ISPs AND COPYRIGHT: DEEP PACKET INSPECTION AND NETWORK NEUTRALITY

Joan Ramos Toledano

Abstract

This paper aims to shed light on a transversal phenomenon, as it affects both the scope of the law and the technology, ethics and certain legally recognized rights. This is the impact that the deep packet inspection technology has in the current internet. Through this technological innovation, effectively used nowadays, the ISPs (Internet service providers) can analyze the content of what passes through their networks, treating it differentially if necessary. Thus, the proposed equal network may be truncated as these companies can monitor traffic on the network (determining a speed limit, prioritizing some connections or just banning them because of the data they are transmitting). In this paper we analyze the impact that this technology can have in a very specific area, the copyright legislation, revealing the intense battle being waged between technology companies and the owners of intellectual property rights. We also discuss how this technology can subvert what the internet is becoming and, finally, how the role of the state is important in the regulation of the technology, for it will determine the interrelationship between technology and society.

Keywords

Copyright; deep packet inspection; network neutrality; ISPs; P2P; intellectual property; legislation.

1. Introduction

In the ever complex field of copyright, one element that generates controversy is the fact that Internet service providers (ISPs) are usually not responsible for the content that is hosted or shared through their network. That is, if a user shares copyrighted files over the Internet, the ISP (e.g., AOL) would not be, a priori, liable. This disclaimer has come to be called *safe harbor* provision, and it is provided by the Digital Millennium Copyright Act, passed in the U.S. on October 28, 1998. European Union has also regulated in this regard, exempting *mere conduit* providers (ISPs, therefore) in a similar sense than the American DMCA (Directive 2000/31/EC).

For those who advocate for more restrictive rules of copyright, this is something that should change, and they propose to revise or amend the rules for ISPs to acquire more responsibility (Levine, 2011). But for many others, such as users or ISPs themselves safe harbor provision is not a problem but a guarantee that allows the Internet to function smoothly, avoiding that the fear of being legally liable turns service providers into vigilantes and possible censors of everything that pass through their networks.

However, technological advances allow increasing control of the information that flows through the network cables. News about espionage of citizen personal data have caused some alarm among the users of many countries. But we are not just talking about government actions of dubious legality, but the possibility that ISPs automatically control what data passes through their networks. The so-called *deep packet inspection* is a reality, and like any technology, the problem lies not so much in its technical possibilities but in the actual use made of them. The interaction between private interests and public regulation becomes therefore a major issue, even more when that particular technology can affect some important subjective rights.

This paper aims to analyze some cases where the safe harbor has played an important role to prevent ISPs to pay the consequences of what users do on their networks. There is also an analysis of some cases in which service providers have used the DPI regarding P2P networks and what has happened as a consequence, for it is a private decision but with public consequences, as we will see.

The goal is therefore to analyze some situations to be addressed by ISPs and how they can affect what has been called *net neutrality*. Because that neutrality, understood also as the power of the users to prevent that decisions are only made from a commercial-private sector point of view, is essential to maintain and if possible to recover an Internet managed mainly by users (Zittrain, 2008). The increasing commercialization of the network sharpens the need for some sense of control by democratic representation organisms, who are responsible for regulating how service providers should behave. As we will see, copyright plays an important role because copyright-holders are primarily interested in the use of DPI against P2P networks.

2. Safe harbor provision and how it is applied

The safe harbor provision regulated in the U.S. DMCA or the European Directive is not universal for all intermediaries as Internet services are concerned. It is not equal the protection that has an ISP than a hosting service provider or search engine. This paper focuses on the responsibility of Internet service providers, as those are mainly who are able to implement a technology like deep packet inspection (Lara & Vera).

It seems obvious that as the safe harbor provision is provided by a legal document it may be modified depending on the political will of each state. However, this provision has been widely accepted in most legal bodies because it has been seen as a way to prevent that ISPs have to continually monitor what is happening within their networks. It is thus intended for the Internet to be a fluid medium, allowing anyone to publish anything - which does not mean, obviously, that it does not have consequences, but they will be *a posteriori*. But, does this safe harbor provision apply uniformly in different states?

