Online infringement of IPRs: overview and rights-holders' strategy guide

Martin Cuell, Hannah Batten, Peter Singfield, Rachel Warren and Neil Parkes
Foot Anstey LLP

The rapid growth of the internet and more recently the rise of high-speed broadband, WiFi and the 3G/4G networks (and the ensuing surge of internet related technologies) has led to a seismic shift in the role of technology in society. Consumer habits and expectations have transformed. There is an increasing desire to remain connected, fuelled by the speed and ease with which we are now able to communicate and access products and services (and the relative affordability of the technology allowing us to do so). This has had a fundamental impact on the way we use, access and exploit intellectual property rights (IPRs). This in turn creates challenges for those seeking to protect their rights online, and opportunities for those seeking to infringe.

This article considers:

- Types of online infringement, particularly the risks around online copyright and trade mark infringement.
- Key strategies for preventing, countering and reacting to it.

It recommends a risk-based and resource sensitive three-step strategy, covering:

- Protection of the underlying IPRs,
- Adopting appropriate measures designed to counter the particular online infringement risks,
- Swift and effective enforcement action when infringing activity is identified.

It also highlights the importance of flexibility in business models, which enables rights-holders to stay ahead of technological developments, and capitalise on new opportunities to mitigate and undermine new or changing infringement risks.

**TYPES OF ONLINE INFRINGEMENT**

Infringement takes many forms, including:

- Piracy: copyright.
- Counterfeit goods, keywords, metatags, and domain names: trade marks.
- Illegal file-sharing of 3D designs: design rights.
- Data theft: database rights.

**Online infringement of copyright**

The Copyright, Designs and Patents Act 1988 (CDPA) governs UK copyright, and protects (sections 1 to 8, CDPA):

- Original literary, dramatic, artistic and musical works.
- Databases (consisting of other copyright works arranged systematically or methodically).
- Sound recordings, films and broadcasts.
- Typographical arrangements of published editions.

Copyright gives the rights-holder the exclusive right to carry out certain restricted acts in relation to the protected work, including (sections 16(1) and 17 to 21, CDPA):

- Copying it.
- Issuing copies to the public.
- Renting/lending it.
- Performing, showing or playing it in public.
- Communicating it to the public by electronic transmission.
- Adapting it (or doing any of the above in relation to adaptations of it).

Infringement occurs when a person does, or authorises someone to do, any of these acts without the rights-holder's consent (section 16(2), CDPA). Online infringement claims commonly rely on allegations of infringing "communications to the public", with recent cases establishing some key principles:

- "Communication to the public" should be interpreted broadly but must involve communication to a new public (a group of people who the rights-holder did not take into account when authorising previous communications of the work) (Sociedad General de Autores y Editores de España (SGAE) v Ravel Holteles SA (Case C-306/05) [2006] ECR I-11519).
- Whether the defendant's activities are profit-making can be relevant but is not essential (Football Association Premier League v QC Leisure; Murphy v Media Protection Services Ltd (Joined cases C-403/08 and C-429/08) [2012] Bus LR 132).
- Supplying technical means for others to infringe can be sufficient, even where the defendant did not participate in the transmission of an infringing work (Twentieth Century Fox v Newzbin [2010] EWHC 608 (Ch)) (Newzbin 1).
- Communication to the public happens where someone allows content on their computer to be uploaded to a P2P file-sharing network (Dramatico Entertainment Ltd v BskyB [2012] EWHC 268 (Ch)) (Pirate Bay).
- Transmission/retransmission using a different technical means from that used originally requires the rights-holder's separate authorisation. It will be a "communication to the public" unless it is merely to ensure or improve reception of the original transmission. In such circumstances there is no need to consider if there is a communication to a "new public" (ITV Broadcasting Ltd v TV Catchup Ltd (Case C-607/11) [2013] Bus LR 1020).
- Hyperlinks or embedded links to copyright works amount to "communications to the public", but with no infringe where they direct users to websites which make the work freely available to internet users with the rights-holder's consent. Such links do
not enable users to access content otherwise unavailable to them and so there would be no communication to a "new public" (Svensson v Retriever Sverige AB (Case C-4666/12 [2014] All ER (EC) 609).

