Social Network Sites (SNS): A harmless remarkable technological phenomenon or a harmful backdoor with long-term unpredictable consequences?

By Konstantina I. Alexopoulou, Lawyer, Athens Bar Association

INTRODUCTION

The vast digitization and the unprecedented dematerialization of copyrighted goods has led to the development of massive online piracy. Facing the ubiquitous issue of online piracy, governments now encounter the possibility of involving Internet intermediaries into the copyright enforcement mechanism by mandatory or voluntary graduated response mechanisms. From an economic point of view, graduated response mechanisms are cost-effective, while any battle against counterfeiting and online piracy seems utopic and inefficient without internet intermediaries' help. Nevertheless, imposing active-preventative rather than passive-reactive obligations on intermediaries may conflict with principles of network neutrality. Policy shift regarding online copyright enforcement requiring from Internet intermediaries activity rather than passivity has significant implications over network neutrality.

In the light of hailing technological evolution, data is processed in new different ways, giving rise to data protection issues that need to be addressed. It is not only a question of quality of data exchange, but also of quantity. Due to Information Technologies enormous quantities of data are exchanged daily on a worldwide scale, representing threats for Intellectual Property breaches and data protection safeguards. Under the Lisbon Treaty, data protection is strengthened within EU countries providing at the same time a valid legal basis for individuals. Any data controllers should proceed in data processing in conformity with principles of necessity, purpose limitation and proportionality. Limitations to the exercise of data protection right are feasible if they are exceptional, duly justified and never affect the essential elements of the right itself.

On the other hand, privacy is no longer a social norm, according to Facebook founder Mark Zuckerberg; such argument is justifying the unexpectedly high rise of social media these last years, reflecting the evolution in ordinary people's attitudes. Such argument also serves as a perfect excuse for the recent modifications of privacy settings in Facebook[1].

The following analysis outlines the debate on the nature of information shared on SNS, while stressing out the numerous privacy and security risks that have emerged for SNS users in the digital environment, especially through the use of mobile phones. The recent international jurisprudence enlightens the various aspects of privacy issues that arise as well as the conflict between the right of privacy and free expression on the one hand and intellectual property rights on the other. This paper also highlights the legal framework regarding ISPs globally, as well as recent legal instruments adopted worldwide in relation to copyright enforcement in the digital environment, providing for a more active participation of ISPs.

I. The nature of information contained in SNS: public or private?

A cutting edge issue arising nowadays refers to the nature of information contained within social network sites such as Facebook or Twitter. A discussion regarding the nature of information available on Facebook should start from Facebook's cornerstone "Facebook is about sharing". Hence, a digital tool created to enable content & data sharing between people, inevitably considers information as public. Facebook is now part of everyday's life of more than 550 million persons, while in 2007, it was used only by 70 million persons, not to mention that Facebook is the largest photo sharing application on the web with more than 14 million photos uploaded daily. Thus, Facebook proved to be a tool flexible, dynamic and socially compelling. As a matter of fact, the default privacy setting in Facebook is "Everyone", entailing that everyone on the Internet including people not logged into Facebook, may access information set to "Everyone", this data being publicly available information. It must be noted that, according to Facebook's Privacy Policy, everyone, by using Facebook, consents to having his personal data transferred and processed in the U.S. It is interesting though that US Courts refrain from broadly concluding that privacy overrides procedural obligations such as the production of evidence.

The security risks emerging for SNS users are enormous as technological evolution creates new means of access and communication which may lead to various infringements. It is crucial to note that according to Facebook Terms and Conditions, which each user has to accept in order to create a Facebook account, a user by posting photos or videos on Facebook (Intellectual Property Content), grants Facebook "*a non- exclusive, transferable, sub-licensable, royalty-free, worldwide license to use any IP content that he posts on or in connection with Facebook ; this license ends when the user deletes this IP content or his account*", which entails that Facebook or any third person authorized by Facebook may use our photos or videos or any other IP content without notice and of course without remuneration, even if Facebook sells such content to third parties. Another interesting detail proving to appear somehow scaring is that a user's content may be used by Facebook even after the user deletes his Facebook account if such content still appears on other people's pages.

According to the above analysis, photos posted on social networking sites become public. Even though published photos remain the property of the user who posted them, in some cases, Courts held that no breach of the right of privacy is made when a third party uses pictures already posted on Facebook. Precisely, in the famous Zahia case in France, a French magazine (VCD) published photos of a famous escort girl (Zahia), taken from her Facebook account, where those pictures where accessible to everyone without her consent. Zahia sued the magazine claiming that an infringement of her privacy right as well as an infringement of her right to her image has taken place, but the court decided that since the girl's photos were directly associated with ongoing judicial proceedings with enormous publicity where she participated, no breach of the privacy right of the right to her image had taken place[2].

Recently, a French Court condemned a young hacker in 5 months of prison because he had intruded the Twitter accounts of American stars and politicians[3].

An interesting financial settlement between Courtney Love and a designer on defamation grounds proved how powerful social media sites may be. The famous rock star had made false statements about the designer on MySpace and Twitter and the designer sued Courtney Love leading to a settlement of $430.000 which according to the designer's lawyer was "the most powerful admission of wrongdoing"[4].

1) US Jurisprudence

Up to now, social network content did not constitute public data; nevertheless recent U.S jurisprudence provides the possibility of allowing the use of such data in court proceedings: according to the NY Supreme Court, the defendant failed to establish a factual predicate with respect to the relevance of the evidence. "Indeed, defendant essentially sought permission to conduct a "fishing expedition" into plaintiff's Facebook account based on the mere hope of finding relevant evidence" [5]. The NY Supreme Court validated the trial's court denial to compel disclosure of the plaintiff's Facebook account in a personal injury action. However, the Supreme Court did not go as far as to confirm the issuance of a protective order for the plaintiff as did the trial court, preventing the defendant from ever seeking the Facebook data. Such decision allows in the future the issuance of an order enabling access to social networking data if a relevant request is well justified. Until recently, litigants, did not realize the importance of information contained in social networking sites. In a recent case where the plaintiff sought damages for personal injuries and loss of enjoyment of life, the defendant requested and the Court granted an order for access to the plaintiff's Facebook and MySpace accounts to gather evidence contradicting the plaintiff's arguments. Indeed, the plaintiff had posted pictures and other public postings that proved she was capable of traveling and working, thus the Court held that these public postings justified the defendant's request, considered as relevant and reasonable[6]. This ruling ordered the plaintiff to give the defendant direct access to log in and view her Facebook and MySpace accounts.

