Internet piracy continues to be a significant problem for rights holders. The creative industries argue that piracy costs the industry £400m a year in lost revenue. In response, several countries around the globe are introducing new regimes to tackle online copyright infringement (“OCI”) and at the same time rights holders, dissatisfied with some of the existing national graduated response regimes, are increasingly turning to the powerful and effective tool of website-blocking injunctions. In this article we explore the national regimes for tackling online piracy in some of the key European countries and look at recent important developments both in Europe and in the rest of the world, notably Australia and Russia.

Europe
In 2000 the European E-Commerce Directive\(^1\) established the principle of “notice and take down” procedures, giving ISPs immunity from liability except where they have been notified of infringement and do not promptly take down the content. The following year, the Information Society Directive\(^2\) came into force, which provided that member states must ensure that rights holders can apply for an injunction against internet intermediaries whose services are used by a third party to infringe a copyright. The CJEU confirmed in the 2014 case of UPC Telekabel Wien GmbH v Constantin Film Verleih GmbH and Wega Filmproduktionsgesellschaft, that Internet service providers (“ISPs”) can be ordered to block access by customers to websites making available infringing content and ISPs are free to choose the measures they use provided those measures target the infringing content and do not unjustly interfere with the users’ right to freedom of information. The IP Enforcement Directive\(^3\) also requires member states to ensure that measures necessary for the enforcement of intellectual property rights shall not be unnecessarily complicated or costly. The directives had to be implemented through national legislation and this has led to inconsistencies in the national legislation of member states.

UK
In the Government’s Review of Intellectual Property in the UK in December 2006 (the Gowers Review) Mr Gowers reported that UK legislation, in particular s97A of the UK Copyright, Designs and Patents Act 1988, was not providing rights holders with sufficient protection against OCI (in particular illegal file-sharing). Under s97A, the High Court has the power to grant an injunction against a service provider, where that service provider has actual knowledge of another person using their service to infringe copyright. Gowers recognised that rights holders and ISPs disagreed over the interpretation and effect of s97A and it was completely untested since 2003. Consequently, in February 2008, the government said it would consult on legislation that would require ISPs and rights holders to co-operate in taking action on OCI, with a view to implementing legislation by April 2009. In July 2008 the UK’s six largest ISPs signed a memorandum of understanding with industry representatives and government under which they committed to working towards a significant reduction in illegal file-sharing. Ultimately, however, the memorandum of understanding failed as rights holders and the ISPs could not agree how the costs of any measures to reduce OCI should be borne.

Consequently, the government was forced to legislate in this area and the relevant provisions were enacted in the UK Digital Economy Act 2010 (‘DEA’). Throughout its passage throughout Parliament, the provisions relating to OCI caused widespread controversy and were heavily amended at each stage.

To deal with OCI, the DEA foresees two phases of regulation. The first phase consists of a mechanism pursuant to which right holders would detect the IP addresses of suspected online infringers and forward these IP addresses to the relevant ISPs. The ISPs would then send warning notices to the suspected infringers. The ISPs would also be required to provide to right holders an anonymous list of subscribers for whom the ISP had previously received a large number of infringement notices from the right holders. This anonymous list would permit right holders to go to court in order to request the name of the relevant subscribers for the purpose of bringing individual copyright infringement actions. The second phase of regulation consists of technical measures that ISPs may be required to implement in order to limit OCI. These technical measures may include the limitation of Internet access for certain subscribers, a measure similar to the French graduated response regime.

---

Both phases are contingent on the adoption of detailed implementing rules by OFCOM. The DEA provides either that the detailed rules would be developed in the form of a code of conduct by industry stakeholders, a code which would then be approved by OFCOM, or in the absence of agreement by industry stakeholders, that the code would be adopted directly by OFCOM. Shortly after adoption of the DEA, OFCOM launched a public consultation regarding the draft code of practice that OFCOM intended to adopt. In the meantime, two ISPs challenged the DEA before the High Court of England on the grounds that the DEA violated several European directives and also constituted a disproportionate restriction on the fundamental rights of Internet users. The High Court validated virtually all provisions of the DEA. After the High Court’s decision, the two UK ISPs lodged an appeal before the Court of Appeal. On March 6, 2012, the Court of Appeal upheld the initial decision of the High Court. Consequently it is now possible for OFCOM to adopt the initial code of obligations that would permit the first phase of the DEA to go into operation. OFCOM issued a new draft of these regulations on 26 June 2012 for public consultation. OFCOM proposes that the costs of the ISPs and OFCOM should be split 75:25 between the copyright owners and the ISPs. There is likely to be considerable debate over this proposal however it is not clear when this will happen. All the current government has said is that based on current plans, and subject to Parliamentary approval, the first notification letters would be sent in late 2015.