Many websites found to infringe copyright by UK courts have not themselves made the infringing content available, but have "authorised" users to infringe. Newzbin I held that this means "the grant or purported grant of the right to do the act complained of" and that it must go beyond "mere enablement, assistance or even encouragement" (per Kitchin J, at [80]). In both Newzbin I and Pirate Bay, the court found the website operators had "authorised" infringement by their users.

Section 107 of the CDPA creates criminal offences where copyright infringement takes place in the course of a business, and with knowledge or reason to believe the actions will infringe. These offences cover:

- Making for sale/hire, or otherwise dealing with (including by importing, possessing and/or distributing) infringing copies.
- Making or possessing articles designed or adapted to create infringing copies.
- Communicating a work to the public (or otherwise than in the course of a business) to the extent to prejudicially affect the rights-holder.
- Performing a literary, dramatic or musical work, or playing/showing a sound recording or film in public.

**Online piracy.** Illegal file-sharing, downloading and streaming of content has become a major issue for the creative industries in recent years. Digital technology introduces easy ways to copy files at little or no cost. The pioneering file-sharing website Napster (1999 to 2001) popularised P2P file-sharing of music, quickly, easily and for free from a user's home. This was new and attractive to users and the legitimate music market initially had no answer to it. Within a year of launching, Napster had over 20 million users and had contributed to, if not triggered, a fall in global record sales.

The music industry was slow to recognise the change in consumer habits and, rather than embracing this new technology, sought to stamp it out through aggressive legal action against sites and users. While effectively leading to Napster's demise, alternatives such as Pirate Bay, BitTorrent and MegaUpload rose to take its place.


Recently, significant increases in internet speeds have enabled the upload/download of larger files, expanding the threat of piracy to the film, broadcasting and gaming industries. A report by Kantar Media (http://stakeholders.ofcom.org.uk/binaries/research/telecoms-research/online-copyright/w4/HIGH_VOLUME_INFRINGERS.pdf) found that 22% of all content consumed online between May 2012 and May 2013 infringed copyright: around 1.5 billion files.

Despite this, the audio-visual content sector's message is increasingly positive. Lawful, cheap and user-friendly services like Spotify and Deazer (music), Netflix, Amazon and Blinkbox (TV and film), and advertising-supported services like YouTube and Vevo, have revolutionised the market and provide alternatives to infringing services. Commentators suggest there is a growing recognition that, faced with a genuinely attractive alternative digital marketplace, users turn away from infringing activities.

Evidence is emerging to support this, and the IFPI Report showed that during 2013 music subscription service revenues grew by 51.3% to exceed US$1 billion for the first time, and paying subscribers reached 28 million (up from eight million in 2010).

Sandvine's Global Internet Phenomena Report 2014 (www.sandvine.com/trends/global-internet-phenomena) revealed Netflix now accounts for 32.39% of all US traffic during peak periods, and BitTorrent just 5.03%. The report also indicated that illegal file-sharing as a whole now makes up just 7% of US daily network traffic (down from 31% in 2008).

For countries where there is a healthy, diverse range of legal services available, these figures are encouraging. However availability of these services varies significantly, and the Sandvine Report clearly illustrates that where they are limited, levels of illegal file-sharing remain high.

It is clear that the availability of legal services that genuinely compete with their illegal counterparts is key to winning the online piracy war. With that in mind, the European Commission recently signalled that a top priority for 2015/2016 is the creation of a Digital Single Market (May 2015). It set out 16 initiatives categorised by three central pillars:

- Better access for consumers and businesses to digital goods and services across Europe.
- Creating the right conditions and a level playing field for digital networks and innovative services to flourish.
- Maximising the growth potential of the digital economy.

The initiatives include:

- Abolishing unjustified "geo-blocking", which denies access to websites based on location or re-routes users to local sites (where pricing may be different).
- Legislating to modernise and harmonise copyright law to improve EU-wide access to online content, for example ensuring online content legally acquired in one member state remains accessible from others (portability), and facilitating the purchase from one member state of content/services available in another. It remains to be seen how territorial exclusivity of some rights such as football broadcasting and British Broadcasting Corporation (BBC) funded services will be addressed.
- Reviewing Directive 2010/13/EU on audiovisual media services, and considering whether this should be adapted or expanded to cover new services and business models.
- Investigating how best to tackle illegal content online, and the role intermediaries play in this process.

