7 IP and the internet

ENTIRE BOOKS ARE DEVOTED to the law of the internet. The aim of this chapter is to identify some of the business (and political) issues posed by the internet in the context of intellectual property protection and risk, and, in conjunction with Chapter 16, proposes strategies for dealing with IP issues.

Trademark and domain name strategies

Domain names are a comparatively recent form of intellectual property. At its most basic, a domain name is an address for a website on the internet, obtained through a contract with a domain name registrar. Domain names are the combination of a second-level domain name, such as profilebooks, and a top-level domain (TLD), such as .com or .co.uk, to create a domain name: profilebooks.com. The Internet Corporation for Assigned Names and Numbers (ICANN) manages much of the domain name system and has contracted with companies that have rights to act as registrars. Domain names can be obtained through a company providing registration services for the desired TLDs. Registering is a simple online process. Rights to a domain name are largely a matter of the contract between the applicant and the registrar.

In 2012, ICANN set up a process for issuing generic top-level domain names (gTLDs) to anyone able to act as a registrar at a cost of $185,000 per application. As well as opening up new domain names

For a quick summary of points to note and strategic considerations, go to page 292

for the public, this allows companies to use a brand name as a TLD, or to have control over a generic term that has business significance, such as .search. ICANN has also set up a trademark clearing house, which will contain a verified database of trademark information supporting the new gTLDs. Registered trademark owners are able to record their marks in the registry and thereby obtain certain protection against or notice of cybersquatters (see below). The gTLD and clearing-house procedures open up new fields of domain-name-related law and practice.

Domain name and trademark strategies should be interlinked but often are not. This is usually because lawyers or trademark agents handle trademark filings and business people or advertising agencies handle the acquisition of domain names. Ideally, selection of a new trademark would involve both a search of prior trademark rights and an assessment of available domain names. A trademark filing programme would also be linked to a domain name registration programme, as the two rights are legally intertwined.

Some common mistakes occur in obtaining domain names. First, they are so simple to obtain that they may be purchased by employees or agencies acting in good faith who forget to transfer ownership to the employer or client, or to keep track of renewal notices, which go to the employee or client. Second, although trademark lawyers are punctilious in recording deadlines for the renewal of trademarks, domain name renewals are sometimes forgotten, with the result that a third party may come in and purchase the domain name.

Companies typically try to protect a name or brand by registering a number of major TLDs (such as .com and .net) and local markets where the name or mark will be important (such as .co.uk or .de or .jp). Some companies also register variants that may be caused by typographical errors or to protect against an adverse use of the name (for example, in US slang, xxxxsucks.com, or the new TLD .sucks). Third-party companies provide domain name management services enabling domain names to be managed as a portfolio.

Cybersquatting

Obtaining a domain name is simply a matter of availability, but there are laws and procedures to protect individuals and companies whose names are wrongfully taken. Domain names have been the subject of IP disputes as a result of cybersquatting, which involves the acquisition of a domain name for a brand, company name or celebrity before the legitimate owner acquires that domain name. Other forms of abuse involve typo-squatting, where a variant of a famous name is registered, or the acquisition of inadvertently lapsed domain names.

Generally, a cybersquatter that adopts a domain name identical or confusingly similar to a trademark in which someone has rights may be prevented from using it. Thus protection of domain names is essentially derived from trademark rights. The Uniform Domain Name Dispute Resolution Policy (UDRP) is an arbitration procedure administered by the World Intellectual Property Organisation (WIPO) and some other organisations. Under this procedure the owner of a registered trademark may obtain transfer of a cybersquatter's domain name that is identical or confusingly similar to the registered trademark.