Twelve months after the initial obligations code comes into force, OFCOM must prepare a report for the Secretary of State containing a detailed assessment as to whether the initial phase consisting of the sending of notices to subscribers has resulted in a decrease in OCI. The Secretary of State can then instruct OFCOM to conduct further assessment, including industry consultation, as to whether additional technical measures should be imposed on ISPs in order to limit the OCI. OFCOM must then prepare a report for the Secretary of State assessing the effect of various technical measures. Based on that report the Secretary of State may make an order that ISPs implement those technical measures.

5 R, on the Application of British Telecommunications PLC and Another v Secretary of State for Culture, Olympics, Media and Sport [2012] EWCA Civ 232.
However, the Secretary of State’s order would first have to be approved by both Houses of Parliament.

In addition to granting the Secretary of State the power to impose technical measures on ISPs, the DEA empowers the Secretary of State to adopt regulations regarding court injunctions requiring service providers to block access to sites for the purpose of preventing OCI. The service providers that could be affected by injunctions of this type would include publishers of websites, hosting providers, and providers of other online services. This was the most controversial aspect of the OCI provisions and was heavily watered down during its passage through Parliament. In its final form, industry must be consulted and, as with the order to impose technical measures, the Secretary of State must gain approval by both Houses of Parliament within a 60 day “super-affirmative” window. The current UK government indicated in 2013 that it did not intend to use this power, in particular as s97A of the UK Copyright, Designs and Patents Act already provides copyright owners with a remedy, which has now been tested by rights holders with success6.

There have now been several applications for website-blocking injunctions in the UK under s97A, all of which have been successful. The success of this remedy for copyright holders has even led to the first occasion on which a website-blocking order has been made in Europe in order to combat trade mark infringement7. In this case, the Judge analysed data submitted on the efficacy of s97A injunctions, which showed a “marked and sustained drop in traffic to targeted websites after blocking injunctions were implemented.” The data also suggested that users of the blocked websites did not circumvent the block (e.g. by using VPNs) but instead used different websites. Consequently, Arnold J was persuaded of the efficacy of awarding a blocking injunction. The claimants also had to show that the relief was necessary, dissuasive, not costly or complicated, struck a “fair balance” between fundamental rights and was proportionate. Arnold J found that the relief met all these conditions.

France

In 2006, France transposed into national law the InfoSoc Directive. The French law, called the “DADVSI” in French, crystallized debates regarding the appropriate measures that should be taken to limit OCI. A number of French parliamentarians argued that the individual downloading of copyrighted content for private purposes should be covered by a compulsory licence for private copying and not considered as infringement. Individual lawsuits against Internet users for file sharing in France were in some cases unsuccessful because judges balked at applying harsh infringement sanctions to teenagers who download music for personal usage. It became clear that French copyright law was ill-adapted to the problem of OCI, in part because France’s penalties for copyright infringement were so severe.

Ultimately, the DADVSI did not create compulsory licencing for private downloading. Instead, the law contained a provision stating that individual peer-to-peer downloads would no longer be considered a crime under French copyright law, but would be considered only a misdemeanour subject only to a low-level fine equivalent to a parking ticket. France’s Constitutional Court held that this lightened sanction regime was unconstitutional because it created two different kinds of punishment for an act of copyright infringement depending solely of the technology used to commit the infringement. The court found that this difference in sanctions violated the constitutional principle of equality of punishment for the same offence.

The DADVSI created a new regulatory authority, then called the “ARMT”, to regulate questions linked to interoperability of technical protection measures. The ARMT was supposed to strike a balance between copyright and freedom of expression by ensuring that technical protection measures do not frustrate legitimate uses of the protected work, or prevent interoperability. However, the ARMT was not given any rulemaking authority. The ARMT was to intervene solely in individual cases, either as a mediator or as an arbitrator to order access to interoperability information in appropriate cases. The ARMT was inactive, in part because music labels did not end up making extensive use of anti-copy measures on CDs. The ARMT survived, however, and ultimately became the French regulatory authority today known as the “HADOPI.”

