From Neutral Thirds to Private Law Enforcers:  
Toward a Criterial Framework for Requests Placed on Internet Service Providers

Nicole S. van der Meulen & Arno R. Lodder  
Vrije Universiteit Amsterdam

*DRAFT*

Abstract

Undeniably the traditional neutral role of ISPs has come under increasing pressure. This is mainly a result of the requests placed on them which are becoming more diverse and far reaching. ISPs are called upon to lead the fight against botnets, combat digital piracy and child pornography, amongst other things. These requests placed upon ISPs are often impractical and sometimes even illegitimate. The primary research objective for this contribution is an analysis of a number of themes which invoke the involvement of ISPs. In particular, we want to make an inventory of the thematic justifications used for the requests. Basically, what interest are ISPs asked to defend and how do these relate to their role within the realm of internet governance? The outcome of this analysis is the development of a preliminary criterial framework for requests placed on ISPs.

1.1 Introduction

On January 18, 2012, over 7,000 websites, including Wikipedia and Google, successfully staged a blackout as a means to protest against legislative initiatives introduced in both chambers of the United States Congress. These initiatives, the Stop Online Piracy Act (SOPA) as well as the Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act (PIPA), both aimed to curb access to digital piracy in the United States. According to their sponsors, the primary objective of both bills was to promote prosperity, creativity, entrepreneurship, and innovation by combating the theft of U.S. property. Or, as the Economist (2011) put it more bluntly, “[t]he bill aims to cut off Americans’ access to foreign pirate websites by squeezing intermediaries.” These intermediaries proved quite displeased by both bills, as the blackout demonstrated. The blackout became a vivid example of the growing tension between internet intermediaries, on the one hand, and others, primarily in the private sector, on the other hand. The conflict is often referred to as Silicon Valley vs. Hollywood. As Lipton (2012: 1344) describes: “[i]dentifying the role of Internet intermediaries in terms of their legal responsibilities is in many ways the foundational challenge of cyberlaw.” She continues by stating how “[t]he legal challenges that are unique to cyberspace law and that differentiate cyberlaw from other fields arise from the ways in which, and extent to which, legislatures and courts are prepared to impose liability on intermediaries for online conduct initiated by others.”

Due to the increasing demands placed on Internet Service Providers (ISPs), from preventing copyright infringements to actively combatting child pornography, they no longer restrict themselves to their primary task of providing internet access. The primary objective for this contribution is an inventory and analysis of the different themes ISPs are called upon to assist with. Up until this point, there is a lack of overview of the themes since they are mainly treated in a fragmented way. The particular focus is on the (legal) justification used to implicate the ISPs and what they are asked to do. Basically, what interest are
ISPs asked to defend and why? The outcome of this analysis provides input for a preliminary criterial framework for requests placed on ISPs.

This paper begins with a discussion on the definition and classification of ISPs. The next section provides an overview of the different themes used to ask and sometimes require ISPs to act. The following section briefly reflects on the fear of potentially going down a slippery slope. Based on these themes and existing regulation with respect to ISPs, we introduce a preliminary criterial framework. This framework should then be the start of the ability to classify requests as acceptable, questionable and unacceptable with the intent to prevent a potential slippery slope.

1.2 Definition of ISPs

The concept of Internet Service Provider seems to be evolving into an umbrella term. Suddenly, the concept is no longer reserved for access and host providers, but also includes companies such as Google, Facebook, Wikipedia and Twitter, amongst others. This development is causing considerable obfuscation for the debate on roles and responsibilities of ISPs, especially since they all maintain a different service character. Especially with respect to the topic addressed in this paper, the increasing demands placed on ISPs. In order to tackle this problem, this paper makes a distinction between the broad and the narrow approach to the concept of ISPs. The broad approach includes companies, which provide services on the internet. As a result, these include Google and the others previously mentioned. The narrow approach focuses on access providers, hosting providers and mere conduit/transitory. The primary focus within this paper is on the narrow approach to the concept of ISPs.

1.3 Overview of themes

In the introduction, we posed the question what interests are ISPs asked to defend and why? This section aims to give an overview of these interests, or rather themes, which are used as a justification to call upon ISPs to take action. Actions may include filtering content, blocking access, either of a particular site or in general or something else. The focus is on the thematic justification, since these are used as a means to an end, action on the side of the ISP. To focus on the action in abstract simplifies the debate and makes ISPs ill-prepared to counter arguments. This is because the actions in and of themselves, filtering content and blocking access or even quarantining users, fall within the technical capabilities of ISPs. Moreover, as shall become evident in the sections on spam and botnets, ISPs do sometimes bring these capabilities into practice. ISPs, after all, also initiate actions themselves, which fall within the same categories in terms of the technical measures. The distinction therefore is in the reasoning or the rationale to implement such measures, which primarily lies within the thematic justification used. To distinguish based on thematic background is therefore a vital ingredient to the overall discussion. We distinguish the following themes: Intellectual Property Rights, Child Pornography, Terrorism, Protection of Children, Botnets and Spam. The last example, Spam, is an area where ISPs have initiated action themselves but is important to discuss in light of the overall development of a criterial framework. This list in not meant to be exclusive, but does feature some of the most prominent examples.