Kathy Eivazi has analyzed an important case that happened in Australia (Eivazi, 2012). In November 2008, iiNet - second largest ISP in Australia, was sued in the Federal Court of Australia for not acting properly against certain users who had allegedly infringed a copyright law, even though the company had been advised by the Australian Federation Against Copyright Theft (AFACT), today named Australian Screen Association. It is important to remark that, according to the Australian copyright law, "a person who authorizes the infringement of copyright is treated as if they themselves personally or directly had infringed copyright" (Eivazi, 2012). Although the AFACT notified the ISP that he had found evidence of illegal downloads by users, iiNet refused to take any action until there was a court order in this regard, so the AFACT had to prove in court that there had been such violation of the copyright. Both first instance and appeal judges considered that iiNet had not authorized copyright infringement of their users, but acted as a mere service provider, not having the obligation to monitor what the users are doing on its network.

As to whether iiNet was entitled to rely on the safe harbor provision, it was irrelevant in the case in court, since an ISP can only claim the provision protection once it has been held liable for copyright infringement. As in this case the two courts that analyzed the case considered that iiNet was not responsible for authorizing that infringement, considering whether it would qualify for the safe harbor provision had no place. However, Judge Cowdroy saw fit to assess whether such a provision would had been applicable because of the "complete vacuum of legislative guidance" on the matter. And he found that, indeed, it iiNet could have benefited from the safe harbor clause. However, the Federal Full Court held unanimously in appeal that while iiNet was not liable for copyright infringement, it would have not been able to be protected by the provision of safe harbor, since he had no "adequate policy for the termination of the accounts of repeat infringers in appropriate circumstances".

We analyze now the situation in a state with a very different legal tradition, Spain. In Europe, the safe harbor provision is provided by Directive 2000/31/EC on Electronic Commerce. But unlike the American DMCA (and other common law tradition countries, as the case of Australia), there is no provision of a notification procedure for copyright infringement, which is a key element in the DMCA. European directives are transposed differently by each member state in the EU. And we specifically analyze Spain as it is a country where the judiciary has been more lax in prosecuting copyright infringements, and more protective of the ISP and even users.

Following the directive, in Spain the law requires that the ISP has actual knowledge that the infringement is taking place. This presents a first hurdle, because since the absence of a procedure for notification of the offense, as required by the DMCA, it is difficult to know when to be considered that the ISP has *actual knowledge* of the infringement. Miguel Peguera describe, based on the European Directive, the only three ways to demonstrate that there has been actual knowledge:

a) That there is a prior decision, either by a court -like iiNet demanded in the Australian case, or by an administrative body.
b) That the copyright infringement is voluntarily recognized.
c) Other measures that may be established - here the European Directive leaves the door open to any other options that the states may incorporate.

If the ISP happened to have actual knowledge of the infringement, it should act diligently to address the issue, thus being able to be protected by the safe harbor provision (Peguera, 2010).

Peguera shows how, in the case of Emi Music Spain v. Bitmailer (an ISP now part of Sarenet, a provider of Internet services to companies), the Spanish courts found not only that the ISP was not responsible for what was happening in their networks, but even that when the infringement was known by the ISP, it was not required to stop providing the Internet access service to the users. This court decision guaranteed something similar to an *Internet right* for the Spanish defendant, as even if he was responsible for copyright infringement, the ISP could not stop providing him Internet access.