Several recent U.S rulings tend to consider postings on Facebook public and deny protective orders for Facebook, MySpace and meetup.com pages, ordering the discoverability of such information[7]. The California Court of Appeal characterized the plaintiff's MySpace post as public, even though the plaintiff deleted it after posting it, thus rejecting a law suit claiming invasion of privacy because the defendant had re-post the initial plaintiff's post[8]. On the contrary, the U.S District Court in Nevada denied a motion requesting to force the plaintiff to allow direct access to her Facebook and MySpace accounts. This case involved claim of sexual harassment at work which led to the plaintiff's suicide attempts after quitting her job. The defendant argued that the plaintiff listed herself as single while married into MySpace, arguing that such finding affects the plaintiff's credibility. The Court refused by ruling, stating that the defendant's arguments represented only "suspicions or speculations as to what information might be contained in the private messages[9] and characterized the defendant's request as "fishing expedition".

Up to now, the US case law has made no general findings about the discoverability of social networking data depending on the nature of the cases or the way the discoverability request is made (directly from the litigant or via the social networking site).

Furthermore, a recent US ruling ruled on the nature of a posting on SNS and held that a posting without the author's consent constituted a breach of state law but not of privacy. More precisely, an employer who allegedly posted to an employee's Facebook and Twitter accounts without her consent faced liability for its actions, according to a federal judge in Illinois[10]. The plaintiff worked as the Director of Marketing, Public Relations and E-Commerce for an interior designer and the plaintiff contended that she created a "popular personal following" on Facebook and Twitter and that she also created a company blog called "Designer Diaries". In September 2009 she had an accident and she was hospitalized for months. During this time the defendant impersonated Maremont by writing Posts and Tweets to her personal Facebook and Twitter followers promoting their company. And even after Maremont asked the Defendants to stop, they continued until she finally changed her account passwords. The court ruled that Maremont had adequately alleged a commercial injury based on the defendants' deceptive use of her name and likeness and that they used her likeness to promote the business without her written consent in the violation of the state law but the court ruled that the Maremont had not adequately developed her alternate argument that defendants' intrusion into her personal "digital life" is actionable under the common law theory of unreasonable intrusion upon the seclusion of another. The case is now proceeding to discovery.

As this case demonstrates, social media litigation is a growing trend. Employers may unwittingly expose themselves to claims by assuming that all online activity related to the business is company property. Employers should clearly distinguish between the personal social media accounts of their employees and those that belong to the business itself. Personal employee accounts, even if used to promote company business, should not be accessed without the employees' express written permission. Clear written policies on social media use are the best way to clarify the respective roles and expectations of employees and employers.

2) Common law jurisprudence

The increasingly decisive role of Facebook in communications is undisputed. According to a 2009 Australian judgement, Facebook was a legally viable way to communicate, even regarding legal documents. The Camberra Supreme Court affirmed a request to serve legal documents via Facebook after repeatedly failing to serve the papers in person[11].

According to a Canadian Court, a litigant could not have serious expectations of privacy given that 366 people had already been granted access to his private site[12]. In this case, the plaintiff, after a serious car accident, sued the car driver seeking damages for the detrimental impact on her enjoyment of life and her inability to participate in social activities. The defendant's attorney discovered (before the trial) a public website with the name of the plaintiff, containing post-accident pictures of the plaintiff at a party as well as a Facebook account with the plaintiff's name and list of 366 Facebook friends; due to privacy settings that the plaintiff had set, access to her Facebook page was restricted. Thus, the opposing party sought for a court order imposing production of Facebook pages potentially containing relevant information. Despite the plaintiff's objection arguing that the defendant was on a "fishing expedition", claiming that only speculations on the real material on the site existed, the judge ordered Facebook pages to be produced, arguing that since Facebook is a

S.N.S where a large amount of photos are posted by its users, it was reasonable to assume that there would be relevant photos on the plaintiff's pages.

Another interesting decision dealing with the production of the access-limited contents of a Facebook profile is the one based on Leduc v. Roman case[13], in which the plaintiff sought damages due to a car accident, claiming suffering various ailments and loss of enjoyment of life. The opposing party discovered the plaintiff's Facebook account, to which access was allowed only to his Facebook friends and requested an order requiring the preservation of all information on Facebook profile and the production of the Facebook profile itself. The plaintiff argued once again that the mere existence of a Facebook account did not entail that relevant to the case material was posted on his Facebook site, trying to differentiate this case from Murphy case[14]. The court held that "(…) Facebook is not used as a means by which account holders carry on monologues with themselves, it is a device by which users share with others information about who they are, what they like, (…) in varying degrees of detail. A party who maintains a private or limited access Facebook profile stands in no different position than one who sets up a publicly available profile. Both are obliged to identify and produce any postings that relate to any matter at issue in an action. (…). To permit a party claiming very substantial damages for loss of enjoyment of life to hide behind self-set privacy controls on a website, the primary purpose of which is to enable people to share information about how they lead their social lives, risks depriving the opposite party of access to material that may be relevant to ensuring a fair trial.[15]"

Facebook has proved to be a professionally dangerous online tool, since several discharges caused by Facebook postings have been registered: For instance, an employee was fired by the American Medical Response for Connecticut, after the employee posted complaints about her boss on Facebook. The case was finally settled, the main argument being that the online comments constituted protective activity and that the discharge violated federal labor law[16]. In UK, an intern at Anglo Irish Bank was fired after his boss discovered an intern's photo at a Halloween party posted in Facebook while he requested a day off due to "family emergency"[17].

3) European Jurisprudence

a. French Jurisprudence

In a recent judgement, the Paris Court of First Instance (Tribunal de Grande Instance de Paris) [18] ordered Facebook France to withdraw a defamatory comment with picture of the Bishop of Soissons and condemned Facebook France to pay a fine of 500€ for each of day of delay in case of non compliance with the decision. Furthermore, the French Court ordered Facebook France to communicate all data permitting the identification of all authors of the defamatory pages as well as to withdraw all defamatory comments on a Facebook page regarding the Bishop and condemned Facebook to pay a fine of 500€ for each of day of delay in case of non compliance with the decision, because Facebook was considered to have incited racial hatred and have reproduced and hosted unlawful content. Nevertheless, Facebook appealed the decision and its appeal was granted on the grounds that Facebook France was not legalized to appear in Court, since it was only a branch office of Facebook UK, which in its turn was completely independent of Facebook Inc, the US company which is the

exclusive editor of the site and the only one controlling the Facebook content. In the meanwhile Facebook France never provided the ordered data, only withdrew the unlawful content.