1.3.1 Intellectual property rights

Intellectual property rights, in particular copyright infringements, are without a doubt among the most debated issue with respect to ISPs. Many years ago, as the Internet boom was still in its relative infancy,
legal efforts to regulate ISPs even maintained a primary focus on copyrights, at least in the United States through the US Digital Millennium Copyright Act (DMCA). The DMCA actually meant to limit liability of ISPs and to install a procedure of notice and takedown to facilitate its process. Even so, as copyright violations continue, the tension also continues to grow. Meyer (2012: 112) writes, “...as piracy levels remain high the role of Internet service providers (ISPs) – so far mainly limited to notice and takedown procedures – is questioned in favor of proactive involvement. Filtering techniques, such as deep packet inspection of online content, are also advocated as a viable means of detecting and removing illegally distributed works.”

This was certainly the case when France introduced its infamous Hadopi legislation in 2009. Through this legislation, ISPs as well as their clients were introduced to the concept of graduated response. The graduated response includes the following steps. When HADOPI, the agency responsible for the execution of the regulation, receives a complaint from a copyright holder or representative, it may commence its three-strike procedure, often referred to as the graduated response. The first step is an email sent to the subscriber. This email is sent based on the IP-address connected to the claim. After this first step, HADOPI requires ISPs to monitor the internet connection of the subscriber. And the subscriber may install a filter. When the subscriber violates the copyright law again, he will receive a certified letter, once again warning him of the violation. If within the year, he engages in another copyright violation and continues to do so, HADOPI requests the ISP to suspend the internet access of the violator, anywhere between two months and one year.

This pro-active involvement of ISPs is generally met with considerable resistance, both from providers as well as subscribers. The graduated response, however, has also become a topic in the United States, where ISPs have agreed to a ‘voluntary graduated response scheme.’ Instead of three strikes, however, the ISPs have introduced a five-strike plan, but overall the idea is the same. Whilst the plan is labeled as voluntary, both Hollywood and the music industry certainly provided sufficient nudges to move this plan from idea to implementation. On July 1, 2012, several of the major ISPs in the United States commenced the activities of their five-strike plan. The “graduated response” is also used in other jurisdictions such as Taiwan, South Korea and New Zealand.

In other countries, ISPs are also called upon to take a pro-active stance to defend the rights of copyright holders as well as their representatives. The Pirate Bay is a prime example of a site, which has become the center of attention in a variety of court cases throughout the last several years.

1.3.1.1 Pirate Bay

The Belgian Anti-Piracy Foundation (BAF) pressed charges against two ISPs, Belgacom and Telenet, requesting the blockage of the Pirate Bay. In July 2010, the Antwerp Commercial Court rejected the claim, considering the demand to block as disproportionate and unnecessary. The following year, however, the Belgian Court of Appeal of Antwerp decided that the two providers had to block access of their users to the Pirate Bay. The last verdict obliged Telenet and Belgacom to set up DNS blocking for 11 URLs of the Pirate Bay within two weeks after the decision.

A similar situation found place in the Netherlands, where in 2012 the Dutch anti-piracy organization BREIN, a foundation which aims to enforce intellectual property rights for the entertainment industry, obtained several court orders that forced ISPs to block access to the Pirate Bay. BREIN first focused itself exclusively on the largest ISP in the Netherlands, Ziggo. XS4ALL joined the case, due to the looming danger of a potential verdict leading to a worrisome precedent. In its decision, the judge ordered Ziggo
and XS4ALL to block a list of 24 websites (of which several were outdated at the moment of the verdict, and others later became outdated), as well as three IP addresses. More importantly, however, is that BREIN received the right to change the list anytime they believe it to be necessary, without judiciary intervention. Certainly, one could argue that the judge did not really take notice of the particular sites anyway, but in a trial at least the opponents have the opportunity to object. Ziggo and XS4ALL can now only follow an order, and start a new trial if they do not agree with a particular IP address or website. If Ziggo or XS4ALL fails to comply they have to pay a daily fine, if BREIN makes a mistake there is no specific consequence described in the verdict.

In its claim, the attorneys representing BREIN refer to existing blockades for spam and viruses and demand an extension of such a blockade to include websites, which infringe upon copyrights. Before this decision, the judiciary refused to agree with BREIN since such a measure failed to meet the criteria of subsidiarity and proportionality. In this verdict, however, the judge indicated that after the lawsuits against the Pirate Bay and the hosting providers, asking access providers was the logical next step. On the proportionality question, the judge indicated that given the amount of illegal as opposed to legal content on the site, the interests of the copyright holders outweigh the interests of the internet users. Basically, ISPs are required to defend the interests of copyright holders against the interest of their own users.

BREIN’s original idea was that with a verdict against one provider, the others would follow. This idea failed. Based on the verdict, BREIN asked other ISPs to start blocking The Pirate Bay voluntarily. Since the ISPs refused, BREIN started new proceedings against other big providers, viz. KPN, UPC, T-Mobile, and Tele2. A difference with the original verdict is that BREIN is not allowed to change the list of sites and IP addresses.