The analysis of these two cases shows the great differences that may exist between different legal bodies for the same clause, the safe harbor provision. Australian courts eventually dismissed the possibility of iiNet to benefit from it because it does not have a system of notification and take-down, while in Spain not only this system did not exist, but knowledge by the ISP did not involve their responsibility or obligation to cease the service. There is no doubt that in Spain there have been legal changes since then, as the Law 2/2011 of 4 March, Sustainable Economy (known as Sinde-Wert Act), and even today a substantial change in the Intellectual Property law is prepared. These changes attempt to bring a more restrictive Spanish legislation, such as the U.S. or France. But it is worth noting, although not the subject of this paper, that these rules have obtained little support of the judiciary, which tends to protect users and ISPs. That is, in Spain the

service providers or users of P2P networks are greatly protected. A different case are the websites that offer protected material, situation itself legally persecuted in Spain. The difficulty comes when the site has a link to another site, so it does not host copyrighted material *sensu stricto* (Peguera, 2010).

What is clear is that we have very different court decisions and arguments depending on the countries and their judges. This seems to be the opinion of Eivazi too, as she states that "this significant ruling has clearly demonstrated the failure of legislation to keep up with technological changes in dealing with online piracy and the liability of online intermediaries such as ISPs in the context of copyright law " (Eivazi , 2012).

The requirement of a court decision by iiNet before taking any action against users highlights the need to properly regulate a controversial area not only because it affects copyright but because it affects to certain situations that begin to be perceived as subjective rights (such as access to a neutral Internet or non-discrimination in the quality of the connection by the programs that are used in the network) even though they do not have a consensual legal recognition. Recourse to judicial proceedings, which also occurs in the Spanish case analyzed, denotes an important legal hole and lack of deliberation by the state bodies with democratic representation that must be addressed to avoid legal uncertainty for all parties involved.

This uneven application of the safe harbor and the lack of adequate regulation can lead to owners of copyright and its media and academic environment to criticize and question the very existence of the safe harbor provision. So believes Levine, who says directly that ISPs should be liable for copyright infringement occurring on their networks, even if they not know about it. What seems clear is that if those who advocate for copyright protection see in Internet a potential enemy, in the technology of deep packet inspection they see an opportunity to easily control certain aspects of it such as P2P networks.

3. Deep Packet Inspection. Altering network neutrality?

The technological development of deep packet inspection has its origin in the early years of the Internet, although it has been in recent years when many *netizens* have known of its existence due to the scandals arising from its use to control P2P, the mainly method for copyright infringement on the Internet. Because ISPs are private companies, the use of DPI is a decision that is up to them, although this may have public consequences. The lack of regulation of the Internet causes that these cases end up being resolved in court or by administrative bodies that make decisions based on the problems that arise, but often without a firm legal basis, because the problem has been addressed first judicially than politically.

DPI is a technology that can *introduce intelligence* on the Internet, which has often been called dumb network. DPI can be used to monitor, speed up, slow down, block, filter

and make decisions about traffic networks from an ISP based on the information contained in the packets (Bendrath & Mueller, 2011). This point is crucial because so far the presumption was, and with this intention apparently was created Internet, that ISPs (who control the physical wire that forms the network we call the Internet) did not have control over the contents of the packages and they did not need to know the content for the packets to be transmitted properly. The Internet is based on the goal that packages must arrive at their destination (Townes, 2012), for which each packet contains the information to be transmitted, but as happens with postal mail, there is no need to check the contents (Abbate, 1999).

Bendrath and Mueller identified the following uses that can be given to DPI: network security, bandwidth management, Governmental surveillance, content regulation, copyright enforcement and ad injection. They say on the infringement of copyright, that the "copyright holders have tried to force ISPs to use DPI to automatically detect and block unauthorized sharing of music or video files. Some U.S. universities have installed DPI to prevent student downloading "(Bendrath & Mueller, 2011). The authors believe, and there are strong arguments to support it, that DPI can be a disruptive technology as it has the power to modify net neutrality by empowering ISPs to control the package content.

But what is important is not so much the existence of a technology such as DPI, which is being developed since many years ago, but the use made of it. Specifically, we are interested to see how DPI can alter the scene of a conflict around the Internet (but not only); a conflict that arises mainly because of the copyright infringement through P2P networks. In this field we cannot just talk about a neutral technology with disruptive potential; we also have to focus on business interests and those who try to defend them (both copyright holders and ISPs, for example). We should also analyze the role played by *states* in a broad sense, for in copyright conflicts there are a lot of differences between judicial decisions or government decisions, as the lasts ones are more prone to be affected by lobby's and economic interests.