There are significant thorny and controversial issues to be addressed, but if changes lead to increased availability of legal content services across the EU, this could help to further reduce European users' use of illegal file-sharing services.

**3D printing.** 3D printing could bring unprecedented disruption to the manufacturing industry in particular. While offering new opportunities, as the quality and affordability of the technology increases, it is expected to trigger an increase in design right, copyright and trade mark infringement. This could be through:

- File-sharing of computer aided design (CAD) files, enabling 3D prints which replicate a "work of artistic craftsmanship" (although the Supreme Court's decision in Lucasfilm Ltd v Ainsworth [2011] UKSC 39 suggests this will be limited, as copyright will not protect practical articles).
- Use of a design in which copyright subsists.
- Use of a registered trade mark.

Due to the technology's infancy, uncertainty remains as to the approach of rights-holders and the courts, caused in part by debate over the copyright status of CAD files. In particular, questions arise over whether they are "computer programs" for the purpose of the CDPA (and the underlying EU Software Directive 2009/24), which could afford protection as literary works under section 31(1)(o).

global.practicallaw.com/ip-guide
With the current lack of 3D printing infringement case-law, it is hard to predict how this area will evolve. What is clear is that the law is not yet equipped to deal with the anticipated growth of this technology, so without further legislative changes there will be numerous questions to answer in the courts.

**Online infringement of trade marks**

Trade marks are a "badge of origin", distinguishing the goods of one business from those of another. They are of huge commercial importance and value, particularly those of well-known and desirable brands.

Infringement occurs in three different ways when a person uses in the course of trade (section 10, Trade Marks Act 1994 (TMA)/Article 9, Regulation (EC) 207/2009 on the Community trade mark):

- A sign identical to the registered trade mark in relation to identical goods and/or services to those for which the mark is registered.
- A sign which is:
  - identical to the registered trade mark where such use relates to similar goods and/or services, or similar to the registered trade mark where such use relates to identical or similar goods and/or services; and
  - that use creates confusion in the minds of the public and a likelihood of an association with the mark.
- A sign which is identical or similar to the registered trade mark, and that use takes unfair advantage of, or is detrimental to, the distinctive character or reputation of the mark without due cause.

Section 92 of the TMA makes counterfeiting a criminal offence. Broadly, this covers the unauthorised use of a registered trade mark (or sign likely to be mistaken for it) in relation to the packaging, advertising, sale, hire and/or distribution of goods for which it is registered, with a view to gain (for the person committing the offence or a third party) or intent to cause loss.

Online trade mark infringement usually involves the infringer taking advantage of a brand’s value and reputation to promote or sell its own products or services (such as counterfeit goods) or through unauthorised use in keywords, metatags or domain names.

**Counterfeit goods.** The International Chamber of Commerce (ICC) has suggested that counterfeiting is "one of the fastest growing economic crimes of modern times". It reduces sales volumes and licensing revenue and can lead to brand dilution and reputational damage.

While counterfeit goods have long been an issue, e-commerce has transformed the global marketplace for them, providing new selling opportunities with reduced risks:

- Infringing goods no longer need to be imported into a target market before being offered for sale, thereby delaying any customs intervention until after payment has been received. This transfers any risk of loss to the purchaser from the counterfeiter.
- Traders can target high value markets while basing themselves in jurisdictions with less stringent laws/attitudes to counterfeiting.
- Physical inspection of the product occurs on delivery and therefore after payment, assisting traders to deceive consumers into thinking they are purchasing a genuine article.

Unlike file-sharing and streaming, legal alternatives (in the form of genuine products) have always been available. Consequently, there are no signs that counterfeiting activities will slow; indeed 3D printing advances may exacerbate the problem. Rights-holders should be pro-active and vigilant and take measures to ensure their rights are adequately protected.

**Key words.** Keyword disputes have been a regular feature in recent years, focusing attention on the extent to which a trade mark owner can prevent the purchase of a key word using its trade mark by a third party, which is then used to draw internet traffic to a competitor’s website. Several cases have considered whether, by selling the key word or publishing the results of a search, the service provider was “using” the trade mark in breach of the TMA (Victor Andrew Wilson v Yahoo UK Ltd [2008] EWHC 361 (Ch)) or 'Ethereal S.A and Ors v Ebay International A.G and Ors [2009] EWHC 1094 (Ch).