---

6 Case of Twentieth Century Fox Film Corporation and Others v British Telecommunications PLC [2011] EWHC 1981 (Ch) and Dramatico Entertainment Limited and Others and British Sky Broadcasting and Others Limited [2012] EWHC 268 (Ch).
7 Cartier International AG and Others v BskyB and Others [2014] EWHC 3354 CH.
Following adoption of the DADVSI, the French President urged right holders, ISPs and several large hosting platforms to sign a charter pursuant to which right holders undertook to make more content available for legal online offers, ISPs and other Internet platforms agreed to implement graduated response and to experiment with filtering, and the government agreed to put into place a legal framework that would support both the development of legal offers and the implementation of a graduated response regime. After signature of the Elysée Agreement, neither right holders nor ISPs took action, and waited for the government to take the first step by putting into place the promised new legal framework for graduated response. The government then proposed the controversial HADOPI law, which would introduce the graduated response regime in France, a regime that could ultimately lead to the temporary suspension of Internet access for repeat infringers.

The first version of the HADOPI law was adopted by both houses of French Parliament, but invalidated in part by the French Constitutional Court. The first version of the law had given the HADOPI administrative agency the power to order the suspension of Internet access for certain repeat infringers after a procedure in which the suspected infringer could present his or her defence. The Constitutional Court found that the suspension of Internet access constituted a serious restriction on freedom of expression and that such a serious measure should only be ordered by a judicial authority, and not by an administrative agency. After invalidation of this portion of the HADOPI law, the government introduced an amended version that provided for an expedited procedure pursuant to which a court would make the ultimate decision as to whether to suspend Internet access for repeat infringers. Highly debated and applied only once, these provisions were deleted by Decree n° 2013-596 of 8 July 2013, even if they remain included in other provisions of the French Intellectual Property Code.

Under the HADOPI graduated response regime, right holder organizations collect IP addresses of suspected infringers using peer-to-peer networks. The evidence is then transmitted to the HADOPI regulatory authority, who then asks the Internet access providers to provide the names of the subscribers corresponding to the IP addresses. According to HADOPI’s activity report for 2013 – 2014, 12,265,004 identification requests were sent in total to the Internet access providers. Three steps are then followed by the HADOPI: In the first one, the HADOPI sends an initial e-mail to the relevant subscribers informing them of their duty to ensure that their Internet access is not used for infringing purposes, and reminding the subscriber of the existence of legal online offers. According to its activity report for 2013 – 2014, the HADOPI has sent out 3,249,481 first warnings. In the second step, repeat infringers then receive a registered letter from the HADOPI stating that the subscriber has been identified again as the source of infringing content, and that if the conduct does not cease the HADOPI may transmit the file to the public prosecutor for sanctions, which may include suspension of Internet access. According to the last figures published by the HADOPI in 2014, 333, 723 registered letters of this type have been sent. For subscribers that continue to show evidence of infringing activity, the HADOPI then selects, in the third step, the files to be reviewed and may ask the relevant subscriber to participate in a hearing. Only professionals and legal entities are now required to attend said hearing. Approximately 60 hearings took place since the beginning of the third step in June 2011. The HADOPI then hands down a decision. Since 2011, 1,289 decisions were handed down by the HADOPI. The HADOPI can send the files to the public prosecutor if the graduated response regime has not put an end to the illicit acts. Among the above mentioned 1,289 decisions handed down, only 116 decisions decided to send the file to the public prosecutor. No public data is available regarding the following court proceedings after these decisions. It appears that around 25 decisions were handed down by the courts and the amounts of the penalties ordered are between 50 and 700 euros. Only one decision ordered the suspension of the Internet access in June 2013, before its deletion in July 2013.

Since the date it was created, the HADOPI has been subject to vocal criticism, particularly from advocates of Internet freedom. A number of influential members of the French socialist party criticized the HADOPI as being a waste of money, an invasion of fundamental rights and ineffective. Since the election of the socialist François Hollande as President of France, and the new socialist majority in Parliament, the future of the HADOPI regulatory authority and of the French graduated response regime was uncertain. Several initiatives were taken to try to amend the regime. In this regard, numerous proposals, reports and recommendations were drafted, such as the
the French socialist party criticized the HADOPI as being a waste of money, an invasion of fundamental rights and ineffective

so-called Lescure report8 dated May 2013, the Imbert Guaretta report of May 20149, the 2014 annual study of the Conseil d’État10, together with charters signed between the stakeholders. However, no amendment was enacted to date.