Although other laws, such as the US Anticybersquatting Consumer Protection Act 1999, enable objections to wrongful domain name registrations, the UDRP usually provides a quicker, less expensive resolution. The remedies available to a trademark holder are cancellation of the wrongful domain name or the transfer of the registration. Filing a case with the UDRP does not prevent either party from filing suit in a national court. ICANN is also establishing a new and simpler procedure, the Uniform Rapid Suspension System, which it says offers "a lower-cost, faster path to relief for rights holders experiencing the most clear-cut cases of infringement".[1]

Geographic and field-of-use rights

In general, except in the case of famous or well-known trademarks, the same trademark can be registered by different companies for, say, crackers and hotels (Ritz). However, a domain name does not on its face indicate what goods and services it covers. A problem arises

when different companies, each with a legitimate trademark, wish to use the same domain name. There is only one web address available for that trademark with a particular TLD. Which company obtains this domain name has been based on first come, first served, with the later registrant having to use another TLD or a variant of its trademark.

For example, Merck & Co, a US pharmaceutical company, has since the first world war been separate from its original German parent, Merck KGaA. The domain name merck.com is used by the US company and merck.de by the German one. The latter forwards US users to an English-language website, which contains a disclaimer: "In the United States and Canada the subsidiaries of Merck KGaA, Darmstadt, Germany, operate under the umbrella brand EMD."[2] This is not cybersquatting, which involves an attempt in bad faith to acquire rights to a domain name before the rightful trademark owner has a chance to register it. In this instance, there are two or more rightful trademark owners. And as noted, steps may need to be taken to avoid customer confusion.

Websites, e-commerce and privacy

The laws relating to websites and the laws relating to personal data are not IP laws as such. However, although the laws relating to personal data establish obligations on the holders of that data, there is no doubt that a large database of personal information may be a hugely valuable intangible asset.

Risk mitigation

Establishing an internet-based business involves potential risks, obligations and liabilities, often of an international nature. A simple website set up in the UK to sell a product may collect personal information about its customers, including credit-card information, and may be subject to comprehensive regulation under EU rules on contracting, data protection and privacy. For example, uses of devices such as cookies (messages given to a web browser by a web server) are subject to EU regulation.

However, if that website sells to US customers as well, it may be subject to federal and state laws governing privacy and security. There

has also been much patent litigation in the United States brought by patent assertion entities (PAEs) and others over various aspects of e-commerce. Companies offering goods, services or software for licence over the internet to US-based customers may risk a claim of patent infringement.

This is an example of where the borderless nature of the internet may result in the risk of potential claims being made. One solution is to build an internet business in a series of steps, starting with the home country and then, through the use of differing domain names and TLDs (for example, .co.uk rather than .com), directing customers to websites created for and tailored to the risks and regulations in a particular country or region. An example is a UK website that does not take orders from customers in a particular country (such as the US), but directs them to an affiliated site established to cater for specifically US issues.

Terms and conditions and architecture

New websites are often created in a haphazard manner. For example, there is a general understanding from review of other websites that there may need to be terms and conditions of use and a privacy policy. But these are often borrowed from some other context and are sometimes spectacularly inapplicable to the business model and technology. There is also typically little co-ordination between the technical architecture of the website and the legal and contractual aspects, so that customers purchasing a product may never have had to agree to terms and conditions of sale, and even if they did, there may be no record of that agreement.

Furthermore, the terms and conditions and privacy policy of the website may bear no resemblance to its business and data practices. Each website generally needs terms and conditions of use, and a privacy policy developed in conjunction with a legal review of how third-party, customer or employee personal information is handled. In the US, the Federal Trade Commission may investigate complaints about companies that are alleged not to live up to their privacy policies using its powers under Section 5 of the Federal Trade Commission Act – and it has done so in cases involving major internet businesses.

Correctly establishing the terms and conditions and the internal and external technical architecture of a website should enable an internet company to mitigate a number of risks, comply with the most immediately applicable regulatory schemes and attempt to control its international exposure. The website architecture should be as secure as possible from third-party hacking and intrusion, and should comply with applicable laws governing security of customer data, including credit-card information.

As well as establishing a secure legal and technical framework, a well-executed website should also address IP issues through correct use of trademarks, copyright notices, and terms and conditions that make clear what is and is not permissible use. The copyright in the content of the website, in terms of text and illustrations, should as far as possible be owned by the website owner so that remedies are available in the event of third-party copying. This may protect a website when competitors or others copy its designs and features; although truly novel web-based operations may also be protectable through patents.