Clarity was provided in the joined cases C-236, 237 and 238/08 Google France, Google Inc. v Louis Vuitton Malletier, referred to the European Court of Justice (ECJ) by the Cour de Cassation on two points:

- Was Google’s Adwords service an infringement?
- Could a search engine provider’s liability be limited under Article 14 of the E-Commerce Directive (2000/31/EC), the “hosting defence”: see Notice and Take-down?

The ECJ decided that:

- Rights-holders can stop third parties from using a search engine keyword identical to its trade mark to advertise goods/services identical to the rights-holder’s, where the advert does not allow the average internet user (or enables them only with difficulty) to ascertain whether the goods/services originate from the rights-holder or a third party.
- A search engine that stores a sign identical to a trade mark as a keyword and organises advertisements on the basis of that keyword does not use the mark.
- A search engine provider can rely on the hosting defence if it did not play an active role that gave it knowledge of, or control over, the data stored, and acted quickly to remove or disable access to the data concerned if it became aware of infringement.
- An advertiser’s purchase of a keyword identical to a trade mark was “use in the course of trade” and a rights-holder can object to the use of the keyword if it interferes with the mark’s function.

Since Google France, Interflora Inc and Anor v Marks & Spencer Plc & Anor [2009] EWHC 1095 (Ch) has been back to court on several occasions. The most significant of these was the appeal against the original 2009 decision, claiming that the judge had erred in holding that the burden of proof was on the third party advertiser to show that its advert was sufficiently clear to exclude a risk of confusion on the part of the average consumer over the origin of the goods/services. Unexpectedly the appeal was successful, so further guidance may emerge when this case is reconsidered. However, given the long-running case history, it is likely to be some time before clarity prevails.

**Cybersquatting.** This is where someone selects a trade mark or name and registers domain names using it (or something similar to it) before the rights-holder. It may be with a view to simple gain (through sale of the domain to the rights-holder at a premium), or to facilitate online fraud from counterfeiting.

The frequency of new generic top level domains (gTLDs) means blanket purchases of domains is an increasingly costly exercise but rights-holders must remain vigilant and ensure they register new gTLDs before third parties. Every new gTLD has a sunrise period before it goes on sale to the public, allowing rights-holders to defensively register domain names.

BT Plc v One in a Million Ltd [1999] 1 WLR 903 is the key case in this area, and considered a claim for passing off where the defendant, a dealer in domain names, had purchased domains including bt.org and marksandspencer.com. The Court of Appeal said that the courts should consider the similarity of the names, the
defendant’s intent, the type of trade and any surrounding circumstances, providing injunctive relief where a defendant is equipped with, or intends to equip another with, an “instrument of fraud”.

It is unclear what would happen where a person purchases a domain incorporating a trade mark and, while not attempting to extract money from the rights-holder, makes minimal use of it, effectively waiting to be contacted by them. In this instance there can be no inference that it is being used as an instrument of fraud. However, if the person requests payment from the rights-holder this will immediately raise grounds under the ICANN Uniform Domain Name Dispute Resolution Policy (UDRP) for proceedings for the transfer of the domain on the basis of bad faith.

Rights-holders who consider that a domain name registration infringes their trade mark can use UDRP proceedings where:

- The domain name is identical or confusingly similar. This will depend on the facts and may require evidence of the likelihood of, or actual, confusion.

- The registrant has no rights or legitimate interests in respect of the domain name. This may be evidenced where the domain is not being used or where the registrant has shown no intention of using it.

- The registrant’s domain name has been registered and is being used in bad faith. This occurs where the registrant acquired the domain primarily to sell, rent, or otherwise transfer it to the rights-holder (or a competitor) for payment exceeding the amount paid by the registrant.

UDRP v legal proceedings. UDRP has three main advantages over trade mark infringement/passing off proceedings:

- UDRP applies internationally, meaning that a successful rights-holder can easily acquire an infringing domain, regardless of the registrant’s location.

- The dispute can be dealt with far more cost-effectively. If a rights-holder’s primary objective is to prevent use of the domain by the registrant and acquire it quickly, UDRP (while potentially slower) is far more cost-effective than an interim injunction.

- Use of UDRP does not prohibit the rights-holder from issuing legal proceedings after the dispute has been resolved, thereby providing it with two separate forms of attack against cyber-squatters.