In the meantime and similarly to other European countries, like the UK, Article 8(3) of the InfoSoc Directive was transposed in the HADOPI law of 12 June 2009 in Article L. 336-2 of the French IP Code. However, although Article 8(3) of the InfoSoc Directive mentions “intermediaries”, the French article mentions “anybody”. In essence, Article L. 336-2 states that: “(...) the court of first instance (...) may order any measure to prevent or cease any copyright or neighbour rights infringement, against anybody likely to contribute to remedy”.

These provisions remained unnoticed at the beginning. However, they were applied twice to date with success. They were applied for the first time in a famous decision “Allostreaming.com” of the Paris Court of First Instance dated 28 November 2013, in which five French ISPs were ordered to block streaming websites. Another decision of the Paris Court of First Instance, ruling in summary proceedings and mentioning the decision of the CJEU of 27 May 2014 “Telekabel”, was rendered against The Pirate Bay on 4 December 2014. In this case, four French ISPs were ordered to block for France and for one year the streaming website www.thepiratebay.se, its eighteen redirection sites mentioned in the order, three mirror sites and a long list of proxies, by any efficient measure, including the blocking of the domain name.

Spain
On 31 December 2011, the Spanish Official Gazette published the Royal Decree 1889/2011, known as the “Sinde Act”11, which first developed the functions of the Spanish Copyright Commission (“SCC”) and implemented the notice and takedown procedure for the protection of copyrights on the Internet. The SCC had been originally created within the Culture Ministry as a national agency for the defence of copyrights and assigned with arbitration and mediation functions. However, its role was enhanced by the controversial anti-Internet piracy “Sinde Act”, which developed a new notice and takedown procedure for the removal of copyright infringing content from the Internet, and created a new division of the SCC (“Section Two”) in charge of dealing with such new procedure. The operation of this new Section Two of the SCC and the possibility of using the notice and takedown mechanism came into force on 29 February 2012.

Due to the limited success of the previous legislative effort, the Spanish Copyright Act has been recently amended by Act 21/2014 of November 4, 2014, which came into force, in general terms, on January 1, 2015. This new reform has (a) further developed the safeguarding of intellectual property rights on the Internet, (b) broadened the liability of intermediary service providers and (c) increased penalties for copyright infringement.

Act 21/2014 establishes a time limit of one year for the Government to ready the preparatory works for a comprehensive reform of the Intellectual Property Act,

The new reform of the Spanish Copyright Act has broadened the liability of ISSPs ad increased penalties for copyright infringement.
and serves as a short-term solution to the most urgent challenges, among which the fight against online piracy is included. In this sense, it introduces the following measures (which entered into force on 5 January 2015):

a) The safeguarding of intellectual property rights on the Internet

Although the “Sinde Act” had implemented the notice and takedown procedure for the protection of copyrights on the Internet, this amendment to the Spanish Copyright Act shows a considerable improvement in the procedure. As a result, the Section Two of the SCC (in charge of the notice and takedown procedure) has been empowered with more effective reaction mechanisms, it has a broader scope of application and it introduces some technical improvements.

The safeguarding procedure is applicable against (i) alleged copyright infringing activities by information society service providers (”ISSPs”) (e.g. blogs, websites, etc.), as long as the service provider has a significant audience in Spain, or if there is a significant volume of non-authorized works displayed on the website, and (ii) ISSPs providing the description and location of presumably infringing works by means of an active contribution (not mere technical intermediation), such as web pages providing structured and classified links to infringing works. Note that the SCC does not act against individuals downloading content, but only against ISSPs.

One of the main innovations brought by the reform is the possibility of initiating the procedure “ex-officio” (i.e. directly by the SCC), with just a previous complaint from the holder of the rights allegedly infringed. Previously, the rights holder had to file a formal request which was much more complex. Now, the complaint from the right holder is only subject to the previous requirement of having requested removal to the ISSP unsuccessfully. Also, it is now possible to make a generic request for removal instead of reporting the infringements one by one.

b) Liability of intermediary service providers

When the SSC issues a resolution confirming copyright infringement, ISSPs may be required to remove infringing content. If the ISSP refuses to collaborate, intermediary service providers (i.e. advertising, electronic payment providers, etc.) may be required by the Copyright Commission to suspend the corresponding service they offer to the ISSP. This includes access providers, which can be ordered to block access to infringing websites aimed at the Spanish territory. Note that, in order to request a suspension of the service or blocking of access, the Copyright Commission has to be previously authorized by a judge.