Privacy and data protection laws

Companies and individuals that have access to individuals' personal information may be under legal obligations concerning use of that information, even if it is not strictly confidential. Examples would be a person's name, address, e-mail address, identification number, employment, medical and financial information, religious affiliation and ethnicity, credit-card numbers and so on. Collection and use of such information on website users, customers and employees may be regulated or prohibited. Companies new to international operations (particularly over the internet), or new to gathering and using personal information, should focus particularly on regulatory and technical (IT security) compliance in the major jurisdictions where they do business.

Over 100 countries now have data protection laws in force and these, as well as companies' own undertakings given through privacy policies on their websites, may limit or restrict the use, disclosure, export or processing of such information, and require minimum standards for confidentiality and security. They may also require

notices to customers of security breaches and unauthorised access by third parties.

Applicable legal regimes are complex. In the US, for example, regulation depends on the industry involved and regulation may occur at both the federal and state level, depending on the industry. In the EU, there is a comprehensive regime that covers the "processing" (itself covering most acts you can think of) of "personal information" (which is also broadly defined). Similar regimes have been adopted in Canada, Japan and many of the free-market countries of Asia, Africa and South America. Thus data protection is something that all internet businesses are forced to recognise and grapple with.

Compliance is a significant cost and administrative burden for companies. In general, outside the area of health care, regulation is lighter in the US than in the EU, but a remarkable decision of the European Court of Justice in May 2014 illustrates the reach and power of data protection law. The court held in *Gonzalez v Google* that Google was responsible for compliance with data protection law in Spain and had to ensure that links to a newspaper article mentioning Gonzalez were disabled in Google's search engine. The implications of the case are still to be worked through, but it shows how control over personal information remains ultimately with the individual not the data collector.

A classic problem for companies based outside the EU is moving personal data about customers or employees in the EU through networks to locations outside it in contravention of EU laws. A proposal to create a new Data Protection Regulation – a uniform but stringent set of privacy standards across the EU – has raised significant concerns among US companies that rely on data collection and use, such as Facebook and Google. The proposed regulation contains a provision that would subject businesses to fines for infringement based on a percentage of their worldwide turnover, in the way that antitrust sanctions have been enforced for a number of years. Whether the eventual percentage enacted proves to be 10%, 5% or 1%, the consequences for breaching this new regulation will be severe. Hence there has been a record level of lobbying against it. Furthermore, the issue of transatlantic data access has been accentuated by the Snowden revelations of US government surveillance.

Even within the US there is unease over data collection and aggregation practices. The commercial incentive to track behaviour on the internet and combine online and offline databases to create "big data" is huge given the holy grail of efficiently targeting online advertising to consumers. As a saying attributed to more than one notable businessman puts it: "Half the money I spend on advertising is wasted; the trouble is I don't know which half." Tracking consumer habits and likes on the internet helps answer that question: hence its great commercial value.

In general, loss or misuse of customers' personal data is a major reputational, legal and financial issue for a corporation, and maybe even disastrous. In the US, there is the possibility of class actions for damages, where individual plaintiffs sue on behalf of all the affected customers, as well as actions by state and federal regulators. Breaches of the existing data protection laws in Europe may involve fines or imprisonment. For any company, customer data use and protection should be on every list of major compliance and risk management issues.

Blogging, social media and IP risks

Employees' use of their own tablets or smartphones for business purposes, the use of cloud-based services to store or back up data, social media, websites, blogging and other internet activities bring with them a variety of IP risks. Proprietary information may be removed from corporate networks and made public or placed in insecure locations. Personal accounts may be set up rather than corporate accounts that can be monitored and terminated. Weak links are created.

When managers or other employees are permitted to blog, or post content, there is a risk that confidential information may be disclosed to the detriment of the company, or statements made that may be legally troublesome in the future. Product launches may be disclosed before patent filings have been made; trademarks may be used in an incorrect manner; statements may be made about patents or other intellectual property that are not correct; and so on. Policies should be developed to address these issues. And security policies should address the use of personal devices and cloud-based services.

