# Anti-piracy strategies

## of CULTURAL AND SPORTS CONTENT

2019 INTERNATIONAL SURVEY

Hadopi

**High Authority** for the dissemination of works and the protection of rights on the internet

# CONTENTS


Page 5 THE METHODOLOGY

Page 6 THESURVEY

Page 7 **PART 1**
MEASURES TO BLOCK OR SHUT DOWN ILLEGAL WEBSITES AND THEIR AVATARS ABROAD

Page 8 **Administrative or judicial blocking orders**

Page 12 **Preventing circumvention practices and the reappearance of illegal content**

Page 17 **Preventing unauthorised access to live sports broadcasts: the development of a "live blocking" system in Europe**

Page 20 **Cooperation between rightholders and a stronger role for public operators**

Page 24 **PART 2**
THE NECESSARY INVOLVEMENT OF END-USERS AND DIGITAL OPERATORS IN THE FIGHT AGAINST PIRACY

Page 25 **The responsibility or at least accountability of end-users**

Page 31 **Strengthening the role of intermediaries in the fight against piracy**

Page 39 **Conclusion**

Page 40 **APPENDIX 1**
COUNTRY FACT SHEETS

# THE METHODOLOGY

The Hadopi Department of Legal Affairs has been monitoring international trends since 2011 and, for the second time, its findings have been compiled into a dedicated report.

This report contains regularly updated information on 23 countries in Europe, North America, Asia, Oceania and Russia, which were chosen for the originality or impact of the tools they employ to tackle online counterfeiting.

It is divided into two parts: a survey summarising the key points and current challenges in the fight against piracy, with reference to the most emblematic national systems; and a set of appendices comprising detailed fact sheets on each of the countries studied, and presenting the legal arrangements in force there and any reform bills being considered.

Each country fact sheet now includes an inset highlighting data from known blocking procedures, as well as local piracy figures.

Most of the information derives from mainly English-written documents provided to us by a network of contacts from public institutions and the private-sector, and from public documents such as press articles, case law and legislation.

This network of contacts has been developed and strengthened over the years through Hadopi's monitoring work, which focuses on current developments in piracy prevention (quantitative reports, legal analyses, public statements, etc.) and in some cases is supported by French embassies or consulates.

The information collected through our monitoring activities has been verified and supplemented wherever possible by large numbers of interviews with qualified local contacts, conducted either in person abroad or by phone. However, the information obtained for each country is not always as precise as we would have liked.

**It should be noted that, given the language barrier and differences in legal systems, the fact sheets may contain approximations or misunderstandings. Asian countries in particular have legal peculiarities that can be difficult to fathom from the French perspective.**

**This report was made public on 7 February 2019 at a symposium on international strategies to tackle online piracy of cultural and sports content.**

# THE SURVEY

**"The real voyage of discovery consists not in seeking new landscapes, but in seeing with new eyes"**
*Marcel Proust.*

Like Proust's voyage of discovery, the benefit of international legal comparisons lies not in the unique characteristics of local legislation, but in the way that legislation can inspire us and potentially change our outlook at the national level.

In terms of protecting cultural and sports content online, such comparisons are essential considering the transnational nature of piracy and the convergence of illegal operators, and the fact that all countries face similar challenges in tackling them. The "notorious markets" lists published by the US administration and the European Commission are a clear illustration of this.

However, while the situation is the same in many of the countries observed, the solutions proposed may differ greatly from one country to the next.

France has played a pioneering role in protecting intellectual property rights on the Internet. Law no. 2009-669 of 12 June 2009, promoting the dissemination and protection of creative works online, was innovative in that it vested a dedicated public authority with a pre-trial mandate to raise end-user awareness of copyright infringement on peer-to-peer networks; it also introduced the possibility of bringing injunctive proceedings against Internet intermediaries at the initiative of rightholders whose copyright has been infringed.

Although other countries have no exact equivalent of Hadopi due to the specificity of its mission and its status, public authorities do seem to play a major role in counterfeit prevention in many countries.

The fight against online piracy has intensified and has been firmly established worldwide for the past ten years or so.

What is more, it has led to a two-way trend whereby rightholders and public authorities are seeking to adapt and diversify their tools and strategies, while illegal operators are looking for technical and legal circumventions. The European Union is calling for coordination between its Member States, hoping to draw on their expertise to develop an action plan inspired by the effectiveness of various national arrangements. Rightholders, like many of America's largest private companies, are pooling their efforts and pursuing joint, targeted criminal or legal action on a global scale.

The shared objectives emerging globally from this international benchmarking are relatively clear:

- simplify and ensure the effectiveness and continuity of judicial and administrative measures for blocking illegal websites, by promoting pragmatic and balanced solutions to counter circumvention practices and avoid flooding the courts with update requests;
- increase obligations on operators who make content available to the public, and more broadly support changes in end-users' practices;
- involve all Internet operators, advertising networks, online payment operators, domain name registrars, search engines, etc. in the fight against piracy;

The fight against piracy now seems to be focused on two major areas: the direct prevention of commercial counterfeiting via administrative or judicial blocking orders, and criminal proceedings against illegal websites (part 1); the broadest possible involvement of end-users and all Internet operators (part 2).

PART 1

# MEASURES TO BLOCK OR SHUT DOWN ILLEGAL WEBSITES AND THEIR AVATARS ABROAD

**Administrative and judicial website blocking are now an integral part of the legal arsenal against counterfeiting in many countries. Leaving aside the question of their cost, these blocking mechanisms require a simplification or at least a clarification of the process for establishing the illegality of websites.**

**While there is consensus on the benefits of these measures, their effectiveness unfortunately reduces over time as considerable efforts are made to circumvent them, requiring rightholders and public authorities to find appropriate solutions.**

**Likewise, the piracy of live sports broadcasts is forcing public authorities and judicial bodies to consider introducing real-time blocking of illegal live streams (a procedure known as "live blocking").**

**As a direct consequence of the acceleration and escalation of anti-piracy through the development of blocking measures, rightholders are forging a common front and public actors are taking on a greater role due to their ability to act globally; that is, on the scale of the Internet.**

# ADMINISTRATIVE OR JUDICIAL BLOCKING ORDERS

Several countries in Europe and worldwide have established administrative procedures under the auspices of a public authority, or *sui generis* judicial procedures obliging technical intermediaries to implement blocking measures to prevent or stop online copyright infringements and, where applicable, sports broadcasting rights.

This type of action is independent of any attempt to hold the intermediary liable; however, the latter is bound by the procedure and is obliged to block a website where possible to permit the desired objective to be attained. Nonetheless, it raises questions regarding the standard of evidence required to establish the illegality of the website in question.

## THE INCREASE IN ADMINISTRATIVE BLOCKING MECHANISMS WORLDWIDE AND MORE PARTICULARLY WITHIN THE EUROPEAN UNION

### WORLDWIDE

Many countries, such as **Switzerland**, have considered or are currently considering implementing an administrative blocking mechanism.

**In the United Kingdom**, blocking measures are implemented by court order, in a context of constructive cooperation between rightholders and Internet service providers. The current British government is, however, considering the possibility of introducing an administrative blocking system in the future. A government report will be published in 2019, analysing the advantages of administrative blocking, its potential impact and the legal basis for incorporating it into the legal corpus.

**South Korea** has set up an administrative blocking scheme that mainly targets websites without local ties. When the public authority responsible for anti-piracy concludes - after consulting with rightholders - that a website has committed large-scale copyright infringement, it notifies the Ministry, which in turn requests the communications regulator to block the site.

**In Russia**, if a website fails to comply with a notice and takedown request, rightholders may refer the matter to the Court of Moscow - the only court in Russia with the necessary jurisdiction - to have the content removed or the service blocked. The Court then notifies its decision to the telecommunications and media regulator (the *Roskomnadzor*), which is responsible for having it enforced. The regulator contacts the hosting provider or the website itself, which then has three days to comply with the decision. If the disputed content is not withdrawn or the illegal activity does not cease within this period, the *Roskomnadzor* may ask Internet service providers to block the website. Should they fail to do so, they incur a fine of 30,000 roubles (approximately 500 euros). To ensure the swift implementation of blocking measures, an interconnection has been established between the regulator and Internet service providers.

### WITHIN THE EUROPEAN UNION

Directive 2000/31 of the European Parliament and of the Council of 8 June 2000, the "e-commerce" directive, provides for the possibility – not specific to copyright law - "*for a court or administrative authority [...] of requiring the service provider to terminate or prevent an infringement* "[1].

On this basis, some Member States have chosen to have a public authority which - upon notification by rightholders, further to verification and depending on the nature of the infringement or the country where the website is located - orders:

*[1] Likewise, Article 3 of Regulation 2015/2120 of 25 November 2015 laying down measures concerning open internet access and amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services and Regulation (EU) No 531/2012 on roaming on public mobile communications networks within the Union provides that:*
*"Providers of internet access services shall not engage in traffic management measures going beyond those set out in the second subparagraph, and in particular shall not block, slow down, alter, restrict, interfere with, degrade or discriminate between specific content, applications or services, or specific categories thereof, except as necessary, and only for as long as necessary, in order to:*
*a) comply with Union legislative acts, or national legislation that complies with Union law, to which the provider of internet access services is subject, or with measures that comply with Union law giving effect to such Union legislative acts or national legislation, including with orders by courts or public authorities vested with relevant powers"*

- hosting providers to remove all or part of the infringed works from the website's servers;
- or Internet service providers to implement blocking measures.

In Italy, Greece and Spain, in addition to the administrative procedures required by the transposed "e-commerce" directive, it is possible to bring injunctive proceedings based on Article 11 of Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights (the "IPRED" Directive) and on Article 8.3 of Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society (also known as "InfoSoc).

In each of the three aforementioned countries, the administrative procedure becomes null and void if the rightholders refer the matter to the courts via injunctive proceedings against the same rogue sites.

In **Italy**, the digital communications regulator *Autorità per le Garanzie nelle Comunicazioni* (AGCOM) may order Internet service providers to block a streaming, live streaming or stream ripping site that contains illegal cultural or sports content. It may also require the hosts of the service to remove specific works notified by the rightholders (this procedure is aimed mainly at sites based in Italy). The financial burden of blocking operations lies with the Internet service providers. AGCOM may impose administrative sanctions in the event of non-compliance with its decisions. The decisions made by AGCOM may be appealed to a judicial body. The procedure may take anything from 3 to 35 days, and may be accelerated in the event of large-scale infringements.

In 2017, **Greece** adopted a law providing for the implementation of an administrative blocking system inspired by the Italian model. The system is enforced by a committee within a public institution responsible for copyright issues. The committee may give formal notice to the website manager to cease the infringement. Otherwise, like in Italy, it may instruct hosting providers (for sites hosted in Greece) or Internet service providers (for sites hosted abroad) respectively to delete all or part of the site's content from their servers or to block the site. In this second scenario, the cost of blocking the site is borne by the Internet service providers.

In **Spain**, the so-called *Sinde* Commission attached to the Ministry of Culture and Sport may give formal notice to the website manager to put an end to the infringement. In the absence of due diligence by a site (particularly those based abroad), the Commission may rule it illegal and request that it be blocked. However, the obligatory enforcement of such blocking decisions by Internet service providers is subject to authorisation by the court of enforcement.

In **Portugal**, a memorandum has been signed by various public and private actors, mainly the General Inspectorate of Cultural Affairs (called IGAC), the Portuguese Association of Telecommunications Operators (APRITEL) and rightholders association MAPINET (a cross-sector piracy prevention organisation). Every month, MAPINET may report 100 websites to IGAC (including sites that circumvent blocking orders), providing evidence that each site contains 500 links to infringing content. IGAC carries out the necessary checks within a few days (48 hours on average), and then instructs Internet service providers to place a DNS block on the site within 48 hours. This is done twice a month according to a schedule set out in the memorandum, so that Internet service providers are required to mobilise their resources and teams at regular, pre-set intervals. The memorandum was signed by Internet service providers after the public authorities "threatened" to deal with the matter through legislation. The blocking costs are borne in practice by the service providers.

## INJUNCTIONS

**In the United States,** the "SOPA" and "PIPA" bills - which notably sought to introduce website blocking – failed in January 2012. Since then, the idea of implementing a reform to establish a site blocking system has been dropped. Injunctive proceedings have notably been replaced by domain name seizure procedures.

Domain name seizures can be obtained via actions carried out by the National Intellectual Property Rights Coordination Center, an anti-counterfeiting organisation that reports to the U.S. Immigration and Customs Enforcement (ICE). In November 2017, as part of a joint Europol-Interpol initiative called "In Our Sites", 20,520 domain names were seized for selling counterfeit products or pirated cultural goods[2]. When end-users attempt to open these sites, they are redirected to an information banner.

In more targeted legal actions to prevent piracy of specific cultural or sports content, US courts may also issue injunctions to registries. In July 2017 and July 2018, at the request of a leading media company, a Federal Court in Florida ordered a temporary seizure of infringing domain names and blocked the revenue stream from advertising operators to the sites in question[3].

**In Australia,** the law provides for injunctive proceedings enabling rightholders to obtain a blocking order against illegal websites.

**Switzerland** has in the past proposed an innovative reform project combining intellectual property rights enforcement with the promotion of legal offer. Under this reform, which ultimately failed, rightholders could take action to block a website only if the copyright-infringing content on the said website was also available legally elsewhere.

**In the European Union,** Article 11 of Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights (the "IPRED" directive) allows rightholders to apply for an injunction against intermediaries whose services are used by a third party to infringe an intellectual property right. A provision similar to Article 11 already featured in Directive 2001/29/EC on the harmonisation of certain aspects of copyright and related rights in the information society (also known as "InfoSoc" (article 8.3)[4].

Such injunctions should be awarded only where necessary and proportionate, for example in cases of large-scale counterfeiting or repeated acts of counterfeiting that are impossible to stop otherwise.

However, the transposition of these directives could conflict with the principle of subsidiarity, whereby rightholders must first take legal action against the websites themselves.

On 29 November 2017, the European Commission published the Guidance Communication on the enforcement of Directive 2004/48/EC. The aim was to clarify provisions such as Article 11 on injunctions, which have been interpreted in various different ways by the Member States. The Commission specified, based on the case law of the Court of Justice of the European Union[5], that the possibility of applying for an injunction is completely unrelated to the possibility of invoking the liability of intermediaries on the basis of Directive 2000/31/EC of 8 June 2000. It stated that courts should be able to order intermediaries to delete or prevent access to copyrighted content online.

*[2] www.europol.europa.eu/newsroom/news/biggest-hit-against-online-piracy-over-20-520-intemet-domain-names-seized-for-selling- counterfeits*
*[3] torrentfreak.com/images/fccb57c7-b666-4495-aa07-783c429e6613.pdf*
*[4] "Member States shall ensure that rightholders are in a position to apply for an injunction against intermediaries whose services are used by a third party to infringe a copyright or related right".*
*[5] CJEU, 12 July 2011, C-324/09 L'Oréal SA and Others v eBay and, 7 July 2016, C-494/15 Tommy Hilfiger. Although intermediaries may avail themselves of the provisions of the e-commerce directive, courts may ask them to stop or prevent the perpetration of acts of counterfeiting.*

Some countries have implemented innovative mechanisms - based for the most part on cooperation with Internet service providers - to offset the delays and costs inherent in legal proceedings and adapt them more effectively to the digital environment. **In Denmark,** rightholders refer just one Internet service provider to the court in site-blocking procedures (pursuant to a voluntary agreement), alternating regularly to reduce legal costs. The blocking orders are then notified to the union of ISPs (Telecom Industry Association Denmark), which forwards them to other Internet service providers. Judicial blocking procedures last from two to six months, including case preparation time, and each ruling may concern dozens of sites.

**In Belgium,** rightholders brought a lawsuit against the three main Internet service providers in January 2018. The parties then filed a joint motion to block approximately thirty illegal sites via 450 domain names, which the judge subsequently granted. The purpose of this joint approach was, among other things, to accelerate the procedure.

**In Italy** in July 2018, a case in which a blocked site had reappeared under a completely different domain name was brought before the Court of Milan, which ruled that the requests of the plaintiff (a publishing group) were admissible and ordered Internet service providers to set up a proactive system. Hence, Internet service providers must block access to illegal content upon simple request of the rightholders. This applies to all websites that, irrespective of the domain name, go on to commit the same infringements as those noted in the initial ruling. In this summary proceedings, the rightholders the Court ordered that the cost of the blocking measures be borne by the rightholders.

## A COMMON LEGAL ISSUE: THE CHARACTERISATION OF ILLEGAL WEBSITES

To ensure that proposed measures against illegal websites do not become obsolescent, ineffective (or even inapplicable), the assumptions and criteria used to qualify a site or service as illegal should be quite flexible.

In some countries, the criteria for qualifying sites as illegal are predefined by law, case law or the administration. In most cases, a range of indicia is created based on a system of thresholds (the number of works or links in question) or on the percentage of illegal content identified.

**In Australia**, the law providing for court-ordered blocking measures was amended in November 2018 to broaden its scope to include all sites that merely have the effect of infringing copyright or facilitating copyright infringement. Previously, the law had applied only to sites that aimed expressly to infringe or enable the infringement of intellectual property rights.

**In Canada**, the court may use the following factors to qualify services as illegal, as provided for by law: whether the person in charge of the said service marketed it as one that could be used to commit acts of copyright infringement; whether the person had knowledge that the service was used to enable copyright infringement; whether the service has any other significant uses besides than enable acts of copyright infringement; measures taken to limit copyright infringement; the benefits derived from copyright infringement and/or the economic viability of providing the service were it not used to commit acts of copyright infringement.

**In Denmark** and the United Kingdom, rightholders must demonstrate that the content available on the website belongs to them and that they have not directly or indirectly consented to it being made available. There is no predefined threshold to ascertain the infringing nature of a website. In principle, one offence is sufficient. However, rightholders focus their actions on sites that offer a substantial number of infringing works.

**In Portugal**, the General Inspectorate of Cultural Affairs (known as “IGAC” ) - which reports to the Ministry of Culture - uses two criteria to ascertain the infringing nature of a site and order it to be blocked: either the number of infringing links notified by rightholders must exceed 500, or the percentage of infringing content on the site must be at least 66%.

**In Italy**, there is no legal threshold above which the number of allegedly illegal works on a given website may give rise to proceedings before the competent regulatory authority (AGCOM). Rightholders may submit a complaint to the authority whenever they that a work has been used without their consent. However, the procedure is shortened from 35 to 12 days where “massive infringements” have been committed. An infringement is considered massive when around 30 illegal works are present on a site.

**In South Korea**, the Korea Copyright Protection Agency (KCC) - which reports to the Ministry of Culture - verifies the content of the site with the rightholders. If more than 70% of the content is illegal, the KCC instructs the communications regulator (the Korea Communications Standards Commission) to block the site.

# TACKLING CIRCUMVENTION OF BLOCKING MEASURES AND THE REAPPEARANCE OF ILLEGAL CONTENT

“Mirror site” is a generic term used worldwide which very broadly encompasses the reappearance and replication of blocked websites and the creation of indirect means of access to them. It highlights the magnitude of piracy and reveals the strategies employed by the administrators of illegal sites to circumvent enforcement measures.

These practices raise both technical and legal questions which can however be addressed through voluntary cooperation actions following court rulings, or through administrative procedures.

## THE TECHNICAL CHALLENGES PRESENTED BY WEBSITE BLOCKING GIVEN THE INCREASE IN CIRCUMVENTION STRATEGIES

The blocking measures implemented by Internet service providers following an administrative or judicial order must meet two key requirements: they must be effective and proportionate.

Both public authorities and case law - particularly at European Union level[6] - agree that blocking measures, although circumventable, have a considerable impact on the ecosystem. In addition, several studies have concluded that blocking measures are effective as they generally lead to an approximate 75% drop in visits to blocked sites.[7].

In countries that implement administrative or judicial blocking measures on a large scale (by the hundreds), it seems that in most cases blocking results directly in the digital death of the target site. According to some, 30% to 40% of blocked sites reappear.

Furthermore, even in countries where blocking measures are very widespread, it is estimated that fewer than 10% of end-users circumvent DNS (Domain Name System) blocks by using a VPN (Virtual Private Network) or a DNS service other than that of their Internet service provider (which is not subject to the blocking order and allows them to access blocked sites).

**In Russia**, a law adopted on 29 July 2017 provides for sanctions against anonymizing services, which may be subject to blocking measures, if they fail to comply with their new obligations. The law requires that operators of VPN services and other such anonimizing systems must make themselves known to the authorities, provide encryption keys for decrypting encrypted messages, and then consult the list of blocked sites provided by the Russian regulator *Roskomnadzor* so that they also can prevent access to them. The encrypted messaging application Telegram has been blocked, leading to the over-blocking of millions of Amazon and Google IP addresses that also used this service.

Most of the legislation in force does not specify the type of technical measures that Internet service providers should implement. Depending on the architecture of their networks and the objective pursued in each case, they can block either the “Domain Name System” (DNS) or the “Internet Protocol” (IP) address of the host server.

**In Europe**, the Court of Justice of the European Union[8] ensures that intermediaries are not required to implement excessively large-scale and costly filtering mechanisms.

In some, mostly Common Law countries **(Australia, Ireland, United Kingdom),** DNS and IP blocks may be implemented alternately depending on the circumstances. However, in the case of IP blocks, Internet service providers must carry out a few essential checks to counter the risk of over-blocking and ensure that the IP address to be blocked is not shared (a single IP address can host various services, both legal and illegal). Notifying the hosting provider is one means of making sure that the address to be blocked is not shared.

*[6] CJEU, 27 March 2014, C-314-12, UPC Telekabel Wien GmbH v. Constantin Film Verleih GmbH.*
*[7] In particular: www.incoproip.com/report/site-blocking-efficacy-report-australia*
*www.incoproip.com/news/portugals-pirate-site-blocking-system-works-great-study-shows*
*www.incoproip.com/report/site-blocking-efficacy-study-united-kingdom*
*papers.ssrn.com/sol3/papers.cfm?abstract_id=2612063*
*[8] CJEU, 24 November 2011, C-70-10, Scarlet Extended SA v Sabam.*

However, in many countries, both public actors and Internet service providers are reluctant to implement IP blocks, particularly because of the risk of over-blocking.

In several countries, while both types of blocking may be imposed by the courts, only DNS blocks are implemented by mutual agreement with Internet service providers (Italy, Denmark).

**DNS blocking** consists in blocking a website's domain name to prevent end-users from accessing it via their Internet service provider. Consequently, when the user attempts to access the site either by directly entering the domain name or through a link (in some cases listed by a search engine), the connection fails. This blocking measure is implemented on the DNS servers of Internet access providers.

The administrators of illegal sites have developed a strategy for circumventing DNS blocks, which consists in reserving several similar domain names in order to make the blocked site (or a copy of the blocked site) accessible under one or more new domain names. Alternative domain names can be connected to the original servers of the blocked site, which - since only the domain name is blocked - are still online and remain accessible via their IP address.

**IP blocking** consists in preventing traffic from or to a predefined IP address, i.e. that of the server hosting the website. IP blocking works regardless of the domain names and URLs used to access the targeted IP address. This method is particularly useful when a server is accessed directly from the IP address, rather than a domain name. This happens, for example, in cases of illegal streaming of live TV programmes.

Finally, site operators can circumvent DNS and IP blocks by creating intermediary systems known as dedicated *proxys*, which consist of servers that can be accessed via a domain name and an IP address different to those of the blocked site. These servers act as a “transparent" intermediary between the end-user and the blocked site, and allow the end-user to access the blocked site indirectly by redirecting inbound and outbound traffic. In this case, the blocking measure should be extended to include the domain name and/or IP address of the proxy in question.

## LEGAL ISSUES RELATED TO THE PREVENTIVE MEASURES IN EUROPE

Circumvention practices are by their very nature hardly predictable in terms of their concrete manifestations, and the technology behind them changes frequently. These practices are difficult to get to grips with and to qualify from a legal standpoint, meaning that States are confronted with two recurring questions.

- What powers do the judiciary or the public authorities tasked with combating piracy already have to prevent such practices, for example through framework or dynamic injunctions against stakeholders?
- Should these new procedures or injunctions be enshrined in legislation or another legal framework and, if so, how precise or general in scope should that legislation or legal framework be to enable swifter and more effective action against circumvention practices?

**In Europe**, Article 8.3 of Directive 2001/29 of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society (InfoSocI) and the final paragraph of Article 11 of Directive 2004/48 of 29 April 2004 on the enforcement of intellectual property rights (IPRED), provide that rightholders may apply for a preventive injunction against intermediaries associated with the initial blocking measures. European case law has interpreted these texts as allowing preventive measures to be obtained from the courts or the public authorities[9].

*[9] CJEU of 12 July 2011, L'Oréal SA and others against eBay International AG and others, ruling on the basis of Article 11 of the IPRED Directive; 24 November 2011, Scarlet Extended SA against Sabam, ruling on the basis of Article 8.3 of the InfoSoc Directive.*

On 29 November 2017, the European Commission published guidance on the enforcement of the IPRED directive[10], which addresses the issue of injunctions to prevent further infringements. The Commission specifies that such injunctions (which do not exist in all countries) should be encouraged, even if they are decided on a case-by-case basis, and that it is up to the Member States to establish the appropriate terms and procedures. The guidance states that the reappearance of mirror sites can also be stopped through public authority or police intervention[11]. The Commission then cites the example of a Belgian court that ordered a block of the website thepiratebay.org, and on *"all domain names linking to related server*", "*the domain names to block being determined*" by the Computer Crime Unit of the Belgian police[12].

## VOLUNTARY MEASURES BASED ON COURT DECISIONS, OR EFFECTIVE ADMINISTRATIVE MEASURES AGAINST MIRROR SITES

### EXAMPLES WHERE VOLUNTARY AGREEMENTS BASED ON COURT DECISIONS HAVE ENABLED THE UPDATING OF JUDICIAL BLOCKING MEASURES

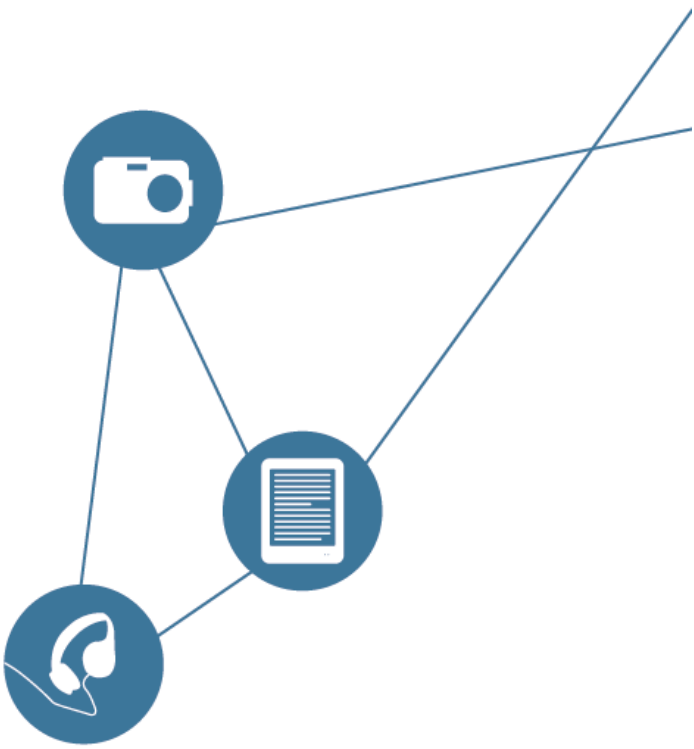
The major difficulty with judicial blocking measures is that rightholders must return to court to update the original decision with additional website addresses (and the new domain names used) or IP addresses enforceable against Internet service providers.

One solution already being explored in some countries is to allow or introduce greater flexibility in the pronouncement of court orders, and to include flexible legal mechanisms enabling blocking measures to be updated more quickly as illegal sites migrate and change.

This also saves time and money for the parties involved and for the courts.

In practical terms, this means that the court may – in addition to blocking the infringing sites referred to in the original decision, and in the context of a dialogue between the parties following that decision – order a block on the domain names and, where applicable, the IP addresses identified by the rightholders and notified to Internet service providers (and/or search engines) for the purpose of updating the decision.

Therefore, with or without legislative change, rightholders and Internet service providers have managed in some countries to agree voluntarily to implement judicial blocks that are effective long term.



*[10] ec.europa.eu/docsroom/documents/26582*

*[11] "Furthermore, injunctions may in certain cases lose some effectiveness because of changes in the subject matter in respect of which the injunction was ordered.This may be, for example, the case of website blocking injunctions, where a competent judicial authority grants the injunction with reference to certain specific domain names, whilst mirror websites can appear easily under other domain names and thus remain unaffected by the injunction.*
*Dynamic injunctions are a possible means to address this. These are injunctions which can be issued for instance in cases in which materially the same website becomes available immediately after issuing the injunction with a different IP address or URL and which is drafted in a way that allows to also cover the new IP address or URL without the need for a new judicial procedure to obtain a new injunction. The possibility of issuing such injunctions exists, inter alia, in the United Kingdom and Ireland. This objective could also be pursued through intervention of a public authority or the police, as it occurred in a specific case in Belgium."*

*[12] Antwerp, 14 February 2013, Cases 2012/FR/303, 2012/PGA/3549, 2012/KC21/262 and Cass. 22 October 2013, P.13.0550.N.*

**In Australia**, a new law passed in November 2018establishes a new type of judicial blocking order aimed at encouraging dialogue and agreement between rightholders and intermediaries involved in the procedure (Internet service providers and search engines).

**In Denmark**, the case law allows rightholders to instruct Internet service providers to block not only sites identified by their domain name but also sites identified by their content and interface, regardless of their domain name extension. Following an agreement between Internet service providers and rightholders, it is now possible to reinforce and extend the scope of court orders requiring Internet service providers to block access to specific websites without having to go back to court, provided that the rightholders are able to provide sufficient evidence. In practice, rightholders use software that is supplied by a private company and is also used by the Motion Picture Association (MPA), which analyses similarities between services and identifies services circumventing blocking measures. In any event, the rightholders guarantee Internet service providers against any disputes over mirror sites.

**In the United Kingdom**, recent blocking decisions show that it is now customary for blocking orders to allow for the updating of domain names and IP addresses. Updates are carried out by Internet service providers at the request of rightholders, who provide updated lists of addresses to block, without going back to court. Both rightholders and Internet access providers are responsible for monitoring the emergence of circumventing services following court orders obtained by the rights holder. The cost of implementing these measures is borne by the Internet service providers.

**In Ireland**, since 2013, court orders have required Internet service providers to subsequently block circumventing sites that allow access to blocked sites, in compliance with a memorandum of understanding now appended to the order. In practice, rightholders regularly provide Internet service providers with an updated list of IP addresses and/or domain names that provide access to the content of blocked sites.

## EXAMPLES OF ADMINISTRATIVE FOLLOW-UP OF BLOCKING MEASURES

Depending on the situation, involving a public authority in monitoring the emergence of sites that circumvent blocking orders can have several advantages. For example, it may:

- establish a methodology or a reference framework for identifying and characterising circumvention services that facilitate or contribute to the accessibility of massively infringing sites, which have previously been subject to blocking measures;
- limit or, failing that, simplify and shorten procedures leading to the court-ordered blocking of sites and services circumventing blocking measures;
- facilitate and secure the implementation of such court orders by Internet service providers, and extend them to other voluntary operators (other Internet service providers, search engines, etc.);
- ensure more systematically that end-users are redirected to a government information page explaining the reasons for the blocking measure and referring them to legal offer.

**In Italy**, the regulation that came into force on 16 October 2018 contains a new Article (8a) on the repetition of offences that have already been subject to an administrative order. At the request of the rightholders, the public authority verifies that a repeat infringement has taken place and then has three days to implement the appropriate measures. Where the infringement has previously been the subject of an administrative order against a hosting provider or Internet service providers, the public authority analyses the similarities between the domain names, the identity of the IP address and the structure of the websites. Any injunctions pronounced may be challenged within five days of notification, before the public authority's College. The latter then has seven days to reach a decision.

**In Portugal**, mirror sites are not afforded special treatment. When submitting their monthly reports to the public authority, rightholders must - within the limit of the total number of sites permitted per notification procedure - include any useful information on mirror sites, just as they did for the sites that originally gave rise to the blocking order.

**In Russia**, the regulator is responsible for both updating the list of blocked sites and implementing blocking measures. A law adopted on 1 July 2017 introduced a simplified system for blocking circumventiion sites through an accelerated administrative procedure that does not require rightholders to return to court.

## THE SPECIFIC CHARACTERISTICS OF STRATEGIES AGAINST PIRACY OF LIVE SPORTS EVENTS: THE EMERGENCE OF A "LIVE BLOCKING" SYSTEM IN EUROPE

Piracy of online sports content has increased considerably in recent years. All you have to do is type the names of the two opposing teams into a search engine just before the match is due to start, and a multitude of links to illegal live streams will come up.

According to a 2016 report by the European Audiovisual Observatory[13], "*The Premier League detected approximately 33,000 unauthorised live streams during the 2012/13 season, and about 17,500 for Bundesliga matches. These figures have been constantly climbing in recent years. This is due in part to the widespread availability of low-cost technologies that facilitate the illegal retransmission of broadcasts with relative ease and little investment. It is also due to the popular appeal of live football broadcast, which makes it a particular target for unauthorized retransmission on the Internet. The quality of the streams themselves is improving rapidly and their use has evolved beyond the home-user, as they are now found in commercial premises, according to the Sports Rights Owners Coalition (SROC)*".

The methods of combating online piracy of sports broadcasts are, in several respects, similar to those already used to tackle copyright infringement, namely:

- cut off the revenue streams to sites and services offering live streaming content or selling illegal access to pay-TV packages;
- make it easier to apply to a court or a public authority for a blocking order against Internet service providers and search engines;
- tackle the reappearance of infringements (services circumventing blocking measures or mirror sites).

It may be the same site or service offering unauthorised access to both encrypted sports channels and pay-TV film channels with exclusive rights for films and TV shows. Such sites and services, in addition to unauthorised access to various channels, offer easy access to works via illegal website links. Thus, in many countries, these two causes interact to advance the fight against online piracy.

*[13] "Audiovisual sports rights between exclusivity and right to information".*

However, legal measures to tackle piracy of sports events raise two specific issues that national legislation or case law endeavour to address in advance: firstly, the establishment of a legal basis to legitimise procedures relating to the protection of sports content and, secondly, the development of specific procedures for blocking the unauthorised streaming of live sports events on the Internet, which means adapting litigation and administrative procedures to allow for punctual, targeted live blocking procedures.