In this context, under the amended Spanish Copyright Act, the lack of cooperation with the Copyright Commission (i.e. not suspending the service) is regarded as a very serious infringement of the Information Society Services and E-Commerce Act 34/2002, of July 11, 2002, sanctioned with fines from €150,001 to €600,000.

In addition, in cases of serious infringements, or where the social impact of the infringement is high, the ISSP can be requested to cease activities for a maximum period of one year. In order to ensure the effectiveness of this measure, intermediary service providers may be requested (if approved by a judge) to suspend the service provided to the ISSP. Here again, the lack of cooperation (i.e. not suspending the service) is regarded as a very serious infringement of the Information Society Services and E-Commerce Act 34/2002, of July 11, 2002, sanctioned with fines from €150,001 to €600,000.

Strictly speaking, these two infringements are really one and the same (both sanction the lack of cooperation of the intermediary service provider), but can be triggered by the two different situations described above.

c) Penalties for copyright infringement

In addition to the penalties for intermediary service providers described above, the amendment provides for increased fines for those ISSPs who do not comply for two or more times with requests for removal. This conduct is regarded as a very serious infringement sanctioned with fines from €150,001 to €600,000. Same penalties are envisaged for the resumption of infringing activities by the same ISSP for two or more times.

Finally, as previously stated in (b), in cases of serious infringements, or where the social impact of the infringement is high, the infringement can lead to the following consequences: (i) the publication of the resolution in the Spanish Official Gazette and in two national newspapers or on the ISSPs website, and (ii) the
ISSP can be requested to cease activities for a maximum period of one year.

As a final note, it must be said that even though these measures have already had an impact\textsuperscript{12}, a regulation developing Act 21/2014 is still pending to be issued by the Government. Thus, the end results and effectiveness of these new measures may still increase in the near future.

**Germany**

The German legislator did not see a need to insert special provisions into German law to implement Article 8(3) and recital 59 of the InfoSoc Directive as it was of the opinion that the possibility for right holders to apply for an injunction against an intermediary was already provided for under the German Copyright Act and Telemedia Act. Further, unlike the UK, France and Spain, no laws have been or are planned to be introduced in Germany obliging ISPs to assist rights holders in the reduction of OCI.

Germany relies on a system to fight OCI in which at first warning letters, including pre-formulated cease-and-desist undertakings, are sent to copyright infringers. These warning letters are a well-known measure in the general populace and already stop a majority of private OCI cases in Germany. If the infringers do not sign the undertaking the rights holders have as a second step the possibility of filing for a preliminary injunction against the infringer to stop the infringing act.

Further Germany has extensive case law concerning the so-called “Störerhaftung” (Breach of Duty of Care) according to which not only the copyright infringer himself can be held liable but also auxiliary persons to the perpetrator of the copyright infringement. The duty of such an auxiliary person is limited to cease and desist and removal. The “Breach of Duty of Care” has three main requirements:

1. The auxiliary person must in some way contribute willingly and causatively to the copyright infringement, e.g. by providing the means of access to websites with pirated content.
2. The auxiliary person must have had the possibility of preventing the copyright infringement.
3. The auxiliary person must also have violated due diligence obligations. This third requirement serves...
as a kind of corrective to prevent the breach of Duty of Care liability from becoming excessive. It is used to incorporate a balancing of interests between the auxiliary person and the rights owners. Generally it is required that the auxiliary person is or should have been aware of the copyright infringement either because the infringement is apparent and easily recognisable in itself or because the auxiliary person has been made aware of the infringement.

Whether these existing German rules really are sufficient to implement the relevant provisions of the InfoSoc Directive is still disputed amongst scholars. In two recent cases, German courts refused to grant an injunction against an access provider based on the existing provisions.

The decision of the Higher Regional Court of Hamburg of 21 November 2013 (U 68/10) concerned a claim of the Society for Musical Performance and Mechanical Reproduction Rights (GEMA) against the biggest German access provider. The defendant offered access to a website where users could access pirated copyright protected works. Although the court recognized the copyright infringement and the general possibility of liability of access providers it dismissed the claim as it deemed the requested blocking measures to be unreasonable. The Court stated that the access provider’s business model was “neutral concerning the content, socially adequate and in accordance with the law”. Further, the blockage could inherently lead to the restriction of access to works which are not protected or not pirated which would result in the potential infringement of third parties’ rights. Lastly the Court claimed that the blocking measures would cause the access provider to violate the confidentiality of telecommunications that is protected under Art. 10 of the German constitution as it could be necessary to use protected information regarding the communication process to achieve the blocking.

