] The basic argument was that a provider is the owner of the mail server, and if the provider has good reason to not want to process specific mails, the provider does not have to. Ab.fab was ordered to stop sending e-mail. Ironically, before the Supreme Court ruled, Ab.fab had already gone bankrupt. The principle question still stood, however: Does the nature of the Internet and the role of ISPs in it conflict with asking a company not to send unsolicited email? As with all rules or principles, exceptions apply. To draw a parallel, if a football stadium is open to the general public, some people causing trouble might be banned from the stadium. After such a measure, the stadium is still open to the general public. In the case of ISPs, certain traffic can be banned from their servers without ISPs losing their neutrality. A similar argument applies to malware and other security measures.

51 In 2004, Lichtman and Posner called for an increased liability, and claimed that since ISPs are largely immune from liability, they have no incentive to act.[48] Harper attacked this proposal by pointing at a fundamental flaw: '[I]t places efficiency ahead of justice. The Internet is a medium, not a thing, and the supply of access to it is peculiarly unsuited to a liability rule like Lichtman proposes.'[49]

52 Nonetheless, Lichtman and Posner's position has been supported by the United Kingdom House of Lords Science and Technology Committee, for example, which stated in 2007 that '(...) although ISPs could easily disconnect infected machines from their networks, there is no incentive for them to do so'.[50]

53 Others echo similar notions. Chandler writes: 'The parties best placed to address cyber insecurity, including (...) ISPs (...) do not face the full consequences of their contributions to cyber insecurity. Accordingly, they do not invest time and money to the socially optimal level of improved security'.[51]

54 Van Eeten & Bauer challenge this assumption: ISPs may '(...) unwittingly reinforce the impression that they have few if any incentives to improve the security of their services'.[52] This occurs through the resistance of ISPs to government intervention and the hesitance to surrender self-regulation. The resistance to government intervention is interpreted by many as an unwillingness to provide more security; yet this is an incorrect conclusion according to Van Eeten & Bauer. The efforts made by ISPs to improve the security of their clients started to escalate during the last decade when ISPs began to understand how improved security turned out to be in their best interest. This is due to costs associated with the insecurity of their clients.

55 As follows from the above discussion on spam and cyber security, ISPs do take initiatives that in themselves go beyond the neutral role of mere transport because they influence their core activities. Both spam and malware directly negatively influence the (access) services. Their aim is to guarantee a properly functioning Internet, in particular access that is not hindered by unwanted (spam) and the undesired (malware) activities of others. This is what justifies their actions. The more these actions by ISPs are related to their core activities, the less influence such actions have regarding their neutral position. In the end it should be the decision of the ISP, and not one imposed by government, for example. Because the decision is up to the ISP, and what they do is objectively good for their users, they can uphold their basic neutral position.

II. Requests related to content: child porn, defamation and right to be forgotten

56 If ISPs have no incentive, external pressure could work. Access providers are in a position to influence what is communicated over the Internet.

57 One should be very cautious in asking assistance from ISPs. The fact that it is technically possible does not make it legally desirable. Let us assume that there is a public meeting room in a building that is hired by a politically motivated group of people. During this meeting, a defamatory poster is put on the wall. Some of the attendees inform the person who is defamed by the poster. He goes directly to the meeting and asks the people in the room to remove the poster. They do not. The defamed person goes to the owner of the room to ask for removal of the poster. If the owner chooses not to do so, can he be held liable? This is a very difficult decision for the third party to make. He has to balance freedom of expression against its possible defamatory nature. Whilst this situation is already difficult to navigate, what about the owner of the meeting room being asked to

block access to the room because of the poster? This is even more difficult to decide, for the impact is bigger. If entrance to the room is blocked, the people cannot have their meeting. This shows the indirectness of access blocking. The first level is asking the person who put the content there to remove it, the second level is asking the same of the hosting ISP, and the access provider only enters at the third level. When a judge orders that access be blocked to a particular website or IP address, this represents an indirectness acceptable only as a last resort. But a judge should be hesitant even then, because the nature of the Internet makes such measures both under- and over-inclusive.