Linking and framing

Linking is where one website connects to another through a link, taking the user to another website. Framing occurs when the second website may be viewed through the original website, so that the user is presented with the original website and the second website on one page. Linking and framing may raise issues under trademark or unfair competition rules if, for example, users are likely to become confused as to the association between the two websites, or if logos of the linked site are used. The terms and conditions of a linked website may also prohibit certain activities.

These practices may also be challenged under copyright law. As a business matter, however, challenges to linking have occurred in contexts where the effect of the link is arguably to divert revenue from the owner of the website. In Germany, this resulted in legislation being passed on ancillary copyright, which was aimed at enabling newspapers to share the revenue of news aggregators, such as Google and Yahoo, which publish small amounts of text in news listings with links to the original site.

Use of trademarks in metatags and search terms

Various online practices aimed at driving traffic to websites or providing targeted advertising using competitors' trademarks are subject to litigation over their legality. The outcome depends on the facts of each case, such as how trademarks are used, what types of advertisements are called up by use of those trademarks and what trademarks those advertisements contain.

For example, in a 2013 case in the UK, Marks & Spencer was found to have infringed Interflora's registered trademark by purchasing "Interflora" as a search term in Google Adwords, thus triggering the display of a link to Marks & Spencer's flower delivery service in a way that on the facts was held to be confusing as to the source of the service. The decision was overruled on appeal in 2014 on the basis that the burden of proof was on the trademark owner:

> *[T]o establish that the advertisement complained of does not enable normally informed and reasonably attentive internet users, or enables them only with difficulty, to ascertain whether the goods*

or services referred to by the advertisement originate from the trade mark proprietor ... or, on the contrary, originate from a third party.

The use of a trademark in meta elements (or metatags – which provide information about webpages that is readable by a search engine) to drive searches to a website not owned by the trademark owner has been found to be a basis for possible trademark infringement in the US. In the case in point, a company marked its website with a competing company's brand so that search engines would pick up the brand and drive traffic to the company's website. However, this type of "initial interest confusion" was found not to be part of EU law by the UK Court of Appeal in the Interflora case.

Cybercrime, trade secrets and hacking

The internet is often the vehicle for cyber-attacks, for example through "spear phishing", where an e-mail to an employee if opened enables malicious code to invade a network. From an IP perspective, use of the internet and public networks presents a risk of loss of trade secret information that needs to be addressed as a part of business planning. Risk identification and mitigation are now regarded as board-level obligations within companies. At a political level, cyber-security and national security cause discord between governments and internet companies and users, who have very different interests in privacy and regulation.

At the administrative level, following a 2013 order from the president, the US National Institute of Standards and Technology issued in February 2014 its *Framework for Improving Critical Infrastructure Cybersecurity*, which provides broadly applicable guidelines on best practices. A 2015 presidential order encourages sharing of information on cyber-security threats. However, there has been significant opposition to proposed legislation to combat hacking and cyber-security threats. The US Cyber Intelligence Sharing and Protection Act is aimed at sharing information about hackers and attacks, but there are concerns about the transfer of personal information to the government in the course of cyber-security investigations. Nevertheless, there is support for creating a federal cause of action for trade secret misappropriation (federal procedures

are generally more effective than their state law counterparts) and closing loopholes in existing applicable criminal legislation such as the US Economic Espionage Act and the US Computer Fraud and Abuse Act.

In the EU, there is also legislation pending that seeks to address similar issues. Under the proposed legislation, providers of "critical infrastructure", such as energy, transport, health care and financial services, would be subject to various obligations relating to security, including that breaches of security would have to be reported to the authorities.

Copyright and piracy

The internet has enabled enormous piracy of copyright material and the easy sale of knock-offs of branded goods. The economics of the music industry have been fundamentally changed by the combination of the digitisation of music, the internet as a means of copying and transmission, and the availability of massive amounts of low-cost digital memory. Pirated copies of TV programmes and films are freely available. Legitimate companies are also pushing the boundaries of copyright law. For example, websites aggregate news stories from news services. And the Google Books project fundamentally alters the publishing industry by copying into digital form millions of books and making those copies searchable. From a US perspective, a number of these issues touch on the doctrine of fair use (see Chapter 4), and the boundaries of the law are constantly being challenged.