Two judgements on the same matter at the council of the "prud'hommes" of Boulogne-Billancourt November 2010 concluded that the employer who produced a Facebook page of which the wall was accessible to the "friends of the friends" did not violate the private life of the two employees, dismissed for breach of discipline. At the point that this method of access surpassed the private sphere, the council considered that the method of proof based on the grounds of the dismissal, was lawful. Precisely, three employees of the corporation Alten had created a Facebook page the goal of which was to criticize their hierarchy. They had chosen to authorize the access "to friends of friends" and most notably the current and the former employees of the business. They had founded the "club of the harmful", virtual club at the core of which was to "making fun" of the superior hierarchic one, all day long, without the boss having ever realized anything and for several months. The court judged that, while participating in these exchanges, the employees had abused the right of expression, in the framework of the business by the item 1121-1 of the French labor code. They harmed the picture of their business infringing the functions of the service recruitment, thus having an effect on future employees. The council specified that while choosing this access method, their posts were likely to be read by exterior people to the business. It concluded that the dismissal "for the incitement of the rebellions against the hierarchy and for denigration towards the corporation Alten" relies on a real and serious cause.

b. Denmark "The Pirate Bay case"

On 5 February 2008, the district court of Frederiksberg, Copenhagen ruled that one of Denmark's largest ISPs, DMT2-Tele2, was assisting its customers in copyright infringement by allowing the use of The Pirate Bay, and that they were to block access to the site[19]. Although the ISP had decided to challenge the verdict with support from the Danish Telecommunication Industries Association, they finally complied with it and blocked access to The Pirate Bay. The Pirate Bay reacted by creating an alternate site (with instructions on how to work around the block), while the International Federation of the Phonographic Industry (IFPI) welcomed the block and encouraged other ISPs to follow suit. The verdict was affirmed in the Eastern High Court of Denmark on 26 November 2008. The Court found it undisputed that the website worked as index and search engine, allowing users of the website to get accessibility to files from each other. On the basis of the production of evidence and argumentation, the court held that an overwhelming part of the material exchanged through the website by the users are protected by copyright, administrated by the claimants and that the claimants had not given permission to the materials publication and accessibility. In addition, it was substantiated that the use of the website had a certain diffusion in Denmark.

Following the court's decision, TDC, Denmark's largest ISP and owner of most of the cables, decided to block access to The Pirate Bay as a preventive measure. Other Danish ISPs have commented that they would prefer not to intervene in their customers' communication, but have reluctantly put the block in effect in order to

avoid fines. Tele2's owner Telenor in turn appealed the high court verdict to the Supreme Court of Denmark, which in April 2009 accepted the case for processing.

c. Sweden

In Sweden, in February 2009 the Pirate Bay site's trial began, for copyright infringement. The defendants sentences imposed on the owners of the site were one year imprisonment and 30 million Swedish kronor (2.7 million euros). In May 2010, The Pirate Bay's Swedish internet service provider finally lost an appeal against an order to stop providing service to the site. Although the service provider had already complied with an earlier order in August 2009 and The Pirate Bay was thereafter hosted elsewhere, in June 2010 the ISP chose also to block their customers from accessing The Pirate Bay in its new location. One of the judges in the case later commented that the court's order didn't require the ISP to control their customers' access to the site, but the ISP wanted to avoid any risk.

The Pirate Bay Case caused political development in Sweden, leading to the creation of a political party called "the Pirate Party"**.** The main purpose of the party is to change the legal framework on copyright. It has also expressed different positions on trade and patent rights of users on the Internet. In 2006 it took part in the general elections in Sweden reaching 0.63%. On May 31, 2006, the Swedish police raided the place occupied by the Pirate Bay, causing the blocking of the page for 3 days. The above raid increased the party's popularity dramatically. In July 2006 the party organized demonstrations in Stockholm and Gothenburg. In February 2009 the Pirate Bay site's trial began, for copyright infringement. Following the disclosure of sentencing in April of that year, members of the party tripled in only one week. It is also very remarkable that the Pirate Party took part in the European Elections in 2009, electing a Member of Parliament after reaching 7,1%. The Swedish example gave impetus to other countries to found similar political parties. Officially, these kind of political parties exist in Germany, Austria, France, Spain, Poland and Finland and unofficially in USA, UK, Denmark, Argentina, Chile, Australia, Nederland's, Portugal, Czech, Slovakia and Slovenia.

d. Greece

In Greece, in March 2010 one of the administrators of the Greek pirate site "gamato.info" was arrested and sent to the Criminal Court by the Authorities of the Electronic Crime. Surveys of prosecutors began after a complaint lodged by the Society for the Protection of Audiovisual Works. As a result of investigations by the authorities, during the three and a half years of «gamato.info » operation, about 800,000 users, downloaded free in total 3.2 million film titles, music and computer software and the damage caused to the plaintiff company reached 15 million euros.

II. Special threats represented by mobile phone access to SNS

Another relative growing-up phenomenon refers to the increasing percentage of cell phone subscribers using their phone for social networking. Such technological development has been facilitated thanks to global positioning satellites permitting to trace a cell phone, while more and more SNS seek to capitalize on location

information, providing services such as showing to users where friends are in real time. Almost 134 million mobile users are estimated to access the SNS in Europe in 2012, most of them being largely unaware of security and privacy risks. Mobile users are exposed to many privacy threats such as identity theft, malware, corporate data leakage, device theft, user's position tracking and data misuse.

Efficient hackers may easily take control of a user's security credentials and then proceed to take full control of the user's account by modifying his setting, by posting malicious comments or even by spreading malicious software[20]. Another serious security risk includes the distribution of malware either through Facebook and Twitter or through the mobile itself, infecting the phone's contacts as well as SNS contacts. It is possible that an infected p/c will post a link containing malicious software, where users click, trusting the friend who posted it, not being aware that their friend has been hacked. One of the most "advanced" techniques used by hackers includes the creation of Twitter new accounts regarding the trendiest topics discussed on Twitter at that time and the posting of related messages. Such messages are contained in Twitter search results, leading unsuspicious users operating these searches to click on the infected link.