58 Requests placed upon ISPs are often impractical and sometimes even illegitimate. The study carried out by Stol et al. on child pornography and Internet filtering illustrates the difficult position of ISPs and the importance of solid legal analysis.[53] As Stol et al. conclude,

> *[f]rom the point of view of constitutional law it is not acceptable that the authorities make use of instruments without sound legal basis in order to reach an otherwise legitimate goal. If the legislature's intention is to designate the blocking of child pornography as a duty of the police, then this should be provided in specific legal jurisdiction.*[54]

59 It has been argued by Dommering[55] that a sound legal defense is impossible. The Dutch Constitution does not permit control in advance (censorship), and this filtering prevents the assessing of particular content. A rebuttal here is that the filtering takes place only on the basis of lists of websites and IP addresses where child porn was already found, so in this respect the control is afterwards and not preventive. However, the Internet changes very quickly, and lists become outdated fast. One can never be sure what exactly is filtered.

60 Privacy breaches are another content-related topic often taking place on the Internet. Also, the Internet hosts various outdated personal information or information one simply does not want to be confronted with any longer. It is not always easy to get this information offline. In a recent proposal, the European Union introduced the right to be forgotten.[56] Again, ISPs are asked to co-operate, which is complicated since they find themselves in the midst of a conflict of interest between freedom of speech and the right to privacy.[57] The one who has published the information is the first point of contact, with the hosting provider coming second. One could imagine that access providers would be asked to block certain content if these first two steps do not work.

III. Copyright infringement: external and preventive actions

61 A couple of years ago the discussion focused on the necessity of increased liability for ISPs; currently ISPs are just asked to carry out certain actions. The Dutch lawsuits by BREIN discussed above are a prime example, as is the French HADOPI law.[58] The background of HADOPI's 'three strikes and you're out', introduced in 2009, is fighting copyright infringements. ISPs play a central role; for example, after a first notice the ISP is to actively monitor the suspect, and after the third 'strike' the person in question is blacklisted. The provider of the violating user as well as other ISPs are to ban the user for a fixed period of up to one year. This means that instead of blocking content, the access provider is to cut off an individual from the Internet. Besides the potential conflict with human rights,[59] this demands from the access provider the enforcement of norms that diametrically oppose their core activity: providing Internet access to people.

62 Of a different nature was the 2011 initiative involving some of the biggest American providers; without any act or verdict, they voluntary agreed to become 'copyright cops'.[60] Probably these providers had reasons to act as such, but it puts their neutral role under pressure. It is difficult for these providers to claim that they do not have to co-operate due to their neutral position if asked by private parties or government to intervene, either repressively or preventively, in cases of digital piracy.

63 There is an important distinction to be made here: on the one hand are ISPs acting voluntarily; on the other hand are ISPs being forced. Just as in cases of child porn, government should not force ISPs to block access, but ISPs may do it on their own initiative. However, once you act freely, you can no longer claim to be neutral as far as similar content is concerned. Once ISPs are more than passively involved with the communication or the flow of information, they cannot rely on the safe harbors created by law. This does not make them necessarily liable, but there is no longer an easy way out. The same is true for access providers: once you voluntary search for copyright violations, for example, third parties can ask you to do so, too.

IV. Statutes and judges

64 We discussed Dutch cases that led to various court orders forcing access providers to block The Pirate Bay. In contrast to what is currently happening within the EU, the US cannot count on the judiciary when it comes to blocking websites. The conditions as formulated in the DMCA/OCILLA, for example, are simply too difficult to meet. That is one reason

why the music industry is trying to get acts pushed through the American Congress. Basically, getting a bill passed is more difficult than convincing a judge. Judges are not elected in the Netherlands (and in most, if not all, EU countries), so judges do not have to take public opinion into account. The US legal initiatives demonstrated that public opinion can influence the decision-making process of the legislature.