**STRATEGIES FOR TACKLING ONLINE INFRINGEMENT**

The ideal way for rights-holders to protect against online IPR infringement is to adopt a policy of thorough protection by all possible means, with a consistent “zero tolerance” approach to enforcement. In reality, very few rights-holders have unlimited resources to protect/enforce their IPRs.

Rights-holders should prioritise. They should adopt a carefully considered and commercial approach to protection, counter measures to infringement, and enforcement, seeking to allocate resources to the most effective actions. Factors to consider include:

- The importance of the IPR.

- Key jurisdictions for the business, and plans for expansion.

- The level of resources required (for example, use of copyright notices and trade mark signs is low-cost, while a complex digital rights management (DRM) mechanism may be expensive to implement and maintain).

- Particular areas of risk.

**Protection**

Rights-holders should:

- Wherever possible, ensure registrations are obtained for all key trade marks/designs in the territories in which it operates/intends to operate.

- Where relevant, seek registration of important copyright works. Although not possible in the UK, some jurisdictions do allow rights-holders to do this.

- Ensure appropriate website terms of use are in place that include clear statements on IPR ownership.

- Make sure content protected by copyright that is uploaded to the internet is always accompanied by a copyright notice (for example, © [year of creation] [name of rights-holder]).

- Ensure trade marks are always accompanied by ® (if registered), or ™ (if unregistered).

**Counter measures**

**DRM technologies.** For rights-holders whose content is (or could be) made available online DRM can be a useful tool for mitigating infringement risk.

DRM enables rights-holders to control access to copyrighted material by removing the consumer’s control over their use of the file, and ensuring that only those with valid permissions can use it. DRM was developed in response to concerns around online piracy, and has been used by film studios, music labels, ebook publishers and streaming stores to curb the redistribution of legally purchased copyrighted digital content.

DRM remains popular with rights-holders but has its critics, particularly over whether it creates a fair end-user experience where users often have multiple devices. Further, relying on online authentication can hinder user experience when servers go down and effectively prevent the user from using their content.

Use of DRM can attract negativity, such as that experienced by Sony between 2005 and 2007, and so rights-holders should consider whether DRM is appropriate, and select the most suitable form necessary to achieve its goal without encroaching on users’ legitimate rights.

**Encryption.** This is a form of DRM that involves the scrambling of data and embedding of a digital signature, engraved during manufacturing or distribution, which can be used to provide evidence of the material’s origins.

Encryption can help rights-holders protect IPRs from being unlawfully shared (and can delay the time it takes for a decrypted copy to become widely available). However like DRM, it is vulnerable to accusations that it violates users’ rights to lawfully use purchased content, and poor engineering can make it vulnerable to modification.

**Monitoring.** Enforcement action, where necessary, should be taken swiftly to minimise damage, so effective monitoring is important. Trade mark attorneys and many law firms offer “watch” services, which warn rights-holders of attempts to register potentially conflicting trade marks in territories covered by the service. They do not however cover infringing use alone, so additional monitoring may be needed.

These additional services clearly come at a cost, and can be provided by third party companies or by purchasing monitoring software. More complex services are also available, combining technology with professional teams that devise and execute brand strategies to combat IPR abuse, monitor supply and distribution chains, detect counterfeits, and identify the locations of infringers.

The benefit of monitoring software has been questioned before the courts, where it was suggested that it may do no more than indicate that someone has the capability to infringe (that is, has an
internet connection) rather than that they have actually done so (Media CAT Ltd v Adams [2011] EWPCC 9). However, evidence from monitoring software has since been accepted as the basis for granting a Norwich Pharmacal order for disclosure of suspected infringers’ identities by internet service providers (ISPs), to enable action to be taken against them (Golden Eye (International) Limited and Others v Telefonica UK Limited [2012] EWHC 723 (Ch)).

European Observatory’s enforcement database. Where the primary online infringement risk is counterfeiting, rights-holders with EU trade marks or registered designs can use the European Observatory’s enforcement database. This is a secure bank of information that can be accessed by customs and law enforcement agencies, and supports information sharing and detection and seizure of counterfeit goods.

Registration is free and enables rights-holders to link their IPRs to the database, and upload details of protected products and information about distribution and sales channels.

Rights-holders can alert authorities via the database and receive notifications when suspicious consignments are found. Where action is required, the database helps to streamline processes by generating pre-completed "applications for action" for submission to customs authorities, enabling them to take action on the rights-holder’s behalf.