## PROTECTING ONLINE SPORTS CONTENT AND THE RIGHTS OF SPORTS ORGANISATIONS IN EUROPE

**In Europe**, the Court of Justice of the European Union considers that: "*sporting events cannot be regarded as intellectual creations classifiable as works within the meaning of the Copyright Directive. That applies in particular to football matches, which are subject to rules of the game, leaving no room for creative freedom for the purposes of copyright. [...] None the less, sporting events, as such, have a unique and, to that extent, original character which can transform them into subject-matter that is worthy of protection comparable to the protection of works. [...] Accordingly, it is permissible for a Member State to protect sporting events, where appropriate by virtue of protection of intellectual property, by putting in place specific national legislation, or by recognising, in compliance with European Union law, protection conferred upon those events by agreements concluded between the persons having the right to make the audiovisual content of the events available to the public and the persons who wish to broadcast that content to the public of their choice.* "[14].

In this respect, it is interesting to note that some national laws in the European Union provide for special related rights or *sui generis* rights for sports event organisers.

**In Italy** for example, a new related right was incorporated into Italian copyright legislation in 2008 to protect sports event organisers. This right stems from the need to protect the investments of these organisations (particularly in football) and to ensure the possibility of an adequate return for investors when negotiating media broadcasting rights[15]. The public authority in charge of anti-piracy ensures the blocking of both cultural and sports content sites, including live streaming sites.

**In Germany,** sports event organisers are granted a specific related right (*Schutz des Veranstalters)*[16], with the same objective of protecting their financial investment.

**In the United Kingdom**, the Football Association Premier League (FAPL) organises the football league championship and holds the television rights to Premier League matches. Its intellectual property rights over the broadcasting of the matches it organises are based on the following legal grounds: firstly, the Clean Live Feed captured by its licensees is recorded, which means that logos can be added when it is broadcast (particularly abroad); secondly, these recordings include a replay of the match highlights. UEFA (Union of European Football Associations) has been granted intellectual property rights over the televised broadcasting of matches, also on the grounds of the replays, logos and music included in the recording either before or during broadcasting.

**In Portugal**, sports content is protected under intellectual property law. Thus, since 1 January 2019, it has been possible to extend the administrative DNS blocking system to sites providing unauthorised access to sports content, and implement "live blocking" measures during the televised broadcasting of sporting events. Dozens live streaming websites were blocked in the first few weeks of operation of this new system.

*[14] CJEU, 4 October 2011, Football Association Premier League Ltd and others against QC Leisure and others (C-403/08) and Karen Murphy against Media Protection Services Ltd (C-429/08).*

*[15] Under Article 28 of Legislative Decree No. 9 of 9 January 2008, sports broadcasting rights are included in related rights pursuant to a new Article 78- quater in the Italian copyright act (Decreto legislativo 9 gennaio 2008, n. 9 recante disciplina della titolarita 'e della commercializzazione dei diritti Audiovisivi sportivi e relativa ripartizione delle risorse) www.wipo.int/edocs/lexdocs/laws/it/it/it199it.pdf. See also T.M.C. Asser Institute, Centre for International & European Law, Instituut voor Informatierecht (IViR), Study on sports organisers' rights in the European Union, Final Report, op. cit.*

*[16] See Article 81 of the Gesetz über Urheberrecht und verwandte Schutzrechte of 1965, in its amended version www.gesetze-iminternet.de/bundesrecht/urhg/gesamt.pdf*

## THE IMPLEMENTATION OF PROCEDURES FOR BLOCKING THE ILLEGAL BROADCASTING OF LIVE SPORTS EVENTS ("LIVE BLOCKING")

**In Italy**, administrative blocking measures apply indiscriminately to all streaming and live streaming sites offering cultural or sports content. These measures consist of permanent DNS blocks, which are identical regardless of the site targeted.

**In the United Kingdom**, judicial blocking measures are also implemented against different types of illegal offer. They consist of IP blocks that are generally temporary, applicable only during the broadcast of a specific sports event.

This practice is referred to as "live blocking". Every week, illegal live streaming sites are blocked for a period approximately equivalent to the duration of the sports event they were planning to broadcast. The rightholders usually draw up a list of the sites in question at the beginning of each week. However, this list can be updated during the week. Some measures may also be taken in real time, when the sports event is broadcast.

Technical investigations carried out in the United Kingdom into "live streaming" seem to indicate that sites and services offering illegal content are supplied directly by a single server that does not have a domain name, but only an IP address (probably dedicated, given the volume of content streamed). IP blocking shuts off traffic from these servers, generating a large-scale "domino effect" across all the sites and services they supply. Conversely, DNS blocking affects the sites and services but not the servers.

However, in view of the risks involved in IP blocking, both courts and public authorities are vigilant as to the proportionality of such measures, and monitor them closely to assess their effectiveness and identify any risks.

Therefore, IP blocking can be considered only if warranted by particular circumstances of time and space, and if it is accompanied by specific procedural guarantees, such as:

- the server(s) targeted by the measures must be used solely or predominantly to enable or facilitate access by certain domestic audiences to illegal content;
- Internet service providers can only be required to do their utmost to block notified services, depending on their network configuration and their resources;
- the server hosting providers must be notified of the planned blocking measures to guarantee their right to an effective remedy;
- Internet service providers must inform their subscribers by electronic means that access to a number of servers involved in the illegal streaming of matches has been blocked by a court decision, and that similar measures will be taken if necessary, throughout the whole season or competition.

**In the United Kingdom**, in March 2017, the High Court agreed to a request from the Football Association Premier League (FAPL) to block servers streaming matches illegally. The court order allowed them to block such servers in real time for the duration of a match, and to do so repeatedly throughout the season (until May 2017). Following this decision, which resulted in the blocking of 5,000 IP addresses, the FAPL filed another request and obtained a similar order for the 2017/2018 season; in July 2018, it proceeded likewise for the 2018/2019 season. In December 2017, the Union of European Football Associations (UEFA) obtained a similar order for the period from February to May 2018. This was also extended last July. It should be noted that Internet service providers have not opposed any of these procedures and have, on the contrary, supported them by cooperating with the rightholders in their implementation. Most of these ISPs are FAPL licensees themselves. A list of servers updated by the rightholders is sent to Internet service providers every week.

# COOPERATION BETWEEN RIGHTHOLDERS AND A STRONGER ROLE FOR PUBLIC OPERATORS

Anti-piracy actions, particularly blocking measures, are very often facilitated by cooperation between rightholders and/or new and stronger methods of public intervention.

## EXPERIMENTS IN JOINT ACTIONS BY RIGHTHOLDERS

### SECTOR-BASED COOPERATION WORLDWIDE

**The music industry** is represented worldwide by the International Federation of the Phonographic Industry (IFPI), which is present in 57 countries, and the CISAC (International Confederation of Societies of Authors and Composers), which has 238 members in 121 countries.

**The audiovisual sector** has taken the fight against piracy to a global level, under the leadership of the Motion Picture Association of America (MPAA). The MPAA represents the interests of the biggest studios in America and has a branch for Europe, the Middle East and Africa (the Motion Picture Association), as well as local offices in numerous countries.

### EXAMPLES IN THE AUDIOVISUAL SECTOR

**In Europe**, the Audiovisual Anti-Piracy Alliance (AAPA)[17] also represents companies that provide content to pay-TV services or develop technologies to secure or facilitate the provision of these services. AAPA's mission is to tackle piracy of copyrighted audiovisual content, in particular by providing technical expertise.

In June 2017, under the aegis of the MPAA, audiovisual rightholders from various countries (38 to date) joined forces to create the Alliance for Creativity and Entertainment (ACE), the goal being to combat piracy on a global scale. In 2018, ACE successfully took action against several links in the ecosystem of devices set up specifically for the purposes of audiovisual piracy.

**In Asia** in 2017, a group of rightholders created the Coalition Against Piracy (CAP) under the aegis of the Cable & Satellite Broadcasting Association of Asia, an association of television service providers in Asia[18]. The purpose of CAP is to combat piracy of audiovisual content in Asia and, in particular, to prevent illegal streaming of audiovisual programmes and the use of set-top boxes and applications that enable illegal access to protected content.

Both ACE and CAP took part in an operation in Australia in late 2017 to shut down a company that was selling pre-loaded set-top boxes enabling unlawful access to on-demand content. The boxes were sold with a one-year subscription to a package of TV channels broadcasted without authorisation[19].

*[17] beIN Sports ,BT, Canal+ Group, Cosmote TV, CryptoGuard, Cyta, Discovery Communications, Fox Networks Group, Irdeto LaLigua, Liberty Global, MCNC, Nagra Kudelski, NDS, Nordic entertainement group, NOS, NOVA, OSM, Premier League, Sky, Skyworth Digital, United Media, Verimatrix, Viaccess Orca, Vodafone Ziggo. Grupo Globo, HBO, Hulu, Lionsgate, Metro-Goldwyn-Mayer (MGM), Millennium Media, NBCUniversal, Netflix, Paramount Pictures, SF Studios, Sky, Sony Pictures Entertainment, Star India, Studio Babelsberg, STX Entertainment, Telemundo, Televisa, Twentieth Century Fox, Univision Communications Inc., Village Roadshow, The Walt Disney Company, and Warner Bros. Entertainment Inc.*

*[18] beIN Sports, casbaa, The Walt Disney Company, Fox Networks Group, HBO Asia, NBCUniversal, Premier League, Turner Asia-Pacific, A&E Networks, Astro, BBC Worldwide, CANAL+, Cignal, Media Partners Asia, National Basketball Association, PCCW Media, Singtel, Sony Pictures Television Networks Asia, TVB, True Visions, TV5MONDE et Viacom International Media Networks.*

*[19] www.casbaa.com/news/casbaa-news/alliance-for-creativity-and-entertainment-ace-and-casbaas-coalition-against-pira- cy-cap-close-down-australian-illicit-streaming-device-operation/*

### CROSS-SECTOR COOPERATION AT THE NATIONAL LEVEL

In some countries, cross-sector coalitions of rightholders have been set up locally to initiate and coordinate legal action against illegal sites and services. Examples of such coalitions include the *Gesellschaft zur Verfolgung von Urheberrechtsverletzungen e.V.* (GVU) in Germany, the *RettighedsAlliancen* in Denmark and the *Stichting* BREIN[20] in the Netherlands.

***Stichting BREIN* (in the Netherlands)** can be translated as the Dutch Association for the Protection of the Rights of the Entertainment Industry. It is tasked with combating piracy and initiating legal proceedings on behalf of its members, who include rightholders in the music, audiovisual, publishing, video games and interactive software industries, as well as the main collective management organisations.

In recent years, the Stichting *BREIN* has initiated court proceedings that have led to major decisions by the EUCJ. These decisions have, in particular, advanced jurisprudence on links to illegally published content[21], the selling of pre-loaded set-top boxes[22] and platforms that enable online sharing of copyrighted works, such as the Pirate Bay[23].

**In the United Kingdom**, rightholders may specify that their action is supported by other rightholders. For example, the Premier League used this *modus operandi* in the proceedings leading to the first live blocking decision in March 2017[24], in order to establish the legitimacy of its action.

Such coalitions may also be formed to facilitate agreements with Internet service providers on the implementation of blocking measures.

**In Denmark**, the *RettighsAlliancen* represents rightholders in the audiovisual, music, publishing, video games and visual arts industries. In 2014, *RettighsAlliancen* reached an agreement with Internet service providers that simplifies injunctive proceedings and guarantees their long-term effects.

**In Portugal**, administrative blocking was introduced in July 2015, following an agreement between the Inspectorate General of Cultural Affairs[25] (IGAC), the Portuguese Association of Telecommunications Operators (APRITEL) and rightholders association MAPINET (a cross-sector anti-piracy organisation).

## THE INCREASED ROLE OF PUBLIC ACTORS

### VERY VARIABLE FORMS OF PUBLIC INTERVENTION

The range of public authorities involved in copyright protection is rather diverse. At the very least, they support and promote private initiatives; in the case of regulators with injunctive powers, they intervene directly.

They may include ministries equivalent to the French Ministry of Culture (South Korea, Spain, Portugal), ministries in charge of the economy or foreign trade (the Anglo-Saxon model), public institutions responsible for registering intellectual property rights and issues, or regulators vested with often rather broad competences on digital matters (Italy, Russia).

*[20] The Bescherming Rechten Entertainment Industrie Nederland.*
*[21] CJEU, 8 September 2016, C 160/15, GS Media BV/ Sanoma Media Netherlands BV, Playboy Interprises International Inc.*
*[22] CJEU, 26 April 2017, Stichting Brein vs Jack Frederik Wullems, known as "Filmspeler", C-527/15.*
*[23] CJEU, 14 June 2017, C-610/15 - Stichting Brein/Ziggo BV, XS4All Internet BV, known as "The Pirate Bay".*
*[24] The March 2017 proceedings that led to the first live blocking decision were supported by the following: i) British Broadcasting Corporation and BBC Worldwide Ltd; ii) DFL Deutsche Fußball Lega GmbH; iii) Liga Nacional de Fútbol Professional; iv) The Football Association Ltd; v) The Scottish Premier League Ltd; vi) The Football League Ltd; vii) England and Wales Cricket Board Ltd; viii) PGA European Tour; ix) The Professional Darts Corporation Ltd; and x) Rugby Football Union.*
*[25] IGAC specialises in the protection of copyright and related rights, and reports to the Ministry of Culture. One of its main tasks is to register works and supervise collective management organisations.*

It is worth noting that even in the United States, where the fight against piracy is essentially conducted by rightholders, the public authorities are thinking about getting more involved, particularly in terms of promoting legal offer, raising awareness among end-users and cutting off the revenue streams to illegal sites through the "follow the money" approach.

**In Italy**, the digital communications regulator *Autorità per le Garanzie nelle Comunicazioni* (AGCOM) is an independent authority created in 1997. It has regulatory and control powers in the electronic communications, audiovisual and publishing sectors. AGCOM is a "convergent" authority which, since 2000, has played a steadily expanding role in copyright protection in sectors where it acts as guarantor and regulator. AGCOM is the only regulator of online cultural and sports content in the European Union. With the transposition of the AMS Directive, it will soon see an increase in its powers to tackle hateful and inappropriate online content. AGCOM is funded primarily by contributions from regulated operators. It employs three hundred and sixty (360) people on a full-time basis, and is currently divided into seven cross-functional departments and five divisions specialising in particular areas of expertise.

**In the United Kingdom**, there is both a communications and content regulator (the Office of Communications or Ofcom) and a government agency (the Intellectual Property Office or IPO). Only the IPO, which is responsible for registering industrial property rights, has general competence to deal with intellectual property matters at present. The IPO conducts awareness-raising and educational initiatives in the area of intellectual property, drawing on the sectoral monitoring activities carried out by Ofcom. The IPO has worked with rightholders to set up an Intellectual Property Crime Unit within the City of London Police. It is also helping to fund an e-mail campaign to inform and raise awareness among rightholders. Individuals may refer a point of law that is leading to confusion to the IPO for clarification. The IPO may also provide an alternative dispute resolution service on some matters relating to intellectual property.

## INTERNATIONAL PUBLIC COOPERATION

International public cooperation can take an extremely wide variety of forms: from conducting bilateral or multilateral negotiations, to administrative, judicial, police or customs cooperation.[26].

**In Europe,** The European Commission is encouraging EU Member States to provide tools, training and adequate support for national judges in the field of intellectual property, in order to obtain swifter, more effective and more coherent decisions, delivering greater legal certainty.

The Commission has stated that it plans to work with the European Observatory on Infringements of Intellectual Property Rights - which is part of the European Union Intellectual Property Office (EUIPO) - to develop the information tools and media needed to facilitate the work of the courts. The Commission has invited Member States to systematically publish judicial decisions relating to intellectual property, and has asserted that any European case law database should be maintained by the EUIPO so that it is more comprehensive and easier to use.

**Globally,** the World Intellectual Property Organisation (WIPO) is also taking an interest in national systems which, it points out, have a limited geographical impact.

It has suggested coordinating these efforts and initiatives on an international scale. The relay centres considered by the WIPO should be based on schemes implemented by the public authorities in each country. The WIPO is calling for more effective international cooperation, for example by setting up a system for informing Member States that an illegal site - that has been blocked in some countries - is operating on their territory, or by strengthening international ties to more effectively monitor and control the allocation of domain names and who owns them.

*[26] Law enforcement agencies in Europe and worldwide can work together under the coordination of Europol and, in particular, the Intellectual Property Crime Coordinated Coalition (IPC3), a dedicated anti-counterfeiting unit.*

## "NAME AND SHAME" INITIATIVES

Government actions can be conducted internationally, thus providing a link between diplomatic institutions to encourage joint cooperation agreements and hence make blocking measures more effective, and also to name and shame unethical operators and markets.

Every year, **the US administration** publishes two lists via the United States Trade Representative (USTR), a government agency that coordinates US trade policy. The sole purpose of these lists is to name and shame unethical behaviour:

- the "Special 301 List", which is issued under a law and identifies countries that do not provide effective protection of intellectual property rights;
- the "Notorious Markets List", which is established independently of any legislative text, identifies websites and physical marketplaces worldwide - except in the United States - that clearly engage in or enable infringement of industrial property rights or copyright. The purpose of the list is to inform the public. It is established based on submissions made primarily by the industries concerned, and an investigation by the USTR. Once the list has been published, the websites on it sometimes contact the USTR to ask what they should do to avoid being listed again the following year.

In December 2018, **the European Union** followed in the footsteps of the United States, publishing its first "Counterfeit and Piracy Watch List"[27] of websites and physical marketplaces outside of the European Union that have been reported to the Commission as infringing or enabling the infringement of intellectual property rights[28]. The aims of this list are to step up action against commercial counterfeiting to protect European interests, and encourage both local authorities and private operators to take anti-counterfeiting measures.

Regarding copyright, a very diverse range of actors are targeted across the entire ecosystem: cyberlockers, stream ripping services, links sites, peer-to-peer links sites, application sites, hosting providers and online advertising industry operators. The list focuses notably on a service called "Cloudflare", which is based in the United States. Cloudflare offers several services, including one that hides the IP address and true identity of the hosting server. It considerably hinders anti-piracy operations by making it difficult to establish the exact location of the website.

The list, which was initially expected to include just 15 to 25 marketplaces, now contains around 50.

The Commission will monitor the actions taken by the local authorities and operators named on the list to reduce intellectual property infringements. The list may also be used in bilateral and multilateral negotiations, and to raise consumer awareness.

*[27] trade.ec.europa.eu/doclib/press/index.cfm?id=1952*

*[28] For the purpose of drawing up the list, the Commission launched a public consultation. The findings were verified by DG Trade, EUIPO and Europol. The marketplaces to be included in the list were then selected.*

PART 2

# THE NECESSARY ENGAGEMENT OF END-USERS AND DIGITAL OPERATORS IN THE FIGHT AGAINST PIRACY

The success of anti-piracy measures requires the involvement of all parties: end users who should be encouraged to behave responsibly and directed towards legal offer, and digital industry professionals who do not wish to make money by facilitating or enabling online counterfeiting.

# THE RESPONSIBILITY OR AT LEAST ACCOUNTABILITY OF END USERS

In addition to tackling the sites that create the service "offering", it is important to consider how to address the role played by end-users as recipients and, in some cases, active participants (in services offering "User Generated Content" or "UGC").

At present, measures applicable to end-users focus essentially on peer-to-peer file sharing and do not cover streaming or direct downloading, given the technical constraints and legal uncertainty involved in establishing the end-user's role.

Depending on the country, additional or alternative prevention measures include promoting legal offer and developing public awareness and communication tools.

## MEASURES TO PREVENT END-USERS FROM ENGAGING IN PEER-TO-PEER FILE SHARING

### END-USERS WARNING SYSTEMS

The feedback on the graduated warning systems implemented by other countries highlights three key points:

- the cooperation of Internet service providers is essential, especially where their involvement is not required by law, insofar as they are not - or are only marginally - held liable for their shortcomings;
- it is difficult to control and share costs (between Internet service providers and rightholders) due to the wide range of subscribers likely to be targeted;
- it is difficult to implement effective sanctions in addition to purely educational measures.

**The United Kingdom** launched its Voluntary Copyright Alert Programme in 2017, which consists in sending out warning e-mails to end-users without imposing punitive sanctions. The programme is part of a global approach involving a wide-reaching awareness campaign. It is based on a (renewable) three-year agreement between rightholders and Internet service providers. The plan is to send out 2.5 million e-mails per year. The warning may refer to several events, and e-mails contain links to the referrals (specifying the work(s) concerned) and to a site containing, *inter alia*, advice for users on how to secure their Internet connection[29].

**In Ireland** in 2009, the main Internet service provider Eircom reached an agreement with the Irish Recorded Music Association (IRMA), whereby Eircom undertook to set up a graduated response system in the music industry. In 2010, rightholders in the music industry wanted to extend the agreement to include other Internet service providers, and took legal action against them for that purpose. The court ruled in favour of the rightholders and a broad outline of the agreement was sketched out. After issuing three notifications to a subscriber, the Internet service provider must inform the rightholders of the situation. The rightholders may then refer the matter to the court to identify the end-user and request that his/her contract with the Internet service provider be terminated or that his/her Internet connection be suspended (unlike the agreement with Eircom, which does not involve recourse to the courts).

**In Canada**, the "Notice and Notice Regime" set out in Canada's Copyright Act is criticised by rightholders because it has a purely educational purpose (even in the event of repeated infringements) and because Internet service providers find it difficult to apply.

**In the United States**, the Copyright Alert System was withdrawn by common consent in the first quarter of 2017, after being in use for four years. The reasons for this were that the return on investment was deemed insufficient, the cost distribution keys were contested by rightholders and Internet service providers, and Internet service providers were reluctant to take action against the offending subscribers. However, some studios continue to issue notifications, mostly for purely educational purposes.
In addition, a recent decision against an Internet service provider has reminded ISPs that they are required under the Digital Millennium Copyright Act (DMCA) to deal with repeated infringements by their customers and to terminate the subscriptions of end-users who have been the subject of repeated complaints, without being enjoined to do so by a court order.

## COMPENSATION SYSTEMS

Traditionally, the law and civil procedure allow all injured persons to obtain compensation in the event that their rights are infringed by a third party. Such redress may be obtained before trial, as part of an amicable settlement following a letter of formal notice from the rights holder to the infringer.

Regarding copyright infringement on peer-to-peer networks, the number of indemnification notices issued directly to offending end-users by the legal counsels of rightholders is rising, on the basis of the rules of civil settlement procedure (Germany, Canada, Sweden, the United States and the United Kingdom).

Besides its low level of acceptability to the general public, this type of action - depending on the legal traditions specific to each country - raises questions regarding the risk of abuse, the role of courts, and the protection of personal data.

This approach also raises financial issues, which are one last impediment to its wide-scale deployment. The costs borne by rightholders are multiplied (network monitoring costs, legal costs and lawyer's fees for seeking a court order to identify the subscriber - and, in particular, serve formal notice on him or her - and identification costs paid to Internet service providers). Now, the burden of legal fees that can be charged to the subscriber has in many cases been capped by the law or the court itself. In any case, the chances of rightholders recovering the requested sums are uncertain at the formal notice stage, unless they subsequently have to take legal action against the end-user in the event that the settlement procedure fails.

*[29] www.get-it-right.org/faq.html*

**Germany** attracts a lot of attention, having enacted legislation to set up a broad-scope compensation system. German rightholders instruct peer-to-peer network monitoring companies to collect the IP addresses of infringing end- users. In accordance with personal data protection rules, rightholders must then obtain a court order authorising the ISP to identify - via an IP address - the subscriber whose Internet connection was used to infringe copyright, and to hand that information over to the rights holder. The aim is not to bring action against the subscriber directly, but to issue prior formal notice. German law provides that the notice sent to the end-user must contain, under penalty of nullity: the name of the rightholders if they are not acting on their own behalf (but through a legal representative); the nature of the right infringed; details of the amounts being claimed (distinguishing legal fees, procedural fees and damages); whether or not the rights holder requires the subscriber to agree in writing to cease sharing the work specified in the letter of formal notice.

**In the United Kingdom**, considering the large number of infringements reported, a court decision referred to as "Golden Eye" provides a legal framework for rightholders to issue indemnification notices to end-users. Under the decision, the rights holder's letter must explain that, despite the injunction to reveal the end-user's identity, the latter is not yet regarded as a counterfeiter; the end-user must respond without undue delay.

## THE ROLE OF END- USERS IN UNLAWFUL STREAMING AND DIRECT DOWNLOADING

**In Europe**, the streaming or direct downloading of content from an illicit source serves as a textbook case, as it raises the question of whether or not to punish unauthorised, temporary acts of reproduction, of which the end- user is not necessarily aware.

An initial ruling by the Court of Justice of the European Union (CJEU) on 5 June 2014[30] specified the legal regime applicable to end- users who stream intellectual works from a legal website. The Court ruled that, where the source was legal, such practices could be subject to the temporary copy exception, and therefore did not have to be expressly authorised as acts of reproduction.

The specific temporary copy exception was created by the 2001 Directive on Copyright and Related Rights in the Information Society to facilitate the functioning of the Internet. The purpose was to provide a legal framework for acts of reproduction respecting several cumulative conditions, to be interpreted strictly[31].

On this point, the Court emphasises that *"the on-screen copies and the cached copies made by an end-user in the course of viewing a website must satisfy the conditions that those copies must be temporary, that they must be transient or incidental in nature, and that they must constitute an integral and essential part of a technological process, while complying with the requirements of the three-step test"*.

More recently, the Court of Justice of the European Union, in Case C-527/15 *Stichting Brein* v *Jack Frederik Wullems* (*or "Filmspeler"*) of 26 April 2017, asked about the legal regime applicable to a end- user who had purchased a pre-loaded multimedia player to search for and access pirated content (on various websites likely to offer such content) and to view that content on a television screen.

While simply viewing streamed content does not, in principle, constitute an infringement of performance rights, as the end- user does not communicate the work to the public, it may violate reproduction rights. The question raised in this case was whether or not the reproduction made by the end- user was lawful.

*[30] CJEU, 4th chamber, 5 June 2014, C-360/13, Public Relations consultants association LTD C/ Newspaper Licensing agency Ltd e.a.: Jurisdata no. 2014-012515. : Jurisdata n°2014-012515.*

*[31] The Court of Justice of the European Union has on three occasions indicated how this exception should be interpreted (CJEU, 4 October 2011, C-403/08, Premier League and C-429 Murphy; CJEU, 14 January 2012, C-302/10, Infopaq 2; CJEU, 5 June 2014, C-360/13). The rights holder may not oppose technical reproductions made in the course of digital transmissions:*

*• volatile copies stored in routers when a work is circulated (necessary act concept),*

*• temporary, transient or incidental copies that form an integral and essential part of a technological process, the sole purpose of which is to enable either transmission in a network between third parties by an intermediary, or a lawful use of a work or other subject-matter to be made. The acts of reproduction should have no separate economic value of their own. Compliance with the latter condition is essential. European case law links it with the requirement to comply with the three-step test.*

The CJEU was required to judge whether or not the end-user, who used the player to view massively infringing streaming sites, was protected under the provisional copy exception. The Court ruled that viewing massively infringing streaming sites via a multimedia player carrying out unauthorised acts of communication was not covered by the provisional copy exception.

To this end, it referred to Directive 2001/29/EC of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society, and to the established case law of the Court of Justice of the European Union, which stipulates that "*a use should be considered lawful where it is authorised by the rightholders or not restricted by law*".

After noting that the rightholders had not authorised the uses in question, the Court considered whether these uses were restricted by law, indicating that this point should be addressed with reference to the three-step test. On this last question, the Court ruled that temporary reproductions of protected works obtained from massively infringing streaming sites should be regarded as conflicting with the normal exploitation of the works and causing unreasonable prejudice to the legitimate interests of the rightholders.

Therefore, this decision provides initial clarifications on the lawfulness of streaming operations carried out by end-users. This issue has, until now, been addressed primarily from a doctrinal point of view due to the incoherence of piracy prevention schemes; incoherence brought about by the differences in the way copyright infringements are handled, depending on the piracy methods used (peer-to-peer file sharing, streaming or direct downloading.

In any event, irrespective of the difficulties, sanctioning end-users - be it for streaming or peer-to-peer file sharing - raises the recurring issue of identifying the infringer, which necessarily means re-examining a concept that already exists in countries such as Germany and France: the Internet subscriber and the obligations incumbent upon him or her.

**In Germany**, the presumption that the subscriber has used his or her Internet connection to commit one or more infringements - as reported by rightholders - is not accompanied by a greater duty of care regarding the security or third-party use of the said connection. Thus, German courts may rule out the subscriber's liability if he or she is able to prove that someone else was using the Internet connection at the time the offence was committed. However, to exonerate themselves of responsibility, subscribers must identify the persons who had independent access to their Internet connection and were therefore likely to have committed the alleged copyright infringement. Nonetheless, the Court of Justice of the European Union specified on 18 October 2018[32] that subscribers must be held liable if they cannot or will not name another adult member of their household.

At this stage, it is difficult to conclude that the decisions taken recently by the Court of Justice of the European Union are such as to clarify how civil and criminal law in EU Member States should deal with the behaviour of endusers who stream works from infringing websites, except in one very specific case where the end- user used a set-top box with full knowledge of its illegality (due to the associated advertisements)[33].

Furthermore, these purely theoretical legal considerations must be accompanied by an analysis of the technical feasibility of such sanctions, particularly in terms of establishing proof. It would seem that, given the current state of streaming technology (which, unlike peer-to-peer networks requires a centralised system), collecting data to identify the offender is likely to lead to an invasion of privacy that could be regarded as disproportionate to the objective pursued[34].

*[32] CJEU, 18 October 2018, C-149/17, Bastei Lübbe GmbH & Co. KG v Michael Strotzer.*
*[33]The box was advertised as follows: "Never pay for films, series or sport again, watch them directly without ads or breaks (no subscription fees, plug&play). Netflix is a thing of the past!"; "Want to watch films, series, sport free of charge? Yes please!" ! "Never have to go to the cinema again thanks to our optimised XBMC software. Free HD films and series, including films recently shown in cinemas, thanks to XBMC".*
*[34]Monitoring streaming and direct download operations is costly and requires substantial technical resources. ISPs are very reluctant to take this kind of measure. Implementing the Deep-Packet Inspection (DPI) solutions needed to monitor networks is a complex process. Furthermore, since many platforms have adopted the HTTPS protocol, the possibility of monitoring online traffic is limited: this encrypted protocol precludes monitoring of the specific content viewed by end-users.*

Finally, it should be pointed out, **in the European Union,** that the case law of the **Court of Justice of the European Union** regarding the "*placement of hyperlinks to illegal content*" by end-users (or "uploaders") seems, in its assessment of the facts, to focus on distinguishing between end-users acting in good faith and those acting in bad faith, and on establishing whether the communication acts in question were carried out for a lucrative or non-lucrative purpose.

**In the Netherlands**, the *Stichting BREIN,* an association of rightholders committed to preventing piracy, has opted for a compensation system focusing exclusively on big file sharers (or "uploaders") who operate on certain social networks via UGC platforms, newsgroups or peer-to-peer software. It uses dedicated IP identification software, approved by the Dutch Data Protection Authority. Rightholders may petition the court to obtain a end- user's identity if necessary. These actions most often result in settlement agreements relating to previous acts of counterfeiting, and an undertaking, under financial compulsion, not to infringe copyright in the future.

**South Korea** introduced a system in 2009 for sending notifications to *"uploaders"* who post content on UGC platforms without authorisation. At the end of the procedure, the end- user's account may be deleted from the platform. This system does not target peer-to-peer networks. In broad terms, it combines a mechanism like ours for reporting illegal content to platforms, with a warning system for "repeat offenders". Moreover, the goal is to win the cooperation of platforms rather than that of Internet service providers. Pursuant to this system, the Ministry of Culture, Sport and Tourism, after checking the material evidence provided by rightholders, may:

- order the platform to remove the infringing content, in accordance with the "notice and takedown" principle;
- issue a warning via the platform to the end- user who made the content available, explaining that, in the event of a repeat offence, their account on the platform may be suspended for a limited period. There are three warnings before a sanction is actually imposed. Sanctions may consist in blocking a user's access to the platform for a maximum period of six months.

## PUBLIC AWARENESS TOOLS

### PUBLIC COMMUNICATION CAMPAIGNS

End- user awareness campaigns focus primarily on the various risks incurred by users when they share or consume content illegally. These communication campaigns may target specific populations, particularly young audiences.

Other strategies include communicating - where appropriate with the support of previously convicted end- users - about the actions taken to prevent counterfeiting and the convictions obtained on numerous media, including those used by end- users to illegally share content (UGC platforms, social networks, etc.).

**In Australia**, an association of rightholders launched a communication campaign on 18 August 2017 called *"*Price of Piracy*"*. It aims to alert consumers to the presence of malware on illegal streaming and peer-to-peer websites. A dedicated website has been created. It includes explanatory videos on the dangers of streaming or downloading illegal content, as well as advertising spots featuring a famous Australian actor.

**In the United Kingdom**, the government plans to share more piracy prevention data with the press, by publishing court rulings for example.

**In Sweden**, the Patent and Trademark Office conducted a government-led communication campaign in May 2018, during which it was reported that the owners of illegal streaming sites make a lot of money and are involved in other illegal networks (selling counterfeit medicines, drugs, etc.).

**In Spain**, the Spanish government launched an awareness campaign in October 2017 called *"No piratees tu futuro"* (don't hack your future); it is aimed at young people and is designed to raise their awareness of the fight against piracy of cultural and sports content. The campaign was conducted and funded by private sector actors as part of a partnership with the Ministry of Culture and Sport. It had a dual objective: to direct people towards legal offer and to inspire empathy by showing the consequences of piracy on the future careers of young people, without focusing on the criminal punishment aspect. The Ministry of the Interior, an association specialising in intellectual property, and the Ministry of Culture and Sport are also producing support materials for teachers and students in preparation for police officers going into schools to raise awareness about the risks of piracy.

### ACTIONS TO PROMOTE LEGAL OFFER

Many countries are setting up portals either for a cross-sectoral audience or for the audiovisual sector alone. Awareness campaigns are being organised to promote legal offer, and are one of the methods used to drive change in end- user behaviour.

**In Sweden**, there are several portals that list legal offer, one of the biggest of which is "*Moviezine*". Another portal, called "*Streamalagligt.se*", is run by the Patent and Trademark Office and provides access to films, series and music.

**In the United Kingdom**, the government launched a copyright campaign in November 2015 called "Get it Right from a Genuine Site". A website was set up as part of the campaign, featuring a list of "genuine" sites as well as animated films to raise young people's awareness of legal offer.

**In Japan**, the "Manga-Anime Guardians" project aims to step up the protection of manga, a very popular cultural product in Japan that generates a lot of income for the rightholders. As part of the project, a website has been created listing the manga legally available online.[35]. The music industry has created a label to help end-users identify legitimate content.

**In South Korea,** the 2015 Clean Site initiative (now known as Copyright OK*)* led to the creation of a dedicated website administered by the public authorities, which certifies the legality of websites providing cultural content. Certified sites can then display the Copyright OK logo on their pages.