65 Recall that on 18 January 2012, over 7,000 websites, including Wikipedia and Google, successfully staged a blackout as a means to protest legislative initiatives introduced in both chambers of the United States Congress. These initiatives, the Stop Online Piracy Act (SOPA) and the Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act (PIPA), both aimed to curb digital piracy in the United States. The primary objectives of both bills was to promote prosperity, creativity, entrepreneurship and innovation by combating the theft of US property. Or, as the Economist put it more bluntly, '[t]he bill aims to cut off Americans' access to foreign pirate websites by squeezing intermediaries'.[61]

66 Beside the general public's opportunity to influence, focus is another difference between legislation and court cases. In court cases the focus is on a single actor (e.g. The Pirate Bay), which makes it easier to decide against him. Also related to focus, proposals for legislation are necessarily abstract, and likewise feel like more of a threat to the general public (e.g. it touches the whole Internet). One additional difference we want to note is that politicians appear to feel more sympathy for the economic arguments of the entertainment industry than judges are expected to. Finally, public opinion can provide correction during the legislative process, whereas in court cases public opinion basically starts only after the decision: only then does the outcome become clear.

67 The neutral position of access providers is no different when it comes to objecting against case law or against acts; only the means of maintaining that neutrality are different.

V. How to draw the line?

68 The list of requests access providers receive is long, so we are not able to discuss them all, such as data retention[62] or online porn blocking.[63] This expanding list, both in terms of what to do and how to do it, forces the need to re-evaluate what is being asked from access providers.

69 There are two basic camps. One camp stresses the importance of Internet freedom, innovation, the neutral role of providers, protection of freedom of speech and privacy. The other camp also stresses innovation, protection of rights and fighting crime. And as with all discussions, there are intermediate positions. We do take a position in this debate, but as with all legal debates – and particularly in those concerning Internet governance topics – we emphasize that there is no obvious right or wrong; instead, it is about balancing and weighing the pros and cons. In the fire of the discussion this is sometimes forgotten, but with sensitive issues it is important to keep this in mind: arguments matter, not who is defending them.

70 In drawing the line between the circumstances under which ISPs should be asked to cooperate and when it is better to leave them alone, at least the following should be taken into account.

71 First, consider the directness of the measure. In a way this is related to but not the same as the question of subsidiarity: if other less burdensome actions are possible, they should be preferred. Directness also concerns how related the proposed action is to the activities of the ISP. The more direct, the sooner action might be asked from ISPs. For instance, if someone wants to take material down, the first response is to go to the one who put it there, next to the hosting provider, and third to the access provider.

72 Second, consider the effectiveness of the measure. Each action serves a goal, but if the goal is hardly reached, someone might take independent action anyway and therefore should not ask this from others. If a measure is merely symbolic or the effects are insignificant, access providers should not be asked to cooperate. Basically, the more effect a measure has, the sooner action might be asked from ISPs. It might be that what is asked for is so important that even the slightest effect is worth carrying out the action. If that is the case, normally the action should be carried out unless the costs (not only financially) associated with the action are disproportional.

73 Third, consider the costs of the measure. This point is related to proportionality: the action should be in proportion to the severity of what is targeted. Again, the costs are not only financial but may also include effort or side effects. The lower the costs, the sooner action might be asked from ISPs. It may not become an argument in itself, or better, not the only argument. If an action scores badly on other aspects, and the only real argument is that it is easy for the access provider to fulfil the request, the ISP should not.

74 Fourth, consider relevance as related to the history of the ISP. If an ISP has cooperated voluntarily in past requests, or has taken independent actions related to what the ISP is now being asked to do, it is harder to refuse assistance. The more related the past activities of the ISP are to what the ISP is now being asked to do, the sooner action might be asked.

75 Fifth, consider the time element. Repressive actions do not concern censorship, whereas preventive actions do.[64] If content is taken down, the action is clearly repressive and concerns only the content taken down. In the case of repressive action, blocking access to websites might even turn into censorship. This has to do with the dynamic nature of the Internet. In the case of cybercrime, for example, assistance in blocking traffic to particular websites (cf. the black-listing of servers sending spam) may also filter out legitimate e-mail. Therefore, any list of sites blocked should be evaluated regularly.

76 Finally, and this is an overreaching element, adequate safeguards should be in place. The points indicated above already imply warranties. In addition, for any action asked from ISPs, there should be a sound legal ground. It is important to rule out arbitrariness. Judiciary intervention can also be part of the safeguards. For instance, at the wrong side of this boundary are black box lists of websites so that ISPs do not know what they are filtering or lists of websites created without judicial intervention.