Multiple objections have been raised against the verdict handed down against ISPs in the Netherlands. First, there is the question of blocking as a legitimate means for ISPs to play a part in the prevention of copyright infringements. Second is the question of effectiveness. The majority of those who understand the workings of the internet identify the ineffectiveness of the measure introduced by BREIN as a means to conquer digital piracy. The claim made by BREIN is how blocking is a method which can be effective in conjunction with other measures. For the judge, this was sufficiently convincing to concur with BREIN, despite research demonstrating the ineffectiveness of blocking by itself.

The verdict in the Netherlands is hardly exclusive. As previously noted, a similar verdict was handed down in Belgium. Other countries include Denmark, Sweden, Italy, Ireland, Finland and the United Kingdom. This is evidently a trend within the European Union, where court orders are easy to obtain and victory appears to be relatively easy to achieve. An important difference to note from a comparative perspective 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, the e-commerce directive sets no specific conditions (Peguera 2009) but generally states in Article 12(3):

“This Article shall not affect the possibility for a court (...) requiring the service provider to terminate or prevent an infringement.”

Hence, in the European Union, the industry turns to the judiciary whereas in the United States additional legislation often becomes the primary focus. All together, there is a general trend toward demanding a more pro-active approach to prevent copyright infringements online. As Hanley (2012: 186) notes, “[h]istorically, domestic (and foreign) legislation has required ISPs to take a passive-reactive
role in the battle against online copyright infringement, such that ISPs have only been obligated to react *ex post* to notices of infringement. However, some commentators believe that the role of ISPs has changed since the beginning of 2007. Their theory is that the ISPs, in reaction to increased pressure from entertainment industries, government legislators, and regulatory agencies, have become more actively involved, such that ISPs must police their networks to prevent copyright infringement *ex ante.*

1.3.1.2 iiNet

In other areas of the world, similar situations exist; at least with respect to private organizations requesting the blockage of sites for purposes of copyright infringements. In Australia, the inability of copyright defenders and ISPs to reach an agreement on a strategy to reduce unlawful downloads apparently led to the Australian Federation Against Copyright Theft (AFACT) bringing an action against iiNet, the third largest Australian ISP. In its claim, the AFACT alleges that iiNet was liable for copyright infringements of its users committed by means of the BitTorrent protocol. This is the first action to test the liability of ISPs in Australia, for infringements committed by its clients through P2P networks (Lindsay 2010). But unlike the verdicts handed down in the Netherlands and Belgium, amongst others, with regard to the Pirate Bay, the Highest Court of Australia ruled against AFACT. According to the Court, “[t]he appellants’ submission, that iiNet should be taken to have authorised the infringements unless it took measures with respect to its customers, assumes obligations on the part of an ISP which the Copyright Act does not impose.” The value in mentioning this case rests in the identification of obligations of ISPs. The appellant, as the Court notes, assumes obligations which are not imposed on ISPs. In its verdict, the Court therefore refers to the legislature and its task to alter that situation, if needed.

1.3.2 Child pornography

Child pornography is among the thorniest issues with respect to justifications for ISPs to act. As Moore, Clayton & Anderson (2009: 16) note, “[d]uring the 1990s, when the Internet came to public attention, policymakers established ‘child pornography’ as the one Internet evil that all governments could agree to ban.” This certainly complicated the position of ISPs, since they recognize the grave nature of the crime, but remain critical of the calls placed upon them for action. This critical stance is difficult to sell since there is the inherent assumption about child pornography that anything must be done to prevent its existence and its transmission. Certain countries and geographic areas voluntarily block access to child pornographic materials. The United Kingdom is a prime example where the major ISPs have installed blockades for sites posted on a blacklist issued by the Internet Watch Foundation (IWF).

At the European level, attempts to stop online child pornography date back to 1996. At that time, the European Commission (EC) adopted the Communication on Illegal and Harmful Content on the Internet (COM (96) 487 final) and the Green Paper on the Protection of Minors and Human Dignity in Audio-Visual and Information Services (COM (96) 483 final). Both documents argued how the international nature of the Internet would require a coordinated response from member states (McIntyre 2010).

More recently, a heated debate took place as the European Parliament, the Council and the Commission drafted a new version of the directive on combating sexual abuse, sexual exploitation of children and child pornography, in particular online. The original position of the European institutions was to make blocking of access to child pornographic material mandatory. Originally, article 21 of the draft stated: “Member States shall take the necessary measures to obtain the blocking of access by Internet users in their territory to Internet pages containing or disseminating child pornography.” Due to the resistance
offered against such a mandatory call, in part due to the ineffectiveness of the measure and the potential threat to internet freedom, the European Union watered down the ultimate version of the directive. Another concern expressed by ISPs is how these measures fail to eliminate child pornography and instead push it deeper into the underground of the internet, which means it is even further out of reach for potential law enforcement measures.

Besides the European level, member states themselves have also made attempts to call upon ISPs to implement means to filter and subsequently block content which contained child pornographic material. The Netherlands is an example in this regard. Stol et al. (2008) provide an overview of the historic background with respect to efforts to request ISPs to filter traffic to block child pornographic material. In 2006, Parliament filed a motion to research such possibilities.