**In Australia**, a campaign to promote legal offer and educate the public on copyright law has been organised by rightholders in the audiovisual sector, who have set up an organisation called "Creative Content Australia". A dedicated website provides education resources for teachers and students, a link to a directory of legal platforms per sector, research reports and answers to frequently asked questions on piracy and cultural content.

*[35]manga-anim-here.com/*

### DISPLAYING USER-TARGETED MESSAGES ON BLOCKED WEBSITES

In addition to blocking measures, more and more Internet service providers are using on-screen messages to inform end- users why the website they are trying to access is not working, and in some cases redirect them to legal offer.

**In Australia**, Music Rights Australia - in its response to the public consultation on the Copyright Amendment (Online Infringement) Act of November 2018 - reported that few Internet Service Providers use the information pages developed by rightholders and prefer to use a page they have developed themselves, thus undermining the consistency of the educational message.

In countries where there is already a high degree of cohesion between rightholders (Denmark) or significant state involvement in the implementation of blocking measures (Italy and Portugal), work is being done to harmonise the wording of these messages and, in some cases, provide links to legal offer.

## STRENGTHENING THE ROLE OF INTERMEDIARIES IN ANTIPIRACY ACTIONS

The pervasive, multifaceted nature of piracy means that a wide variety of tools and strategies are needed to prevent it. It also calls for the involvement of all digital actors, which cannot go on avoiding - either through indifference or inertia - the challenges associated with the profusion of illegal online content.

The first step is to involve hosting providers in this participatory approach – to the extent permitted by their highly protective status – with a view to either removing illegally distributed works or monetising them through content recognition technologies. There is also the matter of how to deal with domain name registries.

Broadly speaking, the measures in place aim to identify ways of increasing the legal scope of anti-piracy arrangements to curb the deployment of illegal offer. Some actors, particularly advertisers and, to some extent, search engines, have embarked on an active approach consisting in improving the processing of notifications sent to them by rightholders.

### THE CENTRAL QUESTION OF THE STATUS OF PLATFORMS

The first question is how to involve willing hosting providers in this approach, while taking their specific features into account. The goal is to use content recognition technologies to enable either the removal or monetisation of illegally distributed works and, where appropriate, the deletion of accounts belonging to repeat offenders.

In practice, platforms such as YouTube, which host “User-Generated Content” (or UGC), have already entered into contractual agreements with rightholders to implement “stay down measures”. The notification of rightholders is facilitated by the content recognition technologies provided by the platform: the rights holder provides fingerprints, the site or service compares these fingerprints with online content and alerts the rights holder, who can choose either to remove the content or to monetise it, for example by sharing the advertising revenues it generates.

The increasingly widespread use of this type of agreement, coupled with the implementation of these technologies by platforms and rightholders, could make it easier to identify recalcitrant websites falsely claiming to be hosting providers.

Some countries[36] have pointed out that such practices can lead to over-blocking, and argue that they increase the risk of private filtering. For example, critics of these technologies point to their limitations when it comes to distinguishing between an illegal reproduction, a parody and a quote, and preventing the re-appropriation of the public space.

There is a great deal of discussion in Europe and the United States about establishing systems for the out-of-court settlement of disputes between rightholders and users invoking their right to use a work.

**In Europe,** the draft directive presented by the European Commission on 14 September 2016 opened the debate on the role that hosting providers could play - through content recognition technologies - in the withdrawal or monetisation of works disseminated without consent.

**In the United States,** a bill tabled in October 2017 aims to create a dedicated body attached to the Copyright Office to handle "small claims" relating to the unlawful use of photographs online, and disputes arising from takedown notices submitted to platforms like YouTube.

**In Switzerland,** there are no specific legal regime for technical intermediaries. A draft reform has therefore been proposed to frame the activities of hosting providers by imposing a specific obligation on those which "*due to [their] technical processes or [their] economic objectives enable legal violations or create a specific risk of such a violation occurring*". They must prevent the reappearance of copyrighted content that has previously been subject to a notice and stay down obligation, by taking any "technical and economic measures that may reasonably be expected [of them], considering the risk of violation".

**In South Korea,** platforms are regarded as a specific type of technical intermediary, a list of which is drawn up by the Ministry. They are under obligation to acquire content recognition or search filtering tools (enabling keyword filtering, for example). Platforms must use these technologies at the request of rightholders. Otherwise, they incur a fine.

## DOMAIN NAME REGISTRIES AND REGISTRARS

Domain name registries and registrars could provide a new means of tackling commercial counterfeiting.

**Registries** are organisations that manage the database of top-level domain names or IP addresses for a given region.

**Registrars** are accredited organisations that add new domain names to registries and provide hosting services for paying customers.

In practice, the registrars that register "generic" top-level domains (.com, .net, .org, etc.) must be accredited by the Internet Corporation of Assigned Names and Numbers (ICANN). National top-level domains (.fr, .eu, .uk, etc.) are managed by local organisations, which usually accredit registrars able to register the related domain names.

*[36]Belgium, the Czech Republic, Finland, Hungary, Ireland and the Netherlands.*

Both registries and registrars can suspend or order the transfer of domain names if the account has been linked to unlawful activities, which, for example, forces massively infringing sites to change their domain names.

Registries set their own rules and may therefore enter into agreements with rightholders or public authorities. Some registrars have introduced policies banning the use of domain names for unlawful purposes. They respond quickly to complaints and act swiftly to suspend or lock the domain names of infringing sites.

Registrars may have their accreditation revoked by the registry if they persistently breach its rules or if they fail to submit reports on notified infringements.

While the possibility of taking action towards or in collaboration with registries is interesting, it may prove ineffective insofar as infringing sites may purchase top-level domain names from countries with little or no copyright protection, through a registrar that shows little interest in protecting rightholders.

On 6 January 2014, the National Arbitration Forum - an ICANN-accredited litigation body - ruled that, in the absence of a court decision, a registrar cannot prevent the transfer of domain names to a third-party registrar, even where the domain names have been red-flagged by investigators.

Furthermore, some registrars do not respond to requests from public authorities in this respect; allegedly they do not enforce court decisions and even use their refusal to comply with notifications and court orders as a selling point.

**In the United States,** in February 2016, the Motion Picture Association of America (MPAA) entered into an agreement with domain name registry Donuts, which manages several extensions including "*.movie*". In May 2016, it signed an agreement with the Radix registry in Dubai, which also manages several extensions, including "*.website*" and "*.online*". These agreements provide for the possibility of suspending the domain names of massively infringing sites reported by the MPAA,[37] and have already led to the suspension of 25 domain names.

**In Spain**, the public authority responsible for piracy prevention may, under court supervision, request that a hosting provider stop hosting a website, or request that the site's domain name be suspended if it ends in ".es" or another extension managed by the national registry.

**In the United Kingdom**, if the City of London Police identifies an infringing site, a letter is sent to the relevant registrar or the organisation that manages the extension under which the domain name is registered, requesting that the domain name be suspended. This approach has met with mixed success among organisations located outside the United Kingdom (the most frequent scenario). The police would like to conclude agreements with domain name management bodies - and indeed registrars - worldwide.

*[37]The MPAA acts as a "trusted notifier", reporting sites that it suspects of infringing copyright to Donuts or Radix. Donuts or Radix then conduct an investigation, starting by contacting the site. If the site fails to respond in a satisfactory manner, or does not respond at all, Donuts or Radix suspends the domain name.*

## ADVERTISING NETWORKS

**In Europe**, research into the funding of websites that infringe copyright or trademark rights shows that 76% of the 5,000 most popular infringing sites belong to reputable brands. This demonstrates the necessity of using tools designed specifically for the complex world of online advertising.[38]

While there is widespread consensus on the utility of measures to identify and cut off the funding sources of infringing sites (based on the "follow the money" approach), questions are now being raised about their implementation, impact and effectiveness.

Consideration should be given not only to optimising and securing existing arrangements, but also to extending them to involve actors other than intermediaries, such as domain name registrars, hosting providers and search engines, thereby enabling them respectively to suspend the domain names of massively infringing sites, stop hosting them, or delist them.

Finally, besides the above-mentioned measures for improving and securing arrangements for cutting off revenue streams, another question needs to be addressed: how to broaden the scope of these arrangements so that the sites disappear once their sources of income have dried up? **The goal therefore is to "bridge the gap" between the observations made during the cut-off process and the legal actions to be taken against the listed sites to allow for a greater number of blocking decisions in the future.**

### VOLUNTARY APPROACHES BETWEEN DIGITAL OPERATORS

In several countries (such as the United States, Japan, Sweden and France), these arrangements rely on the contractual freedom of the signatories within a framework of voluntary self-regulation. They are limited strictly to the private sector; there is no real public intervention and no lists are published.

Therefore, the signatories commit primarily to implement measures to cut off the revenue streams to services that are regarded as infringing intellectual property rights on a commercial scale, and that do not have any substantial lawful purpose. In practical terms, this means inserting warranty clauses into their commercial contracts to prevent the sale of advertising space on infringing sites, and setting up the tools of their choice to monitor the enforcement of these commitments against websites identified as infringing under the terms of the agreements (content verification tools, ad delivery systems or reporting).

This type of arrangement, besides draining the resources of infringing sites, has the additional advantage that it damages the service standards and brand image of the site, thus making it easier for honest consumers to identify it as illegal.

Nonetheless, some massively infringing sites, both in France and abroad, continue to operate for a few years after such arrangements are put in place because they turn to networks that offer poor quality advertising (pornography and online games), other means of payment (virtual currency) or other sources of financing.

However, these methods are not infallible either and the sites develop circumvention strategies. For example, they use link obfuscators - seemingly innocuous intermediary sites featuring ads from traditional advertisers - to take visitors to the illegal content they are looking for.

In addition, **in Europe**, the European Commission has pointed out the legal implications of using such self-regulatory mechanisms in terms of competition, freedom of enterprise and online communication, as well as the need to assess their effectiveness and improve the follow-up of complaints under the responsibility of an independent third party. The Commission's legal analyses (conducted during the drafting of the Memorandum of Understanding on Online Advertising and IPR [MoU] signed at European level on 25 June 2018) suggest that restrictions and safeguards should be introduced henceforth to overcome the aforementioned legal obstacles and prevent private actors from becoming accepted judges of the infringing nature of websites.

*[38] www.white-bullet.com/white-bullet-q3-report-why-are-ad-companies-with-ip-compliance-commitments-still-funding-digital-piracy- and-counterfeiting*

The obligations of the online advertising operators who signed the memorandum depend on their differing degrees of involvement.

Firstly, the signatories undertake to implement measures to cut off the flow of funds to services that have been found by a court (or a public authority with similar powers) to infringe intellectual property rights on a commercial scale, and that do not have any substantial lawful purpose.

In a related and complementary manner, the signatories may be required to take additional action against some services if they have sufficient evidence that these services infringe (or could potentially infringe) intellectual property rights on a commercial scale, and that they do not have any substantial lawful purpose.

**Denmark** has adopted a Memorandum of Understanding (MoU) that places the legal limitations regarding the qualification of infringing sites at the very heart of its strategy, following the precautions raised by the European Commission in this respect. Thus, the list includes sites that have been identified as unlawful by third parties that are independent of the signatories of the MoU - such as a court of law, or national or international public interest bodies or third parties that are able to provide sufficient evidence or guarantees.

**In Japan** in February 2018, nine rightholders' associations and three advertising networks established - with the support of the Japanese government - a non-public list of infringing websites to dry up part of their income. There are several alternative criteria for adding a site to the list: the site must have received more than 50 takedown notices or offered more than 50 unlawful content items or links over a period of three months; it does not provide any tools or information to rightholders that could enable them to issue takedown notices, or it responds to less than 70% of takedown notices from rightholders.

### APPROCHES REQUIRING PUBLIC INTERVENTION

Public intervention is provided for in some countries to more effectively guarantee the reliability and control of sites subject to measures to cut off their income stream, and to better assess the impact and effectiveness of such measures.

However, under these arrangements, the measures to cut off the flow of funds are part of a much broader global system that confers greater powers on public authorities to implement administrative blocking measures against websites (Spain), or on the police in the event of criminal proceedings (United Kingdom).

**In the United Kingdom**, in support of reports by rightholders of massively infringing sites, PIPCU (a specialised unit of the City of London Police) maintains a list of infringing sites likely to face criminal prosecution (the *"*Infringing Website List*"*). The list is available on an automated interface, accessible to nearly 300 voluntary partners in the scheme. PIPCU also monitors the infringing site to trace the chain of advertisers involved in ad delivery on the site. It informs any non-partner advertisers that, in the course of investigations aiming to shut down the site, they may be regarded by the court as accomplices in the infringement of intellectual property law. The police therefore makes the list of contentious websites available to any online advertisers wishing to take voluntary steps to offset their risk of liability.

**In Spain**, the law imposes a similar but mandatory system on advertisers. The *Sinde* Commission - a public body responsible for blocking infringing websites - can identify an infringing site's payment and advertising partners and instruct them to stop working with it. If the partners fail to cooperate, the Commission may fine them up to €300,000.

This approach should not be confused with the "Name and Shame" procedures implemented for example by the USTR in the United States, which consist in publishing lists of not-so-ethical organisations for the purpose of shaming them for their failure to comply with intellectual property rights (including industrial, literary and artistic property rights).

Likewise, in countries that implement administrative blocking measures (such as Italy and Portugal), lists are not published for the purpose of cutting off the sites' income streams, since they are blocked anyway.

## SEARCH ENGINES

Under US law, the liability of search engines is mitigated by "safe harbour" provisions based on the "notice and takedown" principle.

In Europe, Directive 2000/31/EC of 8 June 2000, referred to as the "e-commerce" directive, does not specifically address the role of search engines. When the directive was adopted, search engines were not as sophisticated as they are now.[39] At present the European Commission, in its communications, places search engines in the same category as actors more generically known as content hosting "platforms".

To enable rightholders to report links to infringing content, search engines implement automated "takedown notice" mechanisms. Google, for example, publishes a "Transparency Report"[40] that is updated in real time and shows the number of takedown notices it has received from rightholders, the names of the requesting parties, and the websites concerned.

**The vast majority of countries studied** mention the role that search engines play in piracy prevention, firstly by delisting or demoting illegal offer, and secondly by make legal offer more visible in search results.

### DELISTING INFRINGING SITES

When a website is delisted, the search engine deletes it completely from the search index and therefore from the results. This differs from demotion, where the site is not removed from the search index but is moved to a lower rank in the search results (along with all its pages).

Unless required to do so by a public or judicial authority or by specific legislation, search engines do not implement an internal policy of delisting websites, for reasons of impartiality with regard to content, pluralism, freedom of expression, freedom of enterprise and free competition.

**In Australia**, the Copyright Amendment (Online Infringement) Bill adopted in November 2018 allows rightholders to have a site delisted or demoted. It will also be possible in the future for rightholders to have these measures updated without going back to court, under agreements between the stakeholders.

**In Russia**, parliament recently adopted a law stipulating that search engines are liable to a fine if they provide links to blocked sites and services listed by the local regulator, or to anonymisation services such as VPNs.

However, few countries - with the exception of France, Australia, Russia and Spain - seem to adopt legislation providing a legal framework for the delisting of infringing websites by search engines.

Blocking measures are generally accompanied by an on-screen information and awareness message for visitors to the blocked site.

*[39] Article 21 of the directive (re-examination) stipulated that, every two years, the Commission would draw up a report on the application and adaptation of the directive, particularly with respect to the liability of search engines. Such a report was submitted to the European Parliament on 21 November 2003. It stated that "Whilst it was not considered necessary to cover [...] search engines in the Directive, the Commission has encouraged Member States to further develop legal security for internet intermediaries". The report also mentioned that the Commission would continue to "examine any future need to adapt the present framework in the light of these developments, for instance the need of additional limitations on liability for [...] search engines".*
*[40] www.google.com/transparencyreport/removals/copyright/?hl=fr*

Now, many end- users (approximately 50%) access these messages via a search engine that has directed them to the blocked site. If all the links to a blocked site are delisted, end-users no longer see these educational messages about the blocking measure, which is something that foreign rightholders do not want.

It is widely considered abroad that the most effective way of working with search engines is through self-regulation mechanisms.

### DELISTING LINKS TO INFRINGING WORKS AND DEMOTING ILLEGAL SITES

Copyrightholders seem to have relatively little difficulty in having links to infringing works delisted. However, this type of action taken in isolation has no effect on the indexing of the site itself or on its position in the end- user's search results.

It also means that rightholders must request that a work be de-indexed link by link, and therefore that a website with thousands of pages be taken down page by page. Such procedures are long and costly. Involving search engines is a challenge, not only because of issues regarding the transparency of their operating methods, but also because it is difficult for rightholders to have an illegal site demoted without having to individually report a huge number of links to illegal works on the said site.

Voluntary agreements between rightholders and search engines appear to make it easier for the latter to demote illegal sites upon notification by rightholders. However, these agreements do have limitations, particularly if the domain name or sub-domain name is changed, as it then takes a while for the new site to be demoted.

In the report “How Google fights piracy”[41], Google explains that it has been using a “demotion signal” for several years to make takedown notices from rightholders more effective. The demotion signal establishes a correlation between the takedown notices filed against a website and its ranking in the search results. In the context of local discussions, Google has recently improved the effectiveness of the tool.

One of the issues identified is the difference in the number of notifications submitted per sector. The music sector is quite active (because it can, for example, submit a takedown notice for each individual song on an album), whereas rightholders in the audiovisual and publishing sectors request the takedown of just one film or book. Google has indicated that it now gives greater priority to takedown notices concerning, for example, audiovisual works that have not yet been released or are still showing in cinemas.

**In the United Kingdom**, search engines at this stage are focusing primarily on demoting infringing content in UK search results. In February 2017, an agreement was reached between search engines[42] and rightholders[43], under the aegis of the government. This agreement is a legally non-binding code of conduct. Its purpose is to oblige Google and other leading search engines (Bing, Yahoo, etc.) to comply with rules leading to the demotion or downgrading of massively infringing websites in their search results (and thus remove such sites from the first few pages of results). It seeks to optimise both the results of neutral keyword searches carried out by consumers who are not specifically looking for illegal offer, as well as top-ranked search results (the most relevant in terms of generating traffic to websites). Within the framework of this agreement, discussions took place on the need to prioritise takedown notices and on ways to improve the effectiveness of demotion measures in connection with takedown notices.

**In the United States**, the administration is supporting the development of best practices with a view to finding appropriate solutions to demote massively infringing websites in search engine results. Google is now implementing a tool to prioritise takedown notices, just like in the United Kingdom.

*[41] www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=2ahUKEwjV8rast53fAhUQyRoKHSBwCDsQFjA-BegQICBAC&url=https%3A%2F%2Fblog.google%2Fdocuments%2F27%2FHow_Google_Fights_Piracy_2018.pdf&us-g=AOvVaw1eiX8Dt-YTqOZnVjMn7JQ7*

Another limitation is that this type of measure must, in any event, be accompanied by an improvement in the ranking of legal content. Thus, in the United Kingdom, as a counterpart to the commitments made by search engines, rightholders must ensure that legal content is ranked higher in search results by optimising their Search Engine Optimisation strategy.

### TO MAKE LEGAL OFFER MORE VISIBLE

To make legal offer more visible or presenting legal offer in a separate section has long been ruled out by the search engines themselves, mostly for reasons of impartiality and free competition.

However, two types of initiative can be taken to promote legal offer, which would most likely be acceptable to the search engines:

- improving the coordination of "search" features with "autocomplete" features, in such a way as to prevent suggestions that direct consumers to illegal sites;
- more specifically for Google, developing "watch and listen" features to highlight legal offer within the framework of commercial partnerships. National partnerships can be established with legal platforms, for example in France (music content only), the UK and Australia. The purpose of these commercial agreements is to provide clickable tabs bearing the logos of legal platforms either next to or in front of search engine results, where the end- user has performed a neutral search containing only the author or name of the work and keywords such as "watch" or "listen".

**In the Netherlands** in February 2017, the film industry - after creating a portal with links to legal online offer- launched a search engine that directs end-users looking for a specific audiovisual work to legal offer. This search engine is unique in that it also targets end- users looking to access the work illegally. The description of each work includes keywords such as "torrents or "illegal download", so that end- users who enter these words can be redirected to legal offer. Furthermore, the description of each audiovisual work contains a message to deter end- users from accessing infringing content, for example "Do not download illegal content. Look for legal offer, it's safe and fast too".

# CONCLUSION

The effectiveness of measures to tackle online piracy seems to depend on at least **four key factors.**

## TERRITORIALITY

Piracy is a global challenge characterised by a pervasive and borderless ecosystem: site administrators are often based abroad and take advantage of more lenient legislation to carry out their activities unchecked and unpunished. The aim is therefore to take coordinated and concerted action at the international level to deliver consistent solutions and effective prevention strategies.

## PROPORTIONALITY

The Internet substantially reinforces the exercise of individual freedoms, such as freedom of expression and communication, freedom of trade and industry, and freedom of enterprise. To protect these public freedoms, public authorities must exercise caution in establishing coercive standards, or privacy and personal data protection procedures that are too intrusive considering the objectives pursued. However, a certain degree of public intervention is necessary, not only to prevent offences arising from the dissemination of illegal content, but also to avoid a situation in which the only existing rules are those imposed by cross-border organisations in the private sector.

## ADAPTABILITY

While measures against peer-to-peer file sharing have traditionally been the primary means of combating the piracy of online cultural content, piracy strategies have diversified and both rightholders and public authorities are endeavouring to find new tools to tackle massively infringing sites. There is an international consensus on the need to combine various approaches to effectively tackle piracy, for example appropriate rules and procedures, flexible legal or self-regulation mechanisms, extra-judicial public mechanisms, public communication instruments and targeted actions.

The use of such a broad variety of solutions provides an adequate response to the challenges arising specifically from the development of digital technology, characterised by continuous technological innovation and very rapid changes in consumer usage. The question is, to what extent can such solutions be adapted to changing usages, bearing in mind that the risk of legislative obsolescence is very high in the digital matter. It is essential to monitor usages - particularly emerging uses - constantly, to anticipate possible changes and plan potential solutions in advance.

These actions must be tempered by a great deal of humility regarding our ability to predict future trends. It is vital to ensure that the measures envisaged are technically feasible, and that they are robust enough to withstand the risk of circumvention. Some consideration could be given to developing tools to adapt solutions to changing usages, rather than developing tools to address projected usages.

## ACCEPTABILITY AND SOCIAL COHESION

The role that the Internet plays in the exercise of public freedoms makes it very tricky to decide which public policies are applicable to it, and may even make some of those policies unworkable. However, we must all get involved in the fight against illegal content if we are to continue to take full advantage of the economic, social and societal opportunities offered by the Internet. We must therefore take a multi-pronged approach involving all the stakeholders and using all the tools at our disposal.

Actors in both the public and private sectors are aware of the challenges and are therefore seeking pragmatic and practical solutions compatible with the protective nature of hosting providers. It is important to consider not only the effectiveness of these solutions but also who will finance them, as their sustainability will of course depend on their financial viability.

APPENDIX 1

# COUNTRY FACT SHEETS

# GERMANY

## KEY FIGURES

KNOWN BLOCKING PROCEDURES (SINCE 2006)

**2** NUMBER OF PROCEDURES

**3** NUMBER OF SITES BLOCKED

**13** NUMBER OF DOMAIN NAMES BLOCKED

DEMOGRAPHY

**82.1** POPULATION (2017) [1] *in millions*

**84.4%** INTERNET PENETRATION RATE (2017) [2]

INFRINGEMENTS [3]

**6.5** NUMBER OF VISITS TO ILLEGAL SERVICES (2017) *in billions*

**93** NUMBER OF VISITS TO ILLEGAL SERVICES PER END-USER (2017)

**Breakdown of infringements by access method (2017)** *as a %*


STREAMING

DIRECT DOWNLOAD

PEER-TO-PEER

Germany has a formal notice system aimed specifically at end-users who share works illegally on peer-to-peer networks.

In addition, Germany has gradually committed itself to tackling infringing services.

## EDUCATIONAL AND ENFORCEMENT ACTIONS

### CRIMINAL LAW PROVISIONS

The *Gesellschaft zur Verfolgung von Urheberrechtsverletzungen* e.V. (GVU) is an association of rightholders from various sectors (cinema, television - including some sports channels - video games, collective management and publishing); it is tasked with undertaking criminal proceedings on behalf of its members, with a view to shutting down sites aimed specifically at the German public.

The association focuses its efforts on illegal sites operating on German (or European) territory. Thus, besides having the sites shut down, the GVU hopes – through media coverage of its actions – to unnerve the people behind them, by making it clear that they are not exempt from punishment and that they face heavy sentences.

*1 United Nations Population Fund (UNFPA) - 2017 www.unfpa.org/data/world-population-dashboard*
*2 International Telecommunciations Union (ITU) - 2017 www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx*
*3 MUSO - 2017.*

## INDEMNIFICATION NOTICES

Germany has developed an indemnities-based approach to online piracy, centred on the amicable resolution of civil law disputes between end-users and rightholders. Rightholders may take civil action against end-users identified as having committed online negligence. As an alternative (and prior) to litigation, rightholders suggest to end-users that they settle their dispute through recourse to an amicable dispute resolution procedure.

However, the number of formal notices served is still relatively low compared to the magnitude of piracy. The German press has reported that approximately 109,000 letters are sent per year, and a total of €90.3 million are collected through amicable settlements. Claims for a work such as a film amount to approximately €700 (including all costs).

The risk of substantial fines under this system seems nevertheless to be rather dissuasive considering the low occurrence of peer-to-peer file sharing in Germany.

However, identifying and contacting end-users involves numerous steps and relatively high procedural costs for German rightholders.

- Under the peer-to-peer network monitoring system, German rightholders instruct specialist companies to collect the IP addresses of end-users who make works available on peer-to-peer networks.
- In accordance with personal data protection legislation, Internet service providers must petition the court to identify offending end-users via their IP address. The legal fees for obtaining such identification are set by the court itself and, on average, amount to €200 per request or per work. In addition to these fees, rightholders must pay the Internet service providers €35 for every ten IP addresses submitted for identification.
- Specialised lawyers then draft letters of formal notice and send them to the end-users identified, requesting that they pay a fine to avoid prosecution.
- If the end-user does not agree to an amicable settlement, it is up to the rights holder to bring legal proceedings against him or her. Therefore, it is random whether the sum specified in the letter of formal notice will be paid. In 2013, according to the German press, only 15% of end-users who received such letters actually settled the amount due. Lastly, according to data, only a few hundred lawsuits are filed each year against end-users who fail to comply with a letter of formal notice.

### THE CONTENT OF FORMAL NOTICES IS GOVERNED BY LAW

Such procedures are governed by law to provide stronger guarantees.

From a formal standpoint, the letter of formal notice must contain, under penalty of nullity[4]: the name of the rights holder, the nature of the right infringed, details of the amounts being claimed (distinguishing the various fees and damages), and the commitments that the rights holder expects from the end-user (for example to cease sharing the work specified in the letter).

From a financial perspective, the formal notice system governs the amount of money that can be claimed from end-users.

- The amount of damages that can be claimed is subject to a principle of proportionality, which courts apply according to the works in question (for example, Germany's Federal Court has, in the past, awarded €200 for a music album).
- The amount of procedural costs and lawyer's fees that can be charged to the end-user is capped by law at €500.

*[4]* Article 97a (2) of the German Copyright and Related Rights Act, as amended by the Law of 1 October 2013.

## ESTABLISHED CASE LAW SPECIFIES THE SCOPE OF THIS SYSTEM AND POSSIBLE GROUNDS FOR EXEMPTING END-USEREND-USERS FROM LIABILITY

One question raised by this system is whether Internet subscribers should be held responsible where it appears that they did not commit the unlawful acts themselves.

According to the case law of the Federal Court of Justice, the owner of the Internet connection is presumed to have committed the infringement reported by the rightholders [5]. However, it would appear that German case law does not require subscribers to exercise a duty of care regarding the security of their Internet connection or its use by third parties.

Thus, German courts may rule out the subscriber's liability if he or she is able to prove that someone else was using the Internet connection when the said offence was committed. In the event that the Internet connection was knowingly made available to third parties at the time of the offence, the owner of the connection must - to exonerate themselves of responsibility - identify the persons who had independent access to their Internet connection and are therefore likely to have committed the alleged copyright infringement.

A specific problem arose in Germany when the owner of an Internet connection was asked to identify a member of his own family likely to have committed the offence.

Considering that the Internet connection was used unlawfully by the subscriber's minor child, the Federal Court ruled that subscribers should be held responsible for the offence if they know which of their children has shared copyrighted works illegally, but should not be required to identify that child.[6]

However, parents may be exonerated if they can prove that they have taken steps to secure their Internet connection and educate their children in this regard [7]. Conversely, one court held a father liable for the actions of his minor child, as he had not adequately educated his child about sharing works illegally online [8].

Regarding the unlawful use of an Internet connection by adult members of a subscriber's household, the German Federal Court ruled that the subscriber was not required to provide further details on the offender, considering Article 7 of the Charter of Fundamental Rights of the European Union on respect for private and family life, and the respective provisions of German constitutional law.

The subscriber may be exonerated from responsibility after establishing that he or she could not have committed the infringement, without having to identify and report the household member responsible. The subscriber could not be required to monitor the activities of other household members to obtain this information [9].

The CJEU, having been asked for a preliminary ruling[10], stated on 18 October 2018[11] that German legislation, as interpreted by the German Federal Court, does not strike a fair balance between the fundamental rights in question, namely intellectual property rights, the right to an effective remedy, and the right to respect for one's private and family life.

The Court ruled that the case law of the Federal Court is contrary to European Union law in that it deprives rightholders of the right to an effective remedy. Consequently, subscribers must be held liable if they are unable or unwilling to exonerate themselves by proving that another adult member of the household committed the act of infringement.

*[5]Federal Court of Justice, 8 January 2014, I ZR 169/12.*
*[6]Federal Court of Justice, 30 March 2017, I ZR 19/16.*
*[7]Federal Court of Justice, 15 November 2012, I ZR 74/12.*
*[8]The Court of Leipzig, 30 January 2017, 104 C 7366/16.*
*[9]Federal Court of Justice, 18 May 2017, I ZR 154/15.*
*[10]Request for a preliminary ruling submitted by the Landgericht München I (Germany) on 24 March 2017 – Bastei Lübbe GmbH & Co.KG / Michael Strotzer (Case C-149/17): curia.europa.eu/juris/document/document.jsf?text=&docid=192289&pageIndex=0&doclang=FR&-mode=req&dir=&occ=first&part=1&cid=2734.*
*The German court asked the CJEU whether the fact that the "owner of an internet connection used for copyright infringements through file-sharing" may be excluded from liability "if the owner of that internet connection can name at least one family member who, besides him or her, might have had access to that internet connection, without providing further details, established through appropriate investigations, as to when and how the internet was used by that family member" is compatible with European Union law and, in particular, with the provisions relating to the necessity of implementing effective and persuasive sanctions to ensure the enforcement of intellectual property rights.*
*[11]curia.europa.eu/juris/document/document.jsf?text=&docid=206891&pageIndex=0&doclang=fr&mode=req&dir=&occ=first&part=1.*

The Court stressed that it would be a different matter if, *"for the purposes of preventing what was regarded as an unacceptable interference with family life"*, national legislation provided rightholders with *"another effective remedy, allowing them, in particular, in such a situation, to have the owner of the internet connection in question held liable in tort"*.

## THE SITUATION OF BUSINESSES OFFERING GUEST WI-FI ACCESS TO THEIR CUSTOMERS

New legislation on Wi-Fi came into force on 13 October 2017. It follows the so-called "McFadden" ruling by the CJEU on 15 September 2016[12].

In this case, the Court ruled that the "e-commerce directive"[13], which affords safe harbour protection to technical intermediaries providing access to the Internet, also applies to businesses that offer guest Wi-Fi access to their customers.

German rightholders could no longer - under ordinary law and within the framework of the compensation system - directly hold Wi-Fi access providers responsible for infringements committed by their customers on peer-to-peer networks.

However, the Court of Justice pointed out that such businesses were not exempt from all obligations and could be ordered to secure their network and to refrain, in future, from allowing third parties to infringe protected works via their Internet connection. The new German law takes this ruling into consideration, with the aim of promoting the development of Wi-Fi hotspots in Germany, which, according to the press, may have been hindered by the concerns of businesses about having to compensate rightholders and/or secure their network with a password.

The new law shelters Wi-Fi access providers from liability for acts of infringement committed by their users. It also exempts them from the obligation of securing their network by means of a password and user name. In the explanatory statement submitted to the European Commission, the government noted that such a system - with the lifting of anonymity it implies - would involve the collection of personal data, thus creating additional legal obligations and therefore costs that some businesses could not meet.

They may therefore be held liable on a subsidiary basis only, if the rights holder has previously failed in its action against the actual infringer or the hosting provider (more closely connected with the offence).

The text specifies that businesses may implement security measures on a voluntary basis, such as port filtering to prevent access to peer-to-peer networks or website blocking measures. The possibility of a blacklist system has been raised by the government (for example, a list of German websites that pose a danger to young people, which could be loaded onto the router for filtering).

## THE PROMOTION OF LEGAL OFFER

Private initiatives are being developed to make legal offer more visible. The music union has created a label (PlayFair[14]) granted to websites considered as legal. Right holders in the audiovisual sector have created a portal (*was-ist-vod.de*), which lists platforms offering legal products and services.

*[12] CJEU, 15 September 2016, C-484/14 Tobias McFadden v Sony Music Entertainment Germany GmbH.*
*[13] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, and in particular electronic commerce, in the internal market.*
*[14]www.playfair.org/startseite/*

# ANTI-COUNTERFEITING ACTIONS INVOLVING INTERMEDIARIES

## INJUNCTIVE PROCEEDINGS

### THE LIMITATIONS ARISING FROM THE PRINCIPLE OF SUBSIDIARITY

German rightholders still file lawsuits directly against websites (and their founders), because of their liability. In the area of copyright protection (unlike child pornography prevention for example), German law does not provide for simplified procedures that involve intermediaries irrespective of their liability, or that can be implemented without first exhausting all other remedies. Therefore, Internet service providers rarely receive website blocking requests, as such requests are very difficult to implement according to German legal tradition.

On 1 February 2018, the Munich Regional Court ordered an Internet service provider (Vodafone) to block access to a streaming site as part of a legal action by a rights holder in the music industry (a producer), who complained that a recent and hugely successful work was available via the kino.to galaxy of websites. The rights holder reported that he had not been able to contact the website operator. One of the alleged operators of the service has already been arrested and is being detained in Kosovo[15]; however, the service has continued to operate since the arrest.

### ACTIONS AGAINST HOSTING PROVIDERS

In the music industry, lawsuits against hosting providers enable rightholders to obtain so-called “stay down” orders for individual works or even whole catalogues of work, as well as targeted monitoring measures such as using keyword filtering and controlling the number of links to hosted content[16].