E. Concluding observations

77 In January 2012, a 10-year-old Dutch boy (and obviously many others) could no longer download legal software via his favourite website. This was not because the Court of The Hague had ordered two providers to block The Pirate Bay on January 11, or because SOPA, PIPA or ACTA had entered into force. Instead, it appeared that the US Department of Justice had taken the file-hosting site Megaupload offline. Ironically, or sadly, this was exactly one day after Wikipedia had staged a blackout to protest the SOPA and PIPA initiatives.

78 The Megaupload case is an interesting example of the strong – or better: long – arm of the law. People (such as Kim Dotcom) were arrested by the FBI in New Zealand, amongst others. The link between Megaupload and the US was not clear. Sure, the Internet is accessible all over the world, and information on a website basically enters all jurisdictions.[65] The reason, however, for the US action was that the people behind Megaupload were accused of running an international criminal organization, not only facilitating copyright infringements but also laundering money. This begs the question: Why ask dozens, hundreds, or maybe even thousands of access providers to filter out websites if one action against the provider of the website has the same result?

79 As the discussion of the Pirate Bay case revealed, it is not always easy to take a website offline. In the case of The Pirate Bay, successful court actions only led to shifting from hosting providers in one country to hosting providers in another country, lastly Ukraine.[66] So the call on access providers is comprehensible. Under certain circumstances they could be asked to assist. In this paper we introduced rules of thumb that could help in deciding whether an access provider should cooperate:

3. The more direct the requested action is, the sooner action might be asked from ISPs.

4. The more effect a measure has, the sooner action might be asked from ISPs.

5. The lower the costs, the sooner action might be asked from ISPs.

6. The more related the ISP's past activities are to what the ISP is asked to do, the sooner action might be asked.

7. Repressive action is preferred over preventive, and preventive action needs regular re-evaluation.

80 Notably, adequate safeguards should be in place, in particular a sound legal basis for action. From the US perspective, Lemley, Levine & Post stated:[67]

> *United States law has long allowed Internet intermediaries to focus on empowering communications by and among users, free from the need to monitor, supervise, or play any other gatekeeping or policing role with respect to those communications. Requiring Internet service providers (...) to block access to websites because of their content would constitute a dramatic retreat from that important policy.*

81 We hope that the appeal cases in the Netherlands have outcomes other than that of the first instance decisions. The US policy just described should be enforced (again) in the Netherlands as well as within other European Union countries. Access providers should not be forced to check lists of websites, IP addresses and the like, for it concerns the opposite of what their role should be: providing access. An intermediary basically helps to connect two parties. We should not shut down train stations when the actual threat is somewhere down the line; otherwise we are heading in a direction we do not want to go.[68]

Endnotes

1 The Dutch phrase is often used to emphasize the neutral position of Internet service providers with a difficult-to-translate repetition of words: 'geen boodschap aan de boodschap'.

2 112 STAT. 2860 PUBLIC LAW 105–304—OCT. 28, 1998, 105th Congress. An Act to amend title 17, United States Code, to implement the World Intellectual Property Organization Copyright Treaty and Performances and Phonograms Treaty, and for other purposes. The present paper covers one of the 'other purposes', limitations on liability for ISPs.

3 Directive 2000/31/EC on electronic commerce; see above, footnote 4.

4 For an extensive overview of case law ruled under both initiatives, see M. Martinet Farano (2012), Internet Intermediaries' Liability for Copyright and Trademark Infringement: Reconciling the EU and U.S. Approaches, TTLF Working Papers No. 14.

5 M. Norrgård (2011), Blocking Web Sites – Experiences from Finland, <http://ssrn.com/abstract=1997103>.

6 The High Court of England and Wales ruled on 30 April 2012 after claims from the British Phonographic Industry (BPI) that five ISPs (Sky, Everything Everywhere, TalkTalk, O2 and Virgin Media) should block the Pirate Bay; see e.g. Huffington Post 30 April 2012, <http://huff.to/OGhD5m>.