This reasoning was followed by the Higher Regional Court of Cologne in its decision of 18 July 2014 (6 U 192/11) in a claim against a music file sharing platform. This decision was made after the Telekabel decision of the CJEU. The German Court extensively referred to the Telekabel decision. They concluded from that decision that there is generally the possibility of granting a blocking order in Germany. After clarifying that this general possibility exists in Germany the Court continued to examine extensively whether a blocking order was necessary and acceptable in this particular case. The Court weighed up the rights of the applicant and defendant in a similar way as the Higher Regional Court of Hamburg and decided in favour of the defendant arguing that an injunction granting the blocking of access to a website would be unreasonable for the access provider.

Both decisions are pending before the German Federal Supreme Court.

As the second decision was based on the Telekabel case of the CJEU the German Federal Supreme Court will most likely not overturn the decision on the basis of the principles in that case. It might however be that the German Federal Supreme Court weighs the interests of applicant and defendant differently and therefore reaches a different conclusion. Most likely the German Federal Supreme Court will set high barriers for website-blocking injunctions in Germany in these appeal decisions.

Rest of the World

Outside Europe there have also been significant developments in Asia, notably Australia, where the government has announced new initiatives including amendments to the Australian Copyright Act that will enable rights holders to apply for an injunction requiring ISPs to block websites operated outside of Australia. In Russia, the government has introduced amendments to its anti-piracy law which will come into force on 1 May 2015, extending the regime. At the same time, the Russian government is considering a proposal by the Russian Union of Rightsholders to introduce a fixed royalty fee to be paid by telecom operators to rights holders.

Australia

The Australian government announced in December 13 new initiatives to address concerns about online copyright infringement. A ‘frequently asked questions’ (FAQ) document about the reforms was also released. There were two key planks to the announcement:

a) a call to industry to develop a new industry code within 120 days, or face new binding regulatory arrangements to address online piracy; and

b) amendments to the Copyright Act 1968 (Copyright Act) will be made to enable rights holders to apply for a court order requiring ISPs to block access to websites

operated outside of Australia which provide access to infringing content.

The new measures will be reviewed after 18 months to assess their operation and effect.

The Australian Communications Alliance published a draft code on 20 February 2015\(^{15}\). This draft code is currently in a 30-day public consultation phase before it is finalised and put before the Australian Communications and Media Authority. The consultation phase is required by the Telecommunications Act 1997, but should also assist in addressing criticisms of previous code processes about the level of consumer involvement. The draft code is not yet complete, and is subject to change after this consultation period has ended. One of the key issues for determination – the costs of implementing the code, and who should bear those costs – is still under negotiation and the draft code is currently silent on the issue of costs.

Once finalised, the code will be registered as an industry code under Part 6 of the Telecommunications Act. Compliance with the code will be one of the issues to be assessed by a Court in determining whether an ISP should be held liable for ‘authorising’ any infringements committed by customers under ss. 36 or 101 of the Copyright Act.

The Government set out its expectations and policy objectives for the code in a letter to industry\(^{16}\). The draft code complies with these expectations and objectives by creating a copyright notice scheme. This scheme will allow rights holders to notify ISPs of any infringements of copyright by submitting a report in a standard form to the ISPs, which will identify the IP addresses of suspected online infringers. ISPs will then send a notice to the holders of the account to which that IP address had been allocated at the time of the infringement. In the first instance ISPs will send a notice containing educational material explaining where to access legitimate alternatives and how to avoid copyright infringement online. A second offence will incur a warning notice and a third a final notice. The draft code allows rights holders to request a list of IP addresses that have been sent each of these notices. At this point the rights holders can apply to a federal court or tribunal for an order allowing them to obtain the identity of the holder of any account that has received a final notice from the ISP. It is crucial that until such an order has been obtained, rights holders will not have access to the identities of any alleged infringers.

Final notices can be challenged by account holders, and all challenges will be passed to an adjudication panel, which has an obligation under Article 3.10.13 of the draft code not to disclose the identity of any account holder. The $25 fee for seeking an adjudication has been referred to by the Australian Communications Consumers Action Network (ACCAN) as a “fine by stealth”\(^{17}\).