ISPs resisted the calls to filter content as a means to block child pornography, despite the increasing pressure from, amongst others, the political arena and the media. The exception became UPC, which agreed to monitor in an effort to filter and block child pornographic material (Eggens 2007). This led to much criticism from the remainder of the ISP community. The debate died a slow death in the Netherlands, especially after legal research labeled the request to block as illegitimate (Stol et al. 2008). The police provided a list of sites to be blocked by ISPs. The ISPs could not see the sites that were on the list. In the research by Stol et al. (2008) it appeared that the list was not updated regularly, contained websites that did not distribute child porn and of course missed many sites that did. 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. As Stol et al. (2008: 6) 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.” After the publication of the research the police ceased co-operation with ISPs. During a debate in May 2011, the Minister of Justice, as well as the majority of Parliament, publicly recognized the ineffectiveness of filtering as a countermeasure against child pornography. This is not to say the filtering of child pornography will not return as a topic of discussion in political debate, either at the national or European level.

1.3.3 Terrorism

Ever since the events of September 11, 2001, as well as the bombings in Madrid and London, the War on Terror has been a means to justify many different measures and legislative initiatives. The primary example in the European Union is the data retention directive, which is directly relevant to ISPs. According to the directive, member states will have to store citizens' telecommunications data for six to 24 months stipulating a maximum time period. Under the directive the police and security agencies will be able to request access to details such as IP address and time of use of every email, phone call and text message sent or received. Permission to access the information will be granted only by a court. During the press conference held in light of the evaluation report of the data retention directive in 2011, Malström stated: “I think it is important to recall the circumstances in which this Directive was passed. It was in the aftermath of the bombings in Madrid and London, Europe was on a heightened state of alert. There was enormous pressure on governments to ensure that their police and prosecutors had all the tools that they need for tracking terrorism and other security threats. Telecommunications traffic and location data is one of those tools, which is why the European Union took steps to guarantee that these data would be available if needed for criminal investigation.”
In the United Kingdom, the Communications Data Bill was introduced in Parliament (BBC 2012). The primary justification for this legislative initiative is the ability to improve investigative powers to trace criminals and terrorists. As noted by the Home Office (2012), “[l]egislation is needed to ensure that communications data continues to be available to the police and others in the future as it has in the past. This legislation will replace the communications data provisions of RIPA. Without action by the government there is a growing risk that crimes enabled by email and the internet will go undetected and unpunished.”

Interestingly to note is how, despite the events of September 11, similar efforts to the data retention directive have failed in the United States. The Internet Stopping Adults Facilitating the Exploitation of Today’s Youth (SAFETY) Act of 2009 also known as H.R. 1076 and S.436 would have required providers to "retain for a period of at least two years all records or other information pertaining to the identity of a user of a temporarily assigned network address the service assigns to that user." But the bill never managed to pass into law.

The data retention is a different activity required from ISPs then filtering content and blocking access. This is not meant to marginalize the request placed upon them, but they are not asked to carry out law enforcement like activity. Instead, they are required to facilitate such activities through retaining data.

Terrorism, however, remains a theme with a recurring character, especially in the European Union with respect to requests placed on ISPs. Among the most recent developments is the ‘Clean it project.’ According to the website, the primary aim of the Clean it project is “…to develop a non-legislative ‘framework’ that consists of general principles and best practices.” The objective remains rather vague, but the leakage of a confidential document provides a bit more insight into the plans.

Among the recommendations set forth with respect to the legal framework, the document calls for ‘internet companies’ to be legally obligated to provide law enforcement agencies “with all necessary customer information for investigations of terrorist use of the internet.” Again the focus is on obtaining data to facilitate the terrorist hunt. Moreover, the document also aims to tie into other themes. As noted among the discussion points, “[y]outh protection legislation must (be expanded to) include protection against terrorist use of the internet.” Among the multiple plans for flagging of content and reporting, ISPs are once again implicated. There needs to be a visible ‘police button’ for users to flag terrorist related content. Subsequently, internet companies, the broad term used throughout the document, must maintain sufficient staff to respond to reports. Because, as the document notes, “recognizing illegal, terrorist use of the internet requires specialist knowledge on terrorism, (national) legislation and (national) cultural differences.” This transfers the responsibility on deciding on the legitimacy of the content over to the service provider, which is undesirable. Especially since ISPs specifically want to refrain from playing law enforcers. And ISPs, according to the plans, are to be held liable for not making “reasonable” efforts to use technological surveillance to identify (undefined) “terrorist” use of the Internet. Suffice to say the project as well as the leaked document encountered considerable criticism, for it places, the ISPs, among other companies, in the position of a law enforcer.

1.3.4 Protecting Children

More recently, the notion of creating a safer environment for children online has also gained momentum. This theme includes multiple initiatives, but together they contain the same objective. In
the United Kingdom, for example, ISPs are called upon to restrict access to ‘regular’ pornography (Halliday 2012). The UK government introduced the idea of restricting access to pornography as a default setting, where those who wish to access pornography must opt-in to do so. In addition to potential objections due to the privacy invasive nature of such measures, ISPs themselves also object due to the fact that they once again must function as gatekeepers. Blocking as a mechanism, as previously noted, is not necessarily effective and due to the infrastructure of the internet relatively easy to circumvent. The primary justification for this initiative is to enhance child protection online. A parliamentary inquiry came to the conclusion that ISPs must do more to keep children safe (Halliday 2012). As a result, one of the recommendations was that the Government should initiate a formal review of an Opt-In filter to access adult material on the internet. The public consultation on the matter is drawing to a close, but the idea receives considerable support from Members of parliament. Internet rights campaigners as well as ISPs generally oppose the idea.