7 P.K. Yu (2011), Six Secret (and Now Open) Fears of ACTA. SMU Law Review, Vol. 64, pp. 975-1094, 2011.

8 M.A. Carrier (2012), Copyright and Innovation: The Untold Story. Wisconsin Law Review, Forthcoming. Available at SSRN: <http://ssrn.com/abstract=2099876>.

9 Cyber Intelligence Sharing and Protection Act, Passed the US House of Representatives on 26 April 2012. See <http://thomas.loc.gov/cgi-bin/query/z?c112:H.R.3523>. It is uncertain whether the US Senate will accept the bill; if it does, President Obama has indicated he will not sign it.

10 H.R. 624: Cyber Intelligence Sharing and Protection Act, accepted on 18 April 2013, <http://www.govtrack.us/congress/votes/113-2013/h117>.

11 The access provider was not explicitly mentioned in the two main 1990s regulations; instead, it is commonly designated as a mere conduit (EU Directive) or as transitory communications (DMCA); see further below the section Early days: DMCA and Directive on E-commerce.

12 H.W.K. Kaspersen, Liability of Providers of the Electronic Highway, 12 The Computer Law and Security Report 2006: 290-293.

13 M. Schruers (2002), The History and Economics of ISP Liability for Third Party Content, Virginia Law Review, Volume 88, No. 1, pp 205-64.

14 S. Ardia (2010), Free Speech Savior or Shield for Scoundrels: An Empirical Study of Intermediary Immunity Under Section 230 of the Communications Decency Act. Loyola of Los Angeles Law Review, Vol. 43, No. 2, 2010.

15 Reese nicely characterizes the nature of the exemptions: 'Congress has enacted, in section 512 of the Copyright Act, limitations on the liability of service providers, but conditioned those limitations on a fairly complicated set of conditions.' R.A. Reese, The Relationship between the ISP Safe Harbors and Liability for Inducement. Stanford Technology Law Review, Vol. 8, 2011.

16 R. J. Mann and S.R. Belzley, The Promise of Internet Intermediary Liability. William and Mary Law Review, Vol. 47, October 2005.

17 As defined in § 512 subsection (j).

18 Proposal for a EUROPEAN PARLIAMENT AND COUNCIL DIRECTIVE on certain legal aspects of electronic commerce in the internal market, 18.11.1998, COM(1998) 586 final, p. 3.

19 'A European Initiative on Electronic Commerce', COM(97) 157 final, 16.4.1997.

20 Recital 16 DIRECTIVE 2001/29/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society, OJ, 22.6.2001, L 167/10. The proposal for this Directive was published 10 December 1997, almost a year before the E-commerce Directive: 18 November 1998. The final text, however, was published one year later (June 2000 and June 2001 respectively). The Member States had far more problems agreeing on how to regulate copyright on the Internet than they had to agree on how to regulate e-commerce. For a discussion of this Directive, see M. Vivant (2002), Directive 2001/29/EC on the harmonisation of certain aspects of copyright and related rights in the information society, in Lodder, A.R., Kaspersen, H.W.K. (eds.), eDirectives: Guide to European Union Law on E-Commerce , Kluwer Law International, The Hague, p. 95-117.

21 Proposal for a EUROPEAN PARLIAMENT AND COUNCIL DIRECTIVE on certain legal aspects of electronic commerce in the internal market, 18.11.1998, COM(1998) 586 final, p. 4.

22 At that time some case law already existed on ISP liability. For instance, in the Netherlands a lower court had already ruled on 12 March 1996 in a lawsuit with the Scientology Church and the Dutch ISP XS4ALL (for a translated version of the summons, see <http://kspaink.home.xs4all.nl/cos/dag1eng.html>). The case law was one of the reasons why the European Union considered it necessary to regulate the exemptions to liability: 'to eliminate the existing legal uncertainty and to bring coherence to the different approaches that are emerging at Member State level'. The final ruling by the Dutch Supreme Court on 16 December 2005 (LJN: AT2056) in the abovementioned Scientology v XS4ALL case is one of the few cases where the freedom of speech prevailed over copyright law.