4. Technical decisions and political decisions

4.1. The regulatory role of the State

Internet is a technology with little regulation by most of the states. Because of its structure, essentially international, there is no clear catalog of the Internet rights or how the Internet service should be provided by the ISPs (apart from the contractual rules with customers and certain general rules on how services should be provided in telecommunications, but those depend on the legislation of each state). Internet is therefore a deregulated environment, although the activities that take place within it are subject to the legislation of each state. That is, criminal activity will obviously be prosecuted. Fraud, drug trafficking, pornography... shall not be unpunished for being on the Internet. But there are hardly state rules determining issues like how advertising

should be regulated, or if net neutrality is a desirable goal that states have to protect. And there is also little international regulation about it. The construction and development of *Internet rights* is mainly due to the judges and courts of each state and certain organisms that have assumed such powers, as we will see later, like the U.S. Federal Communications Commission.

The Internet has also been a disruptive technology for copyright, because it has revealed the contradictions of intellectual property. Intellectual creations are subsumed under the form of traditional property primarily to protect the economic value of the creations and their transferability (Smiers, 2006). But these intangible goods, unlike material and physical goods can be endlessly copied, stored and transmitted at practically zero cost. That breaks the existing commercial dynamics of intellectual creations, which when digitalized can be shared freely and endlessly. Internet extends greatly this possibility, as this sharing becomes global. There is a great exception, largely forgotten, of those underdeveloped countries or people without resources who cannot access Internet, obviously.

Because of that situation regarding copyright, states have acted, approving rules that sought to adapt intellectual property to new technological situation. The U.S. DMCA, the so-called HADOPI law in France, the Spanish Sinde -Wert, the British Copyright Designs and Patents Act, the TRIPS Agreement, WIPO as an organization that monitors the implementation of intellectual property... The commercial interests of the copyright-holders companies are well represented and defended in several states and organizations. The "301 U.S. list" of countries that do not adequately prosecute piracy is an example of how economic business interests (in this case, relating to copyright) is defended through state power, which could explain the lack of courage of some countries to properly regulate the safe harbor provision or even DPI, as the copyright industry has no little power and uses it to lobby for achieve state regulation or the lack of it (Levine, 2011).

4.2. A new interest in game

Why then, despite the influence that large copyright companies have and the relative support obtained by the states, file-sharing with P2P networks is nowadays still a regular and somehow accepted activity for a lot of citizens? Despite legal penalties, including the recourse to the criminal code, Internet disconnection penalty or exorbitant fines, people keep sharing with relative impunity through the Internet. There is a reason of technological nature, since encryption methods or proxies may seriously hamper the detection of P2P users. But in the battle between people that defend the sharing of all kinds of content (they are usually very critical of intellectual property and copyright as it is regulated nowadays) and copyright-holders, ISPs are a main element that can change the power balance. Most service providers have not wanted to give in to the pressures and expectations of copyright-holders because they are more interested in maintaining its business of providing Internet service that to enforce the defense of

copyright. And for many people it is obviously an incentive that through Internet access they can obtain lots of *protected* movies, music files or books.

Along with the ISPs, there are other powerful companies whose business is based on the existence of many users, and therefore are less concerned about intellectual property than to turn the Internet in a big market where users are also (or at least) customers and consumers. So, for example, Google makes more money if there are lots of people that use its search engine or see the advertising that it manages. Also Facebook is less concerned about whether the photos uploaded to their servers are protected by copyright than for the fact that they obtain new users every day. And those users in both cases (Google and Facebook) need obviously Internet.

