JULY 2017

INTERNATIONAL SURVEY

Key lessons learned from international benchmarking

Hadopi

INTRODUCTION

The fight against copyright infringement on the Internet is a global challenge facing piracy practices of a large number of web users who moved from peer-to-peer to streaming uses and recently, towards IPTV piracy.

Many countries are concerned with the emergence of multimedia players[1] pre-configured with third-party applications (add-ons), which enable or facilitate access to illegal content. These software packages can be installed on most terminals, in particular set-top TV boxes (sold between 50 and 100 euros). They provide a very cheap service threatening the business model of exclusive live broadcasting rights for sports events and premium content offers. Their attractiveness owes much to the fact that they constitute a one-stop shop as opposed to a somewhat fragmented legal offer potentially perceived by the consumer as expensive to access the same content variety. Actions taken against them are increasing in particular in the United Kingdom, Canada, the United States and Portugal, and right holders internationally rally around an IPTV task force. In a case recently brought before the Court of Justice of the European Union (CJEU) by the Netherlands, this jurisdiction ruled that selling such boxes constitutes a communication act to the public.

Piracy has become a multifaceted and sprawling phenomenon, exceeding the initial question of the sharing of copyrighted works.

Stakeholders, as a result, are pressing hard towards the adoption of a multi-pronged approach to tackle the threat that arises from this parallel ecosystem. Their main recommendations focus on adapting and streamlining judicial procedures', promoting self-regulation based on soft law and extrajudicial mechanisms, building-up synergies between public awareness campaigns and targeted legal actions against large-scale counterfeiting.

However, costs and efficiency assessment of such actions lead public and private actors to reconsider anti-piracy and anti-counterfeiting actions.

Thus, the costs incurred by market players (ISPs and right holders) and the evolution of uses led several countries (Australia, Canada, United States and New Zealand) to review or even drop the implementation of multiple-step warning systems, all of which were devoid of a last stage including a financial penalty. Likewise, in numerous countries, because of financial constraints, right holders do not send formal compensation notices to web users. Instead, they target big down-or up loaders of infringing materials and reinforce applicable sanctions.

In the fight against commercial counterfeiting, actions need to be efficient and financially balanced. With the protected status of hosting providers or territorial limits, other steps are taken to involve actors who can contribute to the fight against copyright infringement by not condoning it or taking benefit from it. The efficiency of a legal action relies on speed and accuracy of gathering evidence of the infringing character of the websites, containing cost of legal actions and preventing "mirror sites" from reappearing.

This summary proposes a typology of existing mechanisms to fight online-counterfeiting, implemented or contemplated in the eighteen countries surveyed, depending whether they are targeting web users (by setting up a mass logic or more targeted) (1) or commercial counterfeiting (by associating digital sector market players in the fight against massive counterfeiting streaming websites, direct download, or links) (2).

As they are aiming at web users, initiatives to promote legal offer – usually a portal – are tied to mechanisms targeting web users.

1. Kodi software is the most familiar.

1 | MECHANISMS FOR WEB USERS: FROM AWARENESS TO REPRESSION

Actions towards web users have different aspects:

- Mass communication to assist users towards the change of their behavior with the use of legal offer raises awareness about the risks of illegal practices. In most countries encouraging and promoting legal offer constitutes the primary aspect of piracy fighting;

- Targeted measures intended for web users who make available copyrighted contents on peer-to-peer networks. These measures include multiple-step warning systems and strictly compensatory solutions. In some cases, both can be combined.

PROMOTING THE LEGAL OFFER AND ENGAGING IN MASS COMMUNICATION CAMPAIGNS

Actions taken to raise web users' awareness address risks associated with sharing or accessing contents illegally, promote legal offer and provide technical advice and resources to help them change their behavior.

These communication actions often take the form of public awareness campaigns, sometimes targeting a specific population, such as young audiences. Thus, in the United Kingdom, before the launch of the multiple-step warning system, an awareness campaign was set up with the broadcast of an advertising campaign called "Get It Right from a Genuine Site" (commercials on television, creation of a dedicated web site)[2] and animated films to raise awareness of legal offer among the younger generation.