In the European Union, in general, the theme of protecting children is also in the spotlight. In May 2012, the European Commission introduced a ‘European Strategy for a Better Internet for Children.’ The European Commission also looks at Member States to strengthen its case. In its strategy it highlights the efforts of the UK, Germany and France by writing, “[i]n the UK internet service providers (ISPs) have adopted a code of practice that promotes "active choice" whose implementation is left for each ISP to decide; in France, ISPs have to provide parental control software free of charge; in Germany a certified “youth protection software” can be used to prevent children from accessing websites providing harmful content.” Besides the European Union, Africa also hopped on the bandwagon to specifically promote initiatives to protect children. The African cyber safety initiative specifically identifies providers and writes “[p]roviders, especially those providing Internet access and service, should be actively involved in promoting information security for children while carrying out their business. They should show more social responsibility by participating actively in forums and related initiatives of this nature” (ITU 2012). Another aspect that fits within this theme is the recently introduced right to be forgotten. The implications, however, at least for right now mainly concern the broader approach of ISPs, since companies such as Google, Facebook and others will face the consequences of this right.

Protecting children is, however, becoming an umbrella defense to ask more and more of ISPs. A prime example is the request made by a British parliamentarian to have ISPs block suicide websites. “The Government will continue to work through [the UK Council for Child Internet Safety (UKCCIS)] to promote active choice on domestic broadband connections and on new internet-enabled devices – prompting consumers to choose which content they wish to be able to access – enabling consumers, should they so choose, to restrict access to the most common content and sites which promote suicide” (Jackson 2012). This is not necessarily objectionable if consumers themselves are in charge of filtering their access, but when ISPs are required to take over this role, as is suggested with the opt-in for pornography, then it enters another debate.

1.3.4 Botnets

The evolution of botnets is considered among the most critical security threats in contemporary society. Since botnets are often deemed as the digital Swiss army knife the ability to mitigate their effects are highly desired. ISPs are once again engaged in the battle against botnets, except this time, ISPs maintain incentives to act. Even so, several years ago legal scholars, amongst others, claimed there was a lack of incentives for ISPs to act. Lichtman and Posner (2004: 2) proclaimed how ISPs “...are today largely
immune from liability for their role in the creation and propagation of worms, viruses, and other forms of malicious computer code.” Interestingly, Lichtman and Posner specifically focus on the role of ISPs with respect to potential threats to cyber security. According to Lichtman and Posner, they join a “growing chorus of legal commentators” who all argue in favor of increased accountability and responsibility for ISPs. The reason for such an increase in accountability and responsibility is to develop incentives for ISPs to improve security. The assumption in the argument of Lichtman & Posner therefore revolves around a lack of inherent incentives for Internet Service Providers to invest in security. This assumption is also found in other sources (see for example House of Lords 2007; Chandler 2006; Huang et al. 2007).

ISPs, however, have sufficient incentives to introduce actions to reduce botnets, ideally eliminate them and improve cyber security overall. Van Eeten and Bauer (2008) have previously demonstrated this. Based on interviews with officials from ISPs, the authors develop ample evidence to demonstrate both the efforts made by the providers and also unravel the incentives behind these efforts. Cyber security efforts began to escalate around 2003 when ISPs began to understand how improved security turned out to be in their best interest. This is due to costs associated with insecurity of their clients. These costs come from ‘security-related’ customer calls. As van Eeten and Bauer (2008: 26) note, “[t]he incentive here is that security incidents generate customer calls, thus quickly driving up the costs of customer care.” There are other incentives. These include costs associated with brand and reputation damage, and infrastructure expansion.

In addition to ‘negative’ or cost dominated incentives, ‘positive’ or benefit oriented incentives also play a role in the decision to engage in improved security and the fight against botnets. According to van Eeten and Bauer, all interviewees mentioned the benefits generated through maintaining reciprocity. This refers to the contacts maintained with other Internet Service Providers, CSIRTS and other related organizations, who can provide assistance during a case. Such assistance and contact is reciprocal, but to maintain such reciprocity ISPs must treat complaints of abuse seriously. As van Eeten and Bauer (2008: 30) conclude, “[t]he more abuse takes place on its network, the more other contacts in the network will ask for intervention.” This, in turn, enforces security since threats from other ISPs provide a powerful incentive for the ‘threatened’ Internet Service Provider to improve security.

Moore et al. (2009: 9 – 10) also underscore the prominent place Internet Service Providers can play in detection and how “ISPs are also uniquely placed to limit the external impact of an infected computer: they control its Internet connection and can disconnect it if need be. Current best practice is less drastic: it is to quarantine infected computers into a ‘walled garden’ subnetwork from which they can access decontamination and software patches but not much else.”