The sheer quantity and ubiquity of infringing material on the internet means that owners of content or branded products are involved in a never-ending effort to stop such piracy. This has led to owners of IP trying to attach liability to internet service providers such as search engines and marketplaces.

The internet has therefore become the main battleground where the rights of copyright owners are tested. It is in some ways a battle between advocates of freedom of speech and a free internet (or business advocates seeking loose internet regulation sheltering behind free speech concerns) and content industries such as music,

publishing, software, TV and film. Even within the US the interests of different regions diverge; northern California, notably Silicon Valley, is home to companies focused on the internet and benefiting from loose regulation and loose liability standards, whereas southern California, around Los Angeles, and New York are home to content industries. These conflicting interests continue to clash over proposed legislation and treaties aimed at reducing piracy.

Liability of ISPs and online markets

Many legitimate companies enable the advertising and sale of pirated products, yet liability is hard to prove and regulation remains lax, being based on a legislative balance between the remedies of IP owners and freedom of the internet that is hotly debated. Under the Digital Millennium Copyright Act (DMCA), which amended US copyright law to address internet and digital issues, a network service provider may avoid liability for copyright infringement as a result of content posted by users, provided that the service provider:

> (A) (i) *does not have actual knowledge that the material or an activity using the material on the system or network is infringing;*
>
> (ii) *in the absence of such actual knowledge, is not aware of facts or circumstances from which infringing activity is apparent; or*
>
> (iii) *upon obtaining such knowledge or awareness, acts expeditiously to remove, or disable access to, the material;*
>
> (B) *does not receive a financial benefit directly attributable to the infringing activity, in a case in which the service provider has the right and ability to control such activity; and*
>
> (C) *upon notification of claimed infringement ... responds expeditiously to remove, or disable access to, the material that is claimed to be infringing or to be the subject of infringing activity.*

The protections are conditional upon the service provider designating an agent to receive notices of claimed infringement. So long as the service provider complies with the statutory requirements and takes down the infringing material upon being notified by the

copyright owner, it may avoid liability and be inside what is often called a "safe harbour".

Similar legislation applies in the EU under the E-commerce Directive (2000/31/EC), where Article 14(1) states that liability may not attach if:

> *(a) the provider does not have actual knowledge of illegal activity or information and, as regards claims for damages, is not aware of facts and circumstances from which the illegal activity or information is apparent; or*
>
> *(b) the provider, upon obtaining such knowledge or awareness, acts expeditiously to remove or disable access to the information.*

Although this may seem fair, infringing copyright material is rife on the internet and the burden of enforcement is on the IP owner. In practice, IP owners may employ people or services to police the internet continually for infringing material. Many legal challenges have been mounted by suppliers of copyright content throughout the world claiming that ISPs are failing in their duties, ignoring red flags indicating infringing material or being wilfully blind, and that they should be liable for enabling the sale of counterfeit products. These challenges have had mixed results, with the decisions tending to support the ISPs.

The increasing amount of internet piracy has led to intense lobbying and political pressure from providers of copyright content, such as the music and entertainment industries, to enact new legislation and enter into IP-focused treaties. Such efforts have been vigorously opposed by telecommunications and internet companies, which often argue that such legislation would curtail free speech.

In the UK in 2011 and 2012 there were legal challenges to provisions of the Digital Economy Act 2010 which required ISPs to send notices to suspected infringers and potentially to cut off service to them. In Ireland, a 2012 government order providing for the possibility of injunctions against ISPs raised significant concerns. In the US, the Stop Online Piracy Act (SOPA), introduced in 2011, aimed to strengthen the ability of US law enforcers to fight online infringement and infringing sales. The legislation came up against well-organised

lobbying and protest from technology companies, which claimed that it could stifle the freedom of the internet, particularly with regard to provisions that might require ISPs to block access to sites that provide infringing material, or stop search engines linking to such sites. The Anti-Counterfeiting Trade Agreement (ACTA) encountered similar opposition in the US and the EU, where it was rejected by the European Parliament. The ACTA was claimed to embody the agenda of the motion-picture industry in particular. It addressed various remedies against copyright infringement and counterfeiting and would require all signatory countries to have similar levels of intellectual property protection.