Other strategies include:

- Communicating, where appropriate with the support of web users who have been convicted, about anti-counterfeiting actions and the convictions (Japan, New Zealand, the Netherlands) and on multiple mediums, such as vectors used by web users to illegally share infringing contents (UGC[3] platforms, social networks, etc.);

- Warning web users about the hazards associated with the browsing of unlawful websites (computer viruses, personal data theft, unsolicited advertising). In fact, Canadian and American reports recommend such an approach. Likewise, in Australia, once copyright holders obtained the first blocking decision at the national level, they associated along with their communication plan a warning about malwares and security risks linked to illicit websites.

LABELLING THE LEGAL OFFER

In Germany, the music union has created a label (Playfair[4]) granted to websites considered as legal. Audiovisual sector's copyright holders have created a portal (was-ist-vod.de) listing platforms offering a legal offer.

In Japan, the music industry has created a label (L Mark) to help web users identify legal offers. In South Korea, the Clean site initiative, launched in 2015 led to the creation of a dedicated website administered by public authorities, which certifies the legality of websites displaying cultural content. Platforms can then include the Clean site logo on their pages. Certification is open to every platform, including those who want to change their model and offer legal content. The certification process requires checking whether the platform ensures copyright protection by allowing the notification of illegal contents, by offering a space dedicated to the promotion of the legality of contents, by implementing a specific policy for repeat offenders, by using dedicated manpower and by cooperating with right holders as well as with the government.

2. www.getitrightfromagenuinesite.org
3. UGC: user generated content.
4. www.playfair.org/startseite

SETTING UP PORTALS DEDICATED TO THE PROMOTION OF LEGAL OFFFER

These portals are set up in a cross-cutting or sectorial approach (in particular through platforms dedicated to audiovisual in Germany, Australia, Denmark, Spain, the United States, Italy, Japan, the Netherlands, Portugal, the United Kingdom, Sweden). In Europe, this initiative was carried out by the European Observatory for intellectual property right infringements of the European Union office for Intellectual property (EUIPO) through the Agorateka project which aims at creating a European aggregator of legal offer. At first, the works relied on the feedback of existing aggregators to accompany pilot countries in the development of their own national aggregators in order to create a European portal of all national aggregators. United Kingdoms' Get It Right from a Genuine Site advertising campaign included a website providing a list of "sincere" websites. Similarly, in Japan, the Manga-anime guardians anti-piracy project, aiming at the reinforcement of mangas' protection, has also created a web site listing legally available mangas on the Internet[5].

DISPLAYING MESSAGES ON HOMEPAGES ON INFRINGING WEBSITES SUBJECT TO A BLOCKING MEASURE

Displaying messages on homepage infringing websites subject to a judicial blocking measure. Homepage mandatory display of information messages explaining the underlying reasons for the infringing website blocking is increasingly being implemented (e.g.: Denmark, Portugal). The Swiss project is more ambitious: it encourages copyright holders to provide legal offer of the infringing content (in any form whatsoever, whether online or not).

ACTIONS ASSOCIATING SEARCH ENGINES TO DEMOTE MASSIVELY COUNTERFEITING WEBSITES

Right holders face the need to perfect their search engine optimization strategy (Search Engine Optimization). In the United Kingdom, search engines[6] and copyright holders[7] signed an agreement in February 2017, under the *aegis* of the Government. In this agreement, which is a non-legally binding code of good practice, Google and other main search engines (Bing, Yahoo, etc.) agreed to sub-reference (and thus removing the results from the first results pages) massively counterfeiting reported websites. The same approach has been adopted in the Netherlands, where some initiatives have been carried out to redirect web users who use the keywords "torrents" or "illegal download" via search engines to the legal offer portal.

MULTIPLE-STEP WARNING SYSTEMS DIRECTED AT INTERNET SUBSCRIBERS WHOSE CONNECTION HAS BEEN ALLEGEDLY USED TO SHARE COPYRIGHTED WORKS VIA PEER-TO-PEER NETWORKS AND APPLICATIONS

Foreign multiple-step warning systems notifying allegedly infringing Internet subscribers and reminding them of copyright legal framework and potential sanctions involved in case of violation are not necessarily combined with a predetermined sanction process or with graduated steps in case of repeat infringement.