ISPs in several countries have commenced activity against botnets. The OECD (2012) provides an overview of initiatives, which have been introduced. For example, several years ago, in 2009, fourteen Dutch ISPs signed a covenant in their fight against botnets. This collective action effort against botnets demonstrates the commitment of ISPs to cyber security. ISPs attempt to execute the covenant through developing the above-mentioned walled garden and temporarily cutting off contaminated computers from the internet as a means to prevent further spreading of the botnet and ultimately to ideally eliminate the botnet. Afterwards computers get connected again. As noted in the press release, “[a] great number of internet providers have already taken measures against affected computers that are connected to their network. To improve these measures the Dutch ISPs are going to exchange knowledge and information on bot networks. This way contaminations will be detected sooner and spreading will be prevented immediately.” Similar efforts have been introduced in the United States
(Gross 2012). In the US, ISPs specifically noted how they believe a private sector, self-policing framework can be a more effective strategy than external regulation (FCC 2012). The efforts in the United States go beyond the fight against botnets to also include internet route hijacking and domain name fraud. Other initiatives include the Botfrei project in Germany.

The difference between these self-initiated collective efforts and the external requests placed on ISPs is not in the execution. Cutting off users from the internet, albeit temporarily, is after all a threat used by the French Hadopi legislation in an effort to reduce digital piracy. The difference rests in the underlying justification for action, which is the primary point of departure for any (legal) action. As noted by Albert Vergeer, “[i]t is important that ISPs collectively battle this problem and protect their customers as well as prevent nuisance to the rest of the internet.” The emphasis is on protecting their customers. And this is logical because they are their lifeblood.

Botnets therefore demonstrate a bit of a hybrid category, where both ISPs as well as external parties recognize the necessity to take action. The discussion mainly rests in how much action ISPs can and want to take. Van Eeten et al. completed a study to determine the extent of botnet infections and the accompanying mitigation efforts made by ISPs in the Netherlands. Based on their analysis, Van Eeten et al. (2011) conclude how ISPs contact approximately 10 per cent of all infected customers. Such a percentage, as the authors note, can easily lead to the conclusion that ISPs take insufficient action to battle the problem. This is, however, a too simplistic conclusion to draw. Van Eeten et al. (2011) state how from an economic perspective a certain level of insecurity is acceptable, since measures to improve secure come paired with considerable costs. But more importantly, the authors argue how it is unreasonable to expect ISPs to fully internalize the problem. Botnets, after all, are a community challenge. As van Eeten et al. (2011: 41) state “…these infections originate in criminal behavior. They are not caused by the ISP itself. Even when we only look at the legitimate market players that can influence the magnitude of this problem, we can see a broader set of players that contribute to this problem: hosting providers, software vendors, computer retailers, registrars, e-commerce companies and, last but certainly not least, the end users themselves, be it home or business users.”

1.3.5 Spam

Whereas the previous themes mainly concern external requests to ISPs, Spam is a vital example of self-initiated action taken by ISPs. This theme is included precisely to demonstrate when ISP action is comprehensible and even essential. According to a 2010 statistic, approximately 88% of email is spam. As a result, ISPs take an active role in controlling the internet traffic through filtering of spam, unsolicited commercial e-mails. There is no other internet governance topic where the scalability characteristic of the internet is so prominently present. The internet protocol makes it relatively easy to send a single e-mail to millions and millions of users. The costs at the side of the sender for reaching so many people are almost absent. Given the content of most spam-messages it is hard to imagine anyone replies to these, but even if only a fraction of the people does it can still be an interesting number for the sender. Traditionally, spam was sent to sell products or services, but it is also used for swindling or the spreading of viruses. What all these have in common is that the users of ISPs usually are not interested in receiving them. That is one of the reasons why ISPs filter e-mail. If they would not, the costs of delivering all of the unsolicited emails would be significant both in terms of the infrastructural burdens as well as potential consumer complaints. Except filtering out e-mail, ISPs can also use black
lists of servers that send spam. This is a more drastic remedy, because it can also mean that internet traffic with a legitimate purpose is stopped.

Although there is law drafted on spam, the reason ISPs are acting is not because they are legally forced to. The regulation differs over the globe, e.g. within the EU there is a ban on spam, whereas in the US the regulation defines under what circumstances spam is allowed (CANSPAM Act). What all these regulations have in common is that they regulate the relation between sender and receiver. The sender is not allowed to sent unsolicited e-mail or only under certain conditions. As is common today, users can make rules to not receive certain e-mail. Although sometimes successful, for spam this does not work that well because senders are usually using many different addresses, and when making rules on the content by a user there is huge chance of false positives and negatives.

The ISPs do not have a role, at least a formal one. The legislator could have chosen to involve ISPs but it did not. This is interesting to observe, and might be explained by the fact that filters were not that good at the time of the drafting of these rules. Today the outcome of the drafting might have been different. Another point worth noting is that some have argued that because of the neutral role of ISPs they should not filter spam. It is true, once they do, they can no longer be considered neutral transporters, not taking notice of the message. For the filtering of spam sometimes the traffic data suffices, but often the content of the message is analyzed. In the Netherlands, a case took place between an ISP, XS4ALL, and a “spam company” Ab.Fab. The Court of Appeal ruled that Ab.fab could not be forced to stop sending spam to the users of XS4ALL. This was just before the ban on spam legislation. XS4ALL went to the Supreme Court. Ironically, Ab.fab could not enjoy its victory at the Court of Appeal since it went bankrupt. On top of that, the Supreme Court ruled that XS4ALL as owner of their servers could decide whether or not they wanted to receive e-mail from Ab.Fab.