Similarly, efforts to attach liability to online marketplaces that allow the sale of "knock-offs" have generally not been successful in the US so long as the site is willing to take down infringing products, and have had mixed results in Europe.

However, in the UK under Section 97A of the Copyright, Design and Patents Act, which predates the Digital Economy Act 2010, the court has the power to grant an injunction against a service provider to block a website "where that service provider has actual knowledge of another person using their service to infringe copyright". This provision has been successfully used to block access to websites infringing copyright, and in 2014 a similar remedy was granted to block websites selling goods that infringed trademark rights.

Working with ISPs

In the absence of court or legislative victories, the film, music and fashion industries have turned to negotiating with major industry players such as Yahoo! and Google to voluntarily take steps to reduce piracy. In September 2013, Google issued a report, *How Google Fights Piracy*. At more or less the same time the Motion Picture Association of America issued its report, *Understanding the Role of Search in Online Piracy*, pointing out the pivotal role of search engines in providing access to pirated material. Google's report is a thoughtful presentation of the issues involved and is worth studying. One example of the focus of ISPs is "following the money". A number have adopted notice and take-down procedures to remove infringing sites from their advertising programmes, which provide revenue for those sites.

Reducing demand for counterfeit products

Current thinking on piracy focuses initially on whether it is being driven by aspects of a company's marketing strategy that may be modified to limit the incentives for counterfeiters, such as simultaneous worldwide publication of a copyright work as opposed to creating unsatisfied demand in certain regions. The music industry is using services that make legitimate digital copies of a copyright work available online at a reasonable price and allowing music to be available through legal streaming services. Over time, the ready availability of legitimate and convenient channels may reduce demand for piracy.

Where tangible products are sold over the internet, supply chain and supplier relationships are audited and examined to determine whether the goods come from genuine suppliers who do not have exclusive supply obligations. Attempts can be made to bring these suppliers into the anti-counterfeiting strategy.

Technological measures can also be used. For example, where copyright files such as software are distributed, licence keys and passwords may assist in limiting copying.

An internet infringement strategy

Infringement of rights over the internet remains a huge and frustrating problem. Solutions differ across industries, but here are some questions to ask:

- Are aspects of the company's worldwide marketing or pricing strategies encouraging piracy through unmet demand? Can these strategies be changed so that online content is available conveniently and legally?
- Are there sources of counterfeit products from within the company's supply chain that can be stopped?
- Are the problems industry-wide? Are there trade association resources that can be marshalled? Can a trade association negotiate with legitimate ISPs or lobby government? What can be done co-operatively with competitors suffering the same problems? Are there steps that a legitimate ISP can be

persuaded to take (for example, reducing the prominence of certain websites or removing infringing sites from advertising programmes)?

- Are ISPs or other intermediaries that do not seem to be legitimate or to be following the normal rules being used? Could they be the target of litigation under current case law?
- Are there technological solutions to piracy that can be used, such as licence keys?
- How can infringement issues be prioritised? For example, which internet activities lose revenue or may threaten ownership of IP rights or their value?
- How can targets be prioritised? For example, which activities are carried out by legitimate companies (which may be the easiest to pursue), which by customers and which by illegitimate companies?
- Can the company make transactions or settlements with legitimate companies using its IP?
- Where are identifiable infringers located?
- Are the company's IP rights registered in these places?
- What is the strength of the applicable legal rights in the company's home country and in other countries? Do any countries have laws that favour particular industries?
- Are any of the activities potentially criminal in any affected jurisdiction? Can law enforcement assist by, for example, seizing infringing websites?