In the United Kingdom, the system of recommendations sent to peer-to-peer users, introduced in the first quarter of 2017 with the support of the Motion Picture Association (MPA) does not impose financial penalties at the end of the process in case of repeat infringement. Financed by right holders and ISPs, it is part of a wide public awareness campaign called "Get it Right from a genuine site". This new strategic approach, under the impulse of public authorities, will be evaluated in three years. These systems rely on self-regulation and voluntary cross-industry initiatives, supported to various degrees, by public Authorities (in the United States and the United Kingdom), by the legislator (Canada, New Zealand, Switzerland, Taiwan) or by judicial courts (Ireland). However, judicial courts being generally required to enforce sanctions, evidence gathering via such systems may provide a base for copyright litigation against subscribers.

5. www.manga-anime-here.com
6. Google, Microsoft (Bing) et Yahoo for the search engines.
7. The British Phonographic Industry (BPI) for music and the Motion picture Association (MPA) for audiovisual.

Such systems aim at:
• Strictly raising public awareness such as in the United Kingdom;
• Facilitating legal proceedings initiated by right holders (New Zealand, Switzerland) even if there is no sanction embedded in such warning systems;
• The implementation by ISPs (in the United States, Ireland, Taiwan) or platforms (South Korea) of mitigation measures directed at their allegedly infringing subscribers, including reduction of Internet connection speeds and redirection to a landing page , if need be under judicial court supervision.

Lessons can be drawn from these systems which, to various degrees, failed to deliver the anticipated results.

A first set of difficulties has to do with the willingness of ISPs to play the rules, especially since they are not legally bound and are barely held responsible for failing to send warnings or fulfilling their commitment to sanction their customers. Right holders do not actually have leverage on the ISPs to that effect.

A second set of difficulties relates to the cost sharing between ISPs and right holders.

Thus, in early 2016, a disagreement on cost sharing prevented the implementation of a gradual response system in Australia. In New Zealand, the system had been limited from the start, to the musical sector, because the audiovisual sector considered that it was too expensive. The musical industry sent notifications from 2011 to mid-2016 but then stopped because it was too costly. A final set of difficulties has to do with the relevancy of these systems as peer-to-peer practices tend to decline in comparison with other copyright infringement practices. Thus the debate focuses on value for the money, better targeting these systems intrinsically limited to peer-to-peer practices and reinforcing related sanctions.

In Canada, right holders criticize the notification system because it is purely educational (even in the event of a repeat offence) and because of the difficulties of implementation with ISPs. Some right holders now directly send allegedly infringing subscribers formal notices including a designated compensation amount for out-of-court settlement.

In the United States, after four years of implementation, it appeared that despite the educational efforts and the warnings sent, some subscribers kept sharing copyrighted works. A return on investment deemed insufficient, the disagreement on the repartition of costs between right holders and ISPs and the latter's reluctance to implement measures to degrade offending subscribers' Internet connection led, by mutual agreement, to the cancelling of the Copyright Alert System in the first quarter of 2017.

COMPENSATION SYSTEMS

Damage compensation may take place before trial as part of an amicable solution after the right holder sent a formal notice to the infringer.

Regarding copyright infringement on peer-to-peer networks, compensation formal notices directly sent to infringing subscribers by the legal counsels of right holders are multiplying (Australia, the United States and the United Kingdom).

In Canada, the warning system, initially intended for educational purposes only, is sometimes being used by American right holders to claim the payment by allegedly infringing subscribers of sums of money. A reverse class action is currently pending. Initiated by a right holder in order to generate case law with a view to reducing the cost of IP addresses identification facilitating a mass compensation litigation against offenders.

In the United Kingdom, considering the number of observed abuses, a court decision called "Golden Eye[8]" provides a legal framework for right holders in so doing and states that:
• The right holder's letter must indicate that despite the injunction to reveal the identity of the subscriber, he/she is not yet regarded as a counterfeiter;
• The response must be sent without undue delay.