Agile business models. Rights-holders should be alive to emerging technologies and consumer trends, and ensure that business models are flexible enough to adapt and grow with them.

Staying ahead of the curve allows rights-holders to identify and address new risks before they become systemic, and puts them in the best possible position to capitalise on opportunities the changes present.

Resistance to disruptive technology is generally futile, so a willingness to embrace it and proactively seek new ways of doing things is a significant weapon against online infringement.

Enforcement

Traditionally the rights-holder takes action against the infringer to bring infringement to an end and recover damages for losses (or an account of profits). However, the speed, simplicity and anonymity that technology provides to infringers has made enforcement of IPRs significantly more difficult.

Action can, in theory, focus on individual users (being either consumers or uploaders/sellers of illegal content or products), or those that provide the means for infringement to take place (that is, websites that host or provide methods for distributing illegal content, or purchasing counterfeit goods). Internet service providers (ISPs), by enabling their subscribers to access infringing content/websites, also play a role, and many recent cases have addressed their responsibilities.

Notice and take-down. Regulations 17 to 19 of the Electronic Commerce (EC Directive) Regulations 2002 (which incorporate the E-Commerce Directive) afford protection to information society services providers (ISSs), including ISPs and auction sites, from liability in certain circumstances.

The most relevant to online infringement is the “hosting defence”, under Regulation 19/Article 14, which grants immunity to an ISS that stores information supplied by a service recipient, provided that both of the following apply:

- It does not have actual knowledge of the unlawful activity or information and, as regards claims for damages, is not aware of facts/circumstances from which the unlawful activity or information is apparent.
- Upon obtaining such knowledge or awareness, it acts expeditiously to remove or to disable access to the unlawful activity or information.

Rights-holders can put a stop to infringing activity, by sending the ISS a “take-down notice”, setting out details of the infringement and asking it to remove or disable access to it. The ISS then has an incentive to take action, or risk losing the protection of the hosting defence.

This notice and take-down procedure is often the first enforcement step taken by rights-holders, and can be an effective and inexpensive solution, particularly for small-scale infringements.

Blocking injunctions. Website blocking injunctions are useful against online infringers where the issue of a “take-down notice” has not been effective in deterring further infringement. Section 97A of the CDPA provides that an injunction may be obtained against a service provider (for example, an ISP) where that service provider has actual knowledge of another person using their service to infringe copyright. The Court would consider all of the following:

- Whether the ISP has received notice (through a means of contact in accordance with Regulation 6(1)(c) of the E-Commerce Directive).
- The extent to which any such notice provides the name and address of the sender.
- Whether the notice establishes the details of the alleged infringement in sufficient detail.

The number of blocking injunctions granted by the courts has increased recently. This may be a reaction to increased occurrences of online infringement, but also indicates the courts' willingness to step in to prevent infringement, even where the target website is not hosting the infringing content but providing hyperlinks to other locations from where it can be streamed/downloaded (see above, Online Infringement of copyright, in particular the commentary on Svensson).

In October 2014 the High Court determined a test case concerning the availability of blocking orders targeted at websites infringing trade marks by selling counterfeit goods (Cartier International AG & Ors v British Sky Broadcasting Limited [2014] EWHC 3354 (Ch)). Without an express provision for trade marks mirroring section 97A of the CDPA, Arnold J held that jurisdiction was available pursuant to the general power to grant injunctions contained in section 37(1) of the Senior Courts Act 1981, read in accordance with Article 11 of Directive 2004/48/EC on enforcement (Enforcement Directive).

Arnold J then identified the following four threshold conditions for a blocking order to be granted (all four must be satisfied):

- The ISPs must be "intemediaries", under Article 11 of the Enforcement Directive.
- The users/operators of the website must be infringing the trade mark.
- The users/operators must be using the ISP's service to infringe.
- The ISP must have actual knowledge of the infringement.