Another frequent phenomenon consists of the spread of business information through SNS leading to unauthorized disclosure of corporate sensitive data, affecting not only user's privacy but also professional reputation[21]. According to the Working Party of Art.29, Directive 95/46/EC on data protection[22] is also applicable to SNS providers even if their headquarters are located outside of the European Economic Area. Pursuant to an Opinion issued by the aforementioned Working Party on Online Social Networking (Opinion 5/2009 on online social networking 12-6-2009)[23], SNS providers are data controllers under the above Directive and on this purpose are recommended to remind SNS users that uploading information about other individuals may violate their privacy and thus, it should be done only with the individual's consent, offer privacy-friendly default settings to reduce the risk of unlawful processing by third parties and make aware SNS users about the privacy risks to themselves and to others when they upload information on the SNS. In other words, the real-time spread of data and information through SNS entail at the same time enormous benefits but can also cause serious damages, threatening users' privacy and personal and professional reputation. It seems that the most secure defence is awareness raising, since technical safeguards may prove to be easily out-to-date.

III. The role of ISPs regarding privacy and security issues in relation to SNS

a) Existing legal framework

Up to very recently, the principle of network neutrality regarding the role of Information Service Provider (ISP) prevailed globally, while no general obligation of monitoring hosted or transmitted content existed for ISPs in most legislations worldwide.

More precisely, according to the Art.(2a) of Directive 2000/31[24] "any service normally provided for remuneration at a distance, by electronic means and at the individual request of a recipient of services" constitutes information society services.

All issues regarding ISPs' liability are addressed in Art.12-15 of the above Directive. In art. 12 & 13[25], the Directive provides the conditions that need to be met for the exemption of an ISP from liability concerning the activities of more conduit and caching while art.14 of the same Directive provides for the exemption from liability when the activity consists of storage of information.

Thus, pursuant to EU law, an ISP is totally exempted from liability in case his activity is merely technical, automatic and passive, proving the absence of knowledge or control of the (data) information transmitted or stored in its communication network. This only refers to the activities of "mere conduit" and "caching" as explicitly analyzed in art. 12 and 13 of Directive 2000/31/EC. Regarding activities such as the storage of information, the ISP is not liable if he has not actual knowledge of illegal activity or information and upon obtaining such knowledge or awareness, he acts expeditiously to remove or disable access to the info. While hosting of information may benefit from an exemption if the requirements set out by Art.14 of 2000/31/EC are met, the ISP may incur potential criminal law or damage liability. According to an interpretation of "actual knowledge" of Art.14(1) of 2000/31/EC, a mere suspicion or assumption regarding the illegal activity would not be sufficient to fulfill the requirements "actual knowledge" but includes only past and present information, activity or facts indicating illegal activity. In light of the above, it must be noted that in many Member States the liability of a service provider, based on art.12,13,14 of Directive 2000/31/EC, would be excluded because of the lack of the subjective fault.

The principle of "notice and take down" is established by Art.14(1)(b) of Directive 2000/31/EC according to which "*Where an information society service is provided that consists of the storage of information provided by a recipient of the service, Member States shall ensure that the service provider is not liable for the information stored at the request of a recipient of the service, on condition that: […] (b) the provider, upon obtaining such* knowledge or awareness, acts expeditiously to remove or to disable access to the information."

The limitations to that principle are set out by Recital 46 of this Directive, which provides that the principle of freedom of expression and of procedures established for this purpose at national level should be observed when enforcing the removal or disabling of access.

It is also important to note that the Directive does not constrain member states to impose a general obligation on ISPs to monitor the information they transmit or to store or to seek the information they transmit or store or to seek actively facts or circumstances indicating illegal activity. Nevertheless, Member States may establish obligations for ISPs to inform promptly the competent public authorities of the alleged illegal activities undertaken or information provided by recipients of their service or obligations to communicate to the competent authorities at their request, information enabling the identification of recipients of their service with whom they have Storage agreements.

At the same time, in case of infringement in relation to hosting activities, (storage of information), a national Court or administrative authority may request the ISP to terminate or prevent such infringement; Member States may simultaneously establish

procedures governing the removal or disabling of access to such infringing information[26].

On this purpose, the Greek Law, transposing the above Directive[27], provides that ISPs are obliged to inform promptly the competent Greek authorities in case of alleged illegal information or activities undertaken by recipients of their service and to announce to the competent authorities at their request information facilitating the identification of recipients of their service with whom they have storage agreements [28].

In addition to the Directive 2000/31, EU has enacted Directive 2004/48/EC[29], pursuant to the provisions of which, Member States shall provide for the measures, procedures and remedies necessary to ensure the enforcement of the IP rights covered by this Directive. Those measures shall be fair and equitable and shall not be unnecessarily complicated or costly entail unreasonable time-limits or unwanted delays. Those measures, procedures and remedies shall also be effective, proportionate and dissuasive[30].

Furthermore, the aforementioned Directive ("the Enforcement Directive") also provides that in case of issuance of a judicial decision finding an infringement of an IP right, the judicial authorities may issue against the infringer an injunction aimed at prohibiting the continuation of the infringement (…) and right holders may apply for an injunction against intermediaries whose services are used by a third party to infringe an IP right[31]. Most of the provisions of Directive 2004/48/EC were transposed in Greek law through Law 3524/2007[32].

Pursuant to Art.8 of the Directive 2004/48/EC, Member States shall ensure that competent judicial authorities may order that information on the origin and distribution networks of the infringing goods/services shall be provided by the infringer and/or third parties found in possession of the infringing goods on a commercial scale or found to be using the infringing services or found to be providing on a commercial scale services used in infringing activities or being indicated as being involved in the production, manufacture or distribution of the said good or services. Thus, the Directive aims at detecting all actors involved in IP infringements, including intermediaries such as ISP, in contrast to TRIPS Agreement, which provides for an option of Member States to grant judicial authorities "the authority to order the infringer to inform the right holder of the identity of third persons involved in the production and distribution of infringing goods[33]. By choosing such wording, the Directive enables the disclosure of information regarding all persons involved in the infringing activities, trying to trace them without the help or cooperation of the infringer. Furthermore, according to Art.11 of Directive 2004/48 in cases where a third party is using the services of an intermediary to infringe an IP right but the true identity of that infringe remains unknown, an injunction may be given against an intermediary requiring the prevention of the continuation of a specific act of infringement as well as the prevention of repetition of the same or similar infringement in the future, under the condition that the principles of efficacy, dissuasiveness and proportionality are met. All conditions and procedures relating to such injunctions should be defined in national law.