In the Netherlands, Stichting BREIN, the right holders association fighting against piracy, chose a compensation

8. High Court of Justice, March 26, 2012, Golden Eye : www.bailii.org/ew/cases/EWHC/Ch/2012/723.html

mechanism which only focuses on big file sharers, regardless of the technology used. It uses a dedicated software, which enables the identification of IP addresses of primo up loaders and/or big up loaders on peer-to-peer networks. The goal is to obtain transactional agreements with the alleged counterfeiters or, if it fails, to prosecute them. The personal data protection authority approved the software in 2016, however it imposed on Stichting BREIN an obligation to prior communicate on the campaign launched with this new software.

Germany attracts a lot of attention because it organizes by law a broad scope compensation system targeting infringing subscribers. German right holders request companies dedicated to peer-to-peer networks surveillance to collect IP addresses of infringing Internet subscribers. In accordance with personal data protection rules, right holders must obtain a judicial court ruling authorizing the ISP to provide them with the identity of the internet subscriber whose connection has been used to commit the alleged infringement. The judge's intervention does not trigger a legal action against the subscriber, but merely gives him/her notice of an alleged infringement of copyright law. The German law[9] provides that the formal notice sent by mail to the subscriber must contain, under penalty of nullity: the right holder's name if he does not act in his/her own name (i.e. through a legal representative), the nature of the violated right, detail of the claimed sums (distinguishing legal fees, procedural fees and damages) and where applicable, the right holder's request to the subscriber to agree in writing not to share the said copyrighted work.

In addition to their unpopularity among the general public, these types of action raise - depending on the legal traditions of each country - questions regarding the risks of abuse and the role of the judge to comply with the adversarial principle and the protection of personal data.

This approach also raises financial constraints which limit its mass deployment due to the multiple costs incurred by right holders (i.e.: networks monitoring costs, legal fees to request the subscriber's identification before the judge, identification costs paid to the ISP, legal fees for the formal notice). Moreover, the law does not permit subscribers to bear such costs and unless the subscriber is brought before a court the likelihood of recovering them is dim.

FIGURES IN GERMANY

In addition to the costs of technical services enabling the finding of the infringement, to identify the subscriber with his/her IP address, right holders must pay:

- Legal fees (lawyers, judicial officer) to petition the court for the disclosure of the subscriber's contact details. It costs approximately 200 euros per request;
- Allowance to the ISP for the identification service, which represents approximately 35 euros per batch of ten IP addresses.

The right holder will then need to pay his/her lawyer to initiate the pre-litigation procedure against the subscriber. Whereas the amounts requested from subscribers are limited:

- The burden of legal fees which can be charged to the subscriber is capped at 500 euros under the German legislation;
- The judge checks the proportionality of damage claims (e.g.: 200 euros for a full music album).

The following figures, dating back 2013, circulated in the press:

- Right holders sent 109.000 mails, requesting 90.3 million euros in compensation;
- The average amount requested by right holders was 830 euros including legal fees;
- 15% of subsribers who received these mails paid the requested amount.

For now, such systems are focusing on peer-to-peer infringement, and are not extended to streaming and direct downloading, due to technical constraints and legal uncertainties in determining the role of the Internet user. In any case and for obvious reasons in terms of efficiency and opportunity, actions directed at commercial counterfeiting are mainly targeting massively infringing web sites.

9. Article 97 a (2) of the copyright and ancillary rights German Act as amended by the law of October 1st, 2013.

2 | NEW MULTI-PRONGED ANTI-PIRACY APPROACHES DEDICATED TO MASSIVELY INFRINGING WEBSITES

At the international level, there is a consensus on the need to fight more efficiently against "commercial counterfeiting", which happens when professionals earn revenues from or by inducing counterfeiting acts on the Internet.

Criminal or civil proceedings initiated by right holders are usually inefficient as it is difficult to identify the managers of these websites since they are frequently located abroad. In this context, different approaches have been adopted to involve market players who, even if they do not participate in counterfeiting acts, can directly contribute to the fight against these web sites. Actions proposed and implemented internationally aim at finding levers to get as many digital actors as possible to participate in the fight against piracy and to reduce the resources of massively infringing websites and to demote them.

Another perspective is to involve webhost providers (while making sure that their status is respected), to allow the withdrawal of copyrighted works when their dissemination has not been authorized or alternatively their monetization by using content recognition technologies has not been implemented.