23 V. McEvedy (2002), The DMCA and the Ecommerce Directive, E.I.P.R. 2002, 24(2), 65-73.

24 Proposal for a EUROPEAN PARLIAMENT AND COUNCIL DIRECTIVE on certain legal aspects of electronic commerce in the internal market, 18.11.1998, COM(1998) 586 final, p. 4.

25 As is well known, these measures are not necessarily effective since circumvention is often quite easy.

26 Section 512(c)(3) of the DMCA.

27 P. Balboni et al. (2008), Liability of Web 2.0 Service Providers – A Comparative Look, Computer Law Review International Issue 3, pp. 65-71.

28 § 512 (j)(2): 'The court, in considering the relevant criteria for injunctive relief under applicable law, shall consider—(A) whether such an injunction, either alone or in combination with other such injunctions issued against the same service provider under this subsection, would significantly burden either the provider or the operation of the provider's system or network; (B) the magnitude of the harm likely to be suffered by the copyright owner in the digital network environment if steps are not taken to prevent or restrain the infringement; (C) whether implementation of such an injunction would be technically feasible and effective, and would not interfere with access to noninfringing material at other online locations; and (D) whether other less burdensome and comparably effective means of preventing or restraining access to the infringing material are available.'

29 M. Peguera (2009), The DMCA Safe Harbors and Their European Counterparts: A Comparative Analysis of Some Common Problems. Columbia Journal of Law & the Arts, Vol. 32, p. 481-512.

30 Subsequently, in February 2012, the Swedish Supreme Court decided not to grant leave on appeal, and the case is now at the European Court of Justice.

31 Court of Amsterdam, 30 July 2009, LJN BJ4298, <www.rechtspraak.nl/ljn.asp?ljn=BJ4298>.

32 Court of Amsterdam, 22 October 2009, LJN BK1067, <www.rechtspraak.nl/ljn.asp?ljn=BK1067>.

33 Court of The Hague, 19 July 2010, LJN BN1445, <www.rechtspraak.nl/ljn.asp?ljn= BN1445>.

34 Court of The Hague, 11 January 2012, LJN BV0549, <www.rechtspraak.nl/ljn.asp?ljn= BN1445>.

35 Judgment of the Court (Grand Chamber) of 12 July 2011. L'Oréal SA and Others v eBay International AG and Others. Case C-324/09.

36 Judgment of the Court (Third Chamber) of 24 November 2011. Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM). Case C-70/10. The filtering asked for was far-reaching; see under 40: 'filtering system would require: first, that the ISP identify, within all of the electronic communications of all its customers, the files relating

to peer-to-peer traffic; secondly, that it identify, within that traffic, the files containing works in respect of which holders of intellectual-property rights claim to hold rights; thirdly, that it determine which of those files are being shared unlawfully; and fourthly, that it block file sharing that it considers to be unlawful'.

37 A report in Dutch by the System and Network Engineering research group is available at <http://bit.ly/S9xcCZ>, J. van der Ham et al. (2012), Review en Herhaling BREIN Steekproeven, 7-9 April 2012.

38 See e.g. D.Y. Choi & A. Perez (2007), Online Piracy and the Emergence of New Business Models, Technovation, Volume: 27 Issue: 4 pp. 168-178.

39 Court of The Hague, 17 April 2012, LJN BW3596, <www.rechtspraak.nl/ljn.asp?ljn= BW3596>.

40 See note 40.

41 For a discussion of the Dutch ex parte practice, see Ex parte decision against The Pirate Bay proxy causes controversy on Future of Copyright: <http://bit.ly/UgmcVj>.

42 Mann & Belzey 2005, see note 11.

43 T. Moore & R. Clayton (2008), The Impact of Incentives on Notice and Take-down. Workshop on the Economics of Information Security (WEIS).

44 Ibidem.

45 G. Sutter (2003): 'Don't Shoot the Messenger?' The UK and Online Intermediary Liability, International Review of Law, Computers & Technology, 17:1, 73-84.

46 Dutch Supreme Court, 12 March 2004, LJN AN8483 (XS4ALL v. Ab.Fab).

47 At that time the EU Directive 2002/58 on electronic communications had been enacted, and included an Article that banned spam in the EU, at least spam sent to natural persons.