According to EU authorities, the right to obtain information from third parties as provided in the Enforcement Directive was not transposed uniformly within EU: some Member States have created a special procedure providing for a right of information as a provisional measure, other Member States have conformed with the Directive, limitating such right only in the context of judicial proceedings. Pursuant to the findings of the Commission Report, an almost unanimous conclusion on the Enforcement Directive, seems to be that "after the transposition of the Directive, national Courts have seen a significant increase in request for information", helping to trace infringers easier,[34] especially directed towards ISPs. Unfortunately the enforcement Directive did not produce impressive results, since damages awarded in IP rights cases did not reflect significant increase after enacting the Directive[35]. Further, right holders complain arguing that nowadays the level of profit made by an IP infringement is substantially higher than the actual compensation awarded by the Courts. Thus, the Commission estimates that courts should possibly review the calculation of damages awarded to right holders, so as to take into account the unjust enrichment of the infringers to the detriment of the right holders. It must be stressed out that, according to the Commission Staff Working Document[36], accompanying the aforementioned Report, Greece has not transposed the Directive in its entirety yet and major Member States were late with the transposition procedure (France, Germany, Sweden and Portugal).

Another crucial remark pointed out by several Member States is the growing difficulty in gathering evidence for infringements committed via the Internet and the insufficiency of the Directive to address this issue. Special reference is made to Greece, where many requests made by right holders for Court orders have been rejected as "vague", when right holders are not able to specify exact details regarding such evidence. It must be noted, finally, that many provisions of the Enforcement Directive set out stricter and broader obligations than the ones provided by TRIPS Agreement[37], where some legal issues are not even covered.

Various data protection and privacy issues are also raised in relation to traffic management policies. ISPs participate in "traffic management" by collecting both content and traffic data of individuals. It is quite obvious and rather easy for an ISP to block or to examine each message or information sent over a network, since each communication is associated to a certain IP address.

First of all, traffic management mechanism may breach the confidentiality of communications guaranteed by Art8 of European Convention for Protection of Human Rights and Fundamental Freedoms and Art.7&8 of the Charter of Fundamental Rights of EU. Currently, the e-Privacy Directive[38] requires consent to enable "….listening, tapping, storage or other kinds of interception or surveillance of communication (…) by persons other than users. The only exemption to this provision is subject to a severe application of the proportionality principle, in order to prevent, investigate, detect or prosecute criminal offences or unauthorized use of the electronic communication system or in order to safeguard national security, defence, public security. Only security reasons justify the by-passing of the user's consent, as provided in Art.4 of the e-Privacy Directive[39]. Consent must be informed, specific and freely given. Such consent needs to be express and the user must be aware about the purposes of the traffic management policies. Furthermore, the user must be able to

understand the language used by the ISP and to understand what he is consenting to and for what purposes.

The proposal of EDPS[40] offering an alternative choice to users, such as internet subscriptions not subject to traffic management, does not seem to provide a viable solution, because it does not handle cases that need special treatment: users tending to breach law and use illegal content, for instance, will not choose of course to be subject to constant data monitoring. It is crucial to highlight that in case of content, according to art.5.1 of e-Privacy Directive[41], all users concerned shall provide their consent and not only the user sending content, which creates inevitably a dead-end situation.

Finally, regarding the Directive 2006/24/EC[42], its provisions are only applicable in the field of protection of IP if the offence has a criminal dimension, not applying to the content of electronic communications.

Recommendations by the Council of Europe

Recently, the Committee of experts on New Media of the Council of Europe has issued draft recommendations[43] and guidelines[44] regarding the protection of human rights by search engines and social networking providers. Some of the main recommendations state that the member states, in cooperation with the private sector actors and civil society, are recommended to develop and promote coherent strategies to protect and promote respect for human rights with regard to social networking services, in particular 1) by ensuring users are aware of possible challenges to their human rights on social networking services as well as on how to avoid having a negative impact on other people's rights when using these services; 2) by protecting users of social networking services from harm by other users while also ensuring all users' right to freedom of expression and access to information. Also, 3) by encouraging transparency about the kinds of personal data that are being collected and the legitimate purposes for which they are being processed, including further processing by third parties and by preventing the illegitimate processing of personal data. In the field of users control over their data the committee recommends that the default setting for users should be that access is limited to self-selected friends; that the users are informed about the need to obtain the prior consent of other people before they publish their personal data, in cases where they have widened access beyond self- selected friends.

b) ECJ jurisprudence

Up to now, the European Court of Justice (ECJ) has not issued an ad hoc decision regarding the role of ISPs in relation to SNS. Thus, the recent ECJ jurisprudence related to ISPS may serve as an enlightening example of future ad hoc decisions.

According to the ECJ, "a fair balance should be struck between the various fundamental rights protected by the Community legal order"[45], more precisely between the right to property, including IP rights and the right to data protection, both constituting fundamental rights directly recognized and expressly protected by the Charter of Fundamental Rights of the EU[46]. Nevertheless, none of the ECJ judgements entail that either right prevails over the other.

Pursuant to ECJ case law[47], ISPs may incur "secondary liability" or "accessory liability", referring to the possible liability of an ISP for infringement committed by users of the service. Furthermore, if the service provider has actual knowledge of illegal activity and is aware of facts or circumstances from which the illegal activity is apparent and upon obtaining such knowledge, does not act expeditiously to remove or to disable access to (infringing) info, then it will be held liable for such infringement on the legal grounds of art.12,13,14 of Directive 2000/31[48].

As already mentioned, regarding ISP liability, the notion of "actual knowledge" of the ISP, as contained in Art.14(1) of 2000/31/EC, does not entail a mere suspicion or assumption regarding the illegal activity. Nevertheless, it is interesting to follow the analysis of the Advocate General in Case C-324/09, who argues that if the ISP provider is notified about an IP infringement and the same user continues or repeats the same infringement, then the notion of "actual knowledge" is concluded and the exemption from liability for the ISP does not apply[49]. It remains to wait whether the Court will approve such approach.

Another anticipated judgment will be the one in case C-461/10, where the Swedish Court requested for a preliminary ruling on (the question) whether Directive 2006/24/EC amending Directive 2002/58/EC (the data storage Directive) precludes the application of a national provision based on Directive 2004/48/EC (the Enforcement Directive), according to which an ISP may be ordered to give a copyright holder information on a subscriber in civil proceedings, thus facilitating the identification of a particular subscriber claimed to have committed an infringement. In the same reference the Swedish Court also asks whether the fact that the Member State has not implemented the data storage Directive despite the fact that the period prescribed for implement action has expired, has any impact on the above ruling[50].