In June 2018, in a procedure initiated by GEMA (the German equivalent of SACEM), the Court of Hamburg ruled that a newsgroups host could be held liable for offences committed by its users[17].

The GVU has set up a platform for centralising takedown notices in the audiovisual sector, which can be used by parties other than GVU members and is backed by the public authorities. This tool should also enable:

- the identification of uncooperative sites that fail to remove content;
- the collection of data on connections between links sites and content sites, which often form “galaxies” with identical operators.

## ACTIONS AGAINST STREAM RIPPING SITES

Sony Music has referred MusicMonster.fm to the Munich Regional Court.

MusicMonster.fm enabled its users to create lists of songs they would like to have copied. It then scanned online radio stations and, when it found one of the songs chosen by a user, it copied it and invited the user to download it in MP3 format. MusicMonster.fm claimed that its actions were legitimate, arguing that its users were not liable to pay royalties as the radio stations had paid their licence fees and therefore the private copying exception applied.

In September 2017, the Court ruled that the stream ripping service could not invoke the private copying exception. On 22 November 2018, the Higher Regional Court of Munich confirmed the first instance decision.

*[15] Munich Regional Court, 1 February 2018, cdn.netzpolitik.org/wp-upload/2018/03/7_O_17752_17-edit.pdf*
*[16] Ruling of 12/07/2012 (Alone in the Dark) and 15/08/2013 (Rapidshare file hosting service).*
*[17] Court of Hamburg, 22 June 2018.*

## ACTIONS TARGETING SOCIAL NETWORKS

In 2015, Germany set up a working group with the main social networks to tackle hateful content more effectively. Considering that the outcome of this voluntary approach was unsatisfactory, in 2017 Germany adopted the Network Enforcement Act (or *NetzDG*) to tackle online hate, racism, violence, terrorism, child pornography and fake news, which came into force on 1 January 2018.

While it does not create a third status, the Act places substantial obligations on social networks with more than two million users. The latter are required to remove clearly illegal content within 24 hours of notification, or within seven days in more complex cases. Should they fail to comply with their obligations, they face a fine of up to €50 million.

Initial assessments of the Act seem to be positive:

- its compatibility with European law no longer seems to be a matter of debate;
- social networks appear to be actively involved in the initiative and no penalties have been imposed;
- the establishment of a contact point has strengthened social dialogue between search engines and public authorities;
- there does not seem to be any risk of Internet censorship.

## ACTIONS TARGETING ONLINE PAYMENT OPERATORS

German rightholders have initiated proceedings against online payment operators with a view to identifying and prosecuting counterfeiters. On 22 March 2017, the Court of Hamburg[18] ruled that online payment operator PayPal must disclose the identity of (i) the administrators of illegal websites financed through PayPal transactions and (ii) the customers of illegal websites who purchase items protected by intellectual property rights, and the administrators of these sites.

In 2016, a German court also ordered PayPal to disclose the identity of an account holder who was selling counterfeit products online[19].

*[18] Court of Hamburg, 22 June 2018.*
*[19] Court of Hamburg, 11 July 2016.*

# AUSTRALIA

## KEY FIGURES

KNOWN BLOCKING PROCEDURES (SINCE 2006)

**2** NUMBER OF PROCEDURES

**79** NUMBER OF SITES BLOCKED

**322** NUMBER OF DOMAIN NAMES BLOCKED

DEMOGRAPHY

**24.5** POPULATION (2017) [1]
*in millions*

**86.5%** INTERNET PENETRATION RATE (2017) [2]

INFRINGEMENTS [3]

**2.6** NUMBER OF VISITS TO ILLEGAL SERVICES (2017)
*in billions*

**122** NUMBER OF VISITS TO ILLEGAL SERVICES PER END-USER (2017)

**Breakdown of infringements by access method (2017)**
*as a %*


**Australia considered implementing measures against end-users and then abandoned the idea. In 2015, however, Australia adopted a law allowing the blocking of massively infringing sites located abroad. An additional law was adopted in November 2018 to allow the blocking of local sites and the implementation of delisting and demotion measures, and to facilitate the blocking and delisting of services circumventing blocking orders, within the framework of agreements referred to in the court order.**

**According to a study published by the Australian Government Department of Communications in July 2015[4], 12% of online content consumers consume all their content illegally, whereas 31% consume a mix of legal and illegal content. Overall, while 43% consume at least some illegal content, 57% of digital cultural content consumers consume all their content legally.**

**According to a study by Kantar Public, published by the Australian government in 2017[5], rates of unlawful consumption of cultural goods remained steady between 2016 and 2017.**

**According to a study published by INCOPRO[6] in February 2018:**

- **traffic to blocked sites has dropped by 53.4% since blocking measures were introduced in 2017;**
- **usage of the top 50 infringing sites has fallen by 35.1% since October 2016, following two blocking injunctions in August 2017. It should be noted that the study does not consider VPN usage.**

*[1] United Nations Population Fund (UNFPA) – 2017.*
*[2] International Telecommunications Union (ITU) – 2017.*
*[3] MUSO - 2017.*
*[4] Online Copyright infringement Research, July 2015, prepared by TNS for the Department of Communications: www.communicationsgov.au/sites/g/files/net301/f/DeptComms%20Online%20Copyright%20Infringement%20Report%20FINAL%20.pdf*
*[5] Consumer Survey on Online Copyright Infringement 2017, A marketing research report, June 2017, Prepared for: Department of Communications and the Arts, Kantar public: www.communications.gov.au/departmental-news/new-online-copyright-infringement-research-released-2017*
*[6] "Site blocking efficacy-Key findings Australia", February 2018, INCOPRO, www.creativecontentaustralia.org.au/research/2018*

# EDUCATIONAL AND ENFORCEMENT ACTIONS

## FAILURE TO IMPLEMENT A GRADUATED WARNING SYSTEM

In 2014, the Australian government encouraged and promoted the creation of a self-regulatory mechanism between Internet service providers and rightholders, giving them six months to set up a graduated warning system. The project did not go ahead, as rightholders and Internet service providers failed to reach an agreement on costs and their distribution.

## FAILURE TO IMPLEMENT A COMPENSATION SYSTEM

2016 saw the end of a very high-profile case in Australia, during which permission was sought to issue compensation formal notices to end-users who had shared the film "Dallas Buyers Club" on peer-to-peer networks. The proceedings were initiated by a rights holder, with the aim of compelling five Internet service providers to identify the owners of 4,700 IP addresses.

The Australian court ruling clarified the boundaries of this type of action, indicating that the identities of the end-users could be disclosed to the rights holder on the proviso that the latter did not demand unreasonable amounts of money from the end-users.

## CRIMINAL PROCEEDINGS

In late 2017, the Coalition Against Piracy (CAP) - an association of video content creators and distributors in Asia[7] - and the Alliance for Creativity and Entertainment (ACE) [8] took part in a successful operation in Australia to shut down a company that was selling pre-loaded set-top boxes enabling unlawful access to on-demand content. The boxes were sold with a one-year subscription to a package of TV channels broadcast without authorisation[9].

Other such actions include an injunction obtained in April 2018 by rightholders in the audiovisual sector, against a service offering a range of pirated television channels.

## PUBLIC AWARENESS CAMPAIGNS

A campaign designed to promote legal offer and educate the public on copyright has been organised by rightholders in the audiovisual sector, who have set up an organisation called Creative Content Australia[10]. A dedicated website provides education resources for teachers and students, a link to a directory of legitimate content per sector[11], research reports and answers to frequently asked questions on piracy and cultural content.

Following a decision to block infringing sites, Creative Content Australia launched a new communication campaign on 18 August 2017 called "Price of piracy", the aim being to alert consumers to the presence of malware on illegal streaming sites and peer-to-peer networks. A dedicated website[12] has been created: it includes explanatory videos on the dangers of streaming or downloading illegal content, as well as advertising spots featuring a famous Australian actor and warning consumers about the consequences of consuming content illegally.

In 2018, the same organisation launched another communication campaign called "Say No to Piracy", which celebrates creation and innovation and highlights the importance of consuming online content legally to protect the screen industries.

*[7] beIN Sports, casbaa, The Walt Disney Company, Fox Networks Group, HBO Asia, NBCUniversal, Premier League, Turner Asia-Pacific, A&E Networks, Astro, BBC Worldwide, CANAL+, Cignal, Media Partners Asia, National Basketball Association, PCCW Media, Singtel, Sony Pictures Television Networks Asia, TVB, True Visions, TV5MONDE et Viacom International Media Networks.*
*[8] Amazon, AMC Networks, BBC Worldwide, BellMedia, Canal + groupe, CBS corporation, Constantin Film, Foxtel, Grupo Globo, HBO, hulu, lionsgate, MGM, Millenium Media, NBCUniversal, Netflix, Paramount, SFStudios, Sky, SonyPictures, Star, StuidoBabelsberg, STXentertainment, Telemundo, Televisia, 20thCenturyFox, Univision Communication Inc, Village Roadshow, Disney, Wb, alliance4creativity.com/*
*[9] www.casbaa.com/news/casbaa-news/alliance-for-creativity-and-entertainment-ace-and-casbaas-coalition-against-piracy-cap-close-down-australian-illicit-streaming-device-operation/*
*[10] www.creativecontentaustralia.org.au*
*[11] www.digitalcontentguide.com.au*
*[12] thepriceofpiracy.org.au/*

# ANTI-COUNTERFEITING ACTIONS INVOLVING INTERMEDIARIES

## JUDICIAL BLOCKING PROCEDURES

The Copyright Amendment (Online Infringement) Act 2015[13], which came into force in June 2015, allows rightholders to seek an injunction ordering Internet service providers to block foreign-based services whose primary purpose is to infringe or enable the infringement of copyright. The law stipulates that the rights holder must contact all the services concerned to notify them of the procedure.

On these grounds, in February and April 2016, rightholders in the audiovisual sector summoned Internet service providers before a federal court to have several websites (including KickassTorrents) and their proxies blocked. In December 2016, the first ruling on the matter[14] stated that the costs of the blocking measures (50 Australian dollars or approximately 35 euros per domain name) must be borne by the rightholders. End-users seeking access to the blocked sites will land on a message explaining that the site has been blocked by judicial decision. On this occasion, Village Roadshow, the audiovisual rights holder behind the blocking procedures, launched a communication campaign in various media on the risks such sites present for users, stressing in particular that they contain a lot of viruses.

Four blocking decisions have been made since then, three in 2017 and one in 2018[15]: three were requested by rightholders in the audiovisual sector and the other by rightholders in the music industry[16]. Over 500 websites were blocked as a result. In April 2018, a galaxy of services illegally offering live pay-TV and on-demand content via an application was also blocked.[17].

In 2018, to reduce procedural costs, pay-TV operator Foxtel asked the court not to call in experts during the trial and to replace the live demonstration of the website's illegality by videos and screenshots. The court agreed to these requests.

The court leaves the choice of the blocking measure to the Internet service providers, specifying that both DNS blocking and IP blocking are acceptable.

## THE NEW LAW ADOPTED IN NOVEMBER 2018[18]

The Copyright Amendment (Online Infringement) Bill 2018 was adopted at the end of November 2018.

- It lessens the burden of proof on rightholders by introducing a rebuttable presumption that the website in question is located abroad.
- It makes it possible to block sites that have the substantive effect of infringing copyright.
- It allows rightholders to have websites delisted or demoted.
- It also enables them to obtain injunctions to block and delist services circumventing blocking orders without having to go back to court, pursuant to agreements between the parties.

From February to March 2018, the Australian government ran a consultation[19] called “Review of the Copyright Online Infringement Amendment” to gather stakeholders’ opinions on the efficiency and effectiveness of the mechanism introduced in 2015, its implementation and any necessary amendments.

Village Roadshow[20] and Foxtel[21] responded by asking the government to amend the law to allow them to bring legal action against

*[13] www.legislation.gov. au/Details/C2015A00080*
*[14] www.judgments.fedcourt.gov.au/judgments/Judgments/fca/single/2016/2016fca1503*
*[15] www.judgments.fedcourt.gov.au/judgments/Judgments/fca/single/2018/2018fca0933*
*[16] www.judgments.fedcourt.gov.au/judgments/Judgments/fca/single/2017/2017fca0435*
*[17] www.judgments.fedcourt.gov.au/judgments/Judgments/fca/single/2018/2018fca0582*
*[18] parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;page=0;query=BillId:r6209%20Recstruct:billhome*
*[19] www.communications.gov.au/have-your-say/review-copyright-online-infringement-amendment*
*[20] “Review of the Copyright Online Infringement Amendment”, Village Roadshow, 15 March 2018.*
*[21] “Review of the Copyright Online Infringement Amendment", Foxtel, 21 March 2018.*

all intermediaries, including Internet service providers and search engines. Foxtel cited a study conducted by the Australian Department of Communications and the Arts, according to which 20% of adults and 50% of illegal users use search engines to find illegal content[22].

In addition, Foxtel requested that the definition of blockable services be amended to include not only websites whose primary purpose is to infringe or enable the infringement of copyright, but also websites that aim to or have the substantive effect of infringing copyright. Foxtel believed that, as a result, file hosting services that host infringing works could also be blocked.

Music Rights Australia stated in their response how important it is to standardise the page end-users see if they attempt to visit a blocked site, as most of the (very many) Internet service providers in Australia use pages they have developed themselves, rather than that created by rightholders.

Music Rights Australia is also concerned about the cost of judicial blocking orders for rightholders: the case law sets that cost at 50 Australian dollars per domain name and per Internet service provider. However, while this seems relatively low, it can quickly become prohibitive insofar as one illegal site can have hundreds of associated websites designed to circumvent blocking orders and there are approximately one hundred Internet service providers in Australia. Lastly, Music Rights Australia pointed out that 27 countries worldwide have issued blocking orders against 2,800 URLs and, in most cases, Internet service providers have not requested compensation for implementing them.

## THE IMPLEMENTATION OF THE "FOLLOW THE MONEY" APPROACH

Since October 2013, in accordance with the Follow the money" approach, Music Rights Australia has been working with an association of stakeholders of the adversiting industry, the Audited Media Association of Australia, to raise their awareness about ad funding of infringing websites, and the harm caused by these sites.

The purpose of this initiative is to disseminate and enforce a code of good conduct to reduce advertising on such sites. Although agreement has been reached and the code of conduct has already been drawn up, some stakeholders are still reluctant to implement it.

## PLATFORM LIABILITY

Australia operates a safe harbour scheme for technical intermediaries but, unlike in other countries, it applies only to Internet service providers and not to other intermediaries such as hosting providers.

Proposals to extend the scheme to hosting providers have been on the table for years.

Then, in April 2017, the government consulted with stakeholders to decide whether or not the scheme should be changed. Rightholders opposed any reform on the grounds of the difficulties encountered by their European and American counterparts in having infringing content removed from hosting platforms. Ultimately, the government has decided not to extend the scheme to hosting platforms for the time being[23].

*[22] Sycamore, Project Harrison: Australian Piracy Behaviours and Attitudes 2017 Wave, page 26, www.creativecontentaustralia.org.au/ research/2018*
*[23] www.legislation.gov.au/Details/C2018A00071*

# BELGIUM

## KEY FIGURES

KNOWN BLOCKING PROCEDURES (SINCE 2006)

**5** NUMBER OF PROCEDURES

**63** NUMBER OF SITES BLOCKED

**564** NUMBER OF DOMAIN NAMES BLOCKED

DEMOGRAPHY

**11.4** POPULATION (2017) [1] *in millions*

**87.7%** INTERNET PENETRATION RATE (2017) [2]

INFRINGEMENTS [3]

**1.3** NUMBER OF VISITS TO ILLEGAL SERVICES (2017) *in billions*

**129** NUMBER OF VISITS TO ILLEGAL SERVICES PER END-USER (2017)

**Breakdown of infringements by access method (2017)** *as a %*


**The system in Belgium combines actions to change the behaviour of end-userend-users with actions against infringing services.**

## EDUCATIONAL AND ENFORCEMENT ACTIONS

Belgium focuses mainly on promoting and raising awareness of legal offer.

To direct end-users to legal offer, the Belgian Entertainment Association (BEA) has created a website that lists legally available films, series, music, books and video games[4].

The BEA launched an awareness campaign in January 2018 to inform end-users of the consequences of illegal downloading.

Subtitles likely to be downloaded by end-users are accompanied by messages such as “do not download illegally”. End-users who download subtitles to go with pirated works may find, for example, Samuel L. Jackson in “The Hitman's Bodyguard” saying “I don't need to do research to know these subtitles are bad” or “you wanted to be a policeman until you downloaded this”.

*[1] United Nations Population Fund (UNFPA) – 2017.*
*[2] International Telecommunications Union (ITU) – 2017.*
*[3] MUSO - 2017.*
*[4] www.onlinefairplay.info/legal-offer/*

# ANTI-COUNTERFEITING ACTIONS INVOLVING INTERMEDIARIES

In 1999, the Belgian Association of Internet Service Providers (ISPA) entered into an agreement with the federal government. This agreement notably provides for cooperation between Internet service providers and the Computer Crime Unit of the judicial police, with the aim of blocking content whose dissemination constituter a criminal offence[5].

In 2005, ISPA and IFPI (which represents the recording industry) concluded an agreement to prevent music sharing in discussion groups. Under this agreement, IFPI may ask Internet service providers to block access to discussion groups that are used to share a large amount of infringing music content or links to such content.

In 2004, the Belgian Society of Authors, Composers and Publishers (SABAM) initiated the first proceedings against an Internet service provider, to block all dissemination of infringing works, particularly via peer-to-peer networks. In 2009, it asked a social network to implement content filtering measures. Preliminary questions were referred to the CJEU during both proceedings, but the rightholders' claims - as they were worded at the time - were deemed disproportionate[6].

Finally, in 2011, Belgium issued its first ever blocking order against two Internet service providers, instructing them to put a DNS block on the Pirate Bay website and on several associated domain names[7]. Following this decision, the Belgian Anti-Piracy Federation (BAF) gave formal notice to other Internet service providers not party to the proceedings to block the sites in question to avoid the costs of legal action against them.

In the context of criminal proceedings, an investigating judge ordered all Internet service providers to block access to thepiratebay.org and to any services linked to the incriminated servers' IP addresses or to content hosted on these servers.

This decision, confirmed by the final court of appeal on 22 October 2013[8], also states that:

- the Belgian police, the Federal Computer Crime Unit (FCCU) and the Regional Computer Crime Unit (RCCU Mechelen) will tell Internet service providers which domain names to block;
- end-users seeking access to one of the domain names in question will be redirected to a public information page.

In January 2018, following a lawsuit by the BEA against the three main Internet service providers (Proximus, Telenet and Voo), the parties filed a joint motion to block around thirty illegal sites via 450 domain names. The purpose of this joint approach was, among other things, to speed up the procedure. Each party bore its own costs.

The parties informed the court that they were retaining the option of referring the matter to it again in the future, in order to have the list updated. On 30 March 2018, the court[9] ordered a DNS block on the 450 domain names and the publication of an information message for end-users.

*[5] merlin.obs.coe.int/iris/1999/7/article4.fr.html*
*[6] CJEU, C-70-/10, Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM) and others, 24 November 2011; CJEU, C-360/10, Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM) v Netlog NV, 16 February 2012.*
*[7] Antwerp Court of Appeal, 26 September 2011, Belgian Anti-Piracy Federation (BAF) v Telenet and Belgacom.*
*[8] Final court of appeal, 22 October 2013, P.13.0550.N, lex.be/en/doc/be/jurisprudence-belgique/cour-de-cassation-arret-22-octobre-2013-bejc_201310223_fr*
*[9] French-speaking Commercial Court of Brussels, Chamber of Cassation, 30 March 2018, role number A/18/00217.*

# CANADA

## KEY FIGURES

DEMOGRAPHY

**36.6** POPULATION (2017) [1] *in millions*

**91.2%** INTERNET PENETRATION RATE (2017) [2]

INFRINGEMENTS [3]

**3.7** NUMBER OF VISITS TO ILLEGAL SERVICES (2017) *in billions*

**112** NUMBER OF VISITS TO ILLEGAL SERVICES PER END-USER (2017)

**Breakdown of infringements by access method (2017)** *as a %*


**US rightholders have requested that Canada be included on the list of countries identified by the US administration in 2017 as not providing effective protection of intellectual property rights.**

**According to a 2018 survey[4], the use of BitTorrent-type peer-to-peer software has decreased sharply in recent years, from 15.1% in 2014 to 1.6% in 2017. On the other hand, 9.7% of Canadian households allegedly own a set-top box preloaded with Kodi-type software, and 70.9% of them use it for piracy purposes. Stream ripping software is also reportedly widespread[5].**

**The Canadian Parliament launched a review of the Copyright Act in December 2017, under the responsibility of the House of Commons Standing Committee on Industry, Science and Technology. In April, the Minister of Innovation, Science and Economic Development and the Minister of Canadian Heritage wrote to the Standing Committee on Industry, Science and Technology, stressing the need for measures to reduce the "value gap" between platforms.**

**Canada's 2012 Copyright Modernisation Act provides for both specific actions against end-users and anti-piracy actions involving intermediaries.**

## EDUCATIONAL AND ENFORCEMENT ACTIONS

### THE EDUCATIONAL WARNING SYSTEM AND INDEMNIFICATION NOTICES

Canada adopted a "Notice and Notice" regime under the 2012 Copyright Modernisation Act, which came into force on 2 January 2015.

*[1] United Nations Population Fund (UNFPA) – 2017.*
*[2] International Telecommunications Union (ITU) – 2017.*
*[3] MUSO - 2017.*
*[4] "Video piracy in Canada", Sandvine Global Internet Phenomena Spotlight, March 2018 www.sandvine.com/hubfs/downloads/reports/Internet-phenomena/sandvine-spotlight-video-piracy-in-canada.pdf*
*[5] musiccanada.com/wp-content/uploads/2017/11/LeCartDeValeur.pdf*

The Act provided a framework for a self-regulation system implemented by Canadian Internet service providers and audiovisual rightholders under a voluntary agreement that had been in place for about a decade. It contains the obligation for Canadian Internet service providers and hosting providers to e-mail the rights holder's warning (or "notice") to the end-user, at their own expense.

The notice must include the name and address of the plaintiff, details of the pirated work and the plaintiff's rights regarding that work, the alleged infringement, and the date and time of the infringement. However, neither the content nor the purpose of the notice have been defined in detail by the texts.

The system is designed purely to educate end-users, since it does not provide directly for sanctions. However, it has been observed that the notice and notice regime may have been misused by rightholders, particularly in the United States, who have used it to ask Internet service providers to send compensation claims to end-users.

Should the Internet service provider fail to pass on a warning, it must explain its reasons to the rights holder. Non-fulfilment of this requirement may result in a court-imposed fine ranging from 5,000 to 10,000 Canadian dollars (or 3,600 to 7,300 euros). Despite this penalty, some Internet service providers allegedly do not forward notices to counterfeiters, or they send only a limited number[6].

Furthermore, under general criminal law, rightholders may take action against end-users who share works on peer-to-peer networks, on the grounds of counterfeiting. The maximum penalty that may be imposed on end-users for non-commercial counterfeiting is a 5,000 Canadian dollars fine (approximately 3,654 euros).

In September 2018[7], Canada's Supreme Court established that rightholders should compensate Internet service providers for providing them with end-users' details so that they can take criminal action against them. The Supreme Court left it to the trial courts to determine the amount of compensation payable. It should be noted that personal data may be stored for a minimum of six months and a maximum of one year in Canada.

## THE CREATION OF A CRIMINAL OFFENCE SPECIFICALLY FOR ADMINISTRATORS OF MASSIVELY INFRINGING SERVICES

Canada's 2012 Copyright Modernisation Act introduced a penalty regime for those who allegedly enable counterfeiting. It is therefore stipulated 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"*.

The law adds that the court may consider the following factors:

- whether the person marketed the said service as one that could be used to commit acts of copyright infringement;
- whether the person had knowledge that the service was used to enable copyright infringement;
- whether the service has any other significant uses other than to enable acts of copyright infringement;
- measures taken to limit acts of copyright infringement;
- the benefits the person received as a result of enabling the acts of copyright infringement, and the economic viability of providing the service were it not used to commit acts of copyright infringement.

Since the law was introduced in 2012, those who operate massively infringing sites shall be treated in the same manner as those who engage in commercial infringement, which means harsher penalties for offenders and greater redress for rightholders.

On this basis, in October 2015, the Federal Court of Canada[8] ordered the Canadian developers of PopcornTime to disable domain names used to download the most popular version of the software. In 2015, several torrent links sites were shut down on the same grounds[9].

*[6] www.iipawebsite.com/rbc/2016/2016SPEC301CANADA.PDF*
*[7] scc-csc.lexum.com/scc-csc/scc-csc/en/item/17254/index.do*
*[8]Federal court, Ottawa, Ontario, 16 October 2015, Paramount Pictures Corporation & Ors v David Lemarier & Ors fr.scribd.com/document/288405925/Injunction*
*[9]www.iipawebsite.com/rbc/2016/2016SPEC301CANADA.PDF*

# ANTI-COUNTERFEITING ACTIONS INVOLVING INTERMEDIARIES

## THE ATTEMPTED ESTABLISHMENT OF AN ADMINISTRATIVE BLOCKING PROCEDURE

In January 2018, Internet service providers and music industry representatives belonging to an organisation called FairPlay Canada[10] petitioned the telecommunications regulator (Canadian Radio-television and Telecommunications Commission - CRTC) to set up a system for blocking infringing sites.

The following mechanism was proposed: a new independent non-profit organisation, the Internet Piracy Review Agency (IPRA) would be responsible, under the aegis of the CRTC, for creating a list of illegal sites.

Upon petition by rightholders, the IPRA would determine whether or not a website should be added to the list after hearing from the owners of the site where necessary, and basing its decision on the criteria set out by the CRTC. Internet service providers would be required to block access to sites on the list.

The sites targeted would be those that blatantly, massively or structurally infringe copyright. The Commission could quickly or automatically extend the blocking decision to sites circumventing blocking measures. The decision would be subject to a public appeal to the Commission, and to an appeal to the Federal Court of Appeal.

The IPRA would be financed by administrative fees paid by the rightholders.

The CRTC launched a consultation on the project, which was ultimately rejected on 2 October 2018. Some organisations support the project, including the Canadian branch of the Motion Picture Association, while others have been much more critical, arguing instead that blocking orders should be issued by the courts.

## THE IMPLEMENTATION OF THE "FOLLOWTHE MONEY" APPROACH

In November 2016, the Canadian Government published a report[11] examining the possibility and opportunity to implement the Follow the money approach. The analysis, based on various foreign models and reports, concludes that the Follow the money approach can help to combat commercial counterfeiting, although it cannot eradicate it on its own.

It stresses that the approach means developing criteria for qualifying sites as illegal, and that tackling these sites requires substantial resources. Therefore, it may be appropriate for the government to step in and support rightholders (as is the case in other countries).

The report also recommends that the government simultaneously step up its efforts to raise public awareness of the social and financial risks inherent in the use of massively infringing sites, since similar efforts have reportedly had a positive impact abroad. It therefore emphasises the possibility of conducting a public awareness campaign, focusing on the risks to users.

Finally, the report recommends reviewing the role played by hosting providers and various online intermediaries because they can help protect the identity of operators of massively infringing sites.

## ACTIONS AGAINST VENDORS OF PIRACY-ENABLING SET-TOP BOXES

Sales of set-top boxes fitted with software to illegally access subscription TV channels are rising. In a partial ruling in June 2016, rightholders obtained their first injunctions from the Federal Court, ordering 62 distributors to stop selling such boxes

*[10] Bell, Cineplex, Directors Guild Of Canada, Maple Leaf Sports and Entertainement, Movie Theatre Association of Canada, Regoers Media.*
*[11]"Examination of the 'follow-the-money' approach to copyright piracy reduction", Prepared by Circum Network Inc. for Canadian Heritage, April 2016.*

[12].

The injunctions were granted on the grounds that these boxes enable the unauthorised communication of copyright protected works to the public, and that the sellers are not just impartial intermediaries. On the contrary, they encourage their customers to dismiss legal means of consuming protected content[13]. These actions have prompted sellers to cease their activities voluntarily, after reaching a compromise with rightholders.

In June 2017, audiovisual rightholders referred the operator of the TV Addons website to the Federal Court, on the grounds that it sells applications to configure the Kodi software for piracy purposes. The operator was accused of infringing copyright by unlawfully communicating dozens of television programs to the public, by developing, hosting, distributing and promoting illegal add-ons.

The procedure started well for the rightholders. The various domain names and social media accounts used by TV Addons were passed on to the litigation team. In addition, a civil search warrant was granted to the plaintiffs, enabling them to enter the defendant's premises to seize and copy evidence in support of their case, before it could be destroyed or falsified. Later in the proceedings, the court ruled that the defendant was communicating works to the public itself, and that it could not legitimately claim to be a hosting provider when the website clearly targets end- -users who want to save themselves the cost of a legal subscription to a television service.

*[12] www. smart-biggar. ca/en/special_feature_print.cfm?id=31*
*[13]Bell Canada et al v. 1326030 Ontario Inc. dba ITVBox.net et al, T-759-16 (2016 FC 612), www.smart-biggar.ca/en/special_feature_printcfm?id=31*

# SOUTH KOREA

## KEY FIGURES

KNOWN BLOCKING PROCEDURES (SINCE 2006)

**15** NUMBER OF PROCEDURES

**474** NUMBER OF SITES BLOCKED

**606** NUMBER OF DOMAIN NAMES BLOCKED

DEMOGRAPHY

**51** POPULATION (2017) [1]
*in millions*

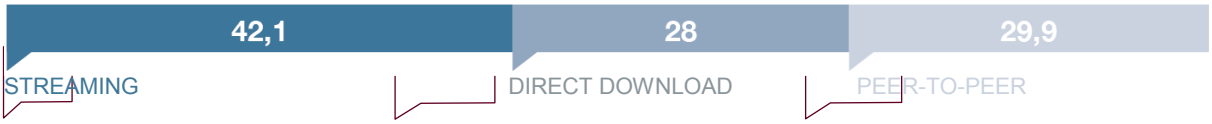
**95.1%** INTERNET PENETRATION RATE (2017) [2]

INFRINGEMENTS [3]

**1.9** NUMBER OF VISITS TO ILLEGAL SERVICES (2017)
*in billions*

**38** NUMBER OF VISITS TO ILLEGAL SERVICES PER END-USER (2017)

**Breakdown of infringements by access method (2017)**
*as a %*




**Since 2009, South Korea has developed a highly comprehensive anti-counterfeiting system, which is implemented by various organisations connected with the Ministry of Culture, Sport and Tourism[4]. Since September 2016, the Korea Copyright Protection Agency (KCoPA) has been primarily responsible for implementing measures to prevent online copyright infringement.**

**The system includes a "graduated response" component that targets both platforms that enable illegal downloading and end-users who download content both on these platforms and via peer-to-peer networks. Added to this are actions to raise awareness and promote legal offer. Measures are also implemented against massively infringing sites.**

## EDUCATIONAL AND ENFORCEMENT ACTIONS

### PRESENTATION OF THE GRADUATED WARNING SYSTEM

In 2009, Korean law established a so-called "graduated response" system whereby warnings are issued to end-users who share content online.

*[1] United Nations Population Fund (UNFPA) – 2017.*
*[2] International Telecommunications Union (ITU) – 2017.*
*[3] MUSO - 2017.*
*[4]Prior to 2016, anti-counterfeiting measures were implemented by several parties:*
*• the Ministry of Culture, Sport and Tourism and the Korea Copyright Commission (KCC), which reports to the Ministry. They are responsible largely for the so-called graduated response system;*
*• the Copyright Protection Centre, a private-sector organisation that handles anti-counterfeiting activities on behalf of the Ministry. It is involved particularly in tackling massively infringing websites.*
*A 2016 law created the Korea Copyright Protection Agency, which has absorbed the Copyright Protection Centre and implements the KCC's piracy prevention role.*

Under this system, once the KCoPA has verified the facts of the case, the Ministry of Culture, Sport and Tourism may order the platform to issue a warning to the end-user who made the disputed content available, specifying that in the event of a repeat offence, his or her account on the platform may be suspended for a limited period of time. Three warnings are sent to the end-user before a sanction is imposed. This procedure also applies to bulletin boards (which seem to be mostly similar to blogs and forums), provided they operate on a for-profit basis. The latter may receive warnings via their hosting provider.

At the end of the graduated procedure, the end-user's account may be suspended from the platform for a maximum period of six months.

Platforms that do not comply with the Ministry's orders risk a fine of around 8,500 euros. Platforms that do comply with the Ministry's orders must submit a confirmatory report swiftly (within five days).

This system differs from the educational procedures employed by other countries in that:

- it is not targeted specifically at peer-to-peer networks;
- the KCoPA is petitioned by rightholders, but it may also be petitioned by end-users if they see content that has been made available illegally. End-users report infringements via a form on a dedicated website, including a screenshot. End-users are informed of the effort to detect illegal content and are even encouraged to participate. Therefore, when they log in to submit a report via a restricted-access platform, they are rewarded with shopping vouchers for example.

The system has been criticised as it is purely administrative in nature, with no possibility of appeal.

## THE PROMOTION OF LEGAL OFFER

South Korea is very active in educating the public, conducting numerous initiatives and campaigns to raise awareness of copyright among young people in particular.

The "Clean Site" initiative to certify the legitimacy of cultural content platforms was launched in 2015. The "Copyright OK" label is now managed by the KCoPA. Certified platforms may display the logo on their site. It is granted for a period of two years.

The certification process introduced in 2015 involves verifying that platforms protect copyright, for example by enabling the notification of illegal content, devoting space to promoting legal content, adopting a specific policy towards end-users who repeatedly infringe copyright, employing people specifically to tackle counterfeiting, cooperating with rightholders and the government, etc.

# MONITORING AND ADMINISTRATIVE BLOCKING MEASURES

In South Korea, platforms constitute a special category of technical intermediaries, a list of which is drawn up by the Ministry. They also have an obligation to use content recognition or search filtering tools (such as keyword filtering). Platforms must use these technologies at the request of rightholders. Otherwise, they incur a fine. A platform that has been fined more than three times could incur a commercial penalty (it could be banned from operating in South Korea).

It would seem, therefore, that the above-mentioned "graduated response" system is coupled with a notice and takedown procedure. The KCoPA also manages the "Illegal Copyrights Obstruction Program" (ICOP), which involves continuously monitoring cyberlockers, peer-to-peer links sites, UGC platforms, blogs, etc., and issuing notice and takedown requests. These actions require close cooperation with platforms rather than Internet service providers.

In 2012, a special system (the "Killer Content Early Warning System") was put in place to pre-emptively monitor the illegal sharing of recent and therefore highly popular works, which are particularly vulnerable to piracy (for example, newly released films and albums).

South Korea has also introduced an administrative blocking system, which mainly targets foreign websites. In the first step of the procedure, the KCoPA verifies the content of the site concerned. If more than 70% of the content is illegal, it requests that the site be blocked. The Ministry then instructs the Korea Communications Standards Commission (KCSC) to proceed with blocking the site. As for sites with local domain names, they may have their domain name withdrawn.