The draft code also provides for oversight of this procedure by allowing for the creation of a Copyright Infringement Panel (“CIP”), consisting of representatives of rights holders, ISPs and the consumer group ACCAN. The CIP will oversee the scheme by authorising the processes by which rights holders will identify infringements of copyright and overseeing the adjudication panel. The CIP will also draft all the relevant documentation such as the notices and material advertising the scheme to the public.

The legislation to implement the new site blocking measures has not yet been released. As such, the precise scope of the measures is not yet known. We do know that site blocking will only apply to overseas websites, as rights holders are not prevented from taking direct infringement action against websites operated within Australia. In considering whether to make a blocking injunction, a court would be required to have regard to the rights of any person likely to be affected by the grant of an injunction, and court rules would operate to allow the court to make any directions it considered appropriate in the circumstances.

In the original Discussion Paper foreshadowing the reforms released in July, the site blocking proposal was limited to sites where the “dominant purpose” of the website was to infringe copyright. Further, it was stated that rights holders would be required to meet any reasonable costs associated with an ISP giving an effect to an order and to indemnify the ISP against any damages claimed by a third party.

In contrast, the December Government announcement refers to site blocking of a website “which provides access to infringing content,” and makes no mention of ISP costs or indemnities. It is unclear whether this represents a shift in policy or whether the legislation to be introduced will more closely reflect the July proposal.

---


Russia

On 24 November 2014, the Russian President signed into law a bill introducing amendments to the so-called Anti-piracy Law and expanding its scope to all types of copyright-protected content available on the Internet, except for photographs (the “Law”). The Law will take effect on 1 May 2015.

Under the Law the following procedure will become available for rights holders wishing to restrict access to audio-visual works which have been placed on the Internet illegally:

The right holder may seek a preliminary injunction before the Moscow City Court against illegal use of content on a particular websites.

Once a preliminary injunction has been obtained, the right holder may file an application with the Russian state authority in charge – Roskomnadzor – seeking restriction of access to the website. Within three business days Roskomnadzor must determine the hosting provider and send an electronic notification requesting the removal of the infringing content;

Within one business day from the date of receipt of notification, the hosting provider must inform the website owner of the need to immediately remove the infringing content from the website or restrict access to such content. The website owner has one business day to remove the infringing content.

If the website owner fails to do so, the hosting provider must restrict access to website within three business days from the date of receipt of Roskomnadzor’s notifications. If the website owner and/or the hosting provider fail to restrict access to the website, Roskomnadzor sends the information on such website to telecom operators, which must restrict access to the website within twenty-four hours.

In addition to the above procedure, the Law allows the right holder to undertake an out-of-court measure by sending a complaint to the website owner. Within 24 hours from the complaint’s receipt the website owner must cease the infringement or present proof evidencing the lawful use of content on the website. To make this work the Law obliges the website owners to disclose his/her name, address and email on the website.

The Law further provides for a possibility of perpetual restriction of access to the website where infringing content was placed repeatedly and this has been confirmed by the court’s ruling. Upon such court’s ruling Roskomnadzor sends the information on such website to telecom operators which in turn must restrict access to the website within twenty-four hours upon receipt of the Roskomnadzor’s notification.

In parallel with the discussion on the amendments to the Law the Russian Union of Right Holders (the “RUR”) has proposed fighting piracy by introducing a fixed royalty fee to be paid by the telecom operators to right holders in exchange for unlimited use of almost all types of content on Internet. It is suggested the royalty will be collected by a collecting society accredited by the state. This initiative is now under consideration by the Russian Government.

These two parallel processes (one – introduction of a thorough anti-piracy legislation; and another – introduction of a fixed royalty fee for unlimited use of content on Internet) clearly do not look like a perfect match.

Conclusion

Is 2015 the year of the website-blocking injunction? The ability for rights holders to apply for website-blocking injunctions against ISPs certainly appears to be a feature of all the new regimes adopted by governments seeking
to reduce OCI in various countries around the world. Following the CJEU ruling in *Telekabel* and the spate of successful applications in the UK over recent times, it seems likely that we will see an increase in the number of websites making available infringing content being blocked both within Europe and elsewhere. This is good news for rights holders although there are concerns that users can easily circumvent certain blocking measures, using VPNs or other methods, particularly if the website is not blocked in every jurisdiction worldwide. Nevertheless, it is encouraging for rights holders that governments are also improving national graduated response regimes for reducing OCI across the globe.