At the same time, the ECJ is called to rule whether Directives 2001/29 and 2004/48 in conjunction with Directive 95/46, 2000/31, 2002/58 permit Member States to authorize a national Court before which substance proceedings have been brought , to order a hosting ISP to introduce for all its customers in abstracto and as a preventive measure at its own cost and for an unlimited period, a system for filtering most of info stored on its servers in order to identify on its servers electronic files containing musical, cimenatographic or audiovisual work in respect of which SABAM claims to hold rights and subsequently to block the exchange of such files[51].

c) Australian Jurisprudence

The Common Law countries have already faced many cases of ISP liability, among which one of the most interesting is the one issued by the Federal Court of Australia that held in a recent judgement[52] that an ISP (namely "iiNet") was not responsible for copyright infringement undertaken by their customers. In this case, ISP's customers infringed copyright. The question was whether iiNet authorized that infringement, by failing to taking any steps to stop infringing conduct. Nevertheless, according to the Australian Court, the knowledge of the infringement by the ISP and the absence of any act to stop it did not entail "authorization", because the provision of Internet access constitutes a precondition and not the "means of the infringement". The Court also held that the mere use of the Internet did not establish per se an infringement to copyright holders. Pursuant to the Court analysis, the "means" of infringement

encompassed the electronic mechanism used to distribute large quantities of data, over which the ISP had no control at all. The Australian Court also held that national law does not allow the notification, suspension and termination of customer accounts, as a relevant measure to prevent copyright infringement. The Court goes further to its analysis stating that unlike the decisions in Kazaa and Cooper, iiNet did not deliberately favour, approve or countenance copyright infringement, because it did not deliberately proceed to any act to achieve an infringing activity. The Court concludes that "an ISP such as iiNet provides a legitimate communicational facility which is neither intended nor designed to infringe copyright"[53]. The aforementioned case resulted in a landmark judgement with great interest for the whole motion picture industry. It is noteworthy that the applicants in the Federal Court proceedings included 33 motion picture companies among which Universal Studios, Paramount Pictures, Warner Bros, Disney, Columbia Pictures, Twentieth Century Fox, Village Road Show, NBC Studios, etc.

The aforementioned judgement was recently appealed by RoadShows Films leading to a dismissal[54] of the appeal. The Court ruled that the ISP conduct did not amount to authorization of the primary acts of infringement on the part of iiNet users. Nevertheless, the Court held that ISPs can be found liable for authorizing their users for infringement under specific circumstances, namely if ISP has been provided with "unequivocal and cogent evidence of the alleged primary acts of infringement" by use of the ISP service in question and copyright owners had proven that they had undertaken to reimburse ISP for the reasonable cost of verifying the particulars of the primary acts of infringement and of establishing and maintaining a regime to monitor the use of the ISP service to determine whether further acts of infringement occur and to indemnify ISP in respect of any liability reasonably incurred by ISP, as a consequence of mistakenly suspending or terminating a service on the basis of allegations made by copyright owners".

Apart from other comments, it is crucial to underline the reserve of the judgement on ISP's liability regarding future infringements. As judge Emmett held "It does not necessarily follow from the failure of the present proceeding that circumstances could not exist whereby iiNet might in the future be held to have authorized primary act of infringement"[55].

d) Italian Jurisprudence

In February 2010 an Italian court in Milan found three Google executives guilty of violating applicable Italian privacy laws. The executives were accused of violating Italian law by having allowed a video showing an autistic teenager being bullied to be posted online. The Google executives were fined and received six- month suspended jail sentences. Richard Thomas, the UK's former Information Commissioner and Senior Global Privacy Advisor to Hunton & Williams said that the case is "ridiculous" and "it is unrealistic to expect firms to monitor everything that goes online." New York Times reported on this case "The court found that Google had an obligation to make users more aware of its EU privacy policies and cited Google's active marketing of its Google Video site as indicative of the company's profit motive for not removing the video sooner."

IV. Notice and take down regime

Since the Enforcement Directive is not obliging Member States to adopt specific provisions regarding the issuance of conditions of injunctions against intermediaries, it is left at the discretion of each State to determine when and how an injunction can be issued against an intermediary. Most national legislations do not choose to involve intermediaries to the injunction procedure. The Commission in its recent Report to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions[56], seems rather favourable regarding the application of "notice and take-down" policy, supporting the view that injunctions should not depend on the liability of intermediaries and that intermediaries should be more involved to the aforementioned injunction procedure.

It is crucial to note that supporters of graduated response systems argue that such systems are well justified on economic grounds because of the obvious reduction of litigation costs associated with copyright enforcement. Not to mention that the US experience shows that only few copyright infringement cases were finally brought to courts, while the majority led to out- of- court settlements with insignificant gain for the plaintiff's (copyright holders), since the fines imposed did not prove to be threatening for IP infringers[57].

Notice and take down procedures are already functioning in Finland, France, US, and Canada and relevant legislation has been enacted but not yet implemented in New Zealand, Spain and UK.

a) HADOPI Law- France

The modified version of Hadopi Law, finally approved by the French Constitutional Council, secures the fair trial principle by vesting the judge with the authority of subscriber accounts termination[58]. Thus, the revised version of Hadopi Law provides that Hadopi Authority could issue the first two warnings to infringes in order to stop their illegal downloads but the third warning would have to be issued by a judge, so as the right to a fair trial and to the principle of the presumption of innocence are preserved. Only after a judicial order, may the suspension of Internet access take place. At the end of 2010, the Hadopi Authority had sent 70000 recommendations by email to internet users. According to the French Law n° 2011 264 (of 11-03-2011), the data collected by Hadopi are automatically transmitted to the judicial authorities in case of a request of a request and preserved during one year.

b) Digital Economy Act-U.K.

The Digital Economy Act 2010 is in force in U.K. as of 12-06-2010, facing though an uncertain future. It has adopted a graduated response scheme reaching to disconnecting Internet accounts used for persistent copyright infringement. It is worth noting that Britain's two largest ISPs, in order to decide whether the Act conflicts with existing EU legislation, have sought for a judicial review of the Act on the grounds of having the potential to harm citizens and impact businesses also claiming that its provisions are not proportionate and do not respect privacy law nor comply with EU law on ISP liability. The High Court of Justice granted the review permission

on November 2010 and now the DEA is to be the subject of judicial review and a parliamentary inquiry.