Without jeopardizing the web host providers' status, the draft directive presented by the European Commission on September 14th, 2016 opens the debate at a European level about the role that they could play, by the contemplated mandatory use of content recognition technologies, in withdrawing copyrighted works when their dissemination has not been authorized or monetizing them. Generalized contractual frameworks between platforms and right holders would make it easier to demonstrate the rebellious behavior of counterfeiting web sites which inappropriately rely on the host provider status protection to evade responsibility for removing infringing content. Their refusal to sign such agreements could be used, in collecting evidence to direct legal proceedings against them.

Several countries also question the involvement of search engines, as they can be used to illegally access copyrighted works (Canada, Denmark, the United States and the United Kingdom) and also domain name registrars and/or organizations managing extensions under which a domain name is registered.

Actions against these web sites, which raise the question of the criteria used to determine the illegality of these web sites, follow two axes.

First of all, the "Follow the money" approach involving advertising and online payment actors in order to drain the revenues from massively counterfeiting web sites has built consensus on its utility, even if its implementation and the effects of such measures are still not clearly identified.

The recourse to the judge is the most compatible way forward, in keeping with the principle of proportionality to obtain the blocking or the removal of massively counterfeiting web sites. Procedures to prevent or stop copyright infringement by requesting an intermediary (when it has the power to do so) to block a web site (for an ISP) or to remove it from search results have emerged. However, their efficiency relies on the difficulties to demonstrate the infringing nature of targeted web sites, the elevated costs for ISPs and the ability to counter the reappearance of "mirror sites".

PREDETERMINATION OF CRITERIA TO QUALIFY MASSIVELY COUNTERFEITING WEB SITES

In some countries, criteria established by Courts are used to qualify a massively counterfeiting web site. Usually, it is about thresholds or percentages of illicit content: 66% of the site or more than 500 illegal itemized works in Portugal, 70% in South Korea. This percentage remains confidential in the United Kingdom for the actions of London's police.

Another approach, in countries where there are less conditions relating to the status of hosting providers, is the characterization of massively counterfeiting web sites without predetermined thresholds. For instance, in Canada, the upgrading of the Copyright Act of 2012 created a dedicated liability regime for professionals convicted of online infringement. The new article provides that "*It is an infringement of copyright for a person, by means of the Internet or another digital network, to provide a service primarily for the purpose of enabling acts of copyright infringement if an actual infringement of copyright occurs by means of the Internet or another digital network as a result of the use of that service*".

In Switzerland, a proposed reform plans to impose an extended withdrawal obligation for platforms whose "business model is based on the encouragement of systematic copyright infringement". The British Government, in its strategy to fight against online counterfeiting for the next four years[10] wants to facilitate court proceedings to block counterfeiting web sites by providing detailed information on the minimum amount of evidence required to block a web site - encourage international cooperation to take steps towards web sites hosted in a foreign country and aiming at the public on the territory of another country, in particular by examining at European level the options for a mutual recognition of the evidence required to obtain injunctions against web sites.

FIRST REPORT ON "FOLLOW THE MONEY" APPROACH

The "Follow the money" approach is now implemented in many countries (Denmark, Spain, the United States, Italy, Japan, the Netherlands, Portugal, the United Kingdom and Sweden) and contemplated as an option in many others (Germany, Australia, Canada, Switzerland).

The implementation of these actions relies on (except in Spain) a self-regulation logic between right holders (who identify web sites which can be financially dried up) and advertising as well as online payment intermediaries (severing their commercial relations with these web sites).

At the European Union level, a draft Memorandum of Understanding (MoU), presented by the European Commission aims at initiating cooperation between right holders and advertising actors to drain the revenues of counterfeiting web sites by entering into voluntary agreements. This document shows the legal limits of these self-regulation mechanisms regarding competition law, the freedom of communication on the Internet as well as the need to evaluate their efficiency and improve the follow-up of complaints.

The initiative is an element of the digital strategy implemented by the European Commission which promotes self-regulation mechanisms dubbed "Follow the money" destined to drain the revenues of pirate websites. The Commission also pointed out that, it would explore other ways to increase service intermediaries' liability in the event that this MoU would fail to be agreed upon.

A first assessment of initiatives implemented in the countries surveyed in our study can be drawn up.