Finally, he held that the court must consider the principles to be applied when deciding whether to grant the injunction, including whether the relief:

- Is necessary.
- Will be effective.
- Will be dissuasive.
- Is not unnecessarily complicated or costly.
- Creates barriers to legitimate trade.
- Is fair and equitable.
- Is proportionate.
To date, the High Court has granted injunctions in relation to:

- Streaming of premier league football matches (Football Association Premier League Limited v BskyB & Ors [2013] EWHC 2057 (Ch)).
- Films (20th Century Fox & Ors v Sky UK & Ors [2015] EWHC 1082 (Ch)).
- Music (EMI Records Ltd & Ors v British Sky Broadcasting Ltd & Ors [2013] EWHC 379 (Ch)).
- Trade marks (Cartier).
- More recently, ebooks (The Publishers Association v BT & Ors, awaiting reported judgment).

While the costs of preparing and making applications for blocking injunctions will undoubtedly prevent the opening of the floodgates, it is expected that the effectiveness of such orders will lead to their use being much more common in future.

**Criminal enforcement and strategy.** We have highlighted that there are a number of criminal offences relating to copyright and trade mark infringement. In addition, various "general" criminal offences may also be committed by those engaging in counterfeiting or piracy.

Often due to the diversity and seriousness of the criminal activity, non IPR-specific offences can be more suited to the type of criminality involved in online infringements, as they provide greater sentencing powers. These might include offences such as conspiracy to defraud, money laundering, making articles for use in fraud, and fraud by false representation. The breadth of offences and sentences can act as a deterrent to potential infringers.

Rights-holders can commence private criminal prosecutions, and this may be a consideration in cases where the prosecuting authorities (such as Trading Standards) are lacking the necessary resources, expertise or appetite to prosecute. The Court of Appeal has confirmed that the police are permitted to exercise their powers to assist a private prosecutor (Scopelight & Ors v Chief Constable of Northumbria Police & Federation Against Copyright Theft [2009] EWCA Civ 1156).

**Industry and political developments.** Enforcement action depends on awareness of the infringing activities. While the burden of identifying infringement remains with the rights-holders, a growing number of initiatives at institutional levels seek to enlist others in identifying persistent offenders, enabling rights-holders to obtain the information needed to enforce their rights, including:

- The Police Intellectual Property Crime Unit (PIPCU), established with a mandate to tackle serious and organised IPR crime affecting physical and digital goods (excluding pharmaceutical products), with a focus on online offences. PIPCU works with rights-holders, representative bodies, and national and international law enforcement to implement initiatives, identify and combat IPR infringement.
- Legislative changes through the Digital Economy Act 2010 (DEA), designed to tackle online copyright infringement. These require ISPs to:
  - notify users of any alleged copyright infringement that it is made aware of by rights-holders; and
  - maintain a list of infringers, to enable rights-holders to more easily obtain the necessary court orders to identify infringers and take action against them.

At the time of writing, the provisions and rights in the DEA have not yet been implemented and therefore these initiatives remain outside the reach of rights-holders at the moment.

- Search engines discouraging access to infringing websites by excluding or lowering them in search results.
- ISPs establishing "Creative Content UK" in response to the delays in implementing the DEA, to raise awareness of copyright by informing those whose internet connections have been used to illegally share copyright material and help them find compelling legal alternatives (www.gov.uk/government/news/new-education-programme-launched-to-combat-online-piracy).
- Advertisers withholding advertising revenue from infringing sites.
- Payment service providers withdrawing services from infringing sites.

Co-operation is crucial to disrupting systematic infringers, and the challenge is incentivising organisations who may not be directly responsible for the infringements (or financially disadvantaged by it) to take an active role in tackling it.

**CONCLUSIONS**

The risks and trends associated with online IPR infringement constantly change with the development of new technologies and services. Rights-holders must therefore remain vigilant and aware of shifts in the technological landscape in which they operate.

Where infringement risks exist, rights-holders should adopt a systematic strategy covering protection of IPRs, use of counter-infringement measures, and enforcement action where necessary. Resource should be focused where it is most needed, recognising that infringing activities are no longer contained within jurisdictional boundaries.

Rights-holders who are agile with their business models and alive to the risks and opportunities that new technologies present will have the best chance of successfully navigating the shifting sands of the internet age.
**Martin Cuell, Partner**

Foot Anstey LLP  
T +44 117 915 4933  
F +44 117 915 4999  
E martin.cuell@footanstey.com  
W www.footanstey.com

**Professional qualifications.** LPC, England and Wales, University of the West of England; PgDip, England and Wales, University of the West of England  

**Areas of practice.** Technology; outsourcing; media; telecommunications; intellectual property; data protection; commercial.