It must be stressed out that the main grounds of ISPs application for judicial review focus on 1) UK Government's failure to give the European Commission sufficient notice for proper scrutiny of legislation, 2) non compliance of Digital Economy Act with existing EU legislation on data protection and privacy, 3) Digital Economy ACT's incompatibility with existing EU e-commerce legislation 4) disproportionality of DEA regarding their impact on ISPs business and consumers. The judge after a long hearing at London's High Court, granted permission for the judicial review on each of the four legal grounds aforementioned.

It is crucial to note that the ISPs confidence regarding a positive outcome on the judicial review is coupled with their attempt to keep the proceedings running in order to exert legal pressure in addition to political pressure on the Government to change its approach. The verdict of the High Court may take up to eight weeks while an appeal from the losing part is extremely likely as well as a possible referral to the European Court of Justice. Thus, it is still unclear whether the anti-piracy measures will be in place.

c) Sinde Law-Spain

Having one of the highest rates of illegal file-sharing in Europe, Spanish Government finally passed regulation (Sinde law), intending to reduce such high levels of illegal file sharing. Unlike France and UK, the Spanish regime includes a fast-track system for closing "unlawful" websites quickly, after a relevant judicial order, as well as the creation of an Intellectual Property Commission, depending on the Ministry of Culture, being in charge of deciding which sites should be blocked or what content is infringing and ask the person responsible for the site to remove it, after getting a judge authorization.

d) Copyright (New Technologies) Amendment Act 2008-New Zealand

New Zealand's legislative approach to graduate response is the Copyright (New Technologies) Amendment Act 2008[59], introducing a notice and take down regime in New Zealand, requiring from ISPs to "adopt and reasonably implement a policy that provides for termination, in appropriate circumstances, of the account with that Internet service provider of a repeat infringer". After a huge public debate, a bill establishing a three-notice regime to discourage illegal file sharing was passed in New Zealand Parliament on 14-4-2011[60]. The regime will come into effect on 1-9-2011 including ISPs sending warning notices to their customers informing them they may have infringed copyright. After receiving notification by ISPs that three warning notices have been sent to users by the ISP, copyright holders may apply to the copyright tribunal for compensation and at the same time request to a District Court for an order requiring the ISP to suspend the account holder's Internet access for up to six months.

V. ACTA AGREEMENT

The ACTA is an ambitious legal project, launched by Japan and U.S in order to create a new international legal framework, establishing international standards on IP rights enforcement. ACTA aims at increasing levels of IP protection in comparison to international standards created by the TRIPS Agreement. ACTA provides for the creation of a new governing body ("ACTA Committee") outside existing international institutions (i.e WTO, WIPO, etc) to address IP enforcement. It is important to note that ACTA is using- as legal foundations- existing international agreements such as TRIPS, trying to address all IP issues that are not covered up to now by TRIPS. ACTA, after its official signing, will constitute the new international standard for intellectual property enforcement. ACTA is based on 3 fundamental pillars, (a) international cooperation, (b) enforcement practices and (c) legal framework for enforcement of IP rights.

ACTA focuses on civil and digital enforcement, border measures and criminal enforcement of IP law on international level. ACTA in its latest released version does not urges participants to introduce mandatory graduated response regimes nor requires disconnection for repeat infringers and more important, omits to refer to any notice and takedown mechanism, only outlining the need of cooperation between right holders and ISPs, in order to address relevant infringements in the digital environment.

In contrast to TRIPS, ACTA contains digital enforcement provisions. Nevertheless, the final draft[61] does not introduce any notice and take down regime, it only stresses out the need to take "effective action against an act of infringement (…), including ***expeditious*** remedies to prevent infringement (…)[62]. It also goes further requiring "endeavour to promote ***cooperative efforts within the business community*** to effectively address trademark and copyright or related rights infringement[63]", which refers to private initiatives between ISPs and users, based on US and Ireland examples. However, the implementation of such private graduated response regimes within EU seems legally risky, since the condition of compliance with fundamental EU law principles such as freedom of expression, fair process, and privacy, may be jeopardized. In addition to the above, ACTA provides for the possibility of countries to permit competent state authorities to "*order an online service provider to* ***disclose expeditiously*** *to a right holder* ***information*** *sufficient to identify a subscriber whose account was allegedly used for infringement, where that right holder has filed a legally sufficient claim of trademark or copyright or related rights infringement, and where such information is being sought for the purpose of protecting or enforcing those rights*[64]". A thorough look at the previous ACTA drafts proves that EU pressures led to the inclusion of specific safeguards regarding the enforcement procedure, relating to freedom of expression, fair process, and privacy.

CONCLUSION

One of the main international priorities regarding IP enforcement remains the adoption of more efficient enforcement regimes either public or private, mandating a more active role for ISPs. ACTA preamble evidences the need for cooperation between right holders and ISPs, in order to address relevant infringements in the

digital environment. Although ACTA does not impose a mandatory international graduated response mechanism, it expressly supports the implementation of private, voluntary graduated response mechanisms in countries where such mandatory systems do not exist, the US and Ireland serving as adequate and efficient examples of private implementation of graduated response regimes. It must be outlined though that advanced technological solutions required to address copyright infringements entail costly investments which seem doubtful during an international recession period.

Thus, the real danger that ACTA represents is the constant global pressure on policymaking towards the establishment of voluntary graduated response regimes worldwide, which may render the principle of network neutrality inactive and possibly hinder fundamental principles such as the freedom of expression and the right to privacy. It goes without saying that the above regimes will have an explicit and direct impact on SNS as well, making it extremely controversial, if not unfeasible, to strike the balance between copyright interests and the fundamental human rights of privacy, freedom of expression and the right to a fair trial.