CROSS-INDUSTRY PARTNERSHIP'S CONTENT AND FRAMEWORK DEPENDS ON THE SECTORS INVOLVED

At first blush, advertising industry (advertisers, advertising agencies notably) seem more committed to abide by the rules of voluntary codes of conduct, hence denying massively infringing websites such revenue streams stemming from well-known brand names than involved in the payment processors.

THE ROLE OF PUBLIC AUTHORITIES

In some countries, the intervention of public Authorities is a guarantee of reliability and adversarial process in characterizing websites as massively counterfeiting, a better impact assessment and efficiency of these voluntary agreements.

In the United Kingdom, in September 2013, the London Police set up the Intellectual Property Crime Unit (PIPCU)

10. "IP enforcement 2020" Protecting Creativity, supporting innovation, IPO, mai 2016 (IPA).and the Publishers Association.

dedicated to copyright infringements. Agreements have been concluded between the PIPCU, right holders[11] and online advertising actors[12]. These Agreements organize the cooperation of signatory parties in establishing lists of massively counterfeiting web sites by the PIPCU upon proposal of right holders and directing action on the part of advertising actors to deprive such sites of advertising revenues.

In Spain, the law allows the "Sinde" commission to request on line payment processors and advertising actors to stop collaborating with web sites which demonstrated a pattern of refusal to remove infringing contents (notice and take down). The law was adopted after self-regulation of private actors failed to deliver expected material results. The Sinde commission issues quarterly reports on the effectivity of the implemented legal framework.

In its Joint Strategic Plan, a copyright defense program for the next three years published in 2016[13], the U.S Administration indicated its willingness to enter in a public-private partnership with payment processors and advertising industry to improve transparency of the operations carried out in these areas with anonymized data by the payment and advertising actors.

In Germany, because of risks of violation of competition law, the implementation of these measures has been limited to self-regulation and has no enforcement mechanism.

SUGGESTIONS TO STRENGTHEN THE EFFECTS OF VOLUNTARY AGREEMENTS

As a result of gradually depriving massively counterfeiting web sites from major brand names' advertisement revenue flows, such sites tend to turn to pornographic or online gaming advertisers, use other types of payment (virtual currency) or other funding sources such as fraudulent channels generated by malwares. As the impact of such measures increases, there is a general expectation that it will deteriorate users' experience in surfing these websites as well as their brand image, and point more clearly towards their illegal character thereby facilitating their identification by good faith customers. In the United Kingdom the PIPCU has teamed up with the Authority granting licenses to online gaming and betting services. Presence of advertisement and links pointing at copyright infringing websites are therefore may cause withdrawal of the licence.

Widening the scope of such voluntary Agreements to collect evidence which may serve to expedite judicial procedures initiated to block or shut down these websites is the next step which is being contemplated in various countries.

In the United Kingdom, the PIPCU is exploring actions which could be implemented with participation of ISPs requested to block websites identified as massively counterfeiting as per a "blacklist". When a web site is registered on PIPCU's "blacklist", a letter is sent to the domain name registrar to request the suspension of the domain name. When websites are registered overseas efforts often fail to deliver material change. The PIPCU is seeking international agreements to collaborate with foreign domain name registrars.

According to a similar logic, in the United States the Motion Picture Association of America (MPAA) signed in February 2016 an agreement with Donuts (which manages several extensions, such as ".movie") then in May 2016 with Radix, located in Dubai, which manages several extensions such as ".website" or ".online". These agreements provide for the suspension of massively infringing websites' domain names upon MPAA's notification. Furthermore, the American Intellectual Property Rights Program published in December 2016 advocates for actions against domain name hopping, used by massively counterfeiting web sites' managers whenever a domain name is suspended or blocked.

SITES BLOCKING MECHANISMS

Site blocking measures are now part of the legal arsenal to fight counterfeiting in most countries. Also, simple injunctions to take appropriate steps can be issued against platforms, such as " Notice and Stay down" measures regarding a work or an entire catalogue (Germany, Spain).