**Non-professional qualifications.** BA Hons, Ancient History, University of Bristol

**Recent transactions**

- Advising an international bank on web compliance in the UK and compliance with the Equalities Act.
- Advising a major UK bank on the development and implementation of internet banking, web compliance and interoperability with back office functions.
- Advising a Bristol based animation studio on their merchandising arrangements, engagement terms, copyright, trade mark ownership, protection and exploitation.
- Advising on commercial, IP and technology matters for a global media company in respect of their acquisition of a UK based technology and media business.
- Advising an energy supplier on intellectual property aspects arising from collateral warranty agreements.

**Languages.** English

---

**Hannah Batten, Associate**

Foot Anstey LLP  
T +44 117 915 4975  
F +44 117 915 4999  
E hannah.batten@footanstey.com  
W www.footanstey.com

**Professional qualifications.** Certificate in IP Transactions, UCL Institute of Brand and Innovation Law; LPC, England and Wales, University of the West of England; LLB, Law, England and Wales, University of the West of England

**Areas of practice.** Intellectual property; technology; commercial; commercial contracts.

**Recent transactions**

- Advising an international TV production group on the management and exploitation of its IP rights and agreements with publishers and broadcasters.
- Advising a national charity on the IP aspects of its sub-contracting arrangements relating to its engagement by a government department to create and deliver a new national database.
- Advising a UK newspaper publishing group on various IP and contractual matters.
- Advising a national bank on an agreement with an online services provider to make services available to the bank's customers.
- Advising a leading engineering and technology company on IP issues arising from a knowledge-sharing arrangement with a UK university.

**Languages.** English
**Professional qualifications.** Law, England and Wales, MA Oxon

**Areas of practice.** Media and intellectual property disputes.

**Recent transactions**
- Acting for the National Farmers Union in proceedings for an anti-harassment injunction, against persons unknown who were engaging in unlawful harassment during opposition of the government’s policy of culling badgers to combat bovine tuberculosis, and the progress of committal proceedings for contempt of court against a protestor following alleged breaches of that injunction.
- Representing national and regional press organisations in a variety of commercial and contentious intellectual property matters relating to brand protection and content management.
- Acting for several retail organisations in the enforcement of their trade mark and design rights, including the co-ordination of registration and enforcement activity across international jurisdictions.

**Languages.** English, French, German

---

**Professional qualifications.** Currently completing the Postgraduate Diploma in Intellectual Property Law and Practice, University of Oxford; PSC, England and Wales, University of the West of England; LPC, England and Wales, University of the West of England; Law with European Studies, England and Wales, LLB Exeter University

**Areas of practice.** Intellectual property litigation.

**Recent transactions**
- Advising a large multi-channel supplier of trade tools and other equipment on trade mark infringement claims, and acting for a variety of retail and media organisations in relation to trade mark oppositions at the IPO and OHIM and on the enforcement of registered trade marks and design rights.
- Acting for a well-known household brand in relation to the passing off of one of their iconic products against defendants based in multiple jurisdictions.
- Advising national and regional press organisations including Local World and Johnston Press Plc on a broad range of contentious Intellectual Property matters.

**Languages.** English, French
Professional qualifications. LPC, England and Wales, College of Law, Chester; Law, LLB (Hons), England and Wales, De Montfort University, Leicester

Areas of practice. Disputes; intellectual property; media.

Recent transactions

Neil joined Foot Anstey in June 2015, prior to which he was a Partner at Wiggin LLP, where he was involved in the following recent matters:

• **Cartier & Ors v BSkyB & Ors** acted for Richemont (owner of brands such as Cartier and Montblanc) in a test case resulting in a landmark judgment establishing availability of court orders requiring internet service providers to block websites selling counterfeit goods online.

• **R v Munaf Zinga** acted for Virgin Media in successfully opposing the defendant’s appeal against his conviction for criminal IP offences, an eight year sentence and a GBP8.7 million criminal confiscation order imposed by the Crown Court, following a successful private prosecution.

• Acted for an international film and TV distributor in the defence and settlement of a multi-million pound royalty audit claim by a music composer, relating to the theme music of a successful TV series.

• Instructed by an online hotel search service in a successful defence of claim for wrongful termination of a multi-million pound advertising agency agreement.