# DENMARK

## KEY FIGURES

KNOWN BLOCKING PROCEDURES (SINCE 2006)

**16** NUMBER OF PROCEDURES

**128** NUMBER OF SITES BLOCKED

**250** NUMBER OF DOMAIN NAMES BLOCKED

DEMOGRAPHY

**5.7** POPULATION (2017) [1]
*in millions*

**97.1%** INTERNET PENETRATION RATE (2017) [2]

INFRINGEMENTS [3]

**0.46** NUMBER OF VISITS TO ILLEGAL SERVICES (2017)
*in billions*

**83** NUMBER OF VISITS TO ILLEGAL SERVICES PER END-USER (2017)

**Breakdown of infringements by access method (2017)**
*as a %*


**Rightholders across several sectors have set up an organisation specifically to combat piracy (the *RettighsAlliancen),* which is funded by its members.**

**In addition to reaching an agreement with Internet service providers to facilitate blocking measures and launching an initiative to promote legal offer, it has implemented a "follow the money" policy with the online advertising industry.**

## EDUCATIONAL AND ENFORCEMENT ACTIONS

### ENFORCEMENT MEASURES

In 2011, the Danish government considered passing a law to implement a graduated response system. Internet service providers have strongly opposed such a system, which they believe would be costly and harmful to their customer relationships. The project has therefore been abandoned.

Some rightholders are trying to establish a compensation scheme in Denmark by asking Internet service providers to disclose the identity of IP address holders. However, on 7 May 2018, a Court of Appeal issued a decision[4] stating that it would not force Internet service providers to disclose the identity of end-users who illegally share cultural content online, given the seriousness of the offence and the need to protect users' personal data.

*[1] United Nations Population Fund (UNFPA) – 2017.*
*[2] International Telecommunications Union (ITU) – 2017.*
*[3] MUSO - 2017.*
*[4] www.domstol.dk/oestrelandsret/nyheder/domsresumeer/Documents/B2451017.pdf*

Following demands from rightholders for greater public sector involvement, it was decided in Spring 2018 to approve the creation of a law enforcement unit dedicated specifically to tackling counterfeiting, although its role - particularly in implementing blocking measures - has not yet been clearly defined.

### THE PROMOTION OF LEGAL OFFER

Up until now, the Danish public authorities have focused primarily on raising awareness. Under a global initiative called "Share with Care", efforts to raise awareness of legal offer - including the dissemination of messages on popular platforms like YouTube and Facebook - are conducted and funded jointly by Internet service providers and rightholders (Rights Alliance), with the support of the Ministry of Culture.

As part of the Share with Care campaign, a portal has been created containing links to a range of legitimate platforms[5]. When end-users attempt to access a blocked site, their Internet service provider displays a message directing them to this portal.

Rightholders also insert advertising messages on illegal sites to alert end-users to the harmful consequences of their illegal actions.

The Rights Alliance, the Ministry of Culture and Internet service providers are currently working on Share with Care 2, which should lead to the creation of a search engine that directs users to legal content per sector (at present, it covers only audiovisual works). The search engine could be integrated into the messages displayed by Internet service providers when users attempt to access blocked sites. The costs should be shared by rightholders.

A campaign called "We Film Lovers" was conducted in 2016 and 2017 to highlight the consequences of unlawful streaming. It was designed primarily to address the rise in illegal streaming of audiovisual content, particularly among young people. The campaign, which struck a humorous note and was broadcast on numerous channels, was well received by the public. In August 2017, it led to a new three-year campaign on the counterfeiting of books, especially textbooks ("We Knowledge Lovers"). This campaign is led by rightholders, the Ministry of Culture and the Ministry of Education and Research, and has also been well received by the public.

Rightholders are currently working with a textbook publisher and a company that specialises in behavioural science to develop an EU-funded campaign aimed at 12 to 16-year olds.

## ANTI-COUNTERFEITING ACTIONS INVOLVING INTERMEDIARIES

In 2013, the Ministry set up the Dialogue Forum to foster discussion between stakeholders in working groups. In May 2015, a declaration of intent was drawn up under the aegis of the Ministry of Culture (Code of conduct to promote lawful behaviour on the Internet)[6]; it was signed by Internet service providers, online advertisers, payment operators (including Mastercard), rightholders, search engines (Google and Microsoft) and various professional organisations including the ICT industry association (IT-Branchen) and Omnicom Media Group. Subsequent to this agreement, several working groups have been formed.

To date, two agreements have been concluded in the frame of these discussions: an agreement with Internet service providers to facilitate blocking, and an agreement with the online advertising industry that functions by reference to a list of unlawful services. Today, the plan is to extend the existing Follow the money scheme to include actors such as payment operators, social networks, search engines and Internet browsers, which could take measures against the listed services. This could be done by the end of 2018.

*[5] www.sharewithcare.dk/*
*[6] www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0ahUKEwjWkeH-y77bAhUGfFAKHen1CJsQFggoMAA&url=https%3A%2F%2Fkum.dk%2Ffileadmin%2FKUM%2FDocuments%2FNyheder%2520og%2520Presse%2FPresse meddelelser%2F2015%2FCode_of_Conduct_-_Engelsk_version.pdf&usg=AOvVaw2rN7m0b4im0_0EmPF_qoJz*

## SITE BLOCKING

The following system was implemented under the 2014 agreement between rightholders and the trade union that represents Internet service providers:

Rightholders refer just one Internet service provider to the court in site-blocking procedures, alternating regularly to reduce legal costs. The blocking orders are then notified to the union of ISPs (Telecom Industry Association Denmark), which forwards them to other Internet service providers. Under the agreement, the latter must put a DNS block on the sites within seven days of notification, without having been involved in the procedure beforehand. Each party bears its own costs. Rightholders must demonstrate that the content available on the site belongs to them and that they have not directly or indirectly consented to it being shared. In principle, one offence is sufficient. However, rightholders focus on sites that provide a substantial number of infringing works. Denmark, like the United Kingdom,does not have a predefined threshold to ascertain the infringing nature of a website.

- Judicial blocking procedures last from two to three months, or three to six months including case preparation time. They may concern dozens of sites. Rightholders always refer Internet service providers to the same court, which has produced a standard pack of evidence to provide.

- The agreement also allows Internet service providers to block mirror sites easily without having to go back to court, provided that the rightholders can produce sufficient evidence. In practice, rightholders use software that is supplied by a private company and is also used by the Motion Picture Association (MPA), which analyses similarities between services and identifies services circumventing blocking orders. In any event, the rightholders guarantee Internet service providers against any disputes with mirror sites.

Furthermore, courts have recently issued dynamic blocking orders enabling rightholders to request the blocking not only of sites identified by their domain name, but also sites identified by their content, type or interface regardless of the domain name extension[7], thus validating the code of conduct after the fact. The union of Internet service providers publishes a list of sites that have been blocked in Denmark on its websites. However, this list is rarely consulted.

Internet service providers use DNS blocking, but rightholders are considering IP blocking given the possibility of circumventinging DNS blocks (using alternative DNS servers) and the rise in unlawful streaming of live TV programmes. Rightholders believe that blocking measures reduce visits from Danish IP addresses to blocked websites by 75% but are concerned about the use of alternative DNS servers.

As for the unlawful streaming of live TV programmes, Danish rightholders believe that it is vital to take action before it becomes even more widespread and the general public becomes accustomed to enjoying such services at a fraction of their normal cost. According to reports, the number of visitors to sites selling illegal access to pay-TV packages rose by 84% between January and December 2017. Likewise, visits to live streaming sites that allow users to watch sports content illegally increased by 28% in 2017. Therefore, the possibility of imposing IP blocks on these sites is being discussed.

Danish rightholders and the IFPI have also recently sought court orders to block stream ripping services.

## THE IMPLEMENTATION OF THE "FOLLOW THE MONEY" APPROACH

Work carried out with the online advertising industry culminated in May 2015 with the so-called *"Adkodex"* initiative, in which rightholders work closely with the industry to ensure they do not place ads on massively infringing sites.

Under this initiative, which is part of the Follow the money approach, Danish rightholders have access to a list of sites that are blocked in Denmark, the London police's list of infringing websites, and other more confidential sources. The Danish list currently contains around 2,500 sites and is updated monthly. The aim is to encourage more actors - including online payment operators, browsers and social networks - to use the list, in order to reduce the flow of funds and traffic to the websites.

The list is not available to the public. Services may contact rightholders to find out if they are on the list.

*[7] rettighedsalliancen.dk/2017/02/08/retsafgoerelse-styrker-blokeringeme-af-de-ulovlige-tjenester-2/*

# SPAIN

## KEY FIGURES

KNOWN BLOCKING PROCEDURES (SINCE 2006)

**7** NUMBER OF PROCEDURES

**21** NUMBER OF SITES BLOCKED

**37** NUMBER OF DOMAIN NAMES BLOCKED

DEMOGRAPHY

**46.4** POPULATION (2017) [1]
*in millions*

**84.6%** INTERNET PENETRATION RATE (2017) [2]

INFRINGEMENTS [3]

**4.2** NUMBER OF VISITS TO ILLEGAL SERVICES (2017)
*in billions*

**108** NUMBER OF VISITS TO ILLEGAL SERVICES PER END-USER (2017)

**Breakdown of infringements by access method (2017)**
*as a %*


**In Spain, the so-called "*Sinde*" law adopted on 4 March 2011 and amended in October 2014 establishes a mechanism for blocking massively infringing sites via a public authority (the *Sinde* commission).**

**In addition, new tools have been developed and dedicated law enforcement units have been created.**

**At the same time, the Spanish government and rightholders are conducting awareness campaigns and measures are being implemented to make legal offer more visible: a portal listing various platforms has been created with the support of the government and the film industry[4]. A search engine for audiovisual works (such as films and TV series) has also been developed under a private initiative[5].**

## EDUCATIONAL AND ENFORCEMENT ACTIONS

### A LAW ENFORCEMENT UNIT DEDICATED TO TACKLING ONLINE INFRINGEMENT

In Spain, a law enforcement unit has been created specially to tackle intellectual property crime.

*[1] United Nations Population Fund (UNFPA) – 2017.*
*[2] International Telecommunications Union (ITU) – 2017.*
*[3] MUSO - 2017.*
*[4] www.mesientodecine.com/index.html*
*[5]www.encuentratupeli.com*

The IT security squad is tasked with combating links sites[6] and the illegal streaming of television content[7].

Numerous operations have been carried out in recent years, including operation CASPER in April 2017. This Spanish police operation was conducted in coordination with Bulgaria, Europol and Eurojust. It uncovered a criminal network operating across Spain and Bulgaria, and specialising in the illegal online broadcasting of 1,000 pay-TV channels Europe wide. Twelve searches were carried out simultaneously, and eight people were arrested. The investigation revealed that the network was controlled by an international criminal organisation.

## ACTIONS AGAINST "QUALIFIED" USERS

Spanish law does not provide for a graduated warning system against end-users, but civil procedure allows rightholders to take action against so-called "qualified" users: for example, end-users who post massive amounts of copyrighted content online[8]. Rightholders may bring proceedings against Internet service providers to obtain the identity of counterfeiters, with a view to prosecuting the latter in the civil or criminal court.

However, in view of recent first instance decisions[9], it seems that Spanish courts consider that identifying offenders by their IP address alone is insufficient, as only the Internet subscriber's details are revealed and he or she may not necessarily be the person who unlawfully shared or downloaded copyrighted works.

The Spanish football league (*LaLiga*) has updated its official smartphone application to enable access to the user's microphone and geolocation data. As soon as the user consents to the activation of these functions, the application - which is only activated when *LaLiga* broadcasts a match - geolocates the sound to make sure the match is being broadcast by an authorised broadcaster. The sound retrieved by the application is automatically converted to a binary code, making it impossible to reconstruct the recording. At this stage, *LaLiga* has not indicated if and how it intends to use this data against end-users.

## AWARENESS CAMPAIGNS

### THE "*NO PIRATEES TU FUTURO*" CAMPAIGN

In October 2017, the Spanish government launched an awareness campaign called *"No piratees tu futuro"* (don't hijack your future); it is aimed at young people and is designed to raise their awareness of the fight against piracy of cultural and sports content. The campaign was developed through a partnership between the Ministry of Culture and Sport, and several private-sector organisations that provided the funding. Thus, more than twenty partnerships were formed with the *Coalición de Creadores e Industrias de Contenidos* (Coalition of Creators and Content Industries), *LaLiga*, communication media, the *Federación de Cines* (the Spanish cinema federation) and the *Administrador de infraestructuras arias* (railway infrastructure manager).

The campaign has a dual objective: to direct people towards legal offer and to inspire empathy by showing the consequences of piracy on the future careers of young people, without focusing on the criminal punishment aspect.

It has been broadcast widely via all types of media: television, radio, cinema, social networks, advertising banners and the press[10]. Celebrities popular with young people (including actors and athletes) took part in launching the campaign. It is planned to last two years but may be extended for a further three. Advertisements in all formats have been produced free of charge by a top audiovisual production and distribution company (MEDIAPRO).

The campaign is being broadcast through agreements with media companies that use their own broadcasting channels and spaces.

*[6] In December 2014, the squad arrested the administrators of the download sites "seriespepito.com" and "peliculaspepito.com" in Madrid and Alicante. The court in Elche, in the province of Alicante, ordered that the sites be blocked.*
*[7] The "Roja Directa" case*
*[8] Article 256 1) 11° de la Ley 1/2000, de 7 de Enero, de Enjuiciamiento Civil.*
*[9] "Dallas Buyers Club" Sentencia CIVIL N° 240/2017, Juzgados de lo Mercantil - Donostia-San Sebastián, Sección 1, Rec 526/2017 de 02 de Noviembre de 2017 et Sentencia CIVIL N° 239/2017, Juzgados de lo Mercantil - Donostia-San Sebastián, Sección 1, Rec 524/2017 de 02 de Noviembre de 2017.*
*[10] Link to the campaign ads: www.youtube.com/playlist?list=PLmAw6SZis81l0oqHSBoRs- 9pGlyyhW0VpZ*

Distribution Thus, Atresmedia, Disney, Discovery Channel, Mediapro, Movistar +, PrisaRadio and Vodafone have broadcast the campaign free of charge on their own spaces.

To encourage partner organisations to run television campaigns, the Ministry also approached the *Comisión Nacional de los Mercados y la Competencia* (the Spanish National Commission on Markets and Competition, which performs similar functions to the French competition authority and is involved in regulating the audiovisual sector) to ensure that campaign ads would not be counted in the broadcasting time that television channels may allocate to advertising.

### AWARENESS CAMPAIGN PROJECT IN SCHOOLS OFTHE MINISTRY OF CULTURE AND SPORT

The Ministry of Culture and Sport, the Ministry of the Interior and an association that specialises in intellectual property are producing support materials for teachers and students in preparation for police officers going into schools to raise awareness about piracy.

### AWARENESS CAMPAIGN IN SCHOOLS BY *COALICION* AND *LALIGA*

This campaign has been up and running for three years. Students are regarded as future professionals in the culture sector and the entertainment business: the aim is to show them the impact that piracy has on employment and the economy, and to make sure they adopt good online content consumption habits.

A total of 15,000 students aged 10 to 13 have taken part in the campaign, across around 100 schools. As a result of the campaign, 80% of students have a very negative opinion of piracy.

## ANTI-COUNTERFEITING ACTIONS INVOLVING INTERMEDIARIES

The laws of 2011 and 2014 introduced an administrative procedure for reporting online copyright infringements, which may lead to websites being blocked. The procedure is implemented by the *Sinde* commission, which is attached to the Ministry of Culture and Sport.

Rightholders can also apply to the civil court to have an infringing website blocked. This is more costly though, which is why rightholders prefer the administrative procedure.

In February 2018, in a case brought by six film and television studios, the Barcelona Commercial Court ruled that two streaming sites were infringing the studios' rights. Consequently, it ordered Spain's main Internet service providers to block access to the sites and to any domain names, sub-domains and IP addresses that might indirectly enable access to them[11].

### THE ADMINISTRATIVE PROCEDURE

Chaired by the Secretary of State for Culture, the *Sinde* commission is composed of two members of the Ministry of Culture and Sport, a member of the Ministry of Energy, Tourism and the Digital Agenda, a member of the Ministry of Justice, a member of the Ministry of Economy and Business and a member of the Ministry of the Presidency, Parliamentary Relations and Equality.

In terms of services, a team of nine people is responsible for examining case files.

Cases are brought before the commission only if the rights holder has tried and failed to contact the website to remove infringing content within 72 hours, and has presented proof of such failure to the commission.

The procedure is free of charge and lasts for three months at most.

*[11]www.poderjudidal.es/search/contenidos.action?action=contentpdf&databasematch=AN&reference=8293989&links=HDFull&optimize=20180220&publicinterface=true*

Any rights holder who finds one or more instances of infringement on a website that hosts content or links to content and has a sufficient connection with Spain[12] (for example, target audience located in Spain, content in Spanish, advertisements in Spanish, payment in euros), may refer the matter to the *Sinde* commission electronically.

The referral file includes the following: identification of the unlawful content, proof of copyright ownership, proof of the infringement, proof of the intention to derive financial profit from the infringement or proof of the actual (or even potential) harm caused, and information relative to the infringer and the hosting provider.

The Commission may be called upon to settle a dispute with a stream ripping site.

When the manager cannot be identified, the commission requests permission from the Central Administrative Court to obtain the necessary information from intermediaries such as hosting providers, search engines, Internet service providers, online payment platforms and advertising intermediaries. If the information is insufficient, it publishes a notice in the Official Journal. Thus, the site manager is deemed to have been informed of the procedure, and the procedure has not been slowed down.

If the commission finds the rightholders' request admissible, it may order the website manager to take the following steps within 48 hours:

- make his or her views known;
- ensure that the content is no longer accessible by permanently removing it from the site (takedown and stay down), or by ceasing the infringing activity.

The primary purpose of the proceedings is to obtain the voluntary cessation of the infringing activity.

If the content is not removed or the service is not shut down within 24 hours, the commission - if it recognises that an infringement has occurred - may instruct the technical intermediaries to take all necessary steps to stop the infringement within 48 hours.

Several injunctions may be issued: cessation of hosting services, DNS and IP blocking by Internet service providers for up to one year if the site is located outside the European Union, delisting of the site from search engine results, suspension of domain names ending with ".es" or with another extension managed by the Spanish registry.

However, the commission must seek judicial authorisation to enforce such decisions. The court ensures that the commission's request complies with the fundamental freedoms provided for in Article 20 of the Spanish Constitution, particularly the right to freedom of expression[13].

The presence of a single infringing work is sufficient to assess the illegality of a site.

In the event of a repeat offence, the Secretary of State for Culture may impose a fine of up to 600,000 euros if - after twice instructing a site to remove infringing content - the content has not been taken down or has reappeared[14]. It is not necessary to return to court to have sites circumventing blocking measures blocked. Rightholders simply have to prove to the technical intermediaries that the new site circumvents a previous order.

On 20 June 2018, after being convicted twice by the commission in June and July 2017, the owner of the Peruvian site "www.x-caleta.com" (now called "www.x-caleta2.com") received its first fine of 375,000 euros for repeated administrative offences. In addition, the fine was published in the local official newspaper and in two national newspapers at the offender's expense, and the sites in question were blocked in Spain for a period of one year.

The *Sinde* commission publishes quarterly reports on its activities[15]. From its creation until July 2018, 603 referrals were submitted to the commission. Half of the referrals did not lead to anything due to admissibility issues. Of the 340 referrals that met the conditions laid down in the law, 32% were closed because the subject of the referral had disappeared (removal of content, discontinuation of activity or failure to identify the infringer).

*[12]The website does not have to be "massively infringing" to be brought before the Commission. This criterion may be used to determine the order in which cases are processed.*

*[13] Article 20 of the Spanish Constitution: "1. The following rights are recognised and protected: a) the right to freely express and disseminate thoughts, ideas and opinions through words, in writing or by any other means of communication; [...] 2. The exercise of these rights may not be restricted by any form of prior censorship. [...] ".*

*[14] Article 195 of the intellectual property code.*

*[15] www.mecd.gob.es/cultura-mecd/areas-cultura/propiedadintelectual/lucha-contra-la-pireria.html*

Of the cases examined by the commission, over one third were closed because the site in question has either complied with the takedown notice or has lapsed.

Rightholders would like to simplify and speed up the procedure to obtain more blocking decisions. In addition, they do not want cases to become moot simply because the commission cannot deal with them swiftly enough.

### THE IMPLEMENTATION OF THE "FOLLOW THE MONEY" APPROACH

The commission also implements a Follow the money policy whereby it can ask payment intermediaries and advertisers to stop working with sites that refuse to remove notified content.

The commission conducts preliminary investigations to identify the payment intermediaries and advertising operators that work with the infringing site. If the payment intermediaries and advertisers do not cease their contractual relationship with the site, the commission may fine them up to 300,000 euros.

The *Coalicion de creadores e industrias de contidos* (Coalition of Creators and Content Industries)[16] has reported the following: 95% of pages on illegal sites contain advertisements, 81% of users are registered on these sites and 8% have paid to access illegal content[17].

*[16] The Coalicion is made up of AEVI (Spanish Video Games Association), CEDRO (Spanish Reproduction Rights Centre), CONECTA (Association of Thematic Pay-TV Channels), EGEDA (an association that manages the rights of audiovisual producers), FAP (Federation for the Protection of Intellectual Property), FEDICINE (Federation of Spanish Film Distributors), PROMUSICAE (Spanish Music Producers), SGAE (Society of Authors and Publishers) and UVE (Spanish Videographic Union).*

*[17]elpais.com/cultura/2018/04/06/actualidad/1523014293_722167.html*

# UNITED STATES

## KEY FIGURES

DEMOGRAPHY

**324.5** POPULATION (2017) [1] *in millions*

**76.2%** INTERNET PENETRATION RATE (2017) [2]

INFRINGEMENTS [3]

**17.9** NUMBER OF VISITS TO ILLEGAL SERVICES (2017) *in billions*

**72** NUMBER OF VISITS TO ILLEGAL SERVICES PER END-USER (2017)

**Breakdown of infringements by access method (2017)** *as a %*


**In the United States, while some lawsuits have been brought against end-userend-users, right holders focus primarily on illegal services.**

**In addition, the government publishes a list of massively infringing services to raise awareness among the public and in States where intellectual property protection is inadequate.**

## EDUCATIONAL AND ENFORCEMENT ACTIONS

### OBLIGATIONS AND ACTIONS PURSUANT TO THE DIGITAL MILLENNIUM COPYRIGHT ACT (DMCA)

The Digital Millennium Copyright Act (DMCA), which defines the liability regime applicable to technical intermediaries, contains provisions aimed at obliging Internet service providers to take specific measures against subscribers who repeatedly commit infringements (up to and including termination of the subscription).

Some rightholders send notifications to Internet service providers, informing them that their subscribers have shared a copyrighted work on peer-to-peer networks.

Several Internet service providers forward these messages to their subscribers, warning them that their connection could be interrupted in the event of a repeat infringement.

A private and entirely voluntary graduated response system (the Copyright Alert System) was in operation from February 2013 to January 2017. Its main purpose was to educate and guide people towards legal alternatives.

The Center for Copyright Information (CCI), whose membership includes rightholders and Internet service providers, oversaw the development of the system and the implementation of awareness-raising activities via a dedicated website containing information on means of securing WiFI

*[1] United Nations Population Fund (UNFPA) – 2017.*
*[2] International Telecommunications Union (ITU) – 2017.*
*[3] MUSO - 2017.*

and legal offer[4]. The agreement stated that the CCI was financed equally by rightholders and Internet service providers.

The rightholders collected IP addresses and the Internet service providers issued alerts accordingly. The penalties that could be imposed at the end of the procedure were only moderately restrictive for subscribers (for example, they could be required to contact their Internet service provider or complete a short online course on copyright, or their Internet speed could be slowed down). However, the possibility of requiring Internet service providers to sanction subscribers by terminating their Internet access was rejected by the parties to the agreement. This was a key point for Internet service providers during the negotiations on the agreement.

In May 2015, the Internet Security Task Force (which includes several independent American studios) concluded that the system was ineffective. It criticised the fact that the number of alerts that Internet service providers could issue was subject to a monthly cap, and argued that purely educational measures had reached their limit. In early 2017, since the parties had failed to reach an agreement on introducing tougher sanctions for repeat infringers (rather than just educational measures), it was decided to scrap the system altogether.

However, some Internet service providers continue to take measures against their subscribers that are similar to those previously implemented under the graduated response system. The graduated response system did not prevent some rightholders - mainly in the adult content sector - from employing other methods, such as claiming compensation from end-users. This continues today: there were over 1,000 claims for compensation in 2017, and 1,700 in the first half of 2018.

On 1 November 2015, the Internet service provider Cox Communications was convicted for its policy towards subscribers, particularly repeat infringers. This Internet service provider was not party to the agreement on the graduated response system but had set up its own graduated system under the DMCA. This system included more than ten stages, at the end of which subscribers' accounts could not actually be suspended. The court ruled that, having failed to comply with the provisions of the DMCA, the Internet service provider could no longer benefit from the limited liability regime applicable to technical intermediaries.

However, this dispute is still ongoing, as the Internet service provider has not yet exhausted its rights of appeal.

### CHANGES UNDER DISCUSSION

In early January 2016, the United States Copyright Office launched a consultation to seek the views of stakeholders on the "Safe Harbour" scheme, the effectiveness of the notice and takedown procedure, the burden and the cost of issuing notices for each of the actors involved, and the effectiveness of the policies adopted by Internet service providers towards repeat infringers. In addition, the 2017-2019 intellectual property protection programme provides that the administration will support and encourage the implementation of best practices in the area of notice and takedown procedures. The Internet Policy Task Force, which reports to the Department of Commerce, will convene stakeholders if necessary to discuss how to make notice and takedown procedures more effective.

Finally, the US administration plans to encourage stakeholders to develop standards and best practices aimed at reducing the use of social networks for unlawful purposes, such as mechanisms to facilitate the notification of copyright infringements.

In the same vein, it will encourage the development of standards and best practices to reduce the number of copyright-infringing applications (counterfeit applications, applications that provide unauthorised access to protected content, etc.).

A bill tabled in October 2017 provides that a body attached to the Copyright Office could be tasked with handling "small claims" copyright disputes. The cost of referring a case to this body would be far lower than that of bringing it to a conventional court.

The body could in particular be tasked with resolving disputes relating to the unlawful use of photographs on the Internet, or the removal of content from platforms such as YouTube.

*[4]www.copyrightinformation.org*

### THE PROMOTION OF LEGAL OFFER

In 2014, the Motion Picture Association of America (MPAA) launched a search engine to direct end-users to legal audiovisual content[5]; it allowed users to search for a particular film or TV series, and told them where they could watch it legally. The site was taken down at the end of 2017, as the MPAA deemed there are now several audiovisual search engines on the market and a substantial legal offer both in the United States (over 140 platforms) and worldwide.

In December 2016, the US administration published its "Joint Strategic Plan", a three-year intellectual property protection programme[6]. This document establishes, amongst other things, that the government will consider the possibility of supporting public-private partnerships to promote legal offer to end-users and inform them of the risks involved in online counterfeiting, such as malware attacks.

## ACTIONS AGAINST INFRINGING SERVICES

### ACTIONS AGAINST ILLEGAL SITES

In the United States, efforts to establish a site blocking system have been dropped since the failure in January 2012 of the so-called SOPA and PIPA bills, which sought to allow website blocking.

Injunctive proceedings have notably been replaced by domain name seizure procedures. Domain names can be seized by the National Intellectual Property Rights Coordination Center, which is responsible for anti-counterfeiting and reports to the US Customs and Immigration Office. In November 2017, as part of a joint Europol-Interpol operation called "In Our Sites", 20,520 domain names selling counterfeit goods or pirated cultural content were seized[7]. When end-users attempt to open the sites, they are redirected to an information page.

In more targeted legal actions to prevent piracy of specific cultural or sports content, courts may also issue injunctions to domain name managers:

- thus, in May 2017, the Indian Cricket Premier League (IPL) obtained an injunction against several websites, preventing them from broadcasting IPL matches. The decision made provision for further injunctions against a group of payment and advertising intermediaries that work with the websites, and against hosting providers, CDNs, registrars and domain name registries[8]. As a result, they were required to cease all services to the websites until the end of the season.
- In 2015, and again in August 2017, American TV network Showtime took action to prevent illegal sites from broadcasting an eagerly awaited boxing match (Mayweather v McGregor). A federal court in California issued a preliminary injunction against 44 different domain names advertising the fight, to prevent them from broadcasting the match during a given period.
- In July 2017, at the request of a major player in the Philippine media industry, a federal court in Florida ordered that the domain names of several infringing websites be temporarily seized and that funds to the sites (which are owned by advertising operators) be cut off[9]. In July 2018, the same rights holder obtained a temporary injunction against some registrars and registries

*[5]www.wheretowhatch.com*
*[6]www.obamawhitehouse.archives.gov/blog/2016/12/12/supporting-innovation-creativity-and-enterprise-charting-path-ahead*
*[7]www.europol.europa.eu/newsroom/news/biggest-hit-against-online-piracy-over-20-520-internet-domain-names-seized-for-selling-counterfeits*
*[8]During the season, the domain names targeted by the injunction may also be withheld by registrars and/or registries (domain names transferred to the law firm representing the rightholders).*
*[9]torrentfreak.com/images/fccb57c7-b666-4495-aa07-783c429e6613.pdf*

to block access to the targeted sites; it also obtained a temporary injunction against the online advertising and payment operators to cut off funds to the sites, and ordered them to provide the court with a detailed inventory of these funds.

Finally, numerous proceedings have been brought directly against illegal actors - for example, those who sell pre-loaded set-top boxes or publish applications for them for piracy purposes - and against stream ripping sites.

In 2015, several rightholders filed a lawsuit against Shava TV and Cres TV for providing set-top boxes and services that enabled users to illegally stream TV programming from Arab and Asian countries. The rightholders won the case in April 2017 and were awarded $25,650,000 in damages.

The initial priority of the Alliance for Creativity and Entertainment (ACE) was therefore to tackle the widespread use of pre-loaded set-top boxes for piracy purposes. ACE was set up in summer 2017 to combat piracy at international level, and currently comprises 38 rightholders from all over the world[10].

In October 2017, ACE brought legal action against TickBox, which was selling - via a dedicated website - a set-top box that enabled access to infringing content. The rightholders claimed compensation and requested that TickBox cease its activities and that all equipment and documents connected with the infringements be seized. At the end of January 2018, the court granted a temporary injunction ordering TickBox to stop facilitating the installation of add-ons, applications or any other illegal software, and to cease all advertising that encouraged counterfeiting. The court deemed that if these measures forced Tickbox into bankruptcy, then the company's business model was not viable without its illegal activities. The judge also asked the parties to reach an agreement regarding boxes already sold. The judge was able to approve the agreement in mid-February. On expiry of the agreement, Tickbox must perform an automatic update that will delete all illegal software from boxes already sold. ACE may also notify Tickbox of any new application or add-on that infringes their rights, and Tickbox must disable it within 24 hours.

In early January 2018, ACE started fresh legal proceedings against Dragon Box Media Inc., which sells the Dragon Box. This case culminated in a settlement agreement last July.

In April 2018, ACE took legal action against the operator of SET TV, which offered a range of pirated TV channels and on-demand content. SET TV has now ceased operating.

As regards the fight against illegal stream ripping, in September 2016 the Recording Industry Association of America (RIAA), the International Federation of the Phonographic Industry (IFPI), and the British Phonographic Industry (BPI) filed a complaint in California against Youtube-mp3, a website run by a company called PMD Technologie UG in Germany. They were seeking very substantial damages, the seizure of the domain name YouTube-mp3, and an order to cease infringing upon their rights in the future. In September 2017, the parties reached an agreement: the website was shut down and Youtube-mp3 agreed to pay compensation (of an undisclosed amount) to the rightholders[11].

## THE ACTIONS OF THE US ADMINISTRATION

### THE PUBLICATION OF LISTS BY THE US ADMINISTRATION

Every year, the US Administration publishes the following lists via the United States Trade Representative (USTR), a government agency that coordinates US trade policy:

- the “Special 301 list”, which is provided for by law and identifies countries that do not provide effective protection of intellectual property rights;
- the “Out-of-Cycle Review of Notorious Markets”, or “Notorious Markets list”, which identifies websites and physical marketplaces that clearly engage in or enable infringement of intellectual property rights. The purpose of this list is to inform the public. The USTR draws up the list according to internally defined criteria that are not disclosed to the public. It is established based on submissions made primarily by the industries concerned, and an investigation by the USTR.

*[10]Amazon, AMC Networks, BBC Worldwide, Bell Canada and Bell Media, Canal+ Group, CBS Corporation, Constantin Film, Foxtel, Grupo Globo, HBO, Hulu, Lionsgate, Metro-Goldwyn-Mayer (MGM), Millennium Media, NBCUniversal, Netflix, Paramount Pictures, SF Studios, Sky, Sony Pictures Entertainment, Star India, Studio Babelsberg, STX Entertainment, Telemundo, Televisa, Twentieth Century Fox, Univision Communications Inc., Village Roadshow, The Walt Disney Company, and Warner Bros. Entertainment Inc.*

*[11]United States District Court, Central District of California, Case No. 2:16-cv-07210-AB-E.*

Once the list has been published, the websites on it sometimes contact the USTR to ask what they should do to avoid being listed again the following year.

In 2018, the USTR devoted a focus to "Illicit Streaming Devices" or ISDs, a term created specifically to describe devices pre-loaded with piracy-enabling add-ons. In the United States, a reported 6.5% of households have purchased such devices and 106 million users subscribe to an illegal television service. And the numbers are rising[12].

The list also highlights websites that generate income from advertising, citing one of White Bullet's quarterly reports, according to which 25 to 30% of all ads on the 5,000 most popular IP infringing sites in the United States, Europe and Australia come from premium brands[13].

It is recalled again this year that the listed services, in addition to enabling copyright infringements, may be dangerous for end-users in terms of personal data theft and cyberattacks. Several sources are cited in support of this[14]. Moreover, the information published on many of the listed services includes an update on the viruses they are likely to spread.

## THE INVOLVEMENT OF INTERMEDIARIES IN THE FIGHT AGAINST COUNTERFEITING

In the US, rightholders and the administration advocate voluntary agreements with as many intermediaries as possible in addition to online payment and advertising operators, for example hosting providers, registries, registrars, CDNs and search engines.