Blocking injunctions are issued:

- Upon request by right holders, on court order with an injunction which may, depending on the countries, be

11. The Federation Against Copyright Theft, the British Recorded Music Industry, the International Federation of the Phonographic Industry – IFPI – and the Publishers Association.
12. The Internet Advertising Bureau (IAB), the Incorporated Society of British Advertisers (ISBA) and the Institute of Practitioners in Advertising IPA).
13. The Federation Against Copyright Theft, the British Recorded Music Industry, the International Federation of the Phonographic Industry – IFPI – and the Publishers Association.

subordinated or not to the active participation (responsibility) in the infringement of the intermediary;

- Or with a public Authority's assistance to notify removal requests and verification operations with the platforms. In this case, the public Authority and the judge operate together (Italy and Spain).

In Spain, when right holders find infringing contents on a web site with material proof of originating from Spain, they may file their complaint to the Sinde commission. If the commission finds the claim to be acceptable, it can request from the website's manager to send his/her observations within 48 hours, make sure that the content is unavailable, request the stay down or the interruption of any activity infringing copyright. The forced execution of these decisions requires an authorization from the judge.

National laws must specify the limits and applicability conditions of these blocking measures balancing the fundamental rights at stake and the need for a flexible and fast procedure to block websites and efficiently fight the appearance of mirror sites.

In that regard, with a view of drafting new legislation updating the 2004/48/EC directive related to the enforcement of intellectual property rights, the European Commission asked Member States to identify persistent obstacles to the implementation of notice and take down and site blocking procedures. The EU inquiry focused on the burden of proof, subsidiarity, the impact of courts' decisions to prevent further infringements and the existence of extra judicial mechanisms.

In addition to costs issues, blocking mechanisms face two major recurring obstacles. Some countries offer original solutions to the requirements for evidence of the website's illegality and the effectiveness of the blocking measures over time.

COST CONTAINMENT AND ALLOCATION

Concerning costs involved in the site blocking procedures, some national legislations provide that such costs should be entirely borne by right holders (Switzerland) or by the ISPs (Russia). In Australia and in the United Kingdom, courts decided that right holders had to bear them.

At the European level, case law remains unclear regarding that matter[14], in particular with "the freedom to conduct a business" of ISPs and "the conditions laid down in Article 3(1) of Directive 2004/48, which requires that measures to ensure the respect of intellectual property rights should not be unnecessarily complicated or costly".

ENFORCEMENT OF MEASURES PREVENTING REPEAT INFRINGEMENTS (MIRROR SITES)

Mirror sites quick reappearance render blocking measures inefficient, hence the emphasis put on fast and efficient judicial follow up procedures to prevent mirror sites from getting on line.

In the UK, a lot of website blocking decisions (at least 163 websites have been blocked up to 2017) directed at ISPs are based on article 97A of the Copyright, Designs and Patents Act of 1988, transposing Article 8.3 of the 2001/29 Directive on copyright.

Courts also use it as a legal basis against mirror sites[15]. In the first blocking requests, right holders argued that ISPs already had the relevant technology to automatically update the addresses to be blocked from a list of URLs within the context of the fight against child pornography (Cleanfeed or similar mechanism). For the purpose of fighting child pornography a list of addresses to be blocked or encrypted is constantly updated and transmitted to ISPs by the Internet Watch Foundation.

Recent case law in the UK indicates that it is now common with blocking injunctions to allow the update of IP addresses and URLs to be blocked. ISPs proceed to this update, without the requirement for a new judicial authorization, based on the information provided by right holders. In Denmark, according to a 2014 voluntary agreement between ISPs and right holders, when a court decision orders an ISP to block sites, other ISPs commit to blocking them within seven days, at their own expenses. In Russia, there is an interconnection between the regulator requesting the blocking and ISPs to facilitate the transmission of information and the update of the list of websites to be blocked.

---

14. CJUE, November 24, 2011, Scarlet Extended SA/ Belgian Society of Authors, Composers and Publishers SCRL (SABAM), C-70/10 ; CJUE, March 27, 2014, UPC Telekabel Wien GmbH/ Constantin Film Verleih GmbH, C-314/12.
15. High Court of Justice, Chancery Division, July 28, 2011, 20th Century Fox Film v British Telecommunications PLC.

HAUTE AUTORITÉ POUR
LA DIFFUSION DES OEUVRES
ET LA PROTECTION
DES DROITS SUR INTERNET

4 rue du Texel - 75014 Paris - France
www.hadopi.fr

Hadopi