Endnotes

[1] www.guardian.co.uk/technology/2010/jam/11/facebook-privacy
[2] www.voici.fr/potins-people/les-potins-du-jour/zahia-perd-son-proces-face-a-vsd/354623, www.lefigaro.fr
[3] http://www.huffingtonpost.com/2010/03/25/twitter-hacker-that-hit-o_n_512800.html
[4] http://newsinfo.inquirer.net/inquirerheadlines/nation/view/20110306-323732/Courtney-Love-says-sorry-pays-430K-in-Twitter-row
[5] Mc Cann v. Harleyville Insurance Company of New York, 20b N.Y App.Div.LEXIS 8396 (Nov. 12, 2010).
[6] Romano v. Steel case Inc., 907 N.Y.S. 2d 650 (2010)
[7] Led better v. WalMart Stores Inc., 2009 U.S. Dist. LEXIS 126859, at 4-5 (D.Colo.Apr.21,2009)
[8] Moreno v. Hanford Sentinel Inc., 172 Cal. App.4th 1125, 1130-31 (2009)
[9] Mackel prang v. Fidelity National Title Agency of Nevada Inc., 2007 US Dist. LEXIS 2379 (D.Nev.Jan.9,2007)
[10] http://www.huntonlaborblog.com/2011/03/articles/employment-policies/look-before-you-tweet-employer-may-be-liable-for-impersonating-employee-on-facebook-twitter/
[11] http://www.telegraph.co.uk/news/newstopics/howaboutthat/3793491/Australian-couple-served-with-legal-documents-via-Facebook.html
[12] Murphy v. Perger (2007) oJ. No 5511 2007 WL 5354848 (ont.S.C.)
[13] Leduc v. Roman, 2008 CanLII 6838 (ont.S.C.), at para.17 [Leduc]
[14] Murphy, supra note
[15] Leduc, supra note, at paragraphs 31-32 & 35.
[16] www.socialnetworkinglawblog.com
[17] www.facebook.com/nde.phd?nde_id=126911673991090
[18] Ordonnance de Référé du 13.04.2010, Tribunal de Grande Instance de Paris, No RG 10/53340, www.scribd.com/doc/29980259/OrdonnanceRéférédeParis
[19] Decision of 5-2-2008, Bailiff's Court of Frederiksberg, FS 14324/2007, available at http://ssrn.com/abstract=1093246
[20] ENISA "Security issues in the context of authentication using mobile devices (mobile eID), 2008, http://www.enisa.europa.eu/act/it/eid/mobile-eid/?searchterm=security
[21]http://www.dailymail.co.uk/news/article-1082437/BA-check-staff-post-comments-smelly-passengers-Facebook.html?To=1490
[22] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal L 281 , 23/11/1995
[23] http://ec.europa.eu/justice_home/fsa/privacy/workinggroup/wpdocs/2009.en.htm

[24] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce') Official Journal L 178 , 17/07/2000
[25] Supra note 24
[26] Art.14§3 Directive 2000/31/EC, supra note 24
[27] Π.Δ 131/2003, ΦΕΚ Α΄ 116/16-05-2003
[28] Art.14 Π.Δ 131/2003
[29] Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of Intellectual Property Rights, Official Journal of the European Union L 157 of 30 April 2004
[30] Art.3 General Obligation, Directive 2004/48/EC, supra note 25
[31] Art.11 Directive 2004/48/EC, ibid
[32] ΦΕΚ Α΄ 15/26-01-2007.
[33] Art.47 TRIPS AGREEMENT, Agreement on Trade-Related Aspects of Intellectual Property Rights, http://www.wto.org/english/tratop_e/trips_e/t_agm0_e.htm
[34] Commission staff working Document, 22.12.2010, COM (2010) 779 final,
[35] Report from the Commission to the European Parliament, the Council, the European economic and social Committee and the Committee of the Regions, Application of Directive 2004/48/EC of the European Parliament and the Council of 29 April 2004 on the enforcement of intellectual property rights SEC(2010) 1589 final
[36] Supra note 30
[37] Supra note 29
[38] Art5§1, Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002, *OJ L 201, 31.7.2002*
[39] Supra note 34
[40] EDPS comments on Net Neutrality and Traffic Management/6-10-2010, available at http://ec.europa.eu/information_society/policy/ecomm/doc/library/public_consult/net_neutrality/comments/04eu_national_regional_ministries_authorities_incl_berec/edps.pdf
[41] Supra note 34
[42] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, Official Journal L 105/54 13.4.2006.
[43]http://www.coe.int/t/dghl/standardsetting/media/mcnm/MC-NM(2010)003_en%20Draft%20Rec%20%20SNS.asp#TopOfPage
[44]http://www.coe.int/t/dghl/standardsetting/media/mc-nm/MC-NM(2011)008_enGuidelines%20for%20soc%20Netw%20prov.asp#TopOfPage
[45] Judgement of 29-01-2008 in the case C-275/06
[46]Art.7,8,17(2), Charter of Fundamental Rights of EU, also available at http://www.europarl.europa.eu/charter/default_en.htm
[47] C-324/29, OJ C 267 of 07.11.2009, p.40
[48] Supra note 24.
[49] http://curia.europa.eu/jcms/upload/docs/application/pdf/2010-12/cp100119en.pdf
[50] Case C-406/10, 2010/C 317/42, OJ 2010 C/317/24
[51] Case C-360/10, 2010/C, 288/30, OJ 2010, C288/18
[52] Road Show Films Pty Ltd v iiNet Limited (n3) [2010] FCA 24, (04.02.2010), www.austlii.edu.au/au/cases/cth/FCA/2010/24.html
[53]As the ISP did not create and did not control the system mechanism allowing the film copying and the mere failure to terminate users, accounts did not signify authorization of copyright infringement.
[54] Road Show Films Pty Ltd v iiNet Limited [2011] FCAFC 23 (24.02.2011), www.austlii.edu.au.au.cases/cth/FCAFC/2011/23.html
[55] Supra note 45
[56] Supra note 35
[57] Decreasing Copyright Enforcement Costs. The scope of graduated response, Olivier Bomsel & Heritiana Ranaivoson, Review of Economic Research on Copyright Issues, 2009, vol. 6 (2), pp.13-29.
[58] Law No 2009-669 of June 12, 2009, amended September 15, 2009, Journal Officiel de la Republique Francaise (J.O.J), http://www.assemblee-nationale.fr/13/pdf/ta/ta0332.pdf
[59]Available at http://www.parliament.nz/en-NZ/PB/Legislation/Bills/b/2/a/00DBHOH_BILL7735_1-Copyright-New-Technologies-Amendment-Bill.htm

[60] Available at http://www.parliament.nz/en-NZ/PB/Legislation/SOPs/4/lb/49DBHOH_SOP1380_1-Copyright-Infringing-File-Sharing-Amendment-Bill.htm
[61] ACTA - December 3, 2010, *available at* http://www.ustr.gov/webfm_send/2417.
[62] ACTA, Section 5, Art. 27.1
[63] ACTA, Section 5, Art. 27.3
[64] ACTA, Section 5, Art. 27.4