### ACTIONS TAKEN BY PAYMENT INTERMEDIARIES

In May 2011, with the support of the Obama administration, a number of agreements were concluded between rightholders and payment intermediaries to prevent both copyright infringements and trademark counterfeiting[15]. Pursuant to these agreements, the RogueBlock initiative[16] was developed to stop the provision of payment means to infringing sites. As part of this initiative, the International Anti-Counterfeiting Coalition (IACC) - which is made up of intellectual property rightholders - developed a secure platform to receive notifications from rightholders. According to the IACC, over 200,000 websites have been reported to date (on the grounds of trademark counterfeiting or copyright infringement). Since 2015, sites that host unlawfully shared content (cyberlockers) have also been targeted under the RogueBlock initiative. However, the system does not seem to be widely used by copyrightholders who prefer to establish relationships of trust directly with payment intermediaries.

### ACTIONS TAKEN BY ONLINE ADVERTISING INTERMEDIARIES

In July 2013, several advertising networks[17] signed a charter of good practice (Best practices guidelines for ad networks to address piracy and counterfeiting).

In February 2015, the Trustworthy Accountability Group (TAG)[18] launched the Brand Integrity Program Against Piracy, which offers tools and services to identify and prevent the risk of advertising being placed on infringing sites. In October 2015, a new programme called "Verified by TAG" was set up to create a list of approved advertisers and media. The TAG membership fee is10,000 US dollars per year.

In June 2017, TAG launched a tool to deter its members from advertising

*[12]www.sandvine.com/hubfs/downloads/archive/2017-global-internet-phenomena-spotlight-subscription-television-piracy.pdf*
*[13] www.white-bullet.com/blog*
*[14]Digital Citizens Alliance, "Enabling Malware", July 2016: media.gractions.com/314A5A9ABBBBC5E3BD824CF47C46EF4B-9D3A76/0057c1cf-28f6-406d-9cab-03ad60fb50e4.pdf;*
*www.digitalcitizensalliance.org/clientuploads/directory/Reports/2017_7The_Gateway_Trojan.pdf;*
*www.pandasecurity.com/mediacenter/src/uploads/2017/02/Pandalabs-2017-Predictions-en.pdf;*
*www.symantec.com/security_response/publications/monthlytopic.jsp*
*[15]MasterCard, Visa International, Visa Europe, PayPal, MoneyGram, American Express, Discover, PULSE, Diners Club and Western Union.*
*[16]www.iacc.org/online-initiatives/rogueblock*
*[17]Media, Adtegrity, AOL, Condé Nast, Google, Microsoft, SpotXchange and Yahoo!.*
*[18]The Association of National Advertisers and the American Association of Advertising Agencies partnered with the IAB to create the Trustworthy Accountability Group (TAG).*

on mobile applications that illegally share copyrighted content. In October 2017, TAG published a study entitled "Measuring Digital Advertising Revenue to Infringing Sites". The study found that advertising revenue to major infringing websites was an estimated 111 million dollars, 83% of which came from non-premium advertisers. The study also found that had the industry not taken action, these websites would have received between 48% and 61% more ad revenue[19]. More recently, TAG signed the European MoU on online advertising and intellectual property rights.

## THE INVOLVEMENT OF REGISTRIES DOMAIN NAME MANAGERS

The intellectual property protection programme published in December 2016 is based on the observation that operators of massively infringing websites switch domain names (a practice known as "domain name hopping"[20]) as soon as a name can no longer be used because it has been either blocked or suspended (see USTR list attached). Consequently, the United States has announced that it will continue to monitor abusive domain name registrations with a view to taking action against such practices.

With this in mind, in February 2016, the MPAA entered into an agreement with domain name registry Donuts, which manages several extensions including ".movie". In May 2016, it signed an agreement with the Radix registry in Dubai, which also manages several extensions, including ".website" and ".online". According to reports, these agreements provide for the possibility of suspending the domain names of massively infringing sites notified by the MPAA[21].

## THE ROLE OF SEARCH ENGINES

In both the United States and the United Kingdom, Google has talked to rightholders about optimising its demotion signal, an algorithm that moves websites down in the search rankings according to the number of infringement notifications received. As stated in the report "How Google fights piracy"[22], Google uses a demotion signal to prioritise takedown notices concerning, for example, audiovisual works that have not yet been released or are still showing in cinemas.

The intellectual property protection programme of December 2016 provides that the US administration support the development of best practices to address, for example, issues relating to the autocomplete function (which predicts the rest of a search term as it is being entered), the downgrading of massively infringing sites, and possible means of diverting traffic away from these sites.

*[19]www.tagtoday.net/pressreleases/study-shows-ad-industry-anti-piracy-efforts-have-cut-pirate-ad-revenue-in-half*

*[20]To do this, operators of massively infringing websites register hundreds or thousands of domain names in several jurisdictions, particularly those that provide little intellectual property right protection. Thus, mirror sites can easily be created, undermining the effectiveness of legal proceedings.*

*[21]In this case, the MPAA would become a trusted notifier and would report suspected infringing websites to Donuts or Radix. Donuts or Radix would then conduct an investigation, starting by contacting the site. If the site fails to respond in a satisfactory manner, or does not respond at all, Donuts or Radix suspends the domain name.*

*[22]www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=2&ved=2ahUKEwjV8rast53fAhUQyRoKHSBwCDsQFjABegQICBAC&url=https%3A%2F%2Fblog.google%2Fdocuments%2F27%2FHow_Google_Fights_Piracy_2018.pdf&usg=AOvVaw1eiX8Dt-YTqOZnVjMn7JQ7*

# GREECE

## KEY FIGURES

KNOWN BLOCKING PROCEDURES (SINCE 2006)

**3** NUMBER OF PROCEDURES

**31** NUMBER OF SITES BLOCKED

**53** NUMBER OF DOMAIN NAMES BLOCKED

DEMOGRAPHY

**11.2** POPULATION (2017) [1] *in millions*

**69.1%** INTERNET PENETRATION RATE (2017) [2]

INFRINGEMENTS [3]

**0.97** NUMBER OF VISITS TO ILLEGAL SERVICES (2017) *in billions*

**125** NUMBER OF VISITS TO ILLEGAL SERVICES PER END-USER (2017)

**Breakdown of infringements by access method (2017)** *as a %*


**Greece very recently adopted an administrative blocking mechanism based on the system in Italy.**

**Measures aimed at end-users are still poorly developped, with the law expressly stating that the anti-piracy system is not applicable to offences committed by end users, regardless of the technology used to share or view works.**

## EDUCATIONAL AND ENFORCEMENT ACTIONS

### CRIMINAL ACTION AGAINST OPERATORS OFFERING ILLEGAL TV SUBSCRIPTIONS

In January 2018, Greece's cybercrime unit took part in a joint police operation led by Cyprus and supported by the Dutch and Bulgarian police forces, Europol and members of the Audiovisual Anti-Piracy Alliance (AAPA) to shut down a network suspected of selling illegal television subscriptions In Greece and Cyprus.

Four suspects were arrested and the servers providing illegal access to television channels were shut down.

### AWARENESS-RAISING ACTIONS

The Hellenic Copyright Organisation (OPI) is tasked with leading discussions on issues of copyright and related rights, and representing Greece globally on such matters. Greece is also in the process of setting up a portal

*[1] United Nations Population Fund (UNFPA) – 2017.*
*[2] International Telecommunications Union (ITU) – 2017.*
*[3] MUSO - 2017.*

containing links to legal offer, and could consider redirecting users to this portal in the event that a website is blocked.

The OPI board of directors comprises seven members, who are appointed for three years by the Ministry. It is funded by a 1% levy on the gross income of collective management organisations. Some of its funding may also come from donations, payments for services rendered, grants from the Ministry of Culture or income from the national lottery.

It is tasked with raising awareness and supervising collective management organisations, and has developed a process for timestamping IP works under the supervision of the Ministry of Culture and Sport.

It organises copyright awareness initiatives in schools and launched a dedicated website in 2016[4].

## ADMINISTRATIVE BLOCKING OF ILLEGAL SERVICES

In 2017[5], a legislative reform provided for an administrative site blocking process that is overseen by the Hellenic Copyright Organisation (OPI).

The so-called "electronic e-commerce directive", as transposed into Greek law, states that illegal websites may be blocked by a public authority. In accordance with this provision, the new administrative blocking mechanism is covered by special copyright legislation. The public authority is involved from the notice and takedown stage, and may ultimately issue a blocking order against Internet service providers.

It is the OPI Committee for the Notification of Copyright and Related Rights Infringement on the Internet that handles procedures relating to the new system. The committee has three constituent members appointed for three years, each of whom has an alternate:

- the President of OPI (who chairs the committee),
- a representative of the Hellenic Telecommunications and Post Commission (Committee Secretary),
- a representative of the Hellenic Data Protection Authority.

Rightholders (including collective management organisations, trade unions and, apparently, holders of related rights in respect of sports broadcasts) may refer matters to the committee after unsuccessfully filing a takedown notice. To do this, they must submit a standard application form provided by the OPI, along with all the additional documents required by the committee.

The initial request may also include alternative domain names and potential future domain names.

The procedure before the committee ends automatically if legal proceedings are initiated on the same subject.

Within ten working days of receiving the referral, the committee examines its admissibility. The referral may be deemed inadmissible if it does not comply with the necessary formalities, if there is ongoing litigation, or if a final ruling has been made.

Where the referral is considered admissible, the committee contacts the administrators and/or owners of the services concerned. Where possible, the committee may also notify the hosting providers and, if the site is hosted abroad, the Greek Internet service providers.

The following information is included in the notification:

- a description of the disputed content;
- the legal provisions that have been breached;
- a summary of the facts and evidence attached to the referral;
- a statement of the adversarial principle, inviting the contentious service to produce - within five days - any relevant evidence that no offence has been committed;

*[4] copyrightschool.gr/index.php/en/*
*[5]LAW no. 4481 (OFFICIAL GOVERNMENT GAZETTE A 100/ 20.7.2017) Collective management of copyright and related rights, multi-territorial licensing in musical works for online use and other issues falling within the scope of the Ministry of Culture and Sport, Article 52.*

- the conditions under which the procedure may be terminated by the withdrawal of the disputed content or by the conclusion of voluntary agreements between the parties.

After the end of the objection period and in any event within 40 to 60 days of receiving the referral[6], the committee must make its decision and notify the stakeholders. The committee may rule that no offence has been committed. Otherwise:

- where the service is hosted in Greece, it may order the hosting provider to remove works in the event of isolated offences, or to stop hosting the website if it finds that massive infringement has occurred;
- where the service is hosted outside Greece, it may order Internet service providers to put an IP or DNS block on it, depending on which is the most appropriate and effective. The committee may also ask Internet service providers to redirect users attempting to access the blocked service to an on-screen information message. Greece is also setting up a portal containing links to legal offer, and could consider redirecting users to it.

In any case, the duration of the IP or DNS block is specified by the committee.

Addressees of the decision must remove or block access to the content within three working days of notification of the committee's decision. Should they fail to comply, the committee may fine them between 500 euros and 1,000 euros per day, depending on the seriousness and recurrence of the offence.

The decision may be appealed before the administrative courts.

Blocking costs are in principle borne by the Internet service providers[7]. However, the rightholders must pay the OPI for all costs relating to administrative blocking decisions, i.e. 372 to 1,240 euros depending on the type of block implemented (DNS or IP for live streaming if necessary) and the number of services/addresses to block (from 1 to 50).

The committee started operating in September 2018 and issued its first three decisions in November the same year[8].

*[6] N.B.: Each of the aforementioned deadlines can be extended twofold.*
*[7] www.opi.gr/index.php/en/committee/request-committee*
*[8] www.opi.gr/en/current-affairs1/news/9379-07-11-2018-decisions-of-the-committee-for-the-notification-of-copyright-and-related-rightsinfringement-on-the-internet*

# INDIA

## KEY FIGURES

KNOWN BLOCKING PROCEDURES (SINCE 2006)

**1** NUMBER OF PROCEDURES

**2** NUMBER OF SITES BLOCKED

**2** NUMBER OF DOMAIN NAMES BLOCKED

DEMOGRAPHY

**1339.2** POPULATION (2017) [1] *in millions*

**29.6%** INTERNET PENETRATION RATE (2017) [2]

INFRINGEMENTS [3]

**11.2** NUMBER OF VISITS TO ILLEGAL SERVICES (2017) *in billions*

**28** NUMBER OF VISITS TO ILLEGAL SERVICES PER END-USER (2017)

**Breakdown of infringements by access method (2017)**
*as a %*


**According to a report published in September 2017, 94% of end-users[4] have unlawfully downloaded music in the past six months and have used Google to find free music - in most cases from illegal sources[5]. Stream ripping services, which are very widespread in India, are also a major problem.**

**In 2017, the video game industry reported that India was the fifth country in the world for the number of shares on peer-to-peer networks. India also ranks second for the unlawful use of video games[6].**

**In response to the piracy problem, in May 2016 the Indian government adopted a national intellectual property rights policy with seven objectives[7], including:**

**raising awareness of intellectual property rights across society as a whole, adopting effective intellectual property laws, and modernising and strengthening dedicated government services and judicial procedures. These actions are to be carried out by various ministries, under the coordination of the Ministry of Trade and Industry.**

**India is a federal republic comprising 29 States and 7 Union territories[8]. Hence, the study of anti-piracy efforts - especially measures against infringing services - is complex and may vary from region to region.**

**Measures to prevent piracy by end-users consist essentially of criminal proceedings and awareness raising; however, legal action may also be taken against illegal websites on Common law grounds.**

*[1] United Nations Population Fund (UNFPA) – 2017.*
*[2] International Telecommunications Union (ITU) – 2017.*
*[3] MUSO - 2017.*
*[4]The "Badvertising Report" produced by Veri-Site reveals that piracy using mobile applications is also on the rise in India.*
*[5]KPMG LAIFC FICCI Report: The 'Digital First' journey: www.laindiafilmcouncil.org/og-content/uploads/documents/1507100573The%20Digital%20First%20journey_Print.pdf*
*[6]iipa.org/files/uploads/2018/02/2018SPEC301INDIA.pdf*
*[7]Press release "Cabinet approves National Intellectual Property Rights Policy", 13 May 2016, www.pib.nic.in/newsite/PrintRelease.aspx?relid=145338;*
*Link to the campaign video: www.youtube.com/watch?v=_-EDT4q_Vis*
*[8]The Union territories, unlike the states, are governed directly by the central government.*

# EDUCATIONAL AND ENFORCEMENT ACTIONS

## THE SYSTEM IMPLEMENTED BY THE POLICE SERVICES

The Cell for Intellectual Property Promotion and Management (CIPAM), which reports to the Department of Industrial Policy and Promotion (DIPP) at the Ministry of Trade and Industry, is in charge of anti-piracy operations.

In January 2017, the Minister of Trade and Industry announced that a tool kit had been created to help police officers across India deal with intellectual property crimes and infringements. The tool kit was developed by CIPAM, the Federation of Indian Chambers of Commerce and Industry, and various private-sector actors.

It is meant to be used in all officer training programs and includes a detailed explanation of each different type of infringement, a checklist for handling complaints and performing searches and seizures, and tips for carrying out searches efficiently.

CIPAM has also worked with rightholders, such as the MPA, to organise training courses for officers in local police academies.

## THE AWARENESS-RAISING SYSTEM

CIPAM is running a social media awareness campaign (with hashtag *#LetsTalkIP* for example), as well as intellectual property rights awareness workshops in schools and colleges.

In August 2017, CIPAM and DIPP organised the first national working group on intellectual property. One of the main communication tools was a video produced jointly by rightholders in the audiovisual sector (the Motion Picture Association - MPA), TV operator Viacom 18, and children's TV channel Nickelodeon[9]. The video features popular children's cartoon characters, who explain that piracy is theft.

The Minister of Trade and Industry unveiled a new anti-piracy campaign in May 2018. Substantial resources were invested in the campaign, which featured famous Bollywood actors[10] in YouTube videos for example. CIPAM and EUIPO are running a campaign aimed specifically at children, featuring a tech-savvy grandmother (IP Nani) who helps the government tackle piracy with the help of her grandson.

CIPAM also works with the National Council of Educational Research and Training to create teaching materials on intellectual property rights: as a result, high school text books contain units on intellectual property rights.

*[9]www.youtube.com/watch?v=_IBPnZweibU*
*[10]See for example www.youtube.com/watch?v=KcqnmXCNRXE*

# ANTI-COUNTERFEITING ACTIONS INVOLVING INTERMEDIARIES

## COURT DECISIONS REGARDING SITE BLOCKING

Rightholders may seek "John Doe" orders[11] against hosting providers where the website administrator is not known.

In 2016, in two separate cases[12], the Mumbai High Court granted "John Doe" orders to take down links at the request of rightholders. Rightholders must give public notification of the decision to the defendants, and allow them four days to lodge an appeal. The pages are blocked for 21 days at most, after which rightholders must refer the matter back to the court if they wish to extend the injunction. Hosting providers must create landing pages for blocked sites, explaining exactly why the site is blocked, providing the rights holder's address, and informing potential grievors that they may refer the matter to court. The Indian film industry uses these orders regularly and is particularly vigilant in the days prior to a film's release. The conditions for implementing such actions are similar to those governing interim proceedings.

In proceedings initiated by the Motion Picture Distributor's Association (MPDA) on behalf of all the studios, the Delhi High Court ordered in October 2017 that two websites be blocked in their entirety, on the grounds that they were structurally infringing. The court also agreed that the studios could update their applications to include sites that circumvent the blocking measures. Subsequently, 78% of Internet service providers complied with the ruling and rightholders reported an 89% decrease in total traffic to the sites.

## THE IMPLEMENTATION OF THE "FOLLOW THE MONEY" APPROACH

Drawing inspiration from PIPCU, the UK's Police Intellectual Property Crime Unit, the Indian authorities have set up cybercrime units in several states.

The Maharashtra state cybercrime unit was created in 2017. Modelled on PIPCU, it investigates suspected infringing websites in the light of various parameters before adding them to a list of sites to monitor.

It then gives formal notice to the websites and their partners to stop their illegal activities. Next, notifications are sent to advertising agencies asking them to stop collaborating with the sites.

At the same time, the unit sends a written complaint to Internet service providers and NIXI (the National Internet Exchange of India, which is responsible for registering local domain names ending with ".in"), asking them to stop providing services to the sites in question. Such requests from the police are based on the Code of Criminal Procedure, which allows preventive action to be taken when a crime is suspected.

NIXI suspends domain names engaged in piracy and verifies the information provided at registration, particularly e-mail addresses. Since June 2017, the unit has had over 25 domain names suspended under this procedure.

*[11] John Doe orders are a common law concept.*
*[12] Balaji Motion Pictures & Anr v Bharat Sanchar Nigam & Ors, and Eros International and Anr v BSNL & Others.*

# IRELAND

## KEY FIGURES

KNOWN BLOCKING PROCEDURES (SINCE 2006)

**4** NUMBER OF PROCEDURES

**13** NUMBER OF SITES BLOCKED

**589** NUMBER OF DOMAIN NAMES BLOCKED

DEMOGRAPHY

**4.8** POPULATION (2017) [1] *in millions*

**84.5%** INTERNET PENETRATION RATE (2017) [2]

INFRINGEMENTS [3]

**0.47** NUMBER OF VISITS TO ILLEGAL SERVICES (2017) *in billions*

**115** NUMBER OF VISITS TO ILLEGAL SERVICES PER END-USER (2017)

**Breakdown of infringements by access method (2017)** *as a %*


**Ireland's anti-piracy system combines an end-user warning procedure and a blocking mechanism. One of the specific features of the Irish system is that these measures may be implemented by different actors, either by virtue of a voluntary agreement or pursuant to a court order.**

## EDUCATIONAL AND ENFORCEMENT ACTIONS

### A GRADUATED WARNING SYSTEM IMPLEMENTED UNDER A BILATERAL VOLUNTARY AGREEMENT

In 2009, a confidential agreement was concluded between Ireland's main Internet service provider (Eircom) and the Irish Recorded Music Association (IRMA), whereby Eircom undertook to implement a graduated response system.

The Internet service provider issues e-mail warnings to subscribers upon receiving their IP address from IRMA. After three such warnings, the Internet service provider may suspend the subscriber's Internet connection for a period of seven days, without the need for court action. In the event of a repeat offence, the connection may be suspended for a year.

This system has not been implemented continuously; up until 2013, when it was definitively approved by Ireland's Supreme Court, it had been temporarily shelved several times due to legal uncertainties regarding

*[1] United Nations Population Fund (UNFPA) – 2017.*
*[2] International Telecommunications Union (ITU) – 2017.*
*[3] MUSO - 2017.*

personal data protection[4].

### THE EXTENSION OF THE SYSTEM PURSUANT TO A COURT ORDER

Rightholders in the music industry wanted to extend the graduated warning system to include other Internet service providers but, in the absence of a voluntary agreement, it was not possible to enforce its implementation until after the 2012 transposition of Article 8.3 of the InfoSocDirective (no. 2001/29/EC) of 22 May 2001, which allows injunctions to be issued against technical intermediaries whose services are used to infringe copyright or a related right.

The Irish court, in a case brought by music rightholders against the Internet service provider UPC (now Virgin), gave the parties time to reach an agreement. After this period, in the absence of agreement, the judge set out a broad outline of the system, subject to periodic review[5]:

- after sending three notifications to a subscriber, the Internet service provider must inform the rights holder of the situation;
- the rights holder may then refer the matter to the court to identify the end-user and request that his/her contract with the Internet service provider be terminated or that his/her Internet connection be suspended (unlike the agreement with Eircom, which does not involve recourse to the courts);
- rightholders are required to pay 20% of all investment expenses incurred by the Internet service provider when implementing the system: these expenses are, however, capped at 940,000 euros. Due to cost considerations, each Internet service provider is authorised to issue no more than 2,500 notifications per month.

Music rightholders have asked two other Internet service providers, Sky and Vodafone, to implement an identical procedure against their subscribers. However, they are refusing to cooperate until they have been ordered to do so by a court of law.

### THE PROMOTION OF LEGAL OFFER

The Industry Trust for Intellectual Property Awareness Ireland, a private organisation comprised of audiovisual actors and focused on promoting copyright and creativity, has launched a platform in Ireland[6] to raise awareness about copyright protection and the importance of using legitimate content sources to encourage creation.

The organisation, which also has a branch in England, has carried out various advertising campaigns in the past seven years, including “Moments worth paying for”. Supported by the film industry, its trailers are shown in Irish cinemas throughout the year[7].

## ANTI-COUNTERFEITING ACTIONS INVOLVING INTERMEDIARIES

### JUDICIAL BLOCKING OF WEBSITES AND THEIR AVATARS

The agreement between IRMA and Internet service provider Eircom also contains provisions enabling the implementation of blocking measures in the music industry. Thus, in 2009, Eircom was ordered to block the Pirate Bay website and its mirror and proxy sites. It was not until the copyright reform of March 2012, which transposed Article 8.3 of the aforementioned InfoSoc directive into Irish law, that rightholders were able to commence proceedings against uncooperative Internet service providers with a view to having certain websites blocked. Several injunctions have been issued since then, forcing Internet service providers

*[4]www.supremecourt.ie/Judgments.nsf/1b0757edc371032e802572ea0061450e/c9861b9cda79509b80257b9d004e9a7a?OpenDocument*
*[5]High Court (Commercial Division), Sony Music Entertainment (Ireland) Ltd & Ors -v- UPC Communications Ireland Limited (No. 1), 27 March 2015: www.courts.ie/Judgments.nsf/09859e7a3f34669680256ef3004a27de/84d0803d3bc9ae1c80257e5100477a3d?OpenDocument. High Court (Commercial Division), Sony Music Entertainment (Irl) Ltd & Ors -v- UPC Communications Irl Ltd (No 3), 17 June 2015: www.courts.ie/Judgments.nsf/0/0C6552224052C76680257E73004E15FB*
*[6]lovemovies.ie/*
*[7]www.industrytrust.co.uk/campaigns/moments/*

to block websites such as the Pirate Bay in June 2013[8] and KickassTorrents in December 2013. Two blocking orders were issued recently:

- On 3 April 2017, the members of the MPA (Motion Picture Association) got the eight largest Internet service providers in Ireland to block three infringing websites[9].
- In January 2018, eight massively infringing streaming and torrent sites[10] were also blocked in view of their large audiences and the presence of thousands of infringing files, and for reasons of "substantial public interest".

Since 2013, court decisions have expressly provided that Internet service providers shall subsequently block any sites circumventing the blocking orders by providing access to blocked sites, in accordance with a memorandum of understanding appended to the order.

In practice, rightholders regularly provide Internet service providers with an updated list of IP addresses and/or domain names that provide access to the content of blocked sites.

*[8]High Court (Commercial Division), 12 June 2013, EMI Records (Ireland) Limited, Sony Music and Entertainment (Ireland) Limited, Universal Music Ireland Limited and Warner Music Ireland Limited - v - UPC Communications Ireland Limited, Vodafone Ireland Limited, Imagine Telecommunications Limited, Digiweb Limited, Hutchinson 3G Ireland Limited, and by order of the Court Telefonica Ireland Limited. www.bailii.org/ie/cases/IEHC/2013/H274.html*
*[9]High Court (Commercial Division), 3 April 2017, Motion Picture Association v Eircom, Sky Ireland, Vodafone, Magnet Networks, Three Ireland, Three Ireland Services.*
*[10]High Court (Commercial Division), 15 January 2018, Motion Picture Association v Eircom, Sky Ireland, Vodafone Ireland, Virgin Media Ireland, Three Ireland, Digiweb, Imagine Telecommunications, Magnet Networks.*

# ITALY

## KEY FIGURES

KNOWN BLOCKING PROCEDURES (SINCE 2006)

**599** NUMBER OF PROCEDURES

**831** NUMBER OF SITES BLOCKED

**1003** NUMBER OF DOMAIN NAMES BLOCKED

DEMOGRAPHY

**59.4** POPULATION (2017) [1] *in millions*

**61.3%** INTERNET PENETRATION RATE (2017) [2]

INFRINGEMENTS [3]

**3.7** NUMBER OF VISITS TO ILLEGAL SERVICES (2017) *in billions*

**102** NUMBER OF VISITS TO ILLEGAL SERVICES PER END-USER (2017)

Breakdown of infringements by access method (2017) as a %


The *decreto legislativo* no. 70/2003 implementing the so-called Electronic Commerce Directive provides that both public and legal authorities may instruct hosting providers and Internet service providers to take any measures necessary to prevent or put an end to harm caused by the sharing of unlawful content via an online public communication service[4]. Therefore, there are two procedures that can lead to a website being blocked: an administrative procedure implemented by an independent authority, the *Autorità per le Garanzie nelle Comunicazioni* (AGCOM), and a judicial procedure.

At the same time, measures are being taken to make legal offer more visible: the Italian Cultural Industries Association (*Confindustria cultura*)[5] has created a portal that lists legitimate platforms in the main digital culture sectors.

The Italian system therefore focuses mainly on tackling illegal services. No punitive measures seem to have been put in place against end-users.

*[1] United Nations Population Fund (UNFPA) – 2017.*
*[2] International Telecommunications Union (ITU) – 2017.*
*[3] MUSO - 2017.*
*[4]As the judicial or administrative authority has oversight functions, it may urgently request that the service provider put an end to an infringement.*
*[5]www.mappadeicontuti.it*

# ADMINISTRATIVE BLOCKING OF ILLEGAL WEBSITES AND THEIR AVATARS

## INITIAL ARRANGEMENTS

### PRESENTATION OF THE REGULATORY AUTHORITY

An independent authority created in 1997, the *Autorità per le Garanzie nelle Comunicazioni* (AGCOM) performs regulatory and oversight functions in the electronic communications, audiovisual and publishing sectors.

AGCOM is funded primarily by contributions from regulated operators (in the electronic communications, audiovisual and postal sectors).

It has three hundred and sixty (360) full-time employees in seven cross-functional departments and five divisions specialising in particular areas of expertise.

AGCOM is a "convergent" authority which, since 2000, has played a steadily increasing role in copyright protection in sectors where it acts as guarantor and regulator (audiovisual, on-demand media services and electronic communications).

AGCOM is therefore responsible for developing and implementing measures against massively infringing sites. As such, on 12 December 2013 it adopted a regulation to protect copyright on electronic communication networks, which came into force on 31 March 2014.

Procedures before AGCOM are brought to an end if legal proceedings are initiated on the same subject: in this event, AGCOM forwards all information in its possession to the court.

### TAKEDOWN OR ADMINISTRATIVE BLOCKING PROCEDURES

Rightholders may apply to AGCOM to enforce the takedown of content published on the Internet without authorisation.

AGCOM informs the website of the rights holder's application and invites it to voluntarily remove the content and to submit any observations within five days. AGCOM also informs Internet service providers and hosting providers when the procedure begins (i.e. the intermediaries referred to in the e-commerce directive).

If the website fails to cooperate, AGCOM has thirty-five days to rule on the rights holder's application.

The regulation to protect copyright on electronic communication networks provides for a twelve-day abridged procedure in the event of "massive infringements". An infringement is considered massive when a website contains around 30 illegal works.

AGCOM's board can either terminate the procedure or find that copyright or a related right has been infringed. The recognition of a related right for sports broadcasts enables AGCOM to order blocking measures against live streaming sites. Blocking orders may also be issued against stream ripping sites.

In accordance with the principle of proportionality, AGCOM issues orders against:

- *hosting providers when the server hosting the contested website is located in Italy. The board may order that the works in question be removed, or prevent access to them in the event of a large-scale infringement;*
- *Internet service providers when the server hosting the works is located outside Italy. The board may order Internet service providers to place a DNS or IP block on an entire site. In practice, only DNS blocking decisions are issued. The financial burden of blocking operations lies with the Internet service providers.*

When the board issues an injunction to take down works or block a website, it may require that end-users attempting to access the blocked pages or website be automatically redirected to a message from AGCOM explaining the measures it has ordered.

AGCOM may impose administrative sanctions in the event of non-compliance with its decisions. The decisions made by AGCOM may be appealed to a judicial body.

As at 30 November 2018, AGCOM had issued 598 injunctions.

## EXTENSION OF AGCOM'S POWERS TO INCLUDE "FLAGRANT INFRINGEMENTS" AND "POTENTIAL REPEAT OFFENCES"

AGCOM's powers were extended under Article 2 of the law of 20 November 2017 transposing Article 8 of Directive 2001/29/EC on copyright, and Articles 3 and 9 of Directive 2004/48/EC on the enforcement of intellectual property rights. The authority may now issue urgent orders to information society service providers to stop flagrant copyright infringements (after a brief assessment of the facts) and remove the threat of imminent harm.

On 16 October 2018, AGCOM adopted a regulation detailing the practical implementation of its orders and the measures required to prevent infringements from recurring.

### EMERGENCY MEASURES

Where there is a risk of imminent harm, the authority may either instruct hosting providers to remove infringing works as a matter of urgency, or order a blocking measure.

Such measures must be taken within three days of the rightholders' referral.

Where the person who published the content online and/or the website manager is contactable, they are also notified of the order and have five days to oppose the decision.

In the event of an appeal, AGCOM's board reaches a decision within seven days.

### POTENTIAL REPEAT OFFENCES

With regard to infringements that have already been the subject of an AGCOM injunction in the past, it is provided that, following the rightholders' referral, the authority will verify that a repeat offence has occurred. In the consultation document drawn up prior to the adoption of the aforementioned regulation, AGCOM provided a description of the method it uses to assess repeat offences.

- *In the event of infringements that have already been the subject of a takedown order against the hosting providers in the past, AGCOM verifies that exactly the same content has effectively reappeared.*
- *In the event of infringements that have already been the subject of a blocking order against a hosting provider or an Internet service provider in the past, AGCOM analyses the similarities between the domain names, the IP address and the structure of the websites.*

If the previous infringement resulted in an injunction against the hosting providers, AGCOM imposes a penalty on them and informs the Criminal Investigation Department. If the previous infringement resulted in an injunction against the Internet service providers, AGCOM provides the latter with a list of new sites to block.

# LEGAL PROCEEDINGS AGAINST ILLEGAL SITES AND WORKAROUND SITES

The Italian system provides for an alternative procedure before the court, which renders any proceedings before AGCOM null and void.

Within this framework, the customs and finance police (*Guardia di Finanza)* has powers to investigate, monitor and punish online infringements. It may submit cases to the courts, which may implement blocking measures against the sites.

In 2016, the *Guardia Di Finanza* developed two different approaches to make its actions more effective. The first is a "follow the money" approach, which does not involve cutting off the funding of infringing sites, but is designed to trace and identify the managers of such sites through investigations conducted by local online advertisers.

The second approach, which is known as the "follow the hosting" approach, enables the true location of websites to be identified. Some sites using anonymisation techniques to make it seem that they are based abroad when they are, in fact, managed from Italy.

Since 2016, the activities of the *Guardia di Finanza* have been stepped up considerably, with the result that several content hosting sites have been blocked.

As concerns websites commonly referred to as mirrors, on 12 April 2018, the Court of Milan ruled that the obligation for Internet service providers to block access to content

already recognised by a court as illegal upon simple notification by the rightholders and without the need for a further court decision is compatible with Article 15 of the Electronic Commerce Directive, whereby *"Member States shall not impose a general obligation on providers [...] to monitor the information which they transmit or store, nor a general obligation actively to seek facts or circumstances indicating illegal activity*".

In July 2017, in a case brought by publishing group Mondadori, the Court of Milan ordered Italy's main Internet service providers to block access to "dasolo.org" and to websites with a similar domain name.

Following the transfer of unlawful content to a website with a completely different domain name ("italiashare.info"), the court was again seized of the matter. It ruled the Mondadori group's requests admissible and ordered the Internet service providers to set up a proactive system.

The latter must therefore block access to unlawful content at the rightholders' request; this applies to all websites which, regardless of their domain name, commit the same infringements as those noted in the initial decision.

# JAPAN

## KEY FIGURES

### DEMOGRAPHY

**127.5** POPULATION (2017) [1] *in millions*

**90.9%** INTERNET PENETRATION RATE (2017) [2]

### INFRINGEMENTS [3]

**4.8** NUMBER OF VISITS TO ILLEGAL SERVICES (2017) *in billions*

**42** NUMBER OF VISITS TO ILLEGAL SERVICES PER END-USER (2017)

Breakdown of infringements by access method (2017) as a %


Japan takes very tough measures against end-users but they are highly targeted and affect only a small number of people.

In March 2018, the Japanese government's spokesperson announced that it was considering taking measures to prevent access to illegal sites and hence reinforce existing arrangements.

## EDUCATIONAL AND ENFORCEMENT ACTIONS

### POLICE ACTIONS

Counterfeiters who publish copyrighted works online are dealt with by the Japanese police. The penalties incurred for sharing such works are ten years in prison and/or a fine of ten million Japanese yen (approximately €80,000).

In February 2016, the Japanese police arrested 44 people suspected of being involved in sharing works online. In various cases in 2017, the Japanese police arrested several people involved in running websites with links to Manga and books.