This situation has been analyzed successfully by Robert Levine in his book Free Ride where he shows how some of these Silicon Valley companies owe some of his growth to the little concern they have for copyright protection. It seems reasonable to assume that if companies like AOL or Google would want to limit the access to copyright protected files they could effectively do so. Google could remove all links suspicious of hosting protected files, and AOL could cut the connection to users that download movies or music. But obviously if Google started to act this way users would end up finding (or creating) another search engine not prone to apply that kind of censorship. And, what would happen if an ISP started using DPI technology to limit P2P networks? Would a private choice have public consequences? Could it provoke the mobilization of citizens and organizations, and the ruling of government agencies?

4.3. The public effects of private choices

The truth is that, although the interests of copyright-holders and ISPs are often different or even contrary, there may be some collusion between the owners of copyright and the service providers because the main way to share protected files, P2P, implies also an important use of bandwidth that ISPs do not like for they want to reduce the saturation of their networks. The case we now analyze occurred between January 2006 and August 2007, when the U.S. service provider Comcast implemented (with the company Sandvine) DPI in its network limiting traffic on P2P networks like Ares, Bit Torrent, eDonkey, FastTrack and Gnutella (Asghari & Mueller , 2012). This decision was taken by the ISP without consulting any public body or agency and without informing its users. It was, therefore, a private decision taken by a private company. When a group of computer experts found out about the P2P limitation in the mid-2007, the case came to light causing a major public debate. The mobilization of the users and some organizations like Free Press caused that the FCC received 20,000 complaints in two and a half months, and opened the debate on net neutrality and the role of ISPs with technologies like DPI.

The Federal Communications Commission (FCC) is an independent U.S. government agency that regulates interstate and international communications of radio, television,

wire, satellite and cable. It was created in 1934, and claimed jurisdiction to rule on the Comcast issue based on the 2005 Internet Policy Statement, in particular because the supplemental jurisdiction contained in Title I. In 2008, the FCC ordered Comcast to stop using DPI to limit P2P and seek other methods to improve bandwidth without discrimination based on protocols (such as Bit Torrent, in this case). Because of this decision and voluntary agreements with the plaintiffs, Comcast started using new methods to ease the congestion of the network. These new methods were based on limiting traffic in areas geographically that were congested, regardless of the protocol that they used, as it happened with P2P. Therefore, the contents of the packets were not inspected anymore. This decision of a public agency like the FCC is relevant because it sets a precedent in a field that did not exist (nor exists) clear regulation on how it should work and it shows that net neutrality may be something politically desirable and protectable.

Comcast had gone to trial against FCC on the grounds that the government agency had no legal authority to take that decision, and in 2010 it won the case, as the appellate court state that the FCC had overstepped when it considered that it could decide about the issue of network management policy based on its Internet Policy Statement of 2005. Nevertheless, in December 2010 the FCC adopted the Open Internet Order, whose rules require transparency, no blocking and no unreasonable discrimination, so that it could decide on cases like Comcast in the future (Asghari & Mueller, 2012). That is, a public agency had clearly positioned itself against some uses of DPI technology because they understood that it meant compromising net neutrality. A private choice by a company like Comcast had caused a public reaction that implied ruling about how the Internet must be.

Also in Canada there has been a controversial case regarding the use of DPI. In this country, the Canadian Radio-Television and Telecommunications Commission (CRTC) is the equivalent to the FCC. Although, and this is a remarkable difference, the regulation of ISPs in Canada is the same as other media, unlike what happens in the U.S. where there is a significant deregulation of the Internet.

Between 2007 and 2008, the two biggest ISPs in Canada, Bell Canada and Rogers Communications Inc. started using DPI. As in the U.S. case, it generated complaints from users (which had not been notified), mainly because it was applied to all the network of these two companies, therefore affecting a group of little ISPs that used Bell Canada and Rogers Communications physical network. So, willy-nilly these small businesses who rented part of the infrastructure, their customers were also affected by DPI technology which, again, was directed against P2P networks. After allegations of breach of contract against the two major ISPs, the case generated a public debate, like it happened in the U.S., moreover when the Comcast case was very recent. However, in 2008 the CRTC ruled in favor of Bell Canada in almost every issue, only warning them because of not notifying the users about the use of the technology, but unless the FCC,

accepting the right of the ISP to use whatever methods they needed to keep their network from saturating.