48 D.G. Lichtman & E.A. Posner, Holding Internet Service Providers Accountable (July 2004). U Chicago Law & Economics, Olin Working Paper No. 217, <http://ssrn.com/abstract=573502>.

49 J. Harper (2005), Against ISP Liability. Regulation, Vol. 28, No. 1, pp. 30-33, Spring 2005.

50 House of Lords: Science and Technology Committee (2007) Personal Internet security: 5th report of session, Vol. 1: Report: 30.

51 J.A. Chandler. Liability for Botnet Attacks. Canadian Journal of Law and Technology (2006), Vol. 5: 1.

52 M.J.G.van Eeten, & J. M. Bauer. Economics of Malware: Security Decisions, Incentives and Externalities. STI Working Paper 2008/1: 26.

53 Stol, W.PH., Kaspersen, H.W.K., Kerstens, J., Leukfeldt, E.R. & Lodder, A.R. (2009). Governmental filtering of websites: The Dutch case. Computer, Law & Security Review, 25(3), 251-262.

54 Ibidem. What happened in the Netherlands was that the police provided a list of sites to be blocked by ISPs. Only the ISPs could see the sites that were on the list. In the research by Stol et al. it appeared that this was not updated regularly, contained websites that did not distribute child porn, and of course missed many sites that did not. An additional problem with the initiative is that child pornography is hardly disseminated via public websites. The constitutional argument against this co-operation between police and ISPs was that the police asked ISPs to filter Internet traffic, which is something the police would not be legally allowed to do. After the publication of the research, the police stopped the co-operation with ISPs.

55 E. Dommering (2008), Filteren is gewoon censuur en daarmee basta (Filtering is always censoring), Tijdschrift voor Internetrecht.

56 In Section 3, Rectification and Erasure, Article 17 (Right to be forgotten and to erasure) in COM(2012) 11 final, 25 January 2012, Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation).

57 G. Sartor (2012), Providers' Liabilities in the New EU Data Protection Regulation: A Threat to Internet Freedoms?, <http://ssrn.com/abstract=2047428>.

58 HADOPI is also known as the Creation and Internet Law and (freely translated) stands for High authority for the dissemination of works and the protection of rights on the Internet (in French: Haute Autorité pour la diffusion des oeuvres et la protection des droits sur Internet); <http://www.hadopi.fr/>.

59 Several countries acknowledge a fundamental, constitutional Internet access right.

60 <http://news.cnet.com/8301-31001_3-20077492-261/top-isps-agree-to-become-copyright-cops/>.

61 Rights and wronged: An American anti-piracy bill tries to stem the global theft of intellectual property, <http://www.economist.com/node/21540234>.

62 F. Bignami (2007), Privacy and Law Enforcement in the European Union: The Data Retention Directive, 8 Chicago Journal of International Law, Spring 2007, p. 233-255.

63 More than a third of Britons support online porn blocking, Daily Telegraph, August 19 2012, <http://bit.ly/S84SiK>.

64 For an overview of Internet filtering practices in Africa and Asia some years ago, see R. Deibert et al. (2008)(eds.), Access Denied, The MIT Press, Cambridge, Massachusetts.

65 A similar development is found in UK courts convicting people posting defamatory statements on Twitter, see e.g. Eurotech 28 March 2012 <http://bit.ly/QEvqFN>: 'Now get this clear: someone from New Zealand feels insulted by an Indian official through a statement posted on Twitter which has its shiny new headquarters in San Francisco. Why would a British judge even accept this case?'

66 Even a drastic action as in the Megaupload case would not have succeeded, since the US can shut down generic top-level domains (.com, .org) but not top-level country domains (piratebay.se).

67 M. Lemley, D.S. Levine & D.G. Post, Don't Break the Internet, 19 December 2011, 64 Stan. L. Rev. Online 34.

68 It could be the first slip on a slippery slope. See M. Schellekens, 'Liability of Internet Intermediaries: A Slippery Slope?', (2011) 8:2 SCRIPTed 154, who argues this is not the case.