### END-USERS WARNING SYSTEM

In 2010, a private group composed of rightholders and the main Internet service providers (the Consortium against Copyright Infringement via File-Sharing Software - CCIF) introduced a warning system for end-users on peer-to-peer networks. The rightholders report incidents of illegal file sharing to the Internet service providers. The Internet service provider then sends an e-mail to the user, asking him or her to delete the illegally shared file. Ultimately, users who continue to share works may be investigated by the police and arrested.

*[1] United Nations Population Fund (UNFPA) – 2017.*
*[2] International Telecommunications Union (ITU) – 2017.*
*[3] MUSO - 2017.*

## AWARENESS-RAISING ACTIONS

The music sector has created a label called "L mark" to help end-users recognise legitimate offers.

Furthermore, in July 2014, the Japanese Ministry of Economy, Trade and Industry (METI), the Japanese Content Overseas Distribution Association (CODA) and the Manga industry launched a project to tackle Manga piracy.

As part of the project, a website has been created that lists Manga available legally online[4].

In March 2018, a public awareness campaign was launched in collaboration with the Chinese and Korean governments to protect popular Manga and Anime characters. Posters and videos are being circulated on platforms such as YouTube, and there are plans to circulate them in schools.

However, according to the headquarters of the intellectual property strategy office[5], it is difficult to raise public awareness without disclosing and thereby publicising the names of illegal sites.

# ANTI-COUNTERFEITING ACTIONS INVOLVING INTERMEDIARIES

## BLOCKING MEASURES

As part of the *Manga-Anime Guardians antipiracy project*, measures have been taken to improve *notice and takedown* procedures. However, given the sheer scale of the piracy problem, they have been deemed inadequate to tackle websites that publish Manga without the authorisation of rightholders.

On 13 April 2018, the Japanese government urged Internet service providers to block websites that infringe copyright and, more specifically, the rights of the Manga and Anime industries, pending the development of a mechanism to prevent access to illegal sites in 2019.

The Japanese government has stressed that these are temporary measures, warranted by the harm caused to rightholders by illegal sites. It is calling for cooperation from Internet service providers, which have already been working with the authorities since 2011 to block access to child pornography websites.

Japan's Internet service providers have voluntarily agreed to put DNS-type blocks on two of the main sites targeted by the government, and have undertaken to block access to other sites at the government's request.

According to the government, these are emergency blocking measures based on the Japanese penal code, which provides that direct action may be taken to *"avert a present danger"*[6].

These measures are highly controversial, since the Japanese Constitution[7] and the Telecommunications Business Act include provisions that protect freedom of expression and expressly prohibit censorship. Critics argue that blocking even infringing sites is illegal. Furthermore, the emergency blocking measures are based on the rule of penal law whereby "*where such an act causes excessive harm, it may lead to a reduction of sentence or exoneration of the offender in light of the circumstances",* which could in this case produce the opposite effect to that intended.

A customer of one of Japan's leading Internet service providers has taken legal action to stop it from implementing blocking measures on the grounds that they breach

*[4]manga-anim-here.com/*
*[5]Cabinet Office's Intellectual Property Strategy Headquarters.*
*[6]Article 37 of the Japanese Penal Code defines the prevention of a present danger as "An act unavoidably performed to avert a present danger to the life, body, liberty or property of oneself or any other person, [which] is not punishable when the harm produced by such act does not exceed the harm to be averted; provided, however, that an act causing excessive harm may lead to the punishment being reduced or may exculpate the offender in light of the circumstances".*
*[7]Article 21 of the Japanese Constitution provides that "freedom of assembly and association as well as speech, press and all other forms of expression are guaranteed […] no censorship shall be maintained, nor shall the secrecy of any means of communication be violated".*

communications confidentiality and the subscription contract, which does not stipulate that Internet service providers may arbitrarily suspend their subscribers' communications.

## THE IMPLEMENTATION OF THE "*FOLLOW THE MONEY*" APPROACH

In February 2018, nine rightholders' associations and three advertising networks established - with the support of the Japanese government – a non-public list of infringing websites to dry up part of their income. The list, which is updated quarterly, is intended for the signatory advertising networks and is used to remove ads placed on the sites by traditional advertisers.

As of 30 September 2018, it included 26 URLs.

There are several alternative criteria for adding a site to the list:

- *it must have received more than 50 takedown notices or offered more than 50 unlawful content items or links over a period of three months;*
- *it does not provide any information to rightholders that could enable them to issue takedown notices, or it responds to less than 70% of takedown notices from rightholders.*

# NEW ZEALAND

## KEY FIGURES

### DEMOGRAPHY

**4.7** POPULATION (2017) [1]
*in millions*

**88.5%** INTERNET PENETRATION RATE (2017) [2]

### INFRINGEMENTS [3]

**0.80** NUMBER OF VISITS TO ILLEGAL SERVICES (2017)
*in billions*

**193** NUMBER OF VISITS TO ILLEGAL SERVICES PER END-USER (2017)

Breakdown of infringements by access method (2017) as a %


In 2011, New Zealand adopted a 'three-strike' graduated response system, which has now been scrapped.

As yet, New Zealand appears to have few tools at its disposal for tackling infringing services.

## EDUCATIONAL AND ENFORCEMENT ACTIONS

In 2011, New Zealand introduced legislation to combat illegal file sharing on peer-to-peer networks.

Under the procedure, rightholders could report copyright infringements to Internet service providers. The latter then sent notifications to the concerned end-users. After three notifications had been sent, rightholders could take legal action to obtain compensation.

The court could impose a fine of up to NZ$15,000 (approximately €9,760).

In practice, only the music sector made use of the system. The audiovisual sector in particular deemed it too expensive (NZ$25 per notification, i.e. approximately €16). The Recording Industry Association of New Zealand (RIANZ - now Recorded Music NZ) had notifications issued from 2011 to mid-2016.

A total of 15,500 notifications were sent by music rightholders, 51 end-users were prosecuted and 21 cases tried.

Rightholders chose to stop using the graduated response system mainly due to the excessive cost and the decline in peer-to-peer activities.

With regard to law enforcement action against illegal services, Sky TV took action against two companies in 2017 (My Box and FibreTV NZ), which sell pre-loaded set-top boxes for piracy purposes. In July 2018, Sky won its case against FibreTV NZ.

*[1] United Nations Population Fund (UNFPA) – 2017.*
*[2] International Telecommunications Union (ITU) – 2017.*
*[3] MUSO - 2017.*

# ANTI-COUNTERFEITING ACTIONS INVOLVING INTERMEDIARIES

A draft reform aimed at combating infringing sites is currently being considered by the New Zealand government.

Meanwhile, rightholders are complaining that there is nothing in their *legal corpus* that expressly allows intermediaries to be asked to block a website.

# THE NETHERLANDS

## KEY FIGURES

### KNOWN BLOCKING PROCEDURES (SINCE 2006)

**1** NUMBER OF PROCEDURES

**1** NUMBER OF SITES BLOCKED

**255** NUMBER OF DOMAIN NAMES BLOCKED

### DEMOGRAPHY

**17** POPULATION (2017) [1] *in millions*

**93.2%** INTERNET PENETRATION RATE (2017) [2]

### INFRINGEMENTS [3]

**1.9** NUMBER OF VISITS TO ILLEGAL SERVICES (2017) *in billions*

**122** NUMBER OF VISITS TO ILLEGAL SERVICES PER END-USER (2017)

Breakdown of infringements by access method (2017) as a %


In the Netherlands, anti-piracy activities are conducted primarily by rightholders via the *Bescherming Rechten Entertainment Industrie Nederland (Stichting* BREIN), an anti-piracy association made up of rightholders from all sectors of the entertainment industry.

The *Stichting* BREIN takes action against both end-users and illegal services. According to its 2016 annual report[4], the Stichting BREIN carried out the following actions in 2016:

- *it conducted 26 cases against uploaders, resulting in financial settlements ranging from €4,800 to €15,000;*
- *it had 231 sites or services shut down, mainly with the cooperation of Dutch hosting providers;*
- *It had 14 Facebook groups shut down for sharing copyrighted works, including a secret Facebook group dedicated exclusively to sharing e-books. The operators ultimately settled for a sum of €7,500 and agreed, under financial compulsion, to cease infringing copyright.*

## EDUCATIONAL AND ENFORCEMENT ACTIONS

In the Netherlands, rightholders have put in place an indemnity scheme based essentially on compromising with end-users who share large volumes of content.

*[1] United Nations Population Fund (UNFPA) – 2017.*
*[2] International Telecommunications Union (ITU) – 2017.*
*[3] MUSO - 2017.*
*[4]Stichting BREIN 2016 Annual Report: www.stichtingbrein.nl/artikelen.php?id=27*

## INDEMNIFICATION NOTICES

The *Stichting* BREIN conducts actions against end-users who share large volumes of content through various channels (Facebook groups, YouTube channels, cyberlockers, Usenet, peer-to-peer software, etc.). The *Stichting* BREIN has also developed dedicated software to identify the IP addresses of *primo uploaders* and/or major *uploaders*, particularly on peer-to-peer networks.

The aim is to conclude settlement agreements with the counterfeiters or, failing that, to press charges against them. Settlement agreements relating to previous infringements may also require end-users, under financial compulsion, to cease infringing copyright in the future. Under such agreements, *uploaders* may, for example, be required to publish or send messages along the following lines: "*Unauthorised sharing and downloading are illegal and cost the creative industry a lot of money*".

The *Stichting* BREIN negotiates these agreements directly with end-users, through its advisers. In its 2016 annual report, it explains that its settlement demands are based on German practice. It seems, however, that the sums obtained by rightholders in the Netherlands are higher, perhaps because they target large-scale uploaders whereas their German counterparts generally issue formal notices concerning just one protected work. An end-user who has shared twelve episodes of a TV series using Torrent software would be fined €400 per episode, i.e. a total of €4,800.

The personal data protection authority approved the new software in 2016; however, it stipulated that the *Stichting* BREIN must use it to promote the upcoming campaign against large-scale uploaders. The *Stichting* BREIN therefore published a press release on social media, explaining that the large-scale *uploaders* it was likely to target included both those who share thousands of works and those who regularly share recent content. Following the campaign, which coincided with the closure of the *KickassTorrents* website, the *Stichting* BREIN reportedly observed a significant decrease in the number of uploaders detectable by the software.

Dutch legislation does not provide for any financial compensation to Internet service providers for processing IP address identification requests. On the other hand, many Internet service providers still require a court order before providing identification data to rightholders.

Some rightholders (including film distributor Dutch FilmWorks) would like to claim compensation not only from large-scale uploaders but from all end-users who share content illegally on peer-to-peer networks. At the end of 2017, the personal data protection authority authorised rightholders to collect personal data for such purposes. Rightholders may simply send a warning to end-users; or they may make a compensation claim which, if unsuccessful, may lead to legal action. Where no action is taken to identify the owner of an IP address, that address must be deleted within three months. Other data may be kept for five years[5].

Government-backed talks between Internet service providers and rightholders are also taking place, with the aim of reaching an agreement on setting up a warning system that does not impose sanctions but sends an information message to end-users who share works illegally on peer-to-peer networks. One Internet service provider has already announced publicly that it will not cooperate with the *Stichting* BREIN in sending warning messages to its subscribers.

## THE PROMOTION OF LEGAL OFFER

In February 2017, after creating a portal with links to legal online offer[6], the film industry developed a search engine that directs end-users looking for a specific audiovisual work to legal offer[7].

This search engine is unique in that it also targets end-users looking to access a work illegally. Indeed, the description of each work includes key words such as "torrents" or "illegal download", so that end-users who enter these words into a search engine can be redirected to legal offer.

[5] autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/besluit_online_handhaving_auteursrechten_dfw.pdf
[6] www.thecontentmap.nl/
[7] www.film.nl/

The description of the work also includes a message to deter end-users from accessing infringing content, for example "*Do not download illegal content. Look for legal offer, it's safe and fast too*".

### ACTIONS AGAINST VENDORS OF PRE-LOADED SET-TOP BOXES

The *Stichting* BREIN has initiated a series of actions against companies that sell pre-loaded set-top boxes for piracy purposes.

Asked for a preliminary ruling, the CJEU held that the marketing of such devices is an act of communication to the public that must be authorised in advance[8], otherwise it constitutes a copyright infringement.

Following this decision, more than 170 companies engaged in this illegal ecosystem were ordered to cease their activities at the request of the *Stichting* BREIN. In October 2017, a company that had developed an interface with a link enabling users to configure Kodi for unlawful purposes, and also offered illegal access to a package of TV channels on a dedicated website, was ordered to cease its activities under penalty of €5,000 per day. The Dutch court held that the link basically allowed end-users to access illegal content, and was in itself an unlawful act of communication to the public.

In May 2018, the *Stichting* BREIN obtained a similar ruling against a company selling packages of illegally available TV channels.

## ANTI-COUNTERFEITING ACTIONS INVOLVING INTERMEDIARIES

### BLOCKING MEASURES

In 2015, the Dutch Supreme Court requested a preliminary ruling from the CJEU[9] to determine whether torrent site the Pirate Bay infringed copyright itself and, if not, whether it could still be blocked.

The court[10] ruled on 14 June 2017 that: *"making available and managing an online platform for sharing copyrighted works, such as the Pirate Bay, may constitute an infringement of copyright"* and that the Pirate Bay may be held liable for listing links to torrent files.

Following this decision, the *Stichting* BREIN obtained a court order for temporary blocking measures[11].

### THE IMPLEMENTATION OF THE "*FOLLOW THE MONEY*" APPROACH

The *Stichting* BREIN works with payment intermediaries and the online advertising industry, and instructs them to stop providing services to infringing sites.

### ACTIONS AGAINST ILLEGAL *LIVE STREAMING* AND THE PRE-LOADED SET-TOP BOX ECOSYSTEM

In January 2018, the Court of The Hague granted the English Premier League an injunction against Dutch hosting provider Ecatel, to stop it providing services that enable the illegal viewing of Premier League matches. Ecatel must respond to takedown notices from the Premier League within 30 minutes.

However, the ban is temporary and services may resume at the end of the match. The ruling follows numerous takedown notices that Ecatel ignored, and is based on the Premier League's intellectual property rights over match broadcasts. The practical significance of the ruling is however tempered by the fact that Ecatel no longer existed at the time it was issued. Nevertheless, the principle behind it is a major victory for the rightholders.

[8] CJEU, 26 April 2017, C-527/15, Stichting Brein v Jack Frederik Wullems, known as "Filmspeler".
[9] Supreme Court of the Netherlands, 13 November 2015, Hoge Raad der Nederlanden, Stichting Brein v Ziggo BV, XS4All Internet BV: www.uitspraken rechtaak.nl/inziendocument?id=ECLI:NL:HR:2015:3307
[10] CJEU, 14 June 2017, C-610/15 - Stichting Brein/Ziggo BV, XS4All Internet BV referred to as "The Pirate Bay".
[11] A first decision in September 2017 ordered these measures against the two main Internet service providers; a second decision in January 2018 ordered the same measures against other ISPs.

# PERU

## KEY FIGURES

KNOWN BLOCKING PROCEDURES (SINCE 2006)

**1** NUMBER OF PROCEDURES

**1** NUMBER OF SITES BLOCKED

**1** NUMBER OF DOMAIN NAMES BLOCKED

DEMOGRAPHY

**32.2** POPULATION (2017) [1] *in millions*

**48.7%** INTERNET PENETRATION RATE (2017) [2]

INFRINGEMENTS [3]

**1.3** NUMBER OF VISITS TO ILLEGAL SERVICES (2017) *in billions*

**83** NUMBER OF VISITS TO ILLEGAL SERVICES PER END-USER (2017)

Breakdown of infringements by access method (2017) as a %


Millions of Peruvian users consume cultural goods illegally every month[4]. At the anti-piracy summit in Lima in October 2017, industry leaders estimated that, in Peru, unlawful consumption generates economic losses of over US$ 150 million, or more than €131.7 million.

The Peruvian authorities have responded by shutting down websites based in Peru, arresting their administrators and instituting proceedings against illegal sites.

## EDUCATIONAL AND ENFORCEMENT ACTIONS

### CRIMINAL LAW PROVISIONS

A rights holder filed a complaint with the special prosecution office for intellectual property crime in Lima, on the grounds that three websites were making films and TV shows available to the public without its authorisation.

On 8 September 2017, the judge granted a search warrant for the suspects' homes and workplaces and authorised their arrest. The prosecution office conducted the investigation with the high-tech crimes division. The warrant also permitted the confiscation of material goods and domain names.

The sites were immediately shut down. At the same time, banners were posted online, advising users that the domain names had been

*[1] United Nations Population Fund (UNFPA) – 2017.*
*[2] International Telecommunications Union (ITU) – 2017.*
*[3] MUSO - 2017.*
*[4] Source: Study conducted in January 2016, "South America Television Piracy Landscape For Alianza Contra La Piratería de Televisión Paga".*

suspended by order of the Second Criminal Court of Lima specialised in intellectual property, and the special prosecution office for intellectual property crime in Lima.

This decision was a first in Peru and was unprecedented in criminal cases: the judge recognised that making protected content available to the public without the rights holder's consent is illegal, and the websites' advertising revenue was a sufficient demonstration of intent.

## ANTI-COUNTERFEITING ACTIONS INVOLVING INTERMEDIARIES

In Peru, the fight against online counterfeiting is led by the National Institute for the Defence of Free Competition and the Protection of Intellectual Property[5] (INDECOPI), an independent public authority that reports to the Prime Minister's office and is responsible for handling disputes concerning copyright and related rights.

INDECOPI recently urged GoDaddy – a large, US-based domain name registry – to suspend the domain names of infringing sites.

In March 2018, the Peruvian Union of Phonogram Producers initiated a dispute against four websites that were making music content available without the rightholders' consent. In May 2018, it initiated a second dispute against five websites on the same grounds. An investigation found, firstly, that both websites generated advertising revenue and, secondly, that both were causing irreparable harm to the rightholders.

INDECOPI issued precautionary measures requiring GoDaddy to suspend the domain names of the contentious websites.

GoDaddy immediately suspended the domain names and did not appeal the decisions.

[5]Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual.

# PORTUGAL

## KEY FIGURES

KNOWN BLOCKING PROCEDURES (SINCE 2006)

**32** NUMBER OF PROCEDURES

**944** NUMBER OF SITES BLOCKED

**1314** NUMBER OF DOMAIN NAMES BLOCKED

DEMOGRAPHY

**10.3** POPULATION (2017) [1] *in millions*

**73.8%** INTERNET PENETRATION RATE (2017) [2]

INFRINGEMENTS [3]

**1.1** NUMBER OF VISITS TO ILLEGAL SERVICES (2017) *in billions*

**139** NUMBER OF VISITS TO ILLEGAL SERVICES PER END-USER (2017)

**Breakdown of infringements by access method (2017)** *as a %*


In Portugal, a website blocking system is implemented under a Memorandum (MoU) concluded in July 2015 between the Inspectorate General of Cultural Affairs[4] (IGAC, which reports to the Ministry of Culture), the Portuguese Association of Telecommunications Operators (APRITEL), rightholders association MAPINET (a cross-sector piracy prevention organisation), the Consumer Directorate-General, advertising industry representatives, and the Portuguese organisation that manages domain names ending in ".pt".

The MoU also provides for the creation and administration of a legal content aggregator[5] by the Portuguese registry. The Portuguese aggregator was created as part of the EUIPO project to develop a pan-European legal content aggregator (Agorateka). The first phase of the project consisted in helping pilot countries like Portugal create their own aggregators, before setting up a European portal connecting all the national aggregators together.

## THE ADMINISTRATIVE BLOCKING OF INFRINGING SERVICES

The Portuguese legislation transposing Directive 2000/31/EC of 8 June 2000, referred to as the "e-commerce" directive, provides that the public authority may establish a copyright infringement during an interim dispute settlement process and instruct Internet service providers to block the website concerned.

*[1] United Nations Population Fund (UNFPA) – 2017.*
*[2] International Telecommunications Union (ITU) – 2017.*
*[3] MUSO - 2017.*
*[4] IGAC specialises in the protection of copyright and related rights, and reports to the Ministry of Culture. One of its main tasks is to register works and supervise collective management organisations.*
*[5]www.ofertaslegais.pt/na*

However, a court order is required[6] to enforce such measures.

In this context, the procedure put in place by the MoU consists of five stages.

- Firstly, MAPINET notifies the platform of the illegal content and requests its removal. At this stage, the MoU targets services specialised in communicating copyrighted works to the public. The MoU does not cover stream ripping services.
- Only if the platform fails to respond or responds negatively does MAPINET collect evidence of its illegal activities and refer the matter to IGAC. The MoU provides that, for each site reported to IGAC, rightholders must demonstrate either that it provides access to at least 500 protected works, or that more than 2/3 of the content hosted is infringing.
- Once IGAC has been seized of the case, it performs a quick sampling inspection of each site. If a site proves to be massively infringing, IGAC instructs Internet service providers to block it (DNS block).
- Internet service providers have fifteen days to block the website. They bear the cost of blocking orders, although the MoU makes provision for the costs to be shared. They post a message advising users that the site has been blocked by IGAC.
- IGAC must then forward all files relating to the blocked services to the prosecutor, as Portuguese law contains a provision equivalent to Article 40 of the French Code of Criminal Procedure, whereby the public authorities must report all crimes and offences of which they are aware. In practice, only services that can be prosecuted in Portugal - bearing in mind the location of their administrators - are reported to IGAC.

Blocking measures are enforced for a period of one year. At the end of this period, rightholders must make a new blocking request. It is therefore difficult to update blocking requests before the one-year period is up.

One of the challenges that Internet service providers faced when the MoU was drawn up was not so much limiting the number of websites to block, but streamlining the processing of blocking requests to minimise the impact and avoid having to create a dedicated team.

In view of this consideration, the MoU provides that rightholders must pool their blocking requests through MAPINET and submit them no more than twice a month (at the beginning of the month and on the 15th of the month). Each request must relate to at least fifty new sites. In practice, rightholders submit requests just once a month, for at least fifty sites.

There is no specific procedure for blocking workaround services but, as the standard blocking procedure is relatively fast, such services can be reported to IGAG monthly when MAPINET submits its requests. Rightholders provide IGAC with the same evidence for a workaround service as they do for the original site.

As of 1 January 2019, sports content, which is protected by intellectual property law in Portugal, may also be subject to DNS blocking measures under the MoU. Websites that make sports content available without authorisation may therefore be subject to live blocking measures during the television broadcasting of sports events.

*[6]DL no. 7/2004 of 7 January, COMÉRCIO ELECTRÓNICO NO MERCADO INTERNO E TRATATAMENTO DE DADOS PESSOAIS, Art. 18.*

# UNITED KINGDOM

## KEY FIGURES

KNOWN BLOCKING PROCEDURES (SINCE 2006)

**23** NUMBER OF PROCEDURES

**175** NUMBER OF SITES BLOCKED

**2335** NUMBER OF DOMAIN NAMES BLOCKED

DEMOGRAPHY

**66.2** POPULATION (2017) [1] *in millions*

**94.8%** INTERNET PENETRATION RATE (2017) [2]

INFRINGEMENTS [3]

**6.3** NUMBER OF VISITS TO ILLEGAL SERVICES (2017) *in billions*

**100** NUMBER OF VISITS TO ILLEGAL SERVICES PER END-USER (2017)

**Breakdown of infringements by access method (2017)** *as a %*


The United Kingdom has many, often innovative, anti-piracy tools. The situation there is unique in that Internet service providers work closely with rightholders and are often rightholders themselves.

The UK system includes measures to deal with end-users who share works illegally on peer-to-peer networks, which essentially consist of promoting and raising awareness of legal offer and conducting educational e-mail campaigns.

As regards the involvement of intermediaries in anti-counterfeiting efforts, the United Kingdom endeavours to use all available levers: implementation of the so-called “follow the money approach”, government-backed agreements between rightholders and search engines, dynamic blocking orders from the courts and, more recently, **live blocking** injunctions to tackle the widespread use of pre-loaded set-top boxes for piracy purposes and, in particular, the illegal viewing of pay-TV channels (especially sports broadcasts) online.

The **Performing Right Society (PRS for music)**, which collects royalties for the music sector, has published figures[4] on the blocking of massively infringing sites from March 2016 to March 2017. PRS reports that since March 2016, 136,000 takedown notices have been issued, 220 sites have been shut down and 275,000 URLs have been delisted from Google UK's search pages. The number of music tracks accessed illegally online fell from 96 million in 2015 to 78 million in 2016, over a similar three-month period (from March to May).

A study conducted by American university **Carnegie Mellon**[5] in April 2016 shows that the blocking of numerous websites in November 2014 led to an increase of around 6% in the use of legal streaming sites such as Netflix.

*[1] United Nations Population Fund (UNFPA) – 2017.*
*[2] International Telecommunications Union (ITU) – 2017.*
*[3] MUSO - 2017.*
*[4] www.billboard.com/articles/business/7727667/prs-for-musics-new-anti-piracy-platform-proves-effective*
*[5] Website Blocking Revisited: The Effect of the UK November 2014 Blocks on Consumer Behavior, Brett Danaher, Michael D. Smith, Rahut Telang, 18 April 2016.*

A 90% drop in visits to the blocked sites was also observed, with no concomitant increase in the use of unblocked sites. However, visits to sites providing connection anonymisation tools (VPNs) surged.

In September 2017, the IPO and the **IP Crime Group** published their annual "IP Crime and Enforcement" report[6]. According to the report, copyright convictions fell from 69 in 2015 to 47 in 2016. Site blocking has been a success: 63 websites and 700 related URLs have been blocked, and traffic to these sites has fallen by 70%.

Nevertheless, the government is working with stakeholders to make blocking measures more effective. In its four-year strategy to prevent online counterfeiting[7], the UK government proposes to facilitate judicial site blocking proceedings. To do this, it aims to establish detailed information on the minimum evidence needed to have a website blocked, and on the international cooperation arrangements required to tackle websites that are hosted in one country and target audiences in another.

At the same time, the possibility of introducing administrative blocking is being explored. In a report entitled "Industrial Strategy: Creative Industries Sector Deal", the government announced that a study will be published in 2019 on the possibility of implementing administrative blocking measures against massively infringing sites. It will consider the evidence for such a system, its potential impact, and how it could be incorporated into the legal corpus.

# EDUCATIONAL AND ENFORCEMENT ACTIONS

## TOUGHER PENALTIES FOR ONLINE COPYRIGHT INFRINGEMENT

The Digital Economy Act 2017, which came into force in April 2017, amended the maximum custodial sentence for online copyright infringement and states that a person who infringes copyright has committed an offence if he or she knows or has reason to believe that such infringement will cause loss to the rights holder. The sentence has increased from two to ten years, bringing it into line with provisions for physical counterfeiting. The possibility of aligning the sanctions for copyright infringement and physical counterfeiting had been under discussion since 2014[8].

## INDEMNIFICATION NOTICES

Rightholders may petition a court[9] to obtain the identity of an end-user who has shared cultural content illegally, and whose IP address has been used on peer-to-peer networks. Once the user's contact details have been obtained, the rightholders may send him or her a letter claiming financial compensation. Otherwise, it is stated that the end-user may be prosecuted.

In practice, the system is mainly used by rightholders in the pornography sector.

In 2012, the "Golden Eye" ruling (named after a pornographic film-maker) provided a framework for such action and specified that[10]:

*[6] "IP Crime and Enforcement: Report 2016/17", IP Crime Group, Intellectual Property Office, 7 September 2017, assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/642324/IP_Crime_Report_2016_-_2017.pdf*
*[7] "IP enforcement 2020" Protecting Creativity, supporting innovation, IPO, May 2016.*
*[8]Martin Brassell FRSA, Dr Ian Goodyer, Inngot Limited, "Penalty fair? Study of criminal sanctions for copyright infringement under the CDPA 1988", Intellectual Property Office, February 2015.*
*[9]According to a common law scheme called Norwich Pharmacal Order.*
*[10]High Court of Justice, 26 March 2012, Golden Eye: www.bailii.org/ew/cases/EWHC/Ch/2012/723.html*

- the rights holder's letter must explain that, despite the injunction to reveal the end-user's identity, the latter is not yet regarded as a counterfeiter;
- The end-user must respond without undue delay.

## THE END-USER WARNING AND EDUCATION SYSTEM

The government - through the Intellectual Property Office (IPO) - supports a private initiative called Creative Content UK, based on a voluntary agreement between rightholders and Internet service providers. The agreement was initially entered into for three years and provides a framework for the Voluntary Copyright Alert Programme, an e-mail warning system that does not incorporate sanctions and was first introduced in mid-January 2017.

Internet service providers may use an e-mail template provided by the rightholders, but have full control over the content. The warning may refer to several events and the e-mails contain links to the referrals (specifying the work(s) concerned) and to a site featuring, *inter alia*, advice for users on how to secure their Internet connection[11].

The programme has reportedly received positive feedback, particularly from the press, and has enjoyed extensive media coverage. Details of the cost - and how it is shared between Internet service providers and rightholders - have not been disclosed.

However, according to a survey conducted in March 2017 by Broadband Genie (a UK comparison service for home broadband, landline and mobile broadband services and TV packages), end-users see the Voluntary Copyright Alert Programme as ineffective.[12].

## AWARENESS CAMPAIGNS

As part of the Creative Content UK initiative, an awareness campaign has been underway since November 2015.

Actions taken have included an advertising campaign called "Get it Right from a Genuine Site", featuring TV ads and a website[13] that contains a list of so-called "genuine" sites and various animated films to raise awareness of legal content for young people.

In 2016, on the initiative of Creative Content UK, teachers were provided with educational resources on what would happen to an actor (for example) if all film viewers engaged in piracy.

By December 2016, the "Get it Right from a Genuine Site" campaign had reached one out of four end-users; 17.5% of those users said that it had changed their views on piracy. However, according to the annual study carried out by Kantar Media for the IPO[14], the proportion of end-users who have consumed illegal content in recent months has remained steady (25%).

A new youth awareness campaign was launched in January 2018, with funding from the IPO and the music industry. It consists of a series of cartoons called "Nancy and the Meerkats"[15], based on a radio series of the same name.

On 28 March 2018, the UK government announced a "Creative Industries Sector Deal" with the Creative Industries Council[16], the purpose of which is to invest in cultural and creative businesses. According to the report "Industrial Strategy: Creative Industries Sector Deal", which presents the objectives pursued,

*[11]www.get-it-right.org/faq.html*

*[12] Out of a sample of 2047 people, 72% said that sending educational letters was unlikely to deter end-users from using illegal services, while 82% said they did not even know the programme existed. According to 60% of respondents, the main cause of illegal downloading is the cost of legal content. The cost of legal content is driven up by the need to take out several subscriptions to get a comprehensive service. However, the respondents were divided on how best to prevent online infringement. For example, the following three measures were regarded as being almost equally effective: threat of legal action (22%), suspension of broadband service (22%), or reduction in the cost of legal content (19%). Finally, only 3.5% of respondents said they had received a warning. Some were unaware that they were committing an illegal act, or at least claimed not to have done it.*

*[13] www.getitrightfromagenuinesite.org*

*[14] www.gov.uk/government/publications/online-copyright-infringement-tracker-survey-8th-wave*

*[15] The episodes are available on the Cracking Ideas website, set up in November 2016 by the IPO: crackingideas.com/third_party/Nancy+and+the+Meerkats*

*[16] The Creative Industries Council was created specifically to represent the creative industries and promote their growth. Its members come from all areas of the creative industries: television, gaming, fashion, music, art, publishing and cinema. www.gov.uk/government/groups/ creative-industries-council*

the government will fund the ”Get it Right” campaign to the tune of £2 million (approximately €2,270,000) over three years.

In late 2017/early 2018, the IPO joined forces with creative industry stakeholders and the non-profit organisation CrimeStoppers to launch an awareness campaign on the use of pre-loaded set-top boxes to access content illegally (particularly live TV programmes)[17]. The campaign consists of four YouTube videos that underline the dangers of such practices (malware infection, identity theft, risks to young people) and urge members of the public to report vendors of pre-loaded set-top boxes to the authorities.

As part of its strategy against online infringement, the UK government is considering sharing more piracy prevention data with stakeholders and public authorities. For example, it is thinking about publishing court rulings to assess their impact.

### ACTIONS AGAINST VENDORS OF PIRACY-ENABLING SET-TOP BOXES

A new form of piracy has grown significantly in recent years and is now a top priority for those involved in piracy prevention, particularly the intellectual property crime unit in the City of London Police: the sale and use of set-top boxes pre-loaded with third-party applications to access illegal online content and/or pay-TV programmes.

According to the police, the Federation Against Copyright Theft (FACT - a professional body created to protect the intellectual property rights of its members) and the IPO, pre-loaded set-top boxes are very popular in the United Kingdom, especially for gaining free access to pay-TV channels. In its report “Cracking Down on Digital Piracy”[18], FACT estimates that one million such boxes have been sold in the United Kingdom in the last two years.

Sellers of these illicit streaming devices are regularly arrested as a result of coordinated action by FACT, the police and the IPO. These arrests and the subsequent convictions are reported in the press, the intention being to send a strong message to people who may think that such devices are legal, and to stem the problem.

The stakeholders’ actions are not confined exclusively to those who sell the devices. They also target those who broadcast paid-for content without authorisation, or who develop illegal applications specifically for piracy purposes.[19].

## ANTI-COUNTERFEITING ACTIONS INVOLVING INTERMEDIARIES

As regards the involvement of intermediaries in anti-counterfeiting efforts, the United Kingdom is one of the most active countries in the world: numerous blocking orders are issued, and rightholders have reached an agreement with Internet service providers to follow up on judicial blocking measures. A court recently issued a “live blocking” order to prevent the illegal streaming of sports content, making the United Kingdom one of the most advanced countries in the world in this respect.

The City of London Police is taking action through the “follow the money” approach, and voluntary agreements have been concluded with search engines.

*[17] The IPO has also conducted a campaign to raise awareness of the terminology relating to this new form of piracy; it introduced terms such as “illicit streaming device” to describe any computer equipment that enables access to infringing content.*
*[18] www.fact-uk.org.uk/files/2017/09/Cracking-Down-on-Digital-Piracy-Report-Sept-2017.pdf*
*[19] For example, Sky TV has sued some of its customers for streaming content illegally: one customer was ordered to pay £16,000 in legal fees and damages, while two publicans - who did not have a licence to broadcast Sky television content to their customers - were fined £20,000 in damages. Likewise, ACE TV - a company incorporated under English law, which provided premium IPTV subscriptions - ceased trading in April 2018 after being threatened by the FAPL. As the FAPL had requested a settlement payment of £600,000, the company went into court-ordered liquidation. It also transferred its customers’ personal data to the FAPL.*

## DYNAMIC BLOCKING INJUNCTIONS

Since 2011, UK courts have issued numerous blocking orders against Internet service providers. As regards copyright, orders thus far have stipulated that Internet service providers must bear the cost of implementing blocking measures, with rightholders paying procedural and evidence gathering costs. However, given the dramatic rise in website blocking cases, Internet service providers are concerned about continuing to shoulder the costs and are trying to overturn the case law.

To ensure the effectiveness of blocking decisions, it is provided that Internet service providers and rightholders may subsequently agree on any updates to the websites concerned without going back to court.

However, a study conducted by the Open Rights Group and published in June 2018 shows that:

- some websites blocked by court order no longer contain any unlawful content and therefore should no longer be blocked;

- the list of blocked sites varies from one Internet service provider to another, creating an unclear picture of the ecosystem. Apparently, Internet service providers do not update their lists in the same manner. According to the Open Rights Group, the situation could be improved by asking courts to insist that Internet service providers publish updated lists of blocked sites[20]. No such list is published at present, mainly because the stakeholders are already seeing an upsurge in the number of end-users bypassing blocking orders by means of VPNs for instance.

## TEMPORARY BLOCKING ORDERS TO PREVENT LIVE STREAMING OF SPORTS CONTENT

The Football Association Premier League (FAPL) runs the Premier League, the leading professional football league championship in England. In 2013, it obtained a court order to block a live streaming site[21].

In March 2017[22], it obtained the first live blocking order requiring the UK's main Internet service providers to directly block servers that deliver streams of match footage illegally.

The order was valid only for the last two months of the 2016-2017 FAPL season, i.e. from 17 March to 22 May 2017. The blocking measures ordered by the court in this case were intended to test the system's effectiveness and inherent risks. Hence their short-term nature.

Following the test period, the FAPL once again referred the matter to court.

The court approved the FAPL's petition to implement the system, ruling that the servers targeted by the FAPL's temporary blocking request were performing an unauthorised act of communication to the public. The fact that the servers were aimed specifically at the general public was clearly demonstrated with the help of the Internet service providers, some of which conducted observations of their network and concluded that a significant volume of traffic to the servers in question came from local subscribers. They also found that traffic was significantly higher during FAPL matches or other sports events.

The July 2017 ruling set out the system in detail, stating that on each match day, Internet service providers must block servers that have unlawfully broadcast live matches over the period in question or have illegally streamed the content of a TV channel scheduled to broadcast an FAPL match. At the end of each period, the FAPL must contact the ISPs to ensure that they lift the blocking measures as soon as possible.

*[20] torrentfreak.com/uk-pirate-site-blocks-opaque-poorly-administered-180603/*
*[21] The Football Association Premier League Ltd v. British Sky Broadcasting Limited & Ors [2013] EWHC 2058 (Ch), 16 July 2013: www. bailii.org/cgi-bin/format.cgi?doc=/ew/cases/EWHC/Ch/2013/2058.html&query=(premier)+AND+(league)*
*[22] The Football Association Premier League Ltd v. British Telecommunications Plc & Ors [2017] EWHC 480 (Ch), 13 March 2017: www. bailii.org/cgi-bin/format.cgi?doc=/ew/cases/EWHC/Ch/2017/480.html&query=(football)+AND+(association)+AND+(premier)+AND+(league)*

In a statement dated 25 July 2017, the FAPL said that it had blocked more than 5,000 IP addresses that were being used to broadcast sports content illegally[23]. The first blocking orders caused a great deal of disruption among Internet service providers[24], with some suggesting that their customers use VPNs.

Spurred on by this initial success, the FAPL petitioned the same court again to obtain another blocking order, this time covering the entire 2017-2018 season. The order was issued on 25 July 2017. It has since been followed by another one in July 2018, covering the 2018/2019 season.[25]

In December 2017, the Union of European Football Associations (UEFA) obtained a similar order covering the period from 13 February 2018 to 26 May 2018[26]. This was also extended in July 2018[27].

Internet service providers did not oppose these procedures. On the contrary, they supported them, probably because most of them are FAPL licensees themselves. The July 2017 decision also specifies that Internet service providers can only be expected to do their best to block notified services, depending on their network set-up and their resources. They may also carry out work on their network that will prevent them from implementing the blocking measures, but they must inform rightholders of this work as soon as possible and make sure it is completed within a reasonable timeframe.

## THE RIGHTS OF THE SPORTS ORGANISATIONS IN QUESTION

FAPL has been actively protecting its rights against piracy for a long time[28]. It is gradually changing things so that it can claim intellectual property rights over the broadcasting of matches it organises. Thus, the FAPL is asserting its rights over:

- clean live feed captured by its licensees[29], provided that it includes a replay of the match highlights;
- matches recorded for an international audience, provided that they are recorded by a national licensee before being broadcast abroad;
- graphics and logos included in footage aimed at international audiences.

UEFA is taking similar action in the UK, claiming intellectual property rights over television broadcasts and any match highlights, logos and music included therein.

Moreover, one of the main impediments to blocking this type of broadcast is that the rights are held by several actors. Therefore, to add weight to its actions, the Premier League states that it is supported by other rightholders[30]. Likewise, the proceedings initiated by UEFA were supported by the FAPL and Formula One World Championship Ltd.

*[23]English Premier League, "Premier League awarded High Court Blocking Order", 25 July 2017.*
*[24] torrentfreak.com/new-first-league-blocking-disrupts-pirate-iptv-providers-170814/*
*[25] The Football Association Premier League Ltd v. British Telecommunications Plc & Ors [2018] EWHC 1828 (Ch), 18 July 2018: www. bailii.org/cgi-bin/format.cgi?doc=/ew/cases/EWHC/Ch/2018/1828.html&query=football+association+premier+league*
*[26] Union of European Football Associations v British Telecommunications Plc & Ors [2017] EWHC 3414 (Ch), 21 December 2017: //www.bailii.org/cgi-bin/format.cgi?doc=/ew/cases/EWHC/Ch/2017/3414.html&query=union+des+associations+europ%E9ennes+de+footbal*
*[27]Union of European Football Associations v British Telecommunications Plc & Ors [2018] EWHC 1900 (Ch), 24 July 2018: www.bailii.org/cgi-bin/format.cgi?doc=/ew/cases/EWHC/Ch/2018/1900.html&query=union+des+associations+europ%E9ennes+de+footbal*
*[28] CJEU, C 403/08 and C 429/08, Football Association Premier League Ltd, NetMed Hellas SA, Multichoice Hellas SA v QC Leisure et al., 4 October 2011. The CJEU was asked for preliminary rulings following the initiation of legal proceedings by the FAPL against:*
*- companies that have provided equipment and decoder cards enabling Premier League matches broadcast by foreign broadcasting bodies to be transmitted in the UK (in this case, a Greek broadcaster);*
*- cafés and restaurants that have shown Premier League matches for their customers, using decoding equipment to access matches broadcast by foreign broadcasting bodies.*
*[29] A broadcaster is tasked with recording matches for the domestic audience.*
*[30] The March 2017 proceedings that led to the first live blocking decision were supported by the following: i) British Broadcasting Corporation and BBC Worldwide Ltd; ii) DFL Deutsche Fußball Lega GmbH; iii) Liga Nacional de Fútbol Professional; iv) The Football Association Ltd; v) The Scottish Premier League Ltd; vi) The Football League Ltd; vii) England and Wales Cricket Board Ltd; viii) PGA European Tour; ix) The Professional Darts Corporation Ltd; and x) Rugby Football Union.*

### WEEKLY UPDATING OF THE FRAMEWORK LIVE BLOCKING INJUNCTION

Pursuant to the framework injunction ordered by the court, every week the FAPL and its service provider[31] identify servers that broadcast sports content via various channels (social networks, illegal playlists, live streaming applications, pre-loaded set-top boxes, etc.). The servers' IP addresses are then forwarded to Internet service providers so that they can put IP blocks in place.

On match days, the Internet service providers block the servers on the list. The list may be updated in real time, manually if necessary. However, some Internet service providers have developed an automatic blocking system. In practice, the list of servers to be blocked is circulated via a secure platform and is updated at least twice on each match day.

Decisions do not contain any provisions on cost sharing arrangements, which therefore remain confidential.

Some provision has been made to ensure the system is fair. For example, server hosts must be notified of intended blocking measures so that affected third parties can take legal action[32]. Within ten working days of implementing the aforementioned decision, Internet service providers must inform their subscribers by electronic means that access to a number of servers involved in the illegal streaming of matches has been blocked by court order, and that similar measures will be taken for the 2017/2018 season. End-users are also informed of the identity of the party that obtained the blocking order and of the fact that they can refer the matter to court.

### THE IMPLEMENTATION OF THE SO-CALLED "FOLLOW THE MONEY" APPROACH

In September 2013, the City of London Police set up a unit specialised in intellectual property crime: The Police Intellectual Property Crime Unit (PIPCU). PIPCU deals with copyright and trademark infringements (covering tangible and digital goods with the exclusion of medicines), especially those committed online.

The unit is subsidised by the IPO[33] and rightholders provide both human and financial support (especially FACT, which mainly represents rightholders in the audiovisual sector). The police may be assisted in their investigations by specialised investigators employed by rightholders.

Agreements have been concluded between PIPCU, rightholders[34] and the online advertising industry[35] with a view to setting up an online portal with a list of massively infringing sites (Infringing Website List) and taking action against them (Operation Creative). The MPA is now involved in this operation[36].

Under the terms of these agreements, rightholders report massively infringing websites to the police, providing evidence to back up their claims.

To determine whether a website is massively infringing or not, they use a statistical method to establish the percentage of illegal content it contains. The percentage must be above 50% (mainly infringing). The rightholders also inform the police if, to their knowledge, a website has been blocked in Europe.

The PIPCU then examines the information provided, conducts its own investigations and decides whether or not to pursue the case further. The criteria used by the police are confidential.

*[31]Friend MTS: www.friendmts.com/about-us/customers/*

*[32] Notifications must include: information that the address has been blocked following a decision by a UK court; the identity of the party that obtained the injunction; a link to the court decision, advice that operators affected by the decision may take legal action.*

*[33] The City of London Police received £2.56 million in 2013 when PIPCU was created, and an additional £3 million in 2014 to keep the unit up and running until mid-2017. A further payment of £3.32 million should keep it going until 2019.*

*[34]The Federation Against Copyright Theft, the British Recorded Music Industry, the International Federation of the Phonographic Industry (IFPI) and the Publishers Association.*

*[35]The local Internet Advertising Bureau (IAB), the Incorporated Society of British Advertisers and the Institute of Practitioners in Advertising.*

*[36] www.cityofiondon.police.uk/advice-and-support/fraud-and-economic-crime/pipcu/pipcu-news/Pages/New-PIPCU-and-MPA- partnership.aspx*

The police contact the site and ask it to regularise its activities within fourteen days or, failing that, to cease operations.

If the site does not respond, it is added to the Infringing Website List.

No court action is necessary.

The list contains 1,200 infringing websites and the (nearly) 300 partners involved in the operation can access it via an automated interface. The list mainly includes links sites (financed essential by advertising revenue) and a few content hosting sites (cyberlockers).

A PIPCU contractor (Pathmatics) monitors the site, using dedicated software (AdRoutes) to trace the chain of advertisers that place ads on it. It informs any non-partner advertisers that they may be regarded as accomplices in the infringement of intellectual property law[37].

PIPCU has contacted the authority responsible for issuing gambling and betting licences (the Gambling Commission). The latter has informed licensees that their licence could be revoked if they advertise on illegal websites[38]. According to the police, the number of licensees advertising on illegal websites has dropped sharply (87% from June 2016 to June 2017).

When a website is added to the list, a letter is also sent to the relevant registrar or to the organisation that manages the extension under which the domain name is registered, requesting that the domain name be suspended. This approach has met with mixed success among organisations located outside the United Kingdom (the most frequent scenario).

## CODE OF CONDUCT APPLICABLE TO SEARCH ENGINES AND EXTENDED TO OTHER INTERMEDIARIES

On 9 February 2017, after more than two years of talks led by the IPO, an agreement was reached with search engines[39] and rightholders[40]. The agreement is a voluntary and legally non-binding code of conduct.

Thus far, the search engines have committed to demoting illegal offer in UK search engine results (e.g. Google.co.uk) by June 2017. Websites considered to be illegal are not deleted from the search index but their pages rank lower in search results.

Websites are classed as illegal based on information exchanged between search engines and rightholders.

For example, the stakeholders have agreed on a set of targets (percentages) that search engines must meet. These targets should relate to neutral key word searches by consumers who are not specifically looking for illegal content.

Promoting or presenting legal offer in a separate section is ruled out, as it raises legal questions regarding free competition.

As a counterpart to the commitments made by search engines, rightholders[41] will ensure that legal offer ranks higher in search engine results by improving their SEO (Search Engine Optimisation) and increasing the online visibility of specific legal content.

The agreement is deemed to have produced satisfactory results, although some adjustments are still needed to make the system more effective[42].

*[37] In January 2017, PIPCU paid visits to eight online advertising actors (advertisers, advertising agencies, advertising intermediaries). PIPCU has declared the system a success, with any residual advertising coming from the pornography and/or gambling sector.*

*[38] Gambling commission: licence conditions and codes of practice, January 2018: Article 16.1.1 - Licence condition: responsible placement of digital adverts (all licences): "1) Licensees must: a) ensure that they do not place digital advertisements on websites providing unauthorised access to copyrighted content".*

*[39] Google, Microsoft (Bing) and Yahoo.*

*[40] The British Phonographic Industry (BPI) for the music industry, and the Motion Picture Association (MPA) for the audiovisual sector.*

*[41] It would seem, for example, that iTunes and Netflix still do not have an SEO strategy and do not appear in search engine results. They would prefer end-users to search directly in their applications, rather than using search engines.*

*[42]For example, one of the problems is that the number of notifications submitted varies from sector to sector. The music sector is much more active than the publishing sector (due mainly to the number of tracks on an album) and more easily has works demoted. Domain and sub-domain name changes are also a problem, as they "wipe the slate clean" and it takes a while for the new site to be demoted.*

Thus, the IPO is working with stakeholders on how to resolve the issue of new domain names, prioritise notifications regarding cinema releases, and better coordinate search and autocomplete functions.

A service provider monitors compliance with the agreement on a quarterly basis. At the end of March 2018, the government published a report called "Industrial Strategy - Creative Industries Sector Deal[43]". The report outlines plans to extend the approach adopted with search engines by organising several roundtables between rightholders, social media and UGC platforms, the online advertising industry and online marketplaces.

The topics addressed are as follows: improving the effectiveness of notice and takedown arrangements, encouraging illegal sites to stop engaging in online infringement, and reducing the costs incurred by rightholders to protect their rights.

*[43] www.gov.uk/government/publications/creative-industries-sector-deal*

# RUSSIA

## KEY FIGURES

KNOWN BLOCKING PROCEDURES (SINCE 2006)

**1448** NUMBER OF PROCEDURES

**397** NUMBER OF SITES BLOCKED

**1448** NUMBER OF DOMAIN NAMES BLOCKED

DEMOGRAPHY

**144** POPULATION (2017) [1]
*in millions*

**76.0%** INTERNET PENETRATION RATE (2017) [2]

INFRINGEMENTS [3]

**16** NUMBER OF VISITS TO ILLEGAL SERVICES (2017)
*in billions*

**146** NUMBER OF VISITS TO ILLEGAL SERVICES PER END-USER (2017)

**Breakdown of infringements by access method (2017)**
*as a %*


According to the Federal Service for Supervision of Communications, Information Technology and Mass Media *(Roskomnadzor)*, legal offer is steadily improving[4] and a portal has been created listing legitimate online services.

However, Russia regularly features on the American administration's list of countries that allegedly host large numbers of infringing websites.

The Russian state policy towards online copyright infringement is based largely on removing, and in some cases blocking copyright-infringing content. The system is frequently updated to make it more effective.

## MEASURES FOR BLOCKING INFRINGING AND WORKAROUND SERVICES

A law passed in 2015 encourages rightholders to report illegal online content and negotiate directly with infringing websites to reduce recourse to blocking procedures.

The system provides that, should discussions with a website fail following a notice and takedown request, rightholders may pursue a fast-track procedure to obtain a blocking order.

The rightholders must first refer the matter to the Court of Moscow - the only court in Russia with the necessary jurisdiction - to have the infringement of their rights established. The Court then notifies its decision to the *Roskomnadzor*, which is responsible for issuing injunctions against technical intermediaries to ensure the decision is enforced.

*[1] United Nations Population Fund (UNFPA) – 2017.*
*[2] International Telecommunications Union (ITU) – 2017.*
*[3] MUSO - 2017.*
*[4] According to a study by J'son&Partners Consulting, the legal streaming offer increased 15% between 2014 and 2015.*

The *Roskomnadzor* contacts the hosting provider or the website, which then has three days to put an end to the infringement. If the disputed content is not withdrawn or the illegal activity does not cease within the three days, the *Roskomnadzor* may ask the technical intermediaries (hosting providers or Internet service providers) to implement measures to block access to the disputed content or site. Should they fail to comply, the intermediaries incur a fine of 30,000 roubles (approximately €500). An "interconnection" has been established between the *Roskomnadzor* and Internet service providers to secure and facilitate information flows, and thus ensure the swift implementation of blocking measures. The *Roskomnadzor* is responsible for updating the list of resources to be blocked in the Federal State Information System (FGIS), while the technical intermediaries bear the cost of blocking measures.

Blocking measures against massively infringing sites, or against sites that repeatedly promote infringing services, may be implemented for an indefinite period. Rightholders may also request that search engines be ordered to delist links to indefinitely blocked sites.

### UPDATING OF BLOCKING MEASURES

A law adopted on 1 July 2017 introduced a simplified system for blocking workaround sites through an accelerated administrative procedure that does not require rightholders to return to court.

The rightholders refer the matter to the Ministry of Telecom and Mass Communications, which then has 24 hours to consult a panel of at least three experts and issue a decision confirming that the site is indeed a mirror site. English and Russian copies of the decision are sent to the website operator and the *Roskomnadzor.*

The *Roskomnadzor* informs the hosting provider of the Ministry's decision and instructs Internet service providers and search engines to respectively block the website and delist its domain name within 24 hours.

It seems, however, that rightholders must obtain a court ruling to have a workaround site blocked indefinitely.

## OTHER ANTI-COUNTERFEITING ACTIONS INVOLVING INTERMEDIARIES

A law adopted on 29 July 2017 extended the scope of the anti-piracy system to include anonymisation services, which can now be blocked if they do not comply with their new obligations. The new law requires that operators of VPN services and other anonymisation systems must make themselves known to the authorities, provide encryption keys for decrypting encrypted messages, and then consult the list of blocked sites provided by the *Roskomnadzor* so that they themselves can prevent access to them.

The encrypted messaging application Telegram was blocked in this way. However, as the application used Amazon and Google infrastructure, millions of IP addresses used by the two companies were also blocked, leading to significant over-blocking.

Russian law also provides that:

ınline services containing advertising content must also consult the FGIS to make sure they are not promoting blocked services or providing links to such services;

Search engines are liable to a fine if they display links to blocked websites and services listed by the *Roskomnadzor* in the FGIS, or to anonymisation services such as VPNs.

Moreover, the domain names of more than 200 infringing websites were blocked in a case referred to Russia's online gaming regulator by the tax authorities, on the grounds that the said websites contained advertisements for illegal online gaming services.

# SWEDEN

## KEY FIGURES

KNOWN BLOCKING PROCEDURES (SINCE 2006)

**1** NUMBER OF PROCEDURES

**2** NUMBER OF SITES BLOCKED

**88** NUMBER OF DOMAIN NAMES BLOCKED

DEMOGRAPHY

**9.9** POPULATION (2017) [1]
*in millions*

**96.4%** INTERNET PENETRATION RATE (2017) [2]

INFRINGEMENTS [3]

**0.99** NUMBER OF VISITS TO ILLEGAL SERVICES (2017)
*in billions*

**104** NUMBER OF VISITS TO ILLEGAL SERVICES PER END-USER (2017)

**Breakdown of infringements by access method (2017)**
*as a %*


Sweden has attracted a lot of media coverage in respect of piracy because it is the birthplace not only of one of the leading providers of legal online music services (Spotify), but also of the Pirate Bay, a prominent torrent site that has been blocked in many countries.

According to a study conducted in January 2017, a quarter of end-users aged between 15 and 74 admit to having streamed or downloaded films illegally in recent months.

The same study reports that the piracy rate has remained relatively steady over the past three years.

The Swedish system for preventing piracy of cultural content consists mainly of actions against websites, although specific measures have been put in place against end-users and website administrators.

## EDUCATIONAL AND ENFORCEMENT ACTIONS

### CRIMINAL LAW PROVISIONS

The policy on commercial counterfeiting includes tough criminal punishment measures, which are enforced by a special law enforcement unit. Sweden has public prosecutors and specialised jurisdictions.

Creators of websites located in Sweden have been given prison sentences of several months[4]. Proposals to tailor sanctions to the gravity of the infringement are being considered.

In November 2016, the tracker Rarat.org was shut down and its owner was arrested following a joint operation by the police, *Rights Alliance* and *PayPal* to identify the recipient of payments made to the site.

*[1] United Nations Population Fund (UNFPA) – 2017.*
*[2] International Telecommunications Union (ITU) – 2017.*
*[3] MUSO - 2017.*
*[4] www.hogstadomstolen.se/Domstolar/hogstadomstolen/Avgoranden/2017/2017-06-12%20B%203878-15 %20dom.pdf*

In June 2017, a joint operation by French and Swedish police resulted in the closure of the Bit Torrents links site and the arrest of its two Swedish-based administrators.

Rightholders have taken legal action against streaming services that provided unauthorised access to their television channels (especially sports channels). On 29 June 2018[5], the operators were sentenced to prison for infringement and ordered to pay up to €20 million in damages.

### THE SENDING OF INDEMNIFICATION NOTICES TO END-USERS

Rightholders may hand over an IP address to a court of law to identify an end-user who has shared cultural content illegally on peer-to-peer networks. Once the Internet service provider has released the end-user's details at the court's request, the rightholders may send him or her a letter of formal notice to pay damages with interest. In the event of non-payment of the said damages and interest, the end-user is informed that he or she is liable to prosecution.

However, these practices are highly controversial. In 2017, a law firm representing a rights holder in the audiovisual sector issued 25,000 letters of formal notice to end-users. In April 2018, the Pirate party sent a letter to the Ministry of Justice requesting that it put an end to such practices.

In Sweden, these practices have become all the more controversial since a court ruling on 21 December 2016 regarding the retention and communication of personal data by Internet service providers.[6] The Stockholm Administrative Court ruled in February 2018 that Internet service providers must disclose the identity of end-users. Internet service provider Bahnhof, which refused to disclose the identity of its subscribers in penal cases other than criminal – and which has been subject to an injunction from the telecommunications regulator since 2016 – has appealed this decision.

### THE PROMOTION OF LEGAL OFFER

Sweden's patent and trademark office has set up a portal called *Streamalagligt.se*[7], which directs users to legitimate content including films, TV series and music. Rightholders have created a similar portal, *Moviezine*, which also enables users to access films and series legally.

A government-led communication campaign[8] was organised in May 2018 to encourage end-users to stream content legally.

## ANTI-COUNTERFEITING ACTIONS INVOLVING INTERMEDIARIES

### COURT DECISIONS REGARDING SITE BLOCKING

Rightholders issue numerous notifications to websites that host streaming content, after finding the content through a links site.

In February 2017[9], an injunction was issued against an Internet service provider to block access to the Pirate Bay website for three years. The Internet service provider risks a fine of approximately €53,000 if it does not comply with the injunction. However, Internet service providers that were not parties to the proceeding said they would not voluntarily block the site unless ordered to do so directly.

*[5] torrentfreak.com/images/StockholmsBein.pdf*
*[6] CJEU, 21 December 2016, C 203/15 and C-698/15, Tele2 Sverige AB (C 203/15) and Secretary of State for the Home Department.*
*[7] www.streamalagligt.se/na/en*
*[8] www.prv.se/en/copyright/streama-lagligt/*
*[9] In the first instance, the judge did not grant the blocking request.*

In May 2018, a coalition of audiovisual rightholders took legal action against another Internet service provider[10] to get the Pirate Bay blocked, along with other websites regarded as infringing. The purpose of the procedure is to have websites blocked as a safeguard measure, until a final ruling is made.

## OTHER MEASURES INVOLVING INTERMEDARIES

### ACTIONS TARGETING DOMAIN NAME REGISTRARS

On 22 December 2017, the Supreme Court ruled that domain names are assets that can be seized by the state. The public prosecution service had instituted proceedings against Sweden's domain name registrar *Punkt SE*, as it considered that "thepiratebay.se" and "piratebay.se" enable and encourage piracy and can therefore be seized by the Swedish state. Indeed, pursuant to section 53-a of the Copyright Act[11], goods that are or will be used for criminal purposes may be seized to prevent other crimes.

### THE IMPLEMENTATION OF THE "FOLLOW THE MONEY" APPROACH

The anti-piracy organisation, Rights Alliance, has joined forces with the online advertising industry to implement a "follow the money" type of initiative. Under the initiative, rightholders draw up a list of infringing sites and forward it to their partners in the advertising industry, who make sure they do not place ads on the listed sites.

*[10] torrentfreak.com/images/Stockholms-TR-PMT7262-18-Aktbil-1.pdf*
*[11] Law relating to literary and artistic property, SFS 1960: 729, amended on 1 April 2011, www.wipo.int/wipolex/en/text.]sp?file_id=290912*

# SWITZERLAND

## KEY FIGURES

### DEMOGRAPHY

**8.5** POPULATION (2017) [1]
*in millions*

**93.7%** INTERNET PENETRATION RATE (2017) [2]

### INFRINGEMENTS [3]

**0.95** NUMBER OF VISITS TO ILLEGAL SERVICES (2017)
*in billions*

**119** NUMBER OF VISITS TO ILLEGAL SERVICES PER END-USER (2017)

**Breakdown of infringements by access method (2017)**
*as a %*


STREAMING | DIRECT DOWNLOAD | PEER-TO-PEER

At the end of 2016, a preliminary copyright reform proposal was published and put out to public consultation. In November 2017, following this consultation, the Federal Council published an amended reform proposal[4]. The preliminary reform proposal provided for a warning system for end-users who share content on peer-to-peer networks, along with an administrative blocking system. Ultimately, however, neither of these measures was adopted.

The proposal submitted to Parliament provides for action against both end-users and websites.

The reform was initiated in 2016 because the US administration had included Switzerland on its Special 301 list of countries that do not provide effective protection of intellectual property rights, on the grounds that it allegedly hosts large numbers of infringing websites.

## EDUCATIONAL AND ENFORCEMENT ACTIONS

In Switzerland, only those who share protected works without authorisation are liable to criminal prosecution, not users who download such works from illegal sources.

According to the Federal Institute of Intellectual Property (IPI), an independent public agency responsible for registering trademarks, patents and designs and handling all other intellectual property issues on behalf of the Swiss government, "*consumers of illegal content will continue [...] not to be liable to prosecution. They will therefore be able to download a piece of music for their own personal use, for example, even if it has been posted online without the rightholders' permission*"[5].

Photographs (including press photos and family and holiday photos) could however be protected against all uses to prevent end-users from reproducing third party photographs without authorisation, particularly on social networks.

*[1] United Nations Population Fund (UNFPA) – 2017.*
*[2] International Telecommunications Union (ITU) – 2017.*
*[3] MUSO - 2017.*
*[4]United Nations Population Fund (UNFPA) - 2017.*
*[5] www.ige.ch/fr/droit-et-politique/evolutions-nationales/droit-dauteur/revision-du-droit-dauteur/tout-ce-que-vous-faut-savoir-sur-le- projet.html*

Concerning works made available without authorisation, the reform proposal submitted to Parliament also provides that copyright owners whose rights have been infringed may take legal action and are therefore entitled to: *"process personal data [...] for the purpose of filing a criminal complaint or reporting an offence [...]. They may also use the data to file incidental civil actions, or to file such actions at the end of criminal proceedings.*

*They are required to declare publicly the purpose, the type of data processed, and the extent of data processing*".

The reform proposal takes a stance opposite to the 2010 Logistep ruling, which focused strongly on protecting personal data. The ruling caused uncertainty as to whether it was legal for rightholders to collect IP addresses for the purpose of taking legal action against copyright infringement. Consequently, it created uncertainty regarding the admissibility of IP addresses as evidence in the prosecution of copyright infringement cases.

## ANTI-COUNTERFEITING ACTIONS INVOLVING INTERMEDIARIES

Switzerland does not have a specific legal regime for technical intermediaries. The reform proposal therefore makes provision for regulating the activities of hosting providers by imposing a specific obligation on those which "*due to [their] technical processes or [their] economic objectives enable legal violations or create a specific risk of such a violation occurring*".

Hosting providers must prevent the reappearance of copyright-protected content that has previously been subject to a notice and stay down obligation, by taking any "*technical and economic measures that may reasonably be expected [of them], bearing in mind the risk of violation*".

The public-private partnership, Stop Piracy, is moreover considering how to implement a "follow the money" approach, with the aim of involving the online advertising industry in the fight against piracy.

# TAIWAN

## KEY FIGURES

DEMOGRAPHY

**23.4** POPULATION (2017) [1] *in millions*

**79.8%** INTERNET PENETRATION RATE (2017) [2]

INFRINGEMENTS [3]

**1.2** NUMBER OF VISITS TO ILLEGAL SERVICES (2017) *in billions*

**63** NUMBER OF VISITS TO ILLEGAL SERVICES PER END-USER (2017)

***Breakdown of illegal uses by access method (2017) -*** *in %*


Taiwanese law provides for a graduated system but it has not been implemented.

In fact, there seem to be very few specific tools for combating infringing services.

## EDUCATIONAL AND ENFORCEMENT ACTIONS

Taiwan introduced a legislative graduated response system in 2009, which provides that technical intermediaries (Internet service providers and hosting providers) must:

- issue notifications to end-users;

adopt a procedure for suspending or terminating the subscriptions or accounts of end-users who have infringed copyright on several occasions.

Otherwise, these end-users would not be covered by the limited liability regime.

However, the practical implementation of the system is not detailed in any legislation.

Music rightholders and an Internet service provider, HiNet, reportedly decided to test the system for six months in 2013. However, according to reports, fewer than 30% of notifications issued by rightholders were actually delivered to subscribers, mainly because end-users are not required to provide Internet service providers with an e-mail address.

## ACTIONS AGAINST INFRINGING SERVICES

Sales of set-top boxes enabling access to illegal content seem to have been very high for several years. According to the International Intellectual Property Alliance (IIPA), an association of American rightholders, there are thirty different brands of these boxes in Taiwan.

The Taiwan Intellectual Property Office (TIPO) notes that it is possible to tackle this form of piracy under substantive law, through the provisions relating to contributory infringement and the circumvention of technical protection measures.

*[1] United Nations Population Fund (UNFPA) – 2017.*
*[2] International Telecommunications Union (ITU) – 2017.*
*[3] MUSO - 2017.*

# VIETNAM

## KEY FIGURES

DEMOGRAPHY

**95.5** POPULATION (2017) [1] *in millions*

**46.5%** INTERNET PENETRATION RATE (2017) [2]

INFRINGEMENTS [3]

**4.9** NUMBER OF VISITS TO ILLEGAL SERVICES (2017) *in billions*

**111** NUMBER OF VISITS TO ILLEGAL SERVICES PER END-USER (2017)

**Breakdown of infringements by access method (2017)** *as a %*


Vietnam is experiencing a sharp increase in illegal online consumption.

The Motion Picture Association has reported that illegal websites in Vietnam have 105 million visitors a month, while legal sites have only 2 million[4].

This trend has been reinforced by the fact that a growing majority of the population has broadband access[5].

The Vietnamese government is aware of this issue and is trying to develop new lines of approach to support a shift towards legal usage.

Vietnam's anti-piracy policy is characterised by the strong involvement of government and administrative authorities, particularly in projects to implement "follow the money" measures. The government also plans to create a criminal court specialised in online copyright infringement.

## ENFORCEMENT ACTIONS

In 2017, the penal code was amended and now provides that individuals who infringe copyright and related rights are liable to up to three years in prison.

The new article also targets legal entities engaged in activities that infringe copyright and related rights: if convicted – on the grounds that their illegal activities have generated a profit of around US$ 500 – they incur a fine ranging from 300 million to 1 billion dong (i.e. US$ 13,000 to approximately US$ 44,000). In the event of a repeated infringement, either the fine is increased to 3 billion dong (i.e. US$ 130,000), or the court orders a two-year suspension of activity.

*[1] United Nations Population Fund (UNFPA) – 2017.*
*[2] International Telecommunications Union (ITU) – 2017.*
*[3] MUSO - 2017.*
*[4] vietnamnews.vn/sunday/features/379196/tv-film-piracy-remain-big-concern-in-vn.html#p8IIRd0OqHf78Vky.97*
*[5] According to the Measuring the Information Society Report 2017 at www.itu.int/en/ITU-D/Statistics/Documents/publications/misr2017/MISR2017_Volume1.pdf, the percentage of people using the Internet in Vietnam increased from 43.5% in 2015 to 46.5% in 2016, and in 2016 there were approximately 47 broadband subscriptions per 100 Vietnamese residents.*

The government plans to create a criminal jurisdiction especially for intellectual property disputes.

## ANTI-COUNTERFEITING ACTIONS INVOLVING INTERMEDIARIES

### TAKEDOWN AND SITE BLOCKING MEASURES

The Ministry of Information and Communication (MIC)[6] and the Ministry of Culture, Sports and Tourism (MCST) have enacted a circular stipulating that intermediary service providers must - at the request of the said Ministries or of any other government department – take down disputed content and stop providing their services if copyright and related rights are threatened.

When rightholders request the removal of unauthorised content, hosting providers comply only if they have received a direct request from the government. The MIC may issue fines of up to 250 million dong (US$ 11,000) for a natural person and 500 million dong (over US$ 22,000) for a legal entity[7].

In 2017, the Broadcasting and Electronic Information Authority, which reports to the MIC, organised a meeting between rightholders in the film industry and the main Vietnamese Internet service providers to discuss the possibility of taking joint action against piracy. Some Internet service providers agreed to consider implementing a procedure to enforce sustainable blocking measures.

### THE IMPLEMENTATION OF THE SO-CALLED "FOLLOW THE MONEY" APPROACH

Conventional "follow the money" initiatives have been developed to dry up the financial sources of illegal sites which, according to the Vietnamese press[8], could be turning an annual profit of over 10 billion dong (US$ 450,000). Hence, the MIC may order the removal of advertisements: in 2018, it ordered the removal of all advertisements from 50 websites.

At the same time, it seems that the Vietnam Content Alliance - composed of Vietnamese and international (mainly American) content producers and distributors - is setting up a system to prevent advertising agencies and the owners of well-known brands from placing ads or selling products on illegal websites.

*[6] Decree No. 17/2017/ND-CP (Decree 17) of the Vietnamese Government.*
*[7] Decree No. 131.*
*[8] A report published by the Ministry of Industry and the Vietnamese Competition Authority in 2017 showed that 44 of the 50 most popular illegal websites were backed by advertising space providers, and 66% of illegal sites were backed by more than one advertising service provider.*