But the debate that was generated around net neutrality forced the CRTC to order a report on traffic management by the ISPs (ITMPs). In October 2009, the CRTC issued a decision (Telecom Regulatory Policy 2009-657) in which they established a framework for regulating the actions that the ISPs can take to manage their bandwidth. This decision obliges ISPs to adequately inform users on these management measures, which can never be discriminatory. It also refers to the need to innovate as the main tool to avoid congestion, rather than limit access to certain Internet services and protocols such as P2P.

Both in the U.S. and in the case of Canada, the arguments raised to the FCC and the CRTC were, at first, contractual. It was argued that ISPs breached the contracts with the users or with other minor ISPs that used the same physical infrastructure. But the argument was not that the ISPs methods were illegal because they altered net neutrality for there was no legal basis for that. Wielding the net neutrality was more a wish than a reality, and both the FCC and the CRTC had to make decisions to timidly regulate a field largely left unattended by the legislative bodies of both states.

These two cases highlight the important role of ISPs in what is called net neutrality. They also show what the use of DPI as a technology can imply, because it can alter the traditional functioning of the Internet. Although this paper does not aim to establish how the Internet has to be, it seems important that, given the significance of the Net, that a public debate takes place, taking into account more than economic and technological interests.

5. Deep packet inspection and Copyright, a complex match

The assumption of copyright under the legal form of property is one of the key elements to understanding copyright. One consequence of this situation is that the defense of the interests of copyright-holders has often followed the same legal course as if it were a physical property. Companies that invest money in cultural production such as films, music or books have fought copyright infringements on the Internet through individualized lawsuits generally directed to the users who download but also to the websites or even to the ISPs, as we have seen.

This strategy has not been particularly productive for the plaintiffs, because even if they were to win the lawsuits (which in many cases has not happened), it implied sue countless people since downloading files via the Internet is a generalized activity assumed to be normal for most Internet users. The Internet is not understood without the option of downloading files. Whether these files are protected by copyright or not does not seem to matter to a lot of people, and even some of them are infringing copyright without knowing that an illegality is being committed. In this sense, DPI is a powerful

tool as it can limit, as we have seen, the Internet traffic substantially. It can for example slow considerably all P2P networks, which are the most used for copyright infringement. We have seen that the use of DPI can cause some problems and reactions, both from citizens or Internet users and from public agencies. But the specific use of DPI to control copyright infringement (and not for network management, as were the cases we analyzed) presents other theoretic problems.

A) First, and already noted, the fact that are the ISPs who have the power to implement DPI within their networks. And they do not seem particularly willing to use it to limit traffic of protected files for this would surely lead to an escape of their clients to another ISP that did not do so.

B) It is technically difficult to know for sure if the contents of a packet circulating through Internet is or is not protected by copyright (Peha & Mateus, 2014). For instance, there is data that demonstrates that ISPs have limited or blocked traffic on P2P networks. But this does not imply that they block or limit traffic of protected files, but all traffic flowing through those networks. And it should be noted that P2P networks are used for much more than copyright infringement. For example, Ubuntu (and other Linux distributions) have for years distributed their operating systems over the Internet, usually via direct download and torrent. Sharing files with the torrent protocol allows to avoid server saturation, so in a way it could be seen as a method of *server management.*

The first problem may be salvageable for there can be, as mentioned, some collusion between ISPs and copyright holders, as the ISPs will also want to limit P2P to avoid network congestion (Bendrath & Mueller, 2011). However, many ISPs have refused to take such measures for fear of losing customers. The second problem is more complex to overcome, precisely because affecting all the P2P network is seen as a discrimination and a behavior that endangers net neutrality. And it seems that this is not only a *netizen* perception but something that public agencies (as seen with the U.S. and Canada cases) take into account.

The technologies and strategies of the copyright holders to identify users who share protected files are varied and different. But one thing they have in common is the ability to affect certain areas in principle unrelated to copyright, such as user privacy and the confidentiality of their communications. Internet, that sometimes seems to be the battlefield on modern copyright, also affects other aspects of life of its users. Copyright-holders have succeeded in their goal of obtaining a legislation that, even if it is turning to be somehow ineffective, seeks to protect copyright on the Internet. The main objective of those companies is to turn every artistic creation and distribution in something that generates profit, something that can be sold. Nowadays is very difficult to create and distribute cultural goods without entering the market and, therefore, accepting copyright (Sunstein, 2006). This is sanctioned by a lot of regional, state and international laws and treaties. For copyright-holders, the Internet is a danger to an

established market and that is why they will try to make ISPs liable or, at least, play in their favour.

The so-called net neutrality has also important pressure groups, whose aim is to relativize the rules that could limit the fluidity and expansion of the Internet. This group is often presented as a group of activists advocating for freedom (in this case, network freedom), but are often intellectually and financially promoted by sectors that are interested in people willing to pay for Internet connection (Levine, 2011). It is the case of ISPs or companies like Google, Facebook or Amazon. In the end, it is a matter of economic benefits. Hollywood companies will say that they are trying to protect *the movies* and Silicon Valley companies will argue that they defend *net neutrality*, but both of them have economic interests of their own.

But in the struggle to defend or to limit the downloading of copyrighted files, technologies come into play, and as the deep packet inspection they can have consequences beyond what is intended. Some of these technologies can have harmful effects clearly highlighting the lack of state and international regulations, especially when they affect rights traditionally recognized by the legal bodies or even constitutions.

This happens with the *swarm infiltration* technique (Peha & Mateus, 2014), that uses a modified P2P client to connect to a P2P network as if it was a user to collect any information about other users sharing files with a specific title and their IP addresses. It appears, however, that there is a margin of error, both in verifying whether or not a computer is sharing protected files and when providing the link between this file and the specific computer. This may lead (and it has occurred) to false accusations. There is a third problem that consists in the difficulty to identify the specific person who has carried out the action, which may not be the same as the owner of the Internet line.

This research technique can be performed directly by a copyright-holder company, because there is no need for the ISP to do anything. That circumstance raises some interesting questions. Thus, for example, how are the names of the persons bound to the IP obtained? This is an information that belongs to the ISP, and it should only share it if there is a court order indicating so. And can anyone who uses the swarm infiltration technique identify the content of the files even if they are not protected by copyright? Remember that P2P networks are used for much more than sharing protected files. The margin of error of this technology could lead to violating the privacy of users or produce erroneous accusations, and those are not pseudo-rights like net neutrality, those are legally provided rights.

But even if ISPs were to use DPI and it was legally accepted by lots of states, users who share files over the Internet are becoming more skilled about how to share avoiding control or surveillance by ISPs, governments or other companies. Apparently, encryption prevents DPI systems to correctly identify traffic users and files using P2P.

In general, P2P programs that are used to share files or systems to break copy protection have always been technically ahead of both laws and companies trying to prevent file-sharing (Zingales, 2012). This frustration is one of the main reasons to explain the increasing pressure from these companies on governments to adopt more restrictive measures. It can be said that the protection of copyright on the Internet has been adopted as a goal by the states and that technological developments like DPI may be used to this regards. Somehow, lots of countries have took private interests as if they were their own when defending copyright, which clashes with many users and even with court decisions. The time to politically address the issue could not be better, as the future regulations of the ISPs and the use of the DPI can define what is going to happen with the Internet in the next years.

6. Conclusions

What we have seen so far is an example of how the safe harbor provision and DPI can affect to net neutrality and how it is perceived in some countries. The analysis of these cases (some of them have been chosen for their relevance or because they are illustrative, but obviously there are a lot more) enlighten us about the legal and political implications that may have the technology and the use made of it.

First, it seems important to emphasize that standardization of the conditions of application of the safe harbor provision would be desirable because right now its interpretation depends on the court decisions of each state. Factors such as the legal and cultural tradition or the intensity of the copyright laws determine the application in the different countries. This homogenization would lead undoubtedly to a deeper discussion about what kind of Internet is desirable. And in this sense there are very few clear political initiatives, apart from isolated statements in election campaigns that never end up being real proposals. Only the copyright protection has gained considerable state support, with little support from some business companies like ISPs, Internet users or, in some countries like Spain, even judges.

Second, and following the opening of a public and political debate about how the Internet should be, a legal regulation about DPI is needed. This technology has a disruptive potential for the Internet and the network neutrality, in addition to other recognized rights that can be affected such as privacy or secrecy of communications. Its potential utility in combating illegal downloads cannot imply an absence of control and regulation. And neither its use should be a purely private decision because, as we have seen, its consequences go further. Internet is much more than a physical network to let some companies do whatever they want with it.

Finally, there is an important issue that cannot be solved only with political decisions: the copyright on the Internet. Surely the battle between file-sharing and defending copyright on the net is a thorny, complex problem that requires a debate with many actors. But in the same way that it has been correctly argued that taking thousands of

P2P users to court is not the legal solution to copyright problems, it appears that DPI or measures that endanger net neutrality as we know it are not the technical solution either. This paper does not aim to solve a major issue like that, but we think that the (re)construction of a relatively open and free Internet (and I say reconstruction because I believe that the growing commercialization of the Internet have turned it into a not so free and open medium) requires the neutrality of the networks through which information passes. And this applies to the pressures that ISPs may receive from copyright-holders and to the decisions that those ISPs may take based on economic and management points of view. The authorities should address this concern, present in many groups of Internet users, because they are those who are in a position to establish the conditions necessary to regulate it. It seems that the time to regulate the Internet and protect it from major economic interests has come, and it is a decision that needs a strong political will.

References

Abbate J. (1999), Inventing the Internet, The MIT Press.

Bendrath R., and Mueller M. (2011), The end of the net as we know it? Deep packet inspection and Internet governance, New Media Society, 13, 1142-1160.

Eivazi K. (2012), Is termination of Internet users' accounts by an ISP a proportionate response to copyright infringement?, Computer Law & Security Review, 28, 458-467.

Lara JC., and Vera F., Responsabilidad de los prestadores de servicios de Internet, online at http://www.derechosdigitales.org/wp-content/uploads/pp03.pdf [accessed 04/27/2014]

Levine R. (2011), Free Ride: How the Internet is destroying the culture business and how it can fight back, Vintage Books.

Mueller M., and Asghari H. (2012), Deep packet inspection and bandwidth management: Battles over BitTorrent in Canada and the United States, Telecommunications Policy, 36, 462-475.

Peguera M. (2010), Internet Service Providers' Liability in Spain, JIPITEC, 1, 151-171.

Peha J., and Mateus A. (2014), Policy implications of technology for detecting P2P and copyright violations, Telecommunications Policy, 38, 66-85.

Smiers, J. (2006), Un mundo sin copyright: Artes y medios en la globalización, Gedisa.

Sunstein, C. (2006), Infotopia. How many minds produce knowledge, Oxford University Press.

Townes, M. (2012), The Spread of TCP/IP: How the Internet Became the Internet, Journal of International Studies, 41, 43-64.

Zamora, J. (2006/2007), Contradicciones de la globalización: surgimiento del copyleft, Revista Telemática de Filosofía del Derecho, 10, 141-174.

Zingales, N. (2012), Digital Copyright, 'Fair Access' and the Problem of DRM Misuse, Boston College Intellectual Property & Technology Forum, 1-36.

Zittrain, J. (2008), The Future of the Internet, Penguin Books.