The importance of spam with respect to the objective of this contribution is how ISPs can act when necessary, as long as it is in their interest as well as the interest of their clients, and arguably in the interest of the internet itself. The other crucial aspect of the actions taken to reduce the negative impact of spam is how ISPs have demonstrated they contain the technical infrastructure and means to carry out this type of filtering which makes them vulnerable, obviously, to external requests to engage this infrastructure for other purposes.

### 1.4 Slippery Slope

Many fear the potential for a slippery slope which is, in part, the underlying reason for moving toward a criterial framework. ISPs, after all, have demonstrated their technical capabilities in filtering content, through spam, as well as blocking access. As a result, the fear on the side of ISPs as well as their clients is that these capabilities, amongst others, can be called upon for a variety of occasions, once they open the door. Basically, if ISPs agree to a request to monitor traffic or otherwise interfere in the activities of their clients for, let’s say, child pornography, others may soon follow. These can include the music industry, the film industry, photographers, publishers, holders of trademarks, and victims of libel, slander, fraud, etc. (Schellekens 2011).

As Schellekens (2011: 155) notes, “[e]ventually, the intermediary would become a gatekeeper to the Internet required to decide about the legality of content, even if nobody complained or where only the slightest or most improbable objections existed against the content.” Schellekens perfectly captures the worry which lingers in the background whenever ISPs are called upon to act. The moment ISPs
themselves are required to determine the legality, or worse the desirability, of the content. Interviewees expressed how this task should not be placed on the shoulders of ISPs. Adherence to the law itself is inherent for any entity, but actually deciding on the content falls outside of the scope of their services. This worry therefore leads to a state of absolutism, where ISPs generally refuse to engage in any sort of activity which can remotely lead them down a slippery slope.

Schellekens (2011) addresses two issues in his conclusion. First, he writes, “we must not be sliding already” (2011: 173). And we are not. The second issue is the requirement of a cut-off point in order to negate the potential for a slippery surface. The absence of a cut-off point is difficult to demonstrate, according to Schellekens. Most importantly, however, “an attitude change to a ‘yes, if’ approach could negate the establishment of a cut-off point. It would lead to a situation in which monitoring duties would be applied by default. An exception would require strong arguments and concomitantly have a small chance of success” (2011: 173). Schellekens therefore recognizes the potential viability of the slippery slope argument. Once a filtering infrastructure is in place, after all, the temptation will definitely be present to use it for purposes other than its original objective. This demonstrates the necessity to have a criterial framework and to maintain its use in subsequent decision. Primarily because requests are going to be made, and simply arguing a slippery slope is an insufficient defense to reject action.

1.5 Toward a criterial framework
As the type and nature of themes, which invoke a responsibility on ISPs, continues to evolve, the first task is to return to the original duty of ISPs: to provide access. Hathaway and Savage (2012), however, identify eight duties for ISPs. These include:

1. Duty to provide a reliable and accessible conduit for traffic and services
2. Duty to provide authentic and authoritative routing information
3. Duty to provide authentic and authoritative naming information
4. Duty to report anonymized security incident statistics to the public
5. Duty to educate customers about threats
6. Duty to inform customers of apparent infections in their infrastructure
7. Duty to warn other ISPs of imminent danger and help in emergencies
8. Duty to avoid aiding and abetting criminal activity

This list is relatively extensive, but with respect to this paper the last duty is particularly relevant: the duty to avoid aiding and abetting criminal activity. Specifically, its broad nature introduces another important point of discussion and challenge related to the question as to what role ISPs play or should play. To state how ISPs need to avoid aiding and abetting criminal activity, can lead to a potential slippery slope depending on the interpretation of aiding and abetting. Providing a criminal with internet access can theoretically be viewed as aiding and abetting, which is therefore an activity subject to requests and legal demands. So where do we draw the line? Dommering (2011), for example, considers the link between providing access to the internet and claiming such access provision facilitates someone to infringe upon copyrights too general. The actual infringement, according to Dommering, takes places by other services outside of the scope of the ISP, who merely provides access. He compares such liability to a situation where someone responsible for road maintenance can also be held liable for any illegal acts carried out on the road. Whereas Dommering (2011) specifically speaks about copyright infringement, his overall argument is valuable input for the development of a criterial framework. Basically, the question which needs to be asked before calling upon ISPs to act is how many other
services are involved in the facilitation of the problem and how close are they to the actual problem? Of course, the main vulnerability of ISPs who provide access is their uniqueness. Certainly the service they provide and the connection to many of the above-discussed themes is general at best, but they are a necessary condition for perpetrators to carry out certain activities.

Ideally, as noted by one of the interviewees, the law provides the criterial framework for the requests, which can be placed upon ISPs. The law, however, is often as fragmented as the themes just reviewed. And the law is a continuously evolving concept, since it is a social construct subject to alterations depending on whatever social climate we find ourselves in. The development of a criterial framework therefore is as much influenced by existing legal standards as it is meant to influence potential legislative ideas in the future. The knife cuts both ways.

As noted in the different themes, certain regulatory attempts exist, both in the United States and the European Union. This begs the question as to the need of the development of a criterial framework. First, the fear of a slippery slope is difficult to empirically assess, but based on the many themes which invoke the participation of ISPs deserves some attention. Second, a criterial framework may find its basis in existing regulation and precedents; it also surpasses that by taking into account other factors, which may fall outside of the legal scope. The question of what role we want ISPs to have and to maintain in contemporary society can be indirectly answered through the preliminary criterial framework.

The regulatory framework does, however, offer certain conditions which can be a source of inspiration for the criterial framework.

The DMCA considers the following four conditions:

1. it would “significantly burden either the provider or the operation of the provider's system or network;”
2. 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;”
3. “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;”
4. whether other less burdensome and comparably effective means of preventing or restraining access to the infringing material are available.”

If anything, the conditions outlined above by the DMCA already highlight a number of crucial aspects which must be taken into account when judging requests made to ISPs, in general not just with respect to intellectual property rights infringements. The criterial framework, however, must have a contingent character, where criteria are ranked in order of priorities. A request, for example, which does not adhere to the first criterion, might adhere to the other criteria, but since they are weighed should still be refused.

First, before even introducing a request, the requesting party must be obligated to investigate alternative sources or parties. This is to demonstrate how necessary it even is to call upon an ISP. In this sense, it may seem as if ISPs are a last resort. This is not necessarily case, but they should certainly not be the de facto party to go to whenever something on the internet stands to be corrected. The question of subsidiarity deserves additional emphasis in light of this preliminary criterial framework.
The second criterion concerns effectiveness. This coincides with the third condition of the DMCA, which identifies both technical feasibility as well as effectiveness. Clearly, effectiveness remains a difficult concept to quantify, especially with respect to Internet related aspects. Effectiveness, however, is a crucial part of the argumentation either in defense of a particular request or in its opposition. The question which is often asked in the United States is whether the countermeasure or the action taken by the ISP is underinclusive. Does it leave too much illegal content untouched and do users have several ways of circumventing the measure?

The motion introduced and won by Brein in the Netherlands is a prime example of how the judiciary ignored the criterion of effectiveness. Or at least, interpreted effectiveness in a rather convoluted manner. This leads to two approaches to effectiveness. Ought the measure taken by the ISP to be effective by itself? Or, should it, as recognized by the judiciary in the Pirate Bay case in the Netherlands, be part of an overall effective strategy? The criterion of effectiveness requires the measure itself to be effective. To warrant the investment made, the criterion needs to prove its value. The activity carried out by ISPs to reduce Spam is justifiable in considerable part due to its effectiveness as well as its positive influence on the overall health of the internet. This comparison illustrates the difference and also emphasizes the need to incorporate the thematic justification for the evaluation of a request placed on ISPs.

This leads into the third criterion, the request must benefit the internet and its users, not a particular party, either private or public. Basically, the action must be necessary in order for the internet to function. Since the primary task of ISPs is to provide access to the internet any request placed upon them or action initiated by them must align with this objective.

The fourth criterion is contingent on the others, for this criterion accepts the request but goes into the details such request must adhere to. This is the cost associated with the request. The requester must bear the cost of the action. In certain areas, such as the United Kingdom, this already happens, but in other places, such as the Netherlands, this is often not the case.

1.6 Conclusion

There is little doubt about the complexity of the legal role of the ISP in contemporary society. Traditionally, third parties facilitating communication and the exchange of information are mere messengers or neutral transporters. The general sense expressed among ISPs, however, is their current transformation into law enforcers rather than neutral third parties. This sense became even stronger in the Netherlands after a judiciary verdict which ordered certain ISPs to block access to the Pirate Bay. The overall feeling is that the demands on ISPs continue to grow, which complicates both their position and their role with respect to their clients. ISPs have come under pressure as a result of various calls for action based on a variety of themes. These include intellectual property rights, child pornography, terrorism, protection of children and botnets. Generally these themes are treated in a fragmented manner, but there is value in observing them holistically in an effort to develop a preliminary framework to challenge the validity of the request, based both on the actual action requested as well as the justification provided for said request. In a preliminary attempt to develop a criterial framework, we have outlined a limited number of criteria including researching the necessity of involvement of the ISP, effectiveness, the benefit to the subscribers and the internet as a whole, and the budgetary support to carry out the request. The next step is to test previous as well as current requests based on these criteria.
Bibliography


Communication on Illegal and Harmful Content on the Internet (COM (96) 487 final)
Communication on European Strategy for a Better Internet for Children (COM (12) 196 final)


Green Paper on the Protection of Minors and Human Dignity in Audio-Visual and Information Services (COM (96) 483 final)


Halliday, J. (2012). Pornography online: David Cameron to consider 'opt in' plan. Available at: http://www.guardian.co.uk/technology/2012/may/04/pornography-online-cameron-opt-in-plan


Internet Stopping Adults Facilitating the Exploitation of Today's Youth (SAFETY) Act of 2009 H.R. 